Public-Key Cryptography: Design and Algorithmic

Fabien Laguillaumie

Université de Caen Basse-Normandie

Public-Key Cryptography: Design and Algorithmic

Fabien LAGUILLAUMIE

Maître de conférences

Mémoire d'habilitation à diriger des recherches

Présenté le 12 décembre 2011 après avis des rapporteurs :

Dario CATALANO, Professor, Università di Catania
Steven GALBRAITH, Professor, University of Auckland
David POINTCHEVAL, Directeur de recherche, CNRS, École Normale Supérieure

Examinateurs :

Dario CATALANO, Professor, Università di Catania
Guillaume HANROT, Professeur, École Normale Supérieure de Lyon
Pascal PAILLIER, CEO and Senior Security Expert at CryptoExperts, Paris
David POINTCHEVAL, Directeur de recherche, CNRS, École Normale Supérieure
Brigitte VALLÉE, Directrice de recherche, CNRS, Caen
Gilles ZÉMOR, Professeur, Université Bordeaux 1

Contents

Introduction

This document presents some of the results I obtained in the last few years in the field of cryptology. They illustrate my main achievements in different aspects of cryptology, as well as the directions I will investigate in the future. My research concerns mostly the design and the security analysis of cryptographic schemes, the underlying computational number theory and the use of these schemes in real-life applications. In this document, I will describe results in the first and second topics. I will essentially describe the results, without proofs which can be found in the corresponding articles.

My PhD thesis focused on signatures with special features, in particular the control of the verification process and anonymity properties. Electronic signatures aim at emulating the traditional hand-written signatures, but they are conceptually very different. For instance, because of their numerical nature, they must depend on the message to prevent trivial copies. But also, to satisfy the many (and sometimes contradictory) security requirements of complex systems like electronic voting, e-cash, or contract signing, the signature must be enriched with additional features. For instance, I designed designated verifier signatures [LLQ06], undeniable and directed signatures [LV10, LV05, LPV05] or ring signatures [HL08, ACGL11]. After my PhD, I subsequently got into encryption, especially encryption dedicated for privacy: I worked in particular on attribute-based encryption, proxy re-encryption [HLR10, CDL11] and plaintext-checkable encryption, which is a new primitive which universally allows, given a plaintext, a ciphertext and a public key, to check whether the ciphertext actually encrypts the plaintext under the key.

I am also interested in the applications of such cryptographic primitives to secure particular systems. For instance, we introduced in [CLM08] the concept of *trapdoor* redactable signatures, which allows some designated entities to modify some specific parts of a signed message and to produce a new signature of the resulting message without any interaction with the original signer. This new cryptographic tool was needed in protocols for group content protection, permitting members of a group to legally distribute a protected content among themselves. In [BHL07], we formalised the aggregation of (identity-based) designated verifier signatures, and in particular the aggregation of MACs, to efficiently authenticate messages in routing protocols for mobile ad-hoc networks. I was also involved in research on e-cash, within the project PACE funded by the French Agence Nationale de la Recherche. In particular, in [C+09] we proposed the first fair e-cash system with a compact wallet that enables users to spend efficiently k coins while only sending to the merchant $\mathcal{O}(\lambda \log k)$ bits (where λ is a security parameter), thanks to a new use of the Batch RSA technique and a tree-based representation of the wallet.

Many of these cryptographic schemes involve the computation of pairings on elliptic curves, introduced in cryptography in 2000 in [Jou00]. Elliptic curves are popular in cryptog-

raphy because, at a fixed level of security, they allow for shorter keys than RSA for instance. Another reason is that some of these curves are equipped with an efficiently computable bilinear map which is cryptographically-friendly, in the sense that it makes possible to achieve cryptosystems with new functionalities. This very popular tool has nevertheless the reputation of being computationally costly, but is still indispensable for many primitives. I studied the algorithmic of this object within the project PACE: we obtained in [BELL10] a generic improvement of Miller's algorithm which gives a faster evaluation for odd embedding degrees. I worked on another mathematical object for the purpose of cryptanalysis, namely quadratic forms (or ideals in quadratic fields). In [CL09, CJLN09], we propose a definitive attack on a large family of very efficient cryptosystems which are based on the arithmetic of ideals in quadratic fields. This cryptanalysis is based on a factoring algorithm for numbers of the form pq^2 for p and q two large prime numbers.

In this manuscript, the first chapter covers my contributions in the computational number theory used in cryptography. It includes an exponential-time factoring algorithm dedicated to numbers of the form pq^2 based on the algorithmic of binary quadratic forms obtained in collaboration with G. Castagnos, A. Joux and P. Q. Nguyen. Its impact on the security of the NICE family of cryptosystems lying in real quadratic field is then discussed. An arithmetic cryptanalysis of the variant in imaginary quadratic fields obtained with G. Castagnos [CL09] is also described. Eventually, a refinement of Miller's algorithm to compute pairings in elliptic curve, in collaboration with J. Boxall, N. El Mrabet and D.-P. Le. [BELL10], is presented.

The second chapter is devoted to the design and security analysis of functional cryptographic schemes. In a first part, I will provide a study of the security of identity-based encryption in terms of anonymity and indistinguishability of ciphertexts, according to the strength of the attacker. This is a joint work with J. Herranz and C. Ràfols [HLR11]. The two last parts concern attribute-based cryptography: the first one presents an attribute-based encryption scheme whose ciphertexts have constant size, from a joint work with J. Herranz and C. Ràfols [HLR10]. The second one directly follows this previous work, since, together with J. Herranz, B. Libert and C. Ràfols, we use our attribute-based encryption to design an attribute-based signature scheme with constant-size signature [HLLR11].

List of Publications

Articles marked with [⋆] are the articles presented in this manuscript, those marked with [T] are results from my PhD thesis.
The articles below can be downloaded at `http://users.info.unicaen.fr/~flaguill/work.php`.

Refereed Journals

- *Attribute-Based Encryption Schemes with Constant-Size Ciphertexts*. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu and Carla Ràfols. To appear in Theoretical Computer Science.
- *Improving the Security of an Efficient Unidirectional Proxy Re-Encryption Scheme.* S. Canard, J. Devigne, F. Laguillaumie. Journal of Internet Services and Information Security; Vol. 1(2/3), 140–160 (2011)
- [⋆] *Relations between Semantic Security and Anonymity in Identity Based Encryption.* J. Herranz, F. Laguillaumie, C. Ràfols. Inf. Process. Lett., Volume 111, Issue 10, 453-460 (2011)
- *A New Efficient Threshold Ring Signature Scheme based on Coding Theory.* C. Aguilar Melchor, P.-L. Cayrel, P. Gaborit, F. Laguillaumie. IEEE Transactions on Information Theory, Volume 57, Number 7, 4833-4842 (2011)
- [T] *Time-Selective Convertible Undeniable Signatures with Short Conversion Receipts*. F. Laguillaumie and D. Vergnaud. Information Sciences, 180(12), 2458-2475 (2010)
- *Aggregate Designated Verifier Signatures and Application to Secure Routing*. R. Bhaskar, J. Herranz and F. Laguillaumie. International Journal of Security and Networks, Special Issue on Cryptography in Networks, Vol. 2, Nos. 3/4, 192–201, (2007)
- [T] *Multi-Designated Verifiers Signatures: Anonymity without Encryption*. F. Laguillaumie, D. Vergnaud. Inf. Process. Lett., Volume 102, Issues 2-3, 30 April 2007, 127–132 (2007)
- [T] *Universal Forgery on Sekhar's Signature Scheme with Message Recovery*. F. Laguillaumie, J. Traoré, D. Vergnaud. Taylor & Francis - International Journal of Computer Mathematics, Volume 81, Numéro 12, 1493–1495 (2004)

Refereed Conferences

- [⋆] *Short Attribute-Based Signatures for Threshold Predicates*. J. Herranz, F. Laguillaumie, B. Libert, C. Ràfols. To appear in Proc. of CT-RSA 2012.
- *Plaintext-Checkable Encryption*. S. Canard, G. Fuchsbauer, A. Gouget, F. Laguillaumie. To appear in Proc. of CT-RSA 2012.
- [⋆] *A Variant of Miller's Formula and Algorithm.* J. Boxall, N. El Mrabet, F. Laguillaumie, D.-P. Le. Proc. of Pairing 2010. Springer LNCS Vol. 6487, 417-434 (2010)

- [⋆] *Constant Size Ciphertext in Threshold Attribute-Based Encryption.* J. Herranz, F. Laguillaumie, C. Ràfols. Proc. of PKC 2010. Springer LNCS Vol. 6056, 19-34 (2010)
- [⋆] *Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses.* G. Castagnos, A. Joux, F. Laguillaumie, P. Nguyen. Proc. of Asiacrypt'09. Springer LNCS Vol. 5912, 469–486 (2009)
- *Fair E-cash: Be Compact, Spend Faster.* S. Canard, C. Delerablée, E. Hufschmitt, A. Gouget, F. Laguillaumie, H. Sibert, J. Traoré, D. Vergnaud. Proc. of ISC'09. Springer LNCS Vol. 5735, 294–309 (2009)
- [⋆] *On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis*. G. Castagnos, F.Laguillaumie. Proc. of Eurocrypt'09. Springer LNCS Vol. 5479, 260–277 (2009)
- Trapdoor *Sanitizable Signatures and their Application to Content Protection.* S. Canard, F. Laguillaumie, M. Milhau. Proc. of ACNS'08. Springer LNCS Vol. 5037, 256–276 (2008)
- *On the Soundness of Restricted Universal Designated Signatures and Dedicated Signatures - How to prove the possession of an Elgamal/DSA signature*. F. Laguillaumie, D. Vergnaud. Proc. of ISC'07, Springer LNCS Vol. 4779, 175–188 (2007)
- *Blind Ring Signatures Secure under the Chosen Target CDH Assumption.* J. Herranz, F. Laguillaumie. Proc. of ISC'06. Springer LNCS Vol. 4176, 117–130 (2006)
- *Efficient Authentication for Reactive Routing Protocols.* R. Bhaskar, J. Herranz, F. Laguillaumie. Proc. of AINA'06 (SNDS'06), Vol. II, IEEE Computer Society, 57–61 (2006)
- [T] *Universal Designated Verifier Signatures Without Random Oracles or Non Black Box Assumptions.* F. Laguillaumie, B. Libert, J.-J. Quisquater. Proc. of SCN'06. Springer LNCS Vol. 4116, 63–77 (2006)
- [T] *Short Undeniable Signatures Without Random Oracles: the Missing Link*. F. Laguillaumie, D. Vergnaud. Proc. of Indocrypt 2005, Springer LNCS Vol. 3797, 283–296 (2005)
- [T] *Universally Convertible Directed Signatures*. F. Laguillaumie, P. Paillier, D. Vergnaud. Proc. of Asiacrypt 2005, Springer LNCS Vol. 3788, 682–701 (2005)
- [T] *Time-Selective Convertible Undeniable Signatures*. F. Laguillaumie, D. Vergnaud. Proc. of CT-RSA 2005 Springer LNCS Vol. 3376, 2005, 154–171 (2005)
- [T] *Designated Verifiers Signature: Anonymity and Efficient Construction from* any *Bilinear Map*. F. Laguillaumie, D. Vergnaud. Proc. of SCN 2004, Springer LNCS Vol. 3352, 107–121 (2005)
- [T] *Multi–Designated Verifiers Signature Schemes*. F. Laguillaumie, D. Vergnaud. Proc. of ICICS 2004, Springer LNCS Vol. 3269, 495–507 (2004)
- [T] *Extending the Boneh-Durfee-de Weger attack to RSA-like Cryptosystems*. F. Laguillaumie, D. Vergnaud , 24th Symposium on Information Theory in the Benelux, 45–52 (2003)

Technical Reports

- *Bilinear Pairings on Elliptic Curves*. J. Boxall, A. Enge, F. Laguillaumie. Livrable public du projet ANR PACE (2009)
- *State of the Art on Cryptographic Tools based on Pairings and Open Problems*. S. Canard, A. Gouget, F. Laguillaumie, P. Paillier, H. Sibert, D. Vergnaud. Livrable public du projet ANR PACE (2009)
- *New Technical Trends in Asymmetric Cryptography* - Chapter *Signatures with special properties*. Public deliverable of the European Network of Excellence in Cryptology

ECRYPT (2007)
– *Efficient and Provably Secure Designated Verifier Signature Schemes from Bilinear Maps*. F. Laguillaumie, D. Vergnaud, rapport de recherche LMNO n° 24 (2003)
– *Short Private Exponent Attacks on Fast Variants of RSA*. M. Ciet, F. Koeune, F. Laguillaumie, J.-J. Quisquater, Technical Report CG-2002/4, UCL Crypto Group, Louvain-la-Neuve (2002)

CHAPTER 1

Computational Number Theory

1.1 Introduction

This chapter is devoted to some of my results which concern the algorithmic aspects of cryptography and it is divided into two different parts.

The first one is related to the numbers of the form pq^2 (p and q are two large primes) and their involvement in cryptography. The starting point of this work was an encryption scheme based on the arithmetic of ideals of imaginary quadratic fields, whose security is related to the hardness of the factorisation of such numbers. In cooperation with Guilhem Castagnos we provide a full cryptanalysis of this system which has been resisting to cryptanalysis for ten years. Then, Antoine Joux and Phong Nguyen joined us to finally break the variant in real quadratic field of this encryption scheme, thanks to an original factoring algorithm specialised for these numbers. I will present this work in the next section; the corresponding publications are the following ones:

- *On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis*. G. Castagnos, F. Laguillaumie. Proc. of Eurocrypt'09. Springer LNCS Vol. 5479, 260–277 (2009)
- *Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses*. G. Castagnos, A. Joux, F. Laguillaumie, P. Nguyen. Proc. of Asiacrypt'09. Springer LNCS Vol. 5912, 469–486 (2009)

The subject of the second part is the computation of pairings on elliptic curves. This object is very popular to design cryptosystems, but it has the reputation of being pretty slow. A particular attention is paid to its efficient computation. The work I will present in this second part is a variant of Miller's classical algorithm to compute these pairings. It is a joint work with John Boxall, Nadia El Mrabet and Duc-Phong Le within the project PACE financed by the Agence National de la Recherche. The corresponding publication is:

- *A Variant of Miller's Formula and Algorithm*. J. Boxall, N. El Mrabet, F. Laguillaumie, D.-P. Le. Proc. of Pairing 2010. Springer LNCS Vol. 6487, 417-434 (2010)

1.2 Cryptography and pq^2.

Public key cryptography is a huge consumer of hard algorithmic problems. If they might be of several flavors (they can be combinatorial like finding a clique in a random graph or they can arise from discrete structures like error correcting codes or lattices), they are

historically arithmetic. The most classical (believed) hard problem is the one of factoring a product of two large (random) primes $N = pq$. It is the heart of the security of the most widespread cryptosystem, RSA [RSA78], as well as of many other. The counterpart of the use of large integers, is their costly manipulation. That is the reason why cryptographers try to improve the efficiency of these systems. Modulus of the form $N = pq^2$ appear in these tries to speed up the operation involving the public key (encryption, verification of a signature) or the secret key (decryption, signature). Among the public-key cryptosystems which require the hardness of factoring large integers of the special form $N = pq^2$, we can mention Okamoto's Esign [Oka90], Okamoto and Uchiyama's encryption [OU98], Takagi's fast RSA variants [Tak98], and the large family (surveyed in [BTV04]) of cryptosystems based on quadratic fields, which was initiated by Buchmann and Williams' key exchange [BW88], and which includes NICE[1] cryptosystems [HPT99, PT99, PT00, JSW08] (whose main feature is a quadratic decryption). These moduli are popular because they allow to reach some special functionalities (like homomorphic encryption) or to improve efficiency (in particular compared to RSA). Moreover, no significant weakness has been found compared to standard RSA moduli of the form $N = pq$: to the best of our knowledge, the only results on pq^2 factorisation are [PO96, Per01, BDH99]. More precisely, [PO96, Per01] obtained a linear speed-up of Lenstra's ECM, and [BDH99, Sect. 6] can factor in time $\tilde{O}(N^{1/9})$ when p and q are balanced.

Furthermore, it is worth noting that computing the *squarefree part* of an integer (that is, given $N \in \mathbb{N}$ as input, compute $(r, s) \in \mathbb{N}^2$ such that $N = r^2 s$ with s squarefree) is a classical problem in algorithmic number theory (cf. [AM94]), because it is polynomial-time equivalent to determining the ring of integers of a number field [Chi89].

Designing algorithms dedicated to the factorisation of these specific numbers is therefore both an algorithmic challenge, as well as a good indicator on the security of the systems whose security relies on the hardness of their factorisation. The results on this section illustrate these two facets. We provide a generic factoring algorithm for pq^2 (which does not affect the security of systems whose security *truly* relies on the factorisation of "random" pq^2) but whose impact on the NICE family of cryptosystems, related to these numbers, is dramatic.

After some notations of the mathematical setting, we present a new algorithm to factor integers of the form $N = pq^2$, obtained in collaboration with Guilhem Castagnos, Antoine Joux and Phong Q. Nguyen based on binary quadratic forms (or equivalently, ideals of orders of quadratic number fields). In the worst case, its heuristic running time is exponential, namely $\tilde{O}(p^{1/2})$.

Then, we will exhibit two full polynomial-time cryptanalysis of the NICE family of cryptosystems: one for the variant in imaginary quadratic fields, obtained in collaboration with Guilhem Castagnos, and another on the variant in real quadratic fields, which is a direct application of the factoring algorithm.

1.2.1 Notations concerning Quadratic Fields and Binary Quadratic Forms

We here define the notations and recall some useful results on quadratic fields and binary quadratic forms.

1. for *New Ideal Coset Encryption*

Let $D \neq 0, 1$ be a squarefree integer and consider the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. If $D < 0$ (resp. $D > 0$), K is called an *imaginary* (resp. a *real*) quadratic field. The *fundamental discriminant* Δ_K of K is defined as $\Delta_K = D$ if $D \equiv 1 \pmod 4$ and $\Delta_K = 4D$ otherwise.

The ring $\mathcal{O}_{\Delta_K}$ of algebraic integers in K is the *maximal* order of K. It can be written as $\mathbb{Z} + \omega_K\mathbb{Z}$, where $\omega_K = \frac{1}{2}(\Delta_K + \sqrt{\Delta_K})$. If we set $q = [\mathcal{O}_{\Delta_K} : \mathcal{O}]$ the *finite* index of any order $\mathcal{O}$ in $\mathcal{O}_{\Delta_K}$, then $\mathcal{O} = \mathbb{Z} + q\omega_K\mathbb{Z}$. The integer q is called the *conductor* of $\mathcal{O}$. The discriminant of $\mathcal{O}$ is then $\Delta_q = q^2\Delta_K$.

Now, let $\mathcal{O}_\Delta$ be an order of discriminant Δ and $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_\Delta$, its norm is $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_\Delta/\mathfrak{a}|$. A *fractional* ideal is a subset $\mathfrak{a} \subset K$ such that $d\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$ for $d \in \mathbb{N}$. A fractional ideal $\mathfrak{a}$ is said to be *invertible* if there exists an another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}_\Delta$. The *ideal class group* of $\mathcal{O}_\Delta$ is $C(\mathcal{O}_\Delta) = I(\mathcal{O}_\Delta)/P(\mathcal{O}_\Delta)$, where $I(\mathcal{O}_\Delta)$ is the group of invertible fractional ideals of $\mathcal{O}_\Delta$ and $P(\mathcal{O}_\Delta)$ the subgroup consisting of principal ideals. Its cardinality is the *class number* of $\mathcal{O}_\Delta$ denoted by $h(\mathcal{O}_\Delta)$. A nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is said to be *prime to* q if $\mathfrak{a} + q\mathcal{O}_\Delta = \mathcal{O}_\Delta$. We denote by $I(\mathcal{O}_\Delta, q)$ the subgroup of $I(\mathcal{O}_\Delta)$ of ideals prime to q.

The group $\mathcal{O}_\Delta^\star$ of units in $\mathcal{O}_\Delta$ is equal to $\{\pm 1\}$ for all $\Delta < 0$, except when Δ is equal to -3 and -4 ($\mathcal{O}_{-3}^\star$ and $\mathcal{O}_{-4}^\star$ are respectively the group of sixth and fourth roots of unity). When $\Delta > 0$, then $\mathcal{O}_\Delta^\star = \langle -1, \varepsilon_\Delta \rangle$ where $\varepsilon_\Delta > 0$ is called the *fundamental unit*. The real number $R_\Delta = \log(\varepsilon_\Delta)$ is the *regulator* of $\mathcal{O}_\Delta$. The following important bounds on the regulator of a real quadratic field can be found in [JLW95]:

$$\log\left(\frac{1}{2}(\sqrt{\Delta - 4} + \sqrt{\Delta})\right) \leq R_\Delta < \sqrt{\frac{1}{2}\Delta}\left(\frac{1}{2}\log\Delta + 1\right). \tag{1.1}$$

The lower bound is reached *infinitely often*, for instance with $\Delta = x^2 + 4$ with $2 \nmid x$. Finally, this last proposition is the heart of both the imaginary NICE [HPT99, PT99, PT00] and the real NICE [JSW08].

Proposition 1 ([Cox99, Proposition 7.20][Wei04, Theorem 2.16]) *Let $\mathcal{O}_{\Delta_q}$ be an order of conductor q in a quadratic field K.*

1. *If $\mathfrak{A}$ is an $\mathcal{O}_{\Delta_K}$-ideal prime to q, then $\mathfrak{A} \cap \mathcal{O}_{\Delta_q}$ is an $\mathcal{O}_{\Delta_q}$-ideal prime to q of the same norm.*
2. *If $\mathfrak{a}$ is an $\mathcal{O}_{\Delta_q}$-ideal prime to q, then $\mathfrak{a}\mathcal{O}_{\Delta_K}$ is an $\mathcal{O}_{\Delta_K}$-ideal prime to q of the same norm.*
3. *The map $\varphi_q : I(\mathcal{O}_{\Delta_q}, q) \to I(\mathcal{O}_{\Delta_K}, q)$, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_K}$ is an isomorphism.*

The map φ_q from Proposition 1 induces a surjection

$$\bar{\varphi}_q : C(\mathcal{O}_{\Delta_q}) \twoheadrightarrow C(\mathcal{O}_{\Delta_K})$$

which can be efficiently computed (see [PT00]). In our settings, we will use a prime conductor q and consider $\Delta_q = q^2\Delta_K$, for a fundamental discriminant Δ_K. In that case, the order of the kernel of $\bar{\varphi}_q$ is given by the classical *analytic class number formula* (see for instance [BV07])

$$\frac{h(\mathcal{O}_{\Delta_q})}{h(\mathcal{O}_{\Delta_K})} = \begin{cases} q - (\Delta_K/q) & \text{if } \Delta_k < -4, \\ (q - (\Delta_K/q))R_{\Delta_K}/R_{\Delta_q} & \text{if } \Delta_k > 0. \end{cases} \tag{1.2}$$

Note that in the case of real quadratic fields, $\epsilon_{\Delta_q} = \epsilon_{\Delta_K}^t$ for a positive integer t, hence $R_{\Delta_q}/R_{\Delta_K} = t$ and $t \mid (q - (\Delta_K/q))$.

The algorithms to compute φ_q and its inverse can be found in [PT00]. The crucial observation is that these algorithms involve only a constant number of integer multiplications and centred euclidean divisions, which means that these algorithm have *quasi-linear complexity*. These algorithms, which need the conductor q as input, will be used to decrypt a ciphertext (they indeed constitute the trapdoor τ of the construction from Figure 1.4 presented later).

The following effective lemma is the core of the imaginary NICE system, as well as of our attack. It actually gives the precise (and computable) structure of the kernel of $\ker \bar{\varphi}_q$ whose elements will serve as randomness to hide the message. A representative $\mathfrak{h}$ of an element of this kernel is part of the public key in the imaginary NICE: we will show in the next section that this element actually holds all the information on the factorisation of the discriminant Δ_q.

Lemma 1 *Let Δ_K be a fundamental negative discriminant, different from -3 and -4, and q a conductor. Then there exists an effective isomorphism*

$$\psi_q: \quad (\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times \,/\, (\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \ker \bar{\varphi}_q.$$

We will denote by $\phi_{\Delta_K}(q) := q\prod_{d|q}\left(1 - \left(\frac{\Delta_K}{d}\right)\frac{1}{d}\right)$ the order of $\ker \bar{\varphi}_q$.

Working with ideals modulo the equivalence relation of the class group is essentially equivalent to work with binary quadratic forms modulo $\mathsf{SL}_2(\mathbb{Z})$ (cf. Section 5.2 of [Coh00]). Moreover, quadratic forms are more suited to an algorithmic point of view. Every ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ can be written as $\mathfrak{a} = m\left(a\mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$ with $m \in \mathbb{Z}$, $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ such that $b^2 \equiv \Delta \pmod{4a}$. In the remainder, we will only consider *primitive* integral ideals, which are those with $m = 1$. This notation also represents the binary quadratic form $ax^2 + bxy + cy^2$, also denoted $[a, b, c]$, with $b^2 - 4ac = \Delta$. This representation of the ideal is unique if the form is normal (see Definition below).

1.2.2 Factoring pq^2 with Quadratic Forms

RELATED WORK. Our algorithm is based on quadratic forms, which share a long history with factoring (see [CP01]). Fermat's factoring method represents N in two intrinsically different ways by the quadratic form $x^2 + y^2$. It has been improved by Shanks with SQUFOF, whose complexity is $\tilde{O}(N^{1/4})$ (see [GW08] for a detailed analysis). Like ours, this method works with the infrastructure of a class group of positive discriminant, but is different in spirit since it searches for an *ambiguous* form (after having found a square form), and does not focus on discriminants of a special shape. Schoof's factoring algorithms [Sch82] are also essentially looking for ambiguous forms. One is based on computation in class groups of complex quadratic orders and the other is close to SQUFOF since it works with real quadratic orders by computing a good approximation of the regulator to find an ambiguous form. Like SQUFOF, this algorithm does not takes advantage of working in a non-maximal order and is rather different from our algorithm. Both algorithms of [Sch82] runs in $\tilde{O}(N^{1/5})$ under

the generalised Riemann hypothesis. McKee's method [McK99] is a speedup of Fermat's algorithm (and was presented as an alternative to SQUFOF) with a heuristic complexity of $\tilde{O}(N^{1/4})$ instead of $\tilde{O}(N^{1/2})$.

SQUFOF and other exponential methods are often used to factor small numbers (say 50 to 100 bits), for instance in the post-sieving phase of the Number Field Sieve algorithm. Some interesting experimental comparisons can be found in [Mil07]. Note that the currently fastest rigorous *deterministic* algorithm actually has exponential complexity: it is based on a polynomial evaluation method (for a polynomial of the form $x(x-1)\cdots(x-B+1)$ for some bound B) and its best variant is described in [BGS07]. Finally, all sieve factoring algorithms are somewhat related to quadratic forms, since their goal is to find random pairs (x, y) of integers such that $x^2 \equiv y^2 \mod N$. However, these algorithms factor generic numbers and have a subexponential complexity.

Our factoring algorithm makes intensive use of the reduction of indefinite forms $f = [a, b, c]$ of positive discriminant Δ which are said to be *reduced* if $\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$, and *normal* if $-|a| < b \leq |a|$ for $|a| \geq \sqrt{\Delta}$, and $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$ for $|a| < \sqrt{\Delta}$. The Lagrange-Gauß process which reduces any indefinite form has a quasi-linear time complexity (see [BV07, Theorem 6.6.4]).

The procedure which transforms a form $f = [a, b, c]$ into a normal one consists in setting s such that $b + 2sa$ belongs to the right interval (see [BV07, (5.4)]) and producing the form $[a, b + 2sa, as^2 + bs + c]$. Once a form $f = [a, b, c]$ is normalised, a *reduction step* consists in normalising the form $[c, -b, a]$. We denote this form by $\rho(f)$ and by `Rho` a corresponding algorithm. The reduction then consists in normalising f, and then iteratively replacing f by $\rho(f)$ until f is reduced.

It returns a reduced form g which is equivalent to f modulo $\mathsf{SL}_2(\mathbb{Z})$. We will call *matrix of the reduction*, the matrix M such that $g = f.M$. The main difference with forms of negative discriminant is that there will in general not exist a unique reduced form per class, but several organised in a cycle structure *i. e.*, when f has been reduced then subsequent applications of give other reduced forms.

If f is an indefinite binary quadratic form, the *cycle* of f is the sequence $(\rho^i(g))_{i\in\mathbb{Z}}$ where g is a reduced form which is equivalent to f.

From Theorem 6.10.3 from [BV07], the cycle of f consists of all reduced forms in the equivalence class of f. Actually, the complete cycle is obtained by a finite number of application of ρ as the process is periodic. It has been shown (in [BTW95] for example) that the period length ℓ of the sequence of reduced forms in each class of a class group of discriminant Δ satisfies

$$\frac{R_\Delta}{\log \Delta} \leq \ell \leq \frac{2R_\Delta}{\log 2} + 1.$$

A very important form is the following:

Definition 1 *Let b be the greatest odd integer less than $\sqrt{\Delta}$ if Δ is odd or the greatest even integer less than $\sqrt{\Delta}$ if Δ is even. The reduced form $[1, b, (b^2 - \Delta)/4]$ of discriminant $\Delta > 0$ is called the* principal form *of discriminant Δ, and will be denoted $\mathbf{1}_\Delta$.*

Let us now describe our factoring algorithm.

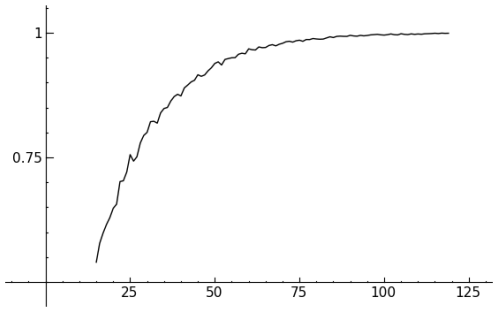

Figure 1.1 – Probability that $|M_k| < |\Delta_q|^{1/9}$ in function of the bit-size λ of p and q

DESCRIPTION OF THE ALGORITHM. Let p and q be two primes of the same bit-size λ and $p \equiv 1 \pmod 4$. Our algorithm factors the integer $\Delta = pq^2$ thanks to the special normalised, but not reduced, quadratic forms $f_k = [q^2, kq, (k^2 - p)/4]$ for some odd integers k. It is clear that if we obtain such a form, we just have to read q^2 from its coefficients and we are done. Here is a solution to find such a form.

First, we prove that $R_{\Delta_q}/R_{\Delta_K}$ forms f_k are principal and we exhibit the generators of the corresponding primitive ideals in the following theorem.

Theorem 1 ([CJLN09]) *Let Δ_K be a fundamental positive discriminant, $\Delta_q = \Delta_K q^2$ where q is an odd prime conductor. Let ε_{Δ_K} (resp. ε_{Δ_q}) be the fundamental unit of $\mathcal{O}_{\Delta_K}$ (resp. $\mathcal{O}_{\Delta_K q^2}$) and t such that $\varepsilon_{\Delta_K}^t = \varepsilon_{\Delta_q}$. Then the principal ideals of $\mathcal{O}_{\Delta_K q^2}$ generated by $q\varepsilon_{\Delta_K}^i$ correspond to quadratic forms $f_{k(i)} = [q^2, k(i)q, (k(i)^2 - p)/4]$ with $i \in \{1, \ldots, t-1\}$ and $k(i)$ is an integer defined modulo $2q$ computable from $\varepsilon_{\Delta_K}^i \mod q$.*

Suppose that we know an indefinite form $\hat{f}_k$, which is the reduction of a form $f_k = [q^2, kq, (k^2 - p)/4]$ where k is an integer. Then $\hat{f}_k$ *represents* the number q^2. More precisely, if $M_k = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})$ is the matrix of the reduction such that $\hat{f}_k = f_k.M_k$, then $\hat{f}_k.M_k^{-1} = f_k$ and $q^2 = f_k(1,0) = \hat{f}_k(\delta, -\gamma)$. Provided they are relatively small compared to Δ_q, the values δ and $-\gamma$ can be found in polynomial time with a new variant of Coppersmith method. Indeed, our algorithm actually relies on the following heuristic, which is supported by our experiments (see Figure 1.1) and illustrated in Figure 1.2.

Heuristic 1 (Real case) *From the principal form $\mathbf{1}_{\Delta_q}$, a reduced form $\hat{f}_k$ such that the matrix of the reduction, M_k, satisfy $|M_k| < \Delta_q^{1/9}$, can be found in $\mathcal{O}(R_{\Delta_K})$ successive applications of Rho.*

On the other hand, we proved the following theorem using a slight variant of the Coppersmith method (using the LLL algorithm) for the case of homogeneous polynomials. For more information on LLL and Coppersmith method, see [NV09].

Theorem 2 ([CJLN09], Theorem 2) *Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree δ with $f(x,0) = x^\delta$, N be a nonzero integer and α be a rational number in $[0,1]$, then*

one can retrieve in polynomial time in $\log N$, δ *and the bit-size of* α, *all the rationals* x_0/y_0, *where* x_0 *and* y_0 *are integers such that* $\gcd(f(x_0, y_0), N) \geq N^{\alpha}$ *and* $|x_0|, |y_0| \leq N^{\alpha^2/(2\delta)}$.

For our purpose, $\delta = 2$, $N = \Delta_q = pq^2$ with p and q of the same size, $\alpha = 2/3$ then $\lambda = 3/2$, it states that we will be able to asymptotically recover δ and $-\gamma$ of certain $\hat{f}_k$ under the condition they are lower than Δ_q^{β} with $\beta = \frac{1}{9}$. We will call HomogeneousCoppersmith the algorithm which implements this method.

Our factoring algorithm will actually work in the principal equivalence class since we can simply exhibit the *principal form* $\mathbf{1}_{\Delta_q}$ of discriminant Δ_q using only this information Δ_q as input (see Definition 1). Our factoring algorithm described in Figure 1.3 can be sketched as follows:

Start from the principal form $\mathbf{1}_{\Delta}$, walk on its cycle (with Rho) until a form $\hat{f}_k$ such that the coefficients of M_k are sufficiently small is found (with HomogeneousCoppersmith), retrieve δ and $-\gamma$ and the non-trivial factor q^2 of Δ_q.

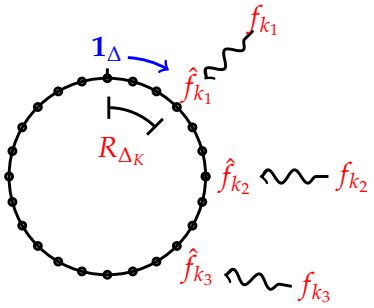

Figure 1.2 – Repartition of the forms $\hat{f}_{k(i)}$ along the principal cycle

COMPLEXITY. Assuming Heuristic 1, starting from $\mathbf{1}_{\Delta_q}$, after $O(R_p)$ iterations, the algorithm will stop on a reduced form whose roots will be found with our Coppersmith-like method (for suitable values of m and t) since they will satisfy the expected $\Delta_q^{1/9}$ bound. The computation of $\gcd(h(x_0, y_0), \Delta_q)$ will therefore expose q^2 and factor Δ_q. The time complexity of our algorithm is then heuristically $O(R_p \mathsf{Poly}(\log \Delta_q))$, whereas the space complexity is $O(\log \Delta_q)$. The worst-case complexity is $O(p^{1/2} \log p \, \mathsf{Poly}(\log \Delta_q))$.

1.2.3 Full Cryptanalysis of the NICE Family of Cryptosystems

We describe in this section a family of encryption schemes based on the arithmetic of ideals of quadratic fields, and demonstrate their full insecurity. These systems somehow fits the following generic framework formalised in [Gjo04].

This construction relies on the self-reducible *splitting problem* (see [Gjo04, Proposition 4.4]. It starts from a finite abelian (multiplicative) group $\mathbb{G}$, two of its subgroups M and R such that $MR = \mathbb{G}$ and $M \cap R = \{1\}$ and the natural isomorphism $\mathbb{G} \xrightarrow{\sim} M \times R$. The morphism $M \times R \longrightarrow \mathbb{G}$: $(m, r) \mapsto mr$ is simply the multiplication, the other way might be

Input: $\Delta_q = pq^2, m, t$
Output: p, q

1. $h \leftarrow \mathbf{1}_{\Delta_q}$
2. **while** (x_0, y_0) not found **do**
   2.1. $h \leftarrow \mathsf{Rho}(h)$
   2.2. $x_0/y_0 \leftarrow \mathsf{HomogeneousCoppersmith}(h, \Delta_q, m, t)$
3. $q \leftarrow \mathsf{Sqrt}(\mathsf{Gcd}(h(x_0, y_0), \Delta_q))$
4. **return** $(\Delta_q/q^2, q)$

Figure 1.3 – Factoring $\Delta_q = pq^2$

hard to compute. The set of all triple $(\mathbb{G}, M, R)$ is associated to a probability space, that we will ignore for simplicity. Two associated problems are useful to design cryptosystem: the first is a computational problem, and the second is a decisional one.

SPLITTING PROBLEM. The *splitting problem* (or *projection problem*) is exactly the computation, given as input the instance $(\mathbb{G}, M, R, c)$ where c is sampled uniformly at random from $\mathbb{G}$, of a pair (m, r) such that $c = mr$. The *trapdoor splitting problem* has an additional trapdoor τ which allows to solve the splitting problem.

SUBGROUP MEMBERSHIP PROBLEM. Another problem is important to prove the semantic security of the constructed encryption scheme : it is called *subgroup membership problem*. It consists, given an instance (G, R, x), to determine whether x is in R or not.

We can find many examples of these problems in the literature. We mention the following subgroup membership problems: quadratic (or higher) residue problem, decisional Diffie-Hellman problem, decision composite residuosity problem, etc. It is possible to implement these problems in groups of publicly unknown order.

GENERIC FRAMEWORK TO DESIGN HOMOMORPHIC SYSTEMS. The generic framework is depicted in Figure 1.4, it allows to design homomorphic cryptosystems. The idea is that the messages live in M and the subgroup R provides the noise to hide the message. We do not discuss how to embed true messages into M, but it is important to note that this embedding in M, as well as sampling its elements are not necessarily trivial. The map τ will usually be the projection $\pi_M : \mathbb{G} \to M$ whose kernel $\ker(\pi_M)$ is isomorphic to R.

This gives a multiplicative homomorphic encryption scheme which can be turned into an additive one by replacing m by g^m for a $g \in G$ if $M \subset \langle g \rangle$ and if it is efficient to extract discrete logarithm in M. The corresponding problems have to be modified accordingly. Gjøsteen proves the two following security results (see [Gjo04, Proposition 5.2, Theorem 5.4]).

Proposition 2 *The public key cryptosystem of Figure 1.4 is one-way if and only if the splitting problem is hard.*

Theorem 3 *The public key cryptosystem of Figure 1.4 is semantically secure if and only if the subgroup membership problem is hard.*

KeyGen:

– Generate a group instance $(\mathbb{G}, M, R, \tau)$ of the trapdoor splitting problem. We suppose that there exists an efficient algorithm to sample elements from R.
– Set $pk \leftarrow (\mathbb{G}, M, R)$ and $sk \leftarrow \tau$.

Encrypt:

– Pick $r \xleftarrow{\$} R$.
– Compute $c \leftarrow mr$
– Output c

Decrypt:

– Compute $(m, r) \leftarrow \tau(c)$
– Output m

Figure 1.4 – General framework for homomorphic encryption

Many cryptosystems fall in this framework. To mention a few, one can cite Goldwasser-Micali [GM84], Benaloh [Ben94], Elgamal [Elg85], Paillier [Pai99], Naccache-Stern [NS98], Damgård-Jurik [DJ01] or Boneh-Goh-Nissim [BGN05]. For further discussion, see also the theses [Gjo04, Cas06].

As already mentioned, another relevant example is the Okamoto-Uchiyama [OU98] cryptosystem, which is the ancestor of Paillier's encryption scheme. Is it one of these cryptosystems whose security relies on the hardness of the factorisation of integers of the form $N = pq^2$.

We will now discuss in more details the NICE family of encryption scheme.

Description of the NICE Family of Cryptosystems

Hartmann, Paulus and Takagi proposed the elegant *NICE* encryption scheme (see [HPT99, PT99, PT00]), based on imaginary quadratic fields and whose main feature was a quasi-linear decryption time. Later on, several other schemes, including (special) signature schemes relying on this framework have been proposed. The public key of these NICE cryptosystems contains a discriminant $\Delta_q = -pq^2$ together with a reduced ideal $\mathfrak{h}$ whose class belongs to the kernel of $\bar{\varphi}_q$. The idea underlying the NICE cryptosystem is to hide the message behind a random element $[\mathfrak{h}]^r$ of the kernel. Applying $\bar{\varphi}_q$ will make this random element disappear, and the message will then be recovered.

In [JSW08], Jacobson, Scheidler and Weimer embedded the original NICE cryptosystem in *real* quadratic fields. Whereas the idea remains essentially the same as the original, the implementation is very different. The discriminant is now $\Delta_q = pq^2$, but because of the differences between imaginary and real setting, these discriminant will have to be chosen carefully. Among these differences, the class numbers are expected to be small with very high probability (see the Cohen-Lenstra heuristics [CL84]). Moreover, an equivalence class does not contain a *unique* reduced element anymore, but a multitude of them, whose number is governed by the size of the fundamental unit.

As already mentioned, the original NICE somehow follows Gjøsteen's framework with $R = \ker \bar{\varphi}_q$ and $M = \left\{ [\mathfrak{a}] \in C(\mathcal{O}_{\Delta_q}), N(\mathsf{Red}(\mathfrak{a})) < \sqrt{|\Delta_p|/4} \right\}$. Essentially, the trapdoor τ

would be the prime q needed to compute φ_q, and as it is not trivial to sample elements of R, one of its generator must be added to the public key. The point is that M is not a subgroup of $C(\mathcal{O}_{\Delta_q})$ (there is no semidirect product), and the embedding of a message into this set actually destroys the homomorphic property, so it is not a direct application of this framework. The main interest of the NICE encryption schemes is the efficiency of the decryption process. It consists in applying the $\bar{\varphi}_q$ surjection to the ciphertext $[\mathfrak{c}]$ to remove the hiding part coming from $\bar{\varphi}_q$'s kernel. This is done by using algorithm with quasi-linear complexity, which makes NICE asymptotically faster than RSA (or any system for which this operation is an exponentiation). This system has actually been implemented on smart cards, with competitive results (see [PT99]).

Despite this apparent benefit, we demonstrate in the following the dramatic weakness of the key-generation, for both imaginary and real variants.

Full Cryptanalysis of the Original NICE

We present in this section a *key-only total break* of the NICE encryption scheme. We can therefore concentrate on the key generation which outputs an element $[\mathfrak{h}]$ of $\ker \bar{\varphi}_q$ as a part of the public key. The public key consists in the reduced representative $\mathfrak{h}$ of $[\mathfrak{h}]$ and a discriminant $\Delta_q = -pq^2$, where p and q primes of the same size and $q > \sqrt{p/3}$.

Other encryption schemes which share this key generation can be found in [HPT99, PT00, BST02, Huh00, PT99], and signature schemes in [Huh01, HM00, BPT04]. *All* these cryptosystems succumb to our attack.

A previous attempt to break this scheme gave rise to a full cryptanalysis under a *chosen-ciphertext attack* by Joux and Jaulmes [JJ00]. Two clever decryption queries allow to recover the factorisation of the discriminant. This attack uses the fact that the decryption fails (*i.e.*, does not recover the plain message) if the norm of the ideal representing the message is greater than $\sqrt{|\Delta_K|/3}$, so that the decoded message will expectedly be one step from being reduced. The relation between two pairs original message/decoded message leads to a Diophantine equation of the form $k = XY$ for a known "random" integer k of the size of the secret primes. The authors suggest to factor this integer to find out X and Y and then factor Δ_q. This attack is feasible for the parameters proposed in [HPT99], but can be defeated by enlarging the key size by a factor of 3. The scheme can resist to this attack by adding redundancy to the message as suggested in [JJ00] and [BST02]. Note that, contrary to ours, Jaulmes and Joux's attack also applies to [HJPT98].

While investigating some claims concerning the hardness of the so-called *Kernel problem* (given $[\mathfrak{h}]$ and Δ_q, factor Δ_q), we experimentally found ideals of the form $[q^2, kq, -]$, for an odd k satisfying $|k| < q$ whose classes belong to the kernel of $\bar{\varphi}_q$. It is actually possible to build a representative set of this kernel with ideals of norm q^2. This is stated in the following theorem whose proof relies on the effective isomorphism from Lemma 1. This is essentially the result of Theorem 1 but for negative discriminants.

Theorem 4 ([CL09], Theorem 2) *Let Δ_K be a fundamental negative discriminant, different from -3 and -4 and q an odd prime conductor. There exists an ideal of norm q^2 in each nontrivial class of* $\ker \bar{\varphi}_q$.

This representation of $\ker \bar{\varphi}_q$ has also been proven useful to obtain q^2-isogeny cycles to compute classical modular polynomials $\Phi_q(X, Y)$ using graphs of q-isogenies, see [BLS11].

KeyGen:
- Let p and q be two primes such that $q > \sqrt{p/3}$.
- Set $\Delta_K = -p$ and $\Delta_q = \Delta_K q^2 = -pq^2$.
- Let $[\mathfrak{h}]$ be an element of $\ker \bar{\varphi}_q$, where $\mathfrak{h}$ is a reduced $\mathcal{O}_{\Delta_q}$-ideal.
- Set $pk \leftarrow (\Delta_q, \mathfrak{h})$ and $sk \leftarrow (p, q)$.

Encrypt:
- A message m is embedded into a reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ with $\log_2(N(\mathfrak{m})) < k$.
- Pick randomly $r \in [\![1, |\Delta_q|^{1/3}]\!]$ and compute $\mathfrak{c} = \mathsf{Red}(\mathfrak{m} \times \mathfrak{h}^r)$.

Decrypt: Compute $\varphi_q^{-1}(\mathsf{Red}(\varphi_q(\mathfrak{c}))) = \mathfrak{m}$.

Figure 1.5 – Simplified Description of the original NICE

In our setting, this means that there exists an ideal of norm q^2 equivalent to the reduced ideal $\mathfrak{h}$ given in the public key. A successful strategy to find this ideal is the following:

i Choose a power r of small odd prime large enough to make ideals of norm q^2 reduced in $C(\mathcal{O}_{\Delta_q r^2})$.

ii Lift $[\mathfrak{h}']$ (where $\mathfrak{h}'$ is equivalent to $\mathfrak{h}$ and prime to r) in this class group $C(\mathcal{O}_{\Delta_q r^2})$:
   (a) Compute $\mathfrak{g} = \mathfrak{h}' \cap \mathcal{O}_{\Delta_q r^2}$, which is an $\mathcal{O}_{\Delta_q r^2}$-ideal.
   (b) Compute the reduced element $\mathfrak{t}$ of the class of $\mathfrak{g}$ raised to the power $\phi_{\Delta_K}(r)$: it has norm q^2.

The algorithm is formally described below.

Algorithm 1: Solving the Kernel Problem

Input: $\lambda \in \mathbb{Z}, \Delta_q = -pq^2 \in \mathbb{Z}, \mathfrak{h} = (a, b) \in I(\mathcal{O}_{\Delta_q}, q)$ with $[\mathfrak{h}] \in \ker \bar{\varphi}_q$ of order > 6

Output: p, q

Initialisation:
1. Set $r' = 3$
2. Set $\delta_{r'} = \lceil \frac{\lambda+3}{2} \frac{\log 2}{\log r'} \rceil$ and $r = r'^{\delta_{r'}}$
3. **If** the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r)$ **then** set r' to the next prime and **goto** 2.
4. Find $\mathfrak{h}' \in [\mathfrak{h}]$ such that $\mathfrak{h}' \in I(\mathcal{O}_{\Delta_q}, r')$ [HJPT98, Algorithm 1]

Core Algorithm:
5. Compute $\mathfrak{g} = \mathfrak{h}' \cap \mathcal{O}_{\Delta_q r^2}$ [PT00, Algorithm 2]
6. Compute $\mathfrak{t} = \mathsf{Red}(\mathfrak{g}^{\phi_{\Delta_K}(r)})$
7. **Return** $p = \Delta_q / \mathrm{N}(\mathfrak{t}), q = \sqrt{\mathrm{N}(\mathfrak{t})}$

Its correctness comes from the following results which explain this commutative diagram:

$$\begin{array}{ccc} \ker \bar{\varphi}_q & \xrightarrow{\quad \hat{s} \quad} & \ker \bar{\varphi}_{qr} \\ \uparrow \psi_q \wr & \circlearrowleft & \uparrow \psi_{qr} \wr \\ (\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times & \xrightarrow{\quad s \quad} & (\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/qr\mathbb{Z})^\times \end{array}$$

Lemma 2 *Let Δ_K be a fundamental negative discriminant, different from -3 and -4 and q an odd prime conductor and r be an odd integer prime to q and Δ_K such that $r > 2q/\sqrt{|\Delta_K|}$. The isomorphism ψ_{qr} of Lemma 1 maps the nontrivial elements of the kernel of this natural surjection*

$$\pi : (\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/qr\mathbb{Z})^\times \twoheadrightarrow (\mathcal{O}_{\Delta_K}/r\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/r\mathbb{Z})^\times$$

to classes of $\ker \bar{\varphi}_{qr} \subset C(\mathcal{O}_{\Delta_K q^2 r^2})$*, whose reduced element has norm q^2.*

Theorem 5 *Let Δ_K be a fundamental negative discriminant, different from -3 and -4 and q be an odd prime conductor. Let r be an odd integer, prime to both q and Δ_K such that $r > 2q/\sqrt{|\Delta_K|}$. Given a class of* $\ker \bar{\varphi}_q$ *and $\mathfrak{h}$ a representative in $I(\mathcal{O}_{\Delta_q}, qr)$, then the class*

$$[\mathfrak{h} \cap \mathcal{O}_{\Delta_q r^2}]^{\phi_{\Delta_K}(r)}$$

is trivial if the order of $[\mathfrak{h}]$ divides $\phi_{\Delta_K}(r)$ and has a reduced element of norm q^2 otherwise.

Again, the proof of correctness of Algorithm 1 is be done by using the effective isomorphisms between $\ker \bar{\varphi}_q$ and $(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times$ and between $\ker \bar{\varphi}_{qr}$ and $(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/qr\mathbb{Z})^\times$. The integer r is an odd integer prime to q and Δ_K such that $r > 2q/\sqrt{|\Delta_K|}$, *i. e.*, such that ideals of norm q^2 are reduced in $C(\mathcal{O}_{\Delta_q r^2})$.

First in Lemma 2, we prove that nontrivial elements of a certain subgroup of the quotient $(\mathcal{O}_{\Delta_K}/qr\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/qr\mathbb{Z})^\times$ map to classes of $\ker \bar{\varphi}_{qr}$ whose reduced element has norm q^2. Actually, this subgroup contains the image of a particular lift of $(\mathcal{O}_{\Delta_K}/q\mathcal{O}_{\Delta_K})^\times / (\mathbb{Z}/q\mathbb{Z})^\times$ following the Chinese remainder theorem: A class $[\alpha]$ modulo q is lifted to a class $[\beta]$ modulo qr such that $[\beta] \equiv 1 \pmod{r}$ and $[\beta] \equiv [\alpha]^{\phi_{\Delta_K}(r)} \pmod{q}$.

Then, in Theorem 5, we prove that the lift computed in steps 4 and 6 of Algorithm 1 corresponds to the lift previously mentioned on the quotients of $\mathcal{O}_{\Delta_K}$. As a result, this lift evaluated on an element of $\ker \bar{\varphi}_q$ either gives the trivial class or a class corresponding to the nontrivial elements of the subgroup of Lemma 2, *i. e.*, a class whose reduced element has norm q^2.

The cost of the initialisation phase is essentially quasi-quadratic in the security parameter. The core of the algorithm consists in applying [PT00, Algorithm 2] whose complexity is quasi-linear in λ, and an exponentiation whose complexity is quasi-quadratic. Finally, we prove that:

Corollary 1 *Algorithm 1 solves the Kernel Problem and totally breaks the NICE family of cryptosystems in quasi-quadratic time in the security parameter.*

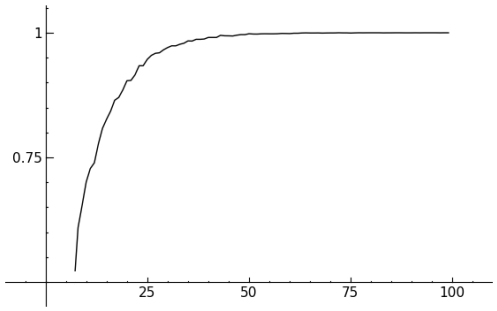

Figure 1.6 – Probability that $|M_k| < |\Delta_q|^{1/9}$ in function of the bit-size λ of p and q

COPPERSMITH APPROACH. A Coppersmith approach on the quadratic form $\hat{h}$ corresponding to the ideal $\mathfrak{h}$ actually works also. The form $\hat{h}$ is the reduction of a form $h = [q^2, kq, (k^2 + p)/4]$ for some integer k (because of Theorem 4), so that there exists a matrix $M_k \in \mathsf{SL}_2(\mathbb{Z})$ such that $\hat{h} = h.M_k$. The following heuristic (also supported by our experiments, see Figure 1.6) implies that we can recover the entries of this matrix using the same Coppersmith method as in the previous section, and therefore totally break the scheme.

Heuristic 2 (Imaginary case) *Given a reduced element $\hat{h}$ of a nontrivial class of* $\ker \bar{\varphi}_q$*, the matrix of reduction M_k is such that $|M_k| < |\Delta_q|^{1/9}$ with probability asymptotically close to 1.*

Full Cryptanalysis of the Real NICE

The core of the design of the REAL-NICE encryption scheme, lightly described in Figure 1.7 is the very particular choice of the secret prime numbers p and q such that $\Delta_K = p$ and $\Delta_q = pq^2$. They are chosen such that the ratio $R_{\Delta_q}/R_{\Delta_K}$ is of order of magnitude of q and that R_{Δ_K} is bounded by a polynomial in $\log(\Delta_K)$. To ensure the first property, it is sufficient to choose q such that $q - \left(\frac{\Delta_K}{q}\right)$ is a small multiple of a large prime. If the second property is very unlikely to naturally happen since the regulator of p is generally of the order of magnitude of $\sqrt{p}$, it is indeed quite easy to construct fundamental primes with small regulator. The authors of [JSW08] suggest to produce a prime p as a so-called *Schinzel sleeper*, which is a positive squarefree integer of the form $p = a^2x^2 + 2bx + c$ with a, b, c, x in $\mathbb{Z}$, $a \neq 0$ and $b^2 - 4ac$ dividing $4\gcd(a^2, b)^2$. Schinzel sleepers are known to have a regulator of the order $\log(p)$ (see [CW05]). Some care must be taken when setting the (secret) a, b, c, x values, otherwise the resulting $\Delta_q = pq^2$ is subject to factorisation attacks described in [Wei04]. We do not provide here more details on these choices since the crucial property for our attack is the fact that the regulator is actually of the order $\log(p)$. The public key consists of the sole discriminant Δ_q. The message is carefully embedded (and padded) into a primitive $\mathcal{O}_{\Delta_q}$-ideal so that it will be recognised during decryption. Instead of moving the message ideal $\mathfrak{m}$ to a different equivalence class (like in the imaginary case), the encryption actually hides the message in the cycle of reduced ideal of its own equivalent class by multiplication of a random principal $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{h}$ (computed during encryption). The decryption process consists then in applying the (secret) map $\bar{\varphi}_q$ and perform an exhaustive search for the padded

KeyGen:
- Let p and q be two primes and let $\Delta_K = p$ and $\Delta_q = \Delta_K q^2 = pq^2$ with R_{Δ_K} small and R_{Δ_q} large.
- Set $pk = \Delta_q$ and $sk = (p, q)$.

Encrypt:
- Embed a formatted message m into a primitive $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ prime to q with $N(\mathfrak{m}) < \lfloor \sqrt{\Delta_K}/4 \rfloor$
- Generate a random $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{h}$ such that $[\mathfrak{h}] \in \ker(\bar{\varphi}_q)$ and pick randomly $r \in [\![1, |\Delta_q|^{1/3}]\!]$
- Compute $\mathfrak{c} = \mathsf{Red}(\mathfrak{m} \times \mathfrak{h}^r)$.

Decrypt:
- Compute $\varphi_q(\mathfrak{c}) = \mathfrak{C}$
- Find the reduced ideal $\mathfrak{M} \in [\mathfrak{C}]$ such that $N(\mathfrak{M})$ contains the predetermined bit pattern of encryption
- Extract m' from $N(\mathfrak{M})$ and m from m'.

Figure 1.7 – Description of NICE in real quadratic fields

message in the *small* cycle of $\bar{\varphi}_q([\mathfrak{mh}])$. This exhaustive search is actually possible thanks to the choice of p which has a very small regulator. Like in the imaginary case, the decryption procedure has a quadratic complexity and significantly outperforms an RSA decryption for any given security level (see Table 3 from [JSW08]). Unfortunately, due to the particular but necessary choice of the secret prime p, the following result states the total insecurity of the REAL-NICE system.

The cryptanalysis is therefore a direct application of the factoring algorithm presented in Section 1.2.2.

Result 1 *Algorithm 1.3 recovers the secret key of REAL-NICE in polynomial time in the security parameter under Heuristic 1 since the secret fundamental discriminant p is chosen to have a regulator bounded by a polynomial in* $\log p$.

1.2.4 Recent Improvements and Perspectives

This cryptanalysis which uses the Coppersmith approach lies on some heuristics, and is therefore not rigorous. These heuristics concern the behaviour of the binary quadratic forms and their reduction process. One of the main issue is the existence of (rare) *unbalanced* forms, which are forms with unusually unbalanced coefficients. Our Coppersmith method fails when applied on such forms. Another issue is the bounds on δ and γ after a reduction with the Gauß algorithm: [BV07] gives $\sqrt{|\delta\gamma|} < q^2/\sqrt{\Delta}\left(1 + 1/\sqrt{\Delta}\right)$, which is not sufficient to get the correct bounds for the Coppersmith method. To overcome these problems, Bernard and Gama propose a new reduction algorithm called RedGL2 which allows

to obtain (optimal) bounds, described in the following theorem, that are the square root of those in [BV07].

Theorem 6 ([BG10], Theorem 2) *Let $f = [a, b, c]$ be a primary-normalised[1] form of discriminant $\Delta > 0$. Given f as input,* RedGL2 *terminates after at most $\left(\frac{\log(|a|/\sqrt{\Delta})}{2\log\omega} + 4\right)$ iterations, where $\omega = \frac{1+\sqrt{5}}{2}$ is the golden ratio. Its output $\mathcal{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $f_r = f.M = [a_r, b_r, c_r]$ satisfies:*

1. $\|M\| \leq 4\sqrt{|a|/|a_r|}$,
2. $(|\alpha\beta\gamma\delta|)^{1/2} \leq |\gamma\delta|^{1/2} \leq \sqrt{21}\sqrt{|a|/\sqrt{\Delta}}$.

In addition, they tune the Coppersmith method to find the unbalanced solutions that we do not get with our method. They propose an algorithm called Rational-BDH that allows to reach the following bounds:

Theorem 7 ([BG10], Theorem 4) *Given an integer $N = pq^r$ (where p and q are unknown), and a bound $\beta < \frac{1}{4}q^{\log q^r / \log N}$, Algorithm* Rational-BDH *terminates in polynomial time, and finds a solution (if it exists) of the equation $\frac{x}{y} \pmod q$ where (x, y) are unknown integers satisfying $|xy| < \beta$.*

This allow to fully prove our heuristic attack.

An significant improvement is possible because our factoring algorithm can also find forms that represent not q^2 but uq^2 for small u. Indeed, the reduction matrix of forms $[uq^2, -, -]$ will have its bottom entries γ_u and δ_u that will satisfy $|\gamma_u\delta_u| < 21u\Delta_q^{1/6}$ according to Theorem 6. On the other hand, Theorem 7 insures that Bernard and Gama's Rational-BDH will recover these values if $21u\Delta_q^{1/6} < \frac{1}{4}\Delta_q^{2/9}$ allowing for u up to $u < \frac{1}{84}\Delta_q^{1/18}$. Now the proportion of such forms can be roughly approximated by $\Delta_q^{1/18}/(h(\Delta_K)R(\Delta_K))$ which is essentially $\Delta_q^{-1/9}$. This analysis suggest that our algorithm have a complexity of $\tilde{O}(\Delta_q^{1/9})$ instead of $\tilde{O}(\Delta_q^{1/6})$, which makes it as competitive as the most efficient exponential time algorithm dedicated to these numbers.

It might be interesting to understand the algorithm which produces the Schinzel sleepers in the real NICE setting, in particular, in the light of the algorithm proposed in [CGRW11] and also to get more families of integers with small regulators.

Designing a subexponential algorithm dedicated to the factorisation of numbers of the form pq^2 would very interesting. Such a method may have to use the fact that this number is a discriminant of a quadratic field like our exponential method. Discriminants of other number fields might also have dedicated factoring algorithm.

1. An indefinite binary quadratic form f is primary-normalised if the largest real root ζ_f^+ of $f(x, 1)$ satisfies $0 < \zeta_f^+ < 1$

1.3 A Variant of Miller's Algorithm to Compute Pairings

This section concerns a different topic in computational number theory for cryptography: it tackles the computation of pairings over elliptic curves.

Since their introduction in a constructive cryptographic context in the early 2000's, pairings over algebraic curves keep being a key tool for the design of complex cryptosystems, and they allowed many breakthroughs to reach versatile, dynamic, efficient and secure cryptographic primitives. Example of their usefulness will appear in the next chapter. In this section, we focus on the algorithmic aspect of these pairings by giving an efficient variant of Miller's algorithm traditionally used to compute them. Ever since it was first described, Miller's algorithm [Mil04] has been the central ingredient in the calculation of pairings on elliptic curves. Many papers are devoted to improvements in its efficiency. For example, it can run faster when the elliptic curves are chosen to belong to specific families (see for example [BLS03, BN06, CHBNW09]), or different coordinate systems (see for example [IJ08, CLN10, BL]). Another standard method of improving the algorithm is to reduce the number of iterations by introducing pairings of special type, for example particular *optimal pairings* [Ver09, HSV06, Hes08] or using addition chains (see for example [BMX06]).

Together with John Boxall, Nadia El Mrabet and Duc-Phong Le, we adopt another approach by exhibiting a slight variant of the so-called Miller's formula which is the heart of the corresponding algorithm. Our formula is less expensive than the original one and this modification gives rise to a *generically* faster algorithm for any pairing-friendly curves.

After a section on some basics on elliptic curves and pairings, we describe our new variant of Miller's algorithm and discuss its complexity.

1.3.1 Backgrounds on Pairings

We let $r \geq 2$ denote an integer which, unless otherwise stated, is supposed to be prime. We let $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$ and $(\mathbb{G}_T, \cdot)$ denote three finite abelian groups, which are supposed to be of order r. A *pairing* is a bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$

We say that the pairing e is *non degenerate* if, for all $P \in \mathbb{G}_1$ with $P \neq 1$, there exists $Q \in \mathbb{G}_2$ with $e(P, Q) \neq 1$ and if for all $Q \in \mathbb{G}_2, Q \neq 1$, there exists $P \in \mathbb{G}_1$ with $e(P, Q) \neq 1$.

We recall briefly one of the most frequent choices for the groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ in pairing-based cryptography. Here, $\mathbb{G}_1$ is the group generated by a point P of order r on an elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic different to r. Thus, $\mathbb{G}_1 \subseteq E(\mathbb{F}_q)$ is cyclic of order r but, in general, the whole group $E[r]$ of points of order dividing r of E is not rational over $E(\mathbb{F}_q)$. Recall that the *embedding degree* of E (with respect to r) is the smallest integer $k \geq 1$ such that r divides $q^k - 1$. A result of Balasubramanian and Koblitz [BK98] asserts that, when $k > 1$, all the points of $E[r]$ are rational over the extension $\mathbb{F}_{q^k}$ of degree k of $\mathbb{F}_q$. The group $\mathbb{G}_2$ is chosen as another subgroup of $E[r]$ of order r. Finally, $\mathbb{G}_T$ is the subgroup of order r in $\mathbb{F}_{q^k}^\times$; it exists and is unique, since r divides $q^k - 1$ and $\mathbb{F}_{q^k}^\times$ is a cyclic group.

For cryptographic purposes, Galbraith, Paterson and Smart first noticed in [GPS08] that three types of pairings have to be implemented:

– Type I: There are efficiently computable isomorphisms $\alpha : \mathbb{G}_2 \to \mathbb{G}_1$ and $\beta : \mathbb{G}_1 \to \mathbb{G}_2$,

– Type II: There is an efficiently computable isomorphism $\alpha : \mathbb{G}_2 \to \mathbb{G}_1$, but none is known in the opposite direction,
– Type III: There is no known efficiently computable isomorphism $\alpha : \mathbb{G}_2 \to \mathbb{G}_1$ or $\beta : \mathbb{G}_1 \to \mathbb{G}_2$.

Let $P \in E(\mathbb{F}_q)$ be an r-torsion point, let D_P be a degree zero divisor with $D_P \sim [P] - [O_E]$, and let f_{r,D_P} be such that $\operatorname{div} f_{r,D_P} = rD_P$. Let Q be a point of $E(\mathbb{F}_{q^k})$ (not necessarily r-torsion) and $D_Q \sim [Q] - [O_E]$ of support disjoint with D_P. Consider

$$e_r^T(P, Q) = f_{r,D_P}(D_Q). \tag{1.3}$$

Weil reciprocity shows that if D_Q is replaced by $D'_Q = D_Q + \operatorname{div} h \sim D_Q$, then (1.3) is multiplied by $h(D_P)^r$. So the value is only defined up to r-th powers. Replacing D_P by $D'_P = D_P + \operatorname{div} h$ changes f_{r,D_P} to $f_{r,D'_P} = f_{r,D_P} h^r$, and the value is well-defined modulo multiplication by r-th powers. If then Q is replaced by $Q + rR$, the value changes again by an r-th power. This leads to adapting the range and domain of e_r^T as follows.

Theorem 8 *The Tate pairing is a map*

$$e_r^T : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r$$

satisfying the following properties:

1. *Bilinearity,*
2. *Non-degeneracy,*
3. *Compatibility with isogenies.*

The *reduced* Tate pairing computes the unique rth root of unity belonging to the class of $f_{r,D_P}(D_Q)$ modulo $(\mathbb{F}_{q^k}^\times)^r$ as $f_{r,D_P}(D_Q)^{(q^k-1)/r}$. In practice, we take Q to lie in some subgroup $\mathbb{G}_2$ of order r of $E(\mathbb{F}_{q^k})$ that injects into $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ *via* the canonical map. The more popular Ate pairing [BGOS07] and its variants (see [MKHO09] for instance) are optimised versions of the Tate pairing when restricted to Frobenius eigenspaces. Besides its use in cryptographic protocols, the Tate pairing is also useful in other applications, such as walking on isogeny volcanoes [IJ10], which can be used in the computation of endomorphism rings of elliptic curves.

However, we concentrate on the computation of $f_{n,D_P}(D_Q)$ (which we write as $f_{n,P}(Q)$ in the sequel). This is done using Miller's algorithm described in the next subsection.

1.3.2 Miller's algorithm

In what follows, $\mathbb{F}$ denotes a field (not necessarily finite), E an elliptic curve over $\mathbb{F}$ and r an integer not divisible by the characteristic of $\mathbb{F}$. We suppose that the group $E(\mathbb{F})$ of $\mathbb{F}$-rational points of E contains a point P of order r. Since r is prime to the characteristic of $\mathbb{F}$, the group $E[r]$ of points of order r of E is isomorphic to a direct sum of two cyclic groups of order r. In general, a point $Q \in E[r]$ that is not a multiple of P will be defined over some extension $\mathbb{F}'$ of $\mathbb{F}$ of finite degree. If P, P' are two points in $E(\mathbb{F})$, s and t are two integers, we denote by

– $\ell_{P,P'}$ a function with divisor $[P] + [P'] + [-(P + P')] - 3[O_E]$,

– v_P a function with divisor $[P] + [-P] - 2[O_E]$,
– $f_{s,P}$ (or simply f_s) a function whose divisor is $s[P] - [sP] - (s-1)[O_E]$.

We abbreviate $\ell_{sP,tP}$ to $\ell_{s,t}$ and v_{sP} to v_s.

The purpose of Miller's algorithm is to calculate $f_{s,P}(Q)$ when $Q \in E[r]$ is not a multiple of P. All pairings can be expressed in terms of these functions for appropriate values of s.

Miller's algorithm is based on the following Lemma describing the so-called *Miller's formula*, which is proved by considering divisors.

Lemma 3 *For s and t two integers, up to a multiplicative constant, we have $f_{s+t} = f_s f_t \frac{\ell_{s,t}}{v_{s+t}}$.*

The usual Miller algorithm makes use of Lemma 3 with $t = s$ in a doubling step and $t = 1$ in an addition step. It is described by the pseudocode in Figure 1.8, which presents the algorithm updating numerators and denominators separately, so that just one inversion is needed at the end. We write the functions ℓ and v as quotients $(N\ell)/(D\ell)$ and $(Nv)/(Dv)$, where each of the terms $(N\ell)$, $(D\ell)$, (Nv), (Dv) is computed using only additions and multiplications, and no inversions. Here the precise definitions of $(N\ell)$, $(D\ell)$, (Nv), (Dv) will depend on the representations that are used (we indicate one such choice when short Weierstrass coordinates and the associated Jacobian coordinates are used). In the algorithm, T is always a multiple of P, so that the hypothesis that Q is not a multiple of P implies that at the functions $\ell_{T,T}$, $\ell_{T,P}$, v_{2T} and v_{T+P} cannot vanish at Q. It follows that f and g never vanish at Q so that the final quotient f/g is well-defined and nonzero.

Algorithm 2: Miller(P, Q, s) usual

Data: $s = \sum_{i=0}^{l-1} s_i 2^i$ (radix 2), $s_i \in \{0, 1\}$, $Q \in E(\mathbb{F}')$ not a multiple of P.
Result: $f_{s,P}(Q)$.
$T \leftarrow P$, $f \leftarrow 1$, $g \leftarrow 1$,;
for $i = l - 2$ **to** 0 **do**
  $f \leftarrow f^2 (N\ell)_{T,T} (Dv)_{2T}$,;
  $g \leftarrow g^2 (D\ell)_{T,T} (Nv)_{2T}$,;
  $T \leftarrow 2T$;
  if $s_i = 1$ **then**
    $f \leftarrow f (N\ell)_{T,P} (Dv)_{T+P}$,;
    $g \leftarrow g (D\ell)_{T,P} (Nv)_{T+P}$,;
    $T \leftarrow T + P$;
  end
end
return f/g

Figure 1.8 – The usual Miller algorithm

1.3.3 The New Variant of Miller's Algorithm

Our improvement come from the following simple observation.

Lemma 4 *For s and t two integers, up to a multiplicative constant, we have*

$$f_{s+t} = \frac{1}{f_{-s} f_{-t} \ell_{-s,-t}}.$$

We shall seek to exploit the fact that here the right hand member has only three terms whereas that of Lemma 3 has four. Our variant of Miller's algorithm is described by the pseudocode in Figure 1.9. It was inspired by the idea of applying Lemma 4 with $t = s$ or $t \in \{\pm 1\}$.

In order to fix ideas, we make our counts using Jacobian coordinates (X, Y, Z) associated to a short Weierstrass model $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}$, so that $x = X/Z^2$ and $y = Y/Z^3$. We suppose that the Jacobian coordinates of P lie in $\mathbb{F}$ and that those of Q lie in some extension $\mathbb{F}'$ of $\mathbb{F}$ of whose degree is denoted by k. We denote by $\mathbf{m}_a$ the multiplication by the curve coefficient a and we denote respectively by $\mathbf{m}$ and $\mathbf{s}$ multiplications and squares in $\mathbb{F}$, while the same operations in $\mathbb{F}'$ are denoted respectively by $\mathbf{M}_k$ and $\mathbf{S}_k$ if k is the degree of the extension $\mathbb{F}'$. We assume that $\mathbb{F}'$ is given by a basis as a $\mathbb{F}$-vector space one of whose elements is 1, so that multiplication of an element of $\mathbb{F}'$ by an element of $\mathbb{F}$ counts as k multiplications in $\mathbb{F}$. We ignore additions and multiplications by small integers.

If S is any point of E, then X_S, Y_S and Z_S denote the Jacobian coordinates of S, so that when $S \neq O_E$, the Weierstrass coordinates of S are $x_S = X_S/Z_S^2$ and $y_S = Y_S/Z_S^3$. As before, T is a multiple of P, so that X_T, Y_T and Z_T all lie in $\mathbb{F}$. Since P and Q are part of the input, we assume they are given in Weierstrass coordinates and that $Z_P = Z_Q = 1$.

The following theorem gives the number of operations involved in our variant of Miller's algorithm.

Theorem 9 *Suppose E is given in short Weierstrass form $y^2 = x^3 + ax + b$ with coefficients $a, b \in \mathbb{F}$. Let $P \in E(\mathbb{F})$ be a point of odd order $r \geq 2$ and let Q be a point of E of order r with coordinates in an extension field $\mathbb{F}'$ of $\mathbb{F}$ of degree k. We assume P and Q given in Weierstrass coordinates (x_P, y_P) and (x_Q, y_Q).*

1. *Using the associated Jacobian coordinates, the algorithms of Figures 1.8 and 1.9 can be implemented in such a way that all the denominators $(D\ell)_{T,T}$, $(D\ell)_{T,P}$, $(Dv)_{2T}$, $(Dv)_{T+P}$ and $(D\ell')_{-T,-P}$ belong to $\mathbb{F}$.*
2. *When this is the case:*
   (a) *Each doubling step of the generic usual Miller algorithm takes $\mathbf{m}_a + 8\mathbf{s} + (5 + 5k)\mathbf{m} + 2\mathbf{S}_k + 2\mathbf{M}_k$ operations while in the generic modified Miller algorithm it requires only $\mathbf{m}_a + 7\mathbf{s} + (5 + 3k)\mathbf{m} + 2\mathbf{S}_k + \mathbf{M}_k$ operations.*
   (b) *Each addition step of the generic usual Miller algorithm takes $4\mathbf{s} + (8 + 5k)\mathbf{m} + 2\mathbf{M}_k$ operations. On the other hand, the generic modified Miller algorithm requires only $3\mathbf{s} + (8 + 2k)\mathbf{m} + \mathbf{M}_k$ operations when line **2** is needed and $3\mathbf{s} + (8 + 3k)\mathbf{m} + \mathbf{M}_k$ operations when line **4** is needed.*

1.3.4 Conclusion and Perspectives

Our algorithm is of particular interest to compute the Ate-style pairings (see [BGOS07, HSV06]) on elliptic curves with small embedding degrees k, and in situations where denominator elimination using a twist is not possible (for example on curves with embedding

Algorithm 3: Miller(P, Q, r) modified

Data: $s = \sum_{i=0}^{l-1} s_i 2^i$, $s_i \in \{0, 1\}$, $s_{l-1} = 1$, h Hamming weight of s, $Q \in E(\mathbb{F}')$ not a multiple of P
Result: $f_{s,P}(Q)$;
$f \leftarrow 1$, $T \leftarrow P$
if $l + h$ *is odd* **then**
  $\delta \leftarrow 1$, $g \leftarrow f_{-1}$
end
else
  $\delta \leftarrow 0$, $g \leftarrow 1$
end
for $i = l - 2$ **to** 0 **do**
1 **if** $\delta = 0$ **then**
    $f \leftarrow f^2 (N\ell)_{T,T}$
    $g \leftarrow g^2 (D\ell)_{T,T}$
    $T \leftarrow 2T$, $\delta \leftarrow 1$
2   **if** $s_i = 1$ **then**
      $g \leftarrow g(N\ell')_{-T,-P}$
      $f \leftarrow f(D\ell')_{-T,-P}$
      $T \leftarrow T + P$, $\delta \leftarrow 0$
    end
  end
3 **else**
    $g \leftarrow g^2 (N\ell)_{-T,-T}$
    $f \leftarrow f^2 (D\ell)_{-T,-T}$
    $T \leftarrow 2T$, $\delta \leftarrow 0$
4   **if** $s_i = 1$ **then**
      $f \leftarrow f(N\ell)_{T,P}$
      $g \leftarrow g(D\ell)_{T,P}$
      $T \leftarrow T + P$, $\delta \leftarrow 1$
    end
  end
end
return f/g

Figure 1.9 – Our modified Miller algorithm

degree prime to 6). A typical example is the case of *optimal pairings* [Ver09], which by definition only require about $\log_2(r)/\varphi(k)$ (where r is the group order) iterations of the basic loop. If k is prime, then $\varphi(k \pm 1) \leq \frac{k+1}{2}$ which is roughly $\frac{\varphi(k)}{2} = \frac{k-1}{2}$, so that at least twice as many iterations are necessary if curves with embedding degrees $k \pm 1$ are used instead of curves of embedding degree k. Heß [Hes08] §5, also mentions pairings of potential interest when k is odd and the elliptic curve has discriminant -4 and when k is not divisible by 3 and the elliptic curve has discriminant -3. We can nevertheless adapt our algorithm for even embedding degrees (most implementations are actually adapted to curves with embedding degree $2^i 3^j$ which allows faster basic arithmetic operations), but the improvement obtained in the generic case is lost.

Experiments have been done which show that our variant saves between 10 and 40% in running time in comparison with the usual version of Miller's algorithm. We have made no attempt to minimise the number of operations, for example by using tricky formulae, so there might be room for further improvements also with curves of special families or with efficient arithmetic.

A study of the impact of our algorithm could be interesting in the case of curves of genus 2. In general, the world of genus 2 pairing friendly curves remains obscure, even in terms of construction of interesting such curves.

CHAPTER 2

Functional Cryptography

2.1 Introduction

In this chapter, I will describe some results which concern the design and the security analysis of systems which can be seen as examples of *functional* cryptography.

This paradigm encompasses the classical public-key cryptography, as well as the identity-based cryptography, but mainly offers a natural framework to implement different natural security policies. The recent concept of functional encryption has been formalised in [BSW11], after it was initiated with Sahai and Waters' fuzzy identity-based encryption [SW05]. The classical process of encryption transforms a plain message into a ciphertext intended to a single user. This user, if (and only if) he possesses the secret key can decrypt. If he does not have this secret key, then, he does not learn any useful information on the message : the decryption procedure is essentially all or nothing. This rigidity is often irrelevant in practice: a natural way to protect data consists in defining a security policy to authorise several users to access (part of) this data. In particular, many users may be able to decrypt a ciphertext, and it might also be desirable that users have the rights to decrypt only a part of some encrypted message (like a redacted document for instance). Besides, new users may have to decrypt data that have been encrypted in the past, not necessary for them, and so it must be possible to generate fresh keys for these users, enabling them to decrypt after while.

The concept of functional encryption naturally captures those of identity-based encryption [Sha84, BF03], anonymous identity-based encryption [BCOP04], key-policy or ciphertext-policy attribute based encryption [SW05, GPSW06], hidden vector encryption [BW07] or inner product encryption [KSW08]. It is a crucial and promising tool for the design of secure complex systems, but the complexity of their expected functionalities makes their construction difficult. The schemes are usually inefficient and secure in models that are not the strongest, and they rely on strong algorithmic assumptions.

The results of this chapter are first a theoretical study of the security of identity-based encryption (IBE) in a joint work with Javier Herranz and Carla Ràfols. In the first section 2.2, I will describe some relations between semantic security and anonymity in different security scenarios: we explore how an IBE scheme can reach both security properties according to the strength of the adversary.

The two last sections contain practical constructions of efficient and secure attribute-based cryptographic schemes. Section 2.3 presents an attribute-based encryption scheme (ABE) which is the first one having *constant size ciphertexts* and a reasonable expressivity (*i.e.,* for threshold policies). This is a joint work with Javier Herranz and Carla Ràfols. Sec-

tion 2.4 describes two attribute-based signature schemes also having the property of having constant-size signatures for threshold policies. Both signature schemes inherit the constant size of their signatures from the constant size of the ciphertexts of an encryption scheme: those from the preceding section for the first, and those from the key-policy ABE by Attrapadung, Libert and de Panafieu [ALP11] for the second. This work was done in collaboration with Javier Herranz, Benoît Libert and Carla Ràfols.

The corresponding articles are:
- *Relations between Semantic Security and Anonymity in Identity Based Encryption*. J. Herranz, F. Laguillaumie, C. Ràfols. Information Processing Letters, Volume 111, Issue 10, 453-460 (2011)
- *Constant Size Ciphertexts in Threshold Attribute-Based Encryption*. J. Herranz, F. Laguillaumie, C. Ràfols. Proc. of PKC 2010. Springer LNCS Vol. 6056, 19-34 (2010)
- *Short Attribute-Based Signatures for Threshold Predicates*. J. Herranz, F. Laguillaumie, B. Libert, C. Ràfols. Submitted, a preliminary version is available at `http://hal.archives-ouvertes.fr/hal-00611651/fr/` (2011)

2.1.1 Identity-based Cryptography

Identity based encryption has been a Grail for cryptographers since the concept was introduced in 1984 by Shamir [Sha84]. More than 15 years and the involvement of pairings have been necessary to finally come up with an efficient identity-based encryption scheme thanks to Boneh and Franklin [BF03]. Cocks independently had a less efficient solution using a completely different approach based on quadratic residues [Coc01].

In this setting, the information needed to encrypt a message is the sole identity of the receiver, say ID. This user has therefore to ask a private key generator to extract a secret key $\mathsf{sk}_{\mathsf{ID}}$ from its identity. More formally, the definition of an identity-based encryption scheme is the following:

Definition 2 *Let k be a positive integer and let $\mathcal{ID} = \mathcal{ID}(k)$ be a set of possible identities. An* identity-based encryption (IBE) *scheme Π handling identities in $\mathcal{ID}$ is a tuple of probabilistic polynomial time algorithms $(\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encrypt}, \mathsf{Decrypt})$ defined as follows.*
- *Setup takes a security parameter 1^k as input and produces the system parameters params and a master key msk.*
- *$\mathsf{Extract}$ takes a security parameter 1^k, the system parameters params, the master key msk and an identity $\mathsf{id} \in \mathcal{ID}$ as inputs. It outputs the secret key $\mathsf{sk}_{\mathsf{id}}$ corresponding to the identity id.*
- *$\mathsf{Encrypt}$ takes a security parameter 1^k, the system parameters params, an identity $\mathsf{id} \in \mathcal{ID}$ and a message $m \in \{0,1\}^*$ as inputs and outputs a ciphertext c.*
- *$\mathsf{Decrypt}$ takes a security parameter 1^k, the system parameters params, a secret key $\mathsf{sk}_{\mathsf{id}}$ and a ciphertext c as inputs, and outputs a message m.*

These algorithms have to satisfy the correctness *property: for all $k \in \mathbb{N}$, $\mathsf{id} \in \mathcal{ID}$ and $m \in \{0,1\}^*$,*

$$\Pr\Big[(\mathsf{params}, \mathsf{msk}) \xleftarrow{\$} \mathsf{Setup}(1^k), \mathsf{sk}_{\mathsf{id}} \xleftarrow{\$} \mathsf{Extract}(1^k, \mathsf{params}, \mathsf{msk}, \mathsf{id}),$$
$$c \xleftarrow{\$} \mathsf{Encrypt}(1^k, \mathsf{params}, \mathsf{id}, m) : \mathsf{Decrypt}(1^k, \mathsf{params}, \mathsf{sk}_{\mathsf{id}}, c) = m\Big] = 1\,.$$

The security of identity-based encryption scheme follows the security of traditional public key encryption. The strongest and accepted security notion for encryption is the indistinguishability under chosen message attacks (IND-CCA). It is natural to extend this notion to identity-based encryption scheme. The main difference is that the traditional semantic security concerns a random public key (not chosen by the adversary). In the identity-based scenario, the protocol must remain secure even if the adversary knows the secret key corresponding to certain identities (these secret keys are computed using the secret master key). So one has to take into account that the adversary may gain information from private key extraction queries.

Another important security property is the *anonymity*, which means that a ciphertext does not leak any information on the identity of the recipient. It corresponds to the notion of *key-privacy* for public key encryption [BBDP01]. Halevi gave in [Hal05] a simple sufficient condition for public-key encryption that provides data privacy to reach key-privacy. Essentially, this condition means that a random encryption of a random message is independent of the public key. Abdalla *et al.* extended this condition to identity-based encryption in [A+08].

Such properties can be defined in either a *selective* or an *adaptive* scenario, which differ on the moment where the attacker chooses the identity that is the target of the attack. In the selective scenario, the attacked identity is chosen before all by the attacker (at the beginning of the security game) whereas in the adaptive scenario, this identity is chosen along with the challenge plaintexts, after some private key extraction queries.

Section 2.2 provides a theoretical study of the relations between these selective and adaptive notions, for identity-based encryption schemes enjoying at the same time some security and anonymity properties.

2.1.2 Attribute-based Cryptography

Attribute-based cryptography has emerged in the last years as a promising primitive for digital security. For instance, it provides good solutions to the problem of anonymous access control. In a ciphertext-policy attribute-based encryption scheme, the secret keys of the users depend on their attributes. When encrypting a message, the sender chooses which subset of attributes must be held by a receiver in order to be able to decrypt.

ENCRYPTION. The first paper dealing explicitly with attribute-based encryption (ABE) was [GPSW06]. Two different and complementary notions of ABE were defined there: key-policy ABE, where a ciphertext is associated to a list of attributes, and a secret key is associated to a policy for decryption; and ciphertext-policy ABE, where secret keys are associated to a list of attributes (i.e. credentials of that user) and ciphertexts are associated to policies for decryption. It seems that ciphertext-policy ABE can be more useful for practical applications than key-policy ABE. Another related notion is that of fuzzy identity-based encryption [SW05], which can be seen as a particular case of both key-policy and ciphertext-policy ABE.

A construction of a key-policy ABE scheme was provided in [GPSW06], while the first ciphertext-policy ABE scheme was proposed in [BSW07], but its security was proved in the generic group model. Later, a generic construction to transform a key-policy ABE scheme into a ciphertext-policy ABE scheme was given in [GJPS08], with the drawback that the size of the ciphertexts is $\mathcal{O}(s^3)$, if s is the number of attributes involved in the decryption policy.

The most efficient ciphertext-policy ABE schemes in terms of ciphertext size and expressivity can be found in [Wat11, DHMR10], the size of a ciphertext depending linearly on

the number of attributes involved in the specific policy for that ciphertext. For example, in the case of (t, s)-threshold decryption policies, where there are s involved attributes and a user can decrypt only if he holds t or more attributes, the size of the ciphertexts in one of the schemes in [Wat11] is $s + \mathcal{O}(1)$, whereas the size of the ciphertexts in the scheme in [DHMR10] is $2(s - t) + \mathcal{O}(1)$. Both schemes admit however general policies (general monotonic access structures) and make use of secret sharing techniques. Emura *et al.* suggested a scheme with short ciphertexts [EMN09] but, as in the Cheung-Newport realization [CN07], policies are restricted to a single AND gate.

All the constructions mentioned so far only achieve security under selective attacks, a model in which the attacker specifies the challenge access structure before the setup phase. The first CP-ABE scheme with full security has appeared very recently [LO+10]. The size of the ciphertexts in this scheme is $2s + \mathcal{O}(1)$.

A concept which is more generic than attribute-based encryption is that of predicate encryption [KSW08]: the decryption policy, chosen by the sender of the message, is hidden in the ciphertext, in such a way that even the receiver gets no information on this policy, other than the fact that his attributes satisfy it or not. Because of this additional strong privacy requirement, current proposals for predicate encryption consider quite simple (not very expressive) policies.

SIGNATURES. Attribute-based signatures (ABS) have been introduced more recently than encryption in [MPR08] (see also [SS09, L+10, LK10]). They are related to the notion of (threshold) ring signatures [RST01, BSS02] or mesh signatures [Boy07], but offer much more flexibility and versatility to design secure complex systems, since the signatures are linked not to the users themselves, but to their attributes. As a consequence, these signatures have a wide range of applications, like private access control, anonymous credentials, trust negotiations, distributed access control mechanisms for ad hoc networks or attribute-based messaging (see [MPR08] for detailed descriptions of applications). In terms of security, ABS must first satisfy unforgeability, which guarantees that a signature cannot be computed by a user who does not have the right attributes, even if he colludes with other users by pooling together their secret keys. The other security requirement is the privacy of user's attributes, in the sense that a signature should not leak any information about the actual attributes that have been employed to produce it.

The schemes proposed by Maji, Prabhakaran, Rosulek in [MPR08] support very expressive signing predicates, but their most practical one is only proven secure in the generic group model. The scheme of [OT11] is claimed to be "almost optimally efficient", although its signatures' length grows linearly in the size of the span program (which is greater than the number of involved attributes in the signing predicate). Our result shows that specific families of predicates (e.g., threshold predicates) allow for more compact signatures. Other instantiations in [MPR08] are secure in the standard model, but are substantially less inefficient (*i. e.* signatures consist of a linear number of group elements in the security parameter) as they use Groth-Sahai proofs for relations between the bits of elements in the group. In the standard model, Okamoto and Takashima designed [OT11] a *fully* secure ABS which supports general non-monotone predicates. The scheme is built upon dual pairing vector spaces [OT08] and uses proof techniques from functional encryption [LO+10]. Escala, Herranz and Morillo also proposed in [EHM11] a fully secure ABS in the standard model, with the additional property of revocability, meaning that a third party can extract the identity of a signer in case of dispute (thanks to a secret that can be computed by the master entity). As it turns

out, *none* of the previous schemes achieves constant-size signatures.

In Section 2.4, we propose the first two attribute-based signature schemes with constant size signatures. Their security is proven in the selective-predicate and adaptive-message setting, in the standard model, under chosen message attacks, with respect to some non-interactive (falsifiable) algorithmic assumptions related to bilinear groups. The described schemes are for the case of threshold predicates, but they can be extended to admit some other (more expressive) kinds of monotone predicates.

EXAMPLE OF APPLICATION.

Let us consider for example the case of *anonymous access control*: a system must be accessible only to those who have received the appropriate rights, which are defined by the system administrator. Let us imagine how such a process could be implemented with a standard public key encryption scheme. First, a user A claims that he is actually user A. Second, the system sends to this user a challenge: a ciphertext computed with the public key of A (obtained from a certification authority), for some random plaintext. Third, A decrypts and sends back the plaintext. Fourth, if the plaintext is correct, the system checks if user A must have access to the system, and if so, A is accepted. This solution has some weaknesses, the main one being the lack of anonymity, as user A must reveal his identity to the system. Furthermore, each time the system wants to change its access control policy, it has to update the database containing all the users that have the right to access the system.

A more desirable solution, employing encryption, would be as follows. First, in a (possibly interactive, physical) registration process, every potential user receives a secret key that depends on his age, his job, his company, his expertise, etc., in short, on his *attributes*. Later, the system defines his policy for access control as a (monotonic) family of subsets of attributes: attributes in one of such subsets must be held by a user in order to have the right to access the system; in particular, in an extreme case, this policy can contain a unique subset with the unique attribute 'right to access system X'. When a user tries to access the system, he receives as a challenge a ciphertext computed by the system, on a random message, using the current access policy. If the policy changes, the system administrator just has to take into account the new policy for generating the future challenges. A user is able to decrypt the challenge only if his attributes satisfy the considered policy. In this way, if a user answers such a challenge correctly, he does not leak who he is, only the fact that his attributes satisfy the access control policy.

2.2 Semantic Security and Anonymity in Identity-Based Encryption

Identity-based encryption with semantic security *and* anonymity is not only interesting as a cryptographic primitive, but also because it can be used to design other primitives such as public key encryption with keyword search, as proved in [BCOP04, A+08]. The first anonymous IBE scheme is indeed Boneh and Franklin's [BF03], although that was not explicitly stated, but its main drawback is the fact that security proofs are carried out in the random oracle model. The scheme in [AG09] is also fully (or adaptively) anonymous under the quadratic residuosity assumption (in particular, it does not employ bilinear pairings), but again in the random oracle model. There exist IBE schemes which are semantically secure in the standard model (see for instance those from [BB04a, BB04b, Wat05, Nac07, CS05]),

but achieving anonymity at the same time seems considerably harder. The first identity-based schemes enjoying anonymity in the standard model are those in [BW06] and [Gen06]. The first fully anonymous *hierarchical* identity-based encryption scheme was provided in [LO+10] (from the construction of their inner product encryption supporting delegation). The first one with constant size ciphertext comes from [DIP10] as a modification of the scheme from [LW10]. These schemes are mainly based on bilinear maps. Recently, some constructions of (hierarchical) identity-based encryption schemes in a lattice setting have been proposed [CHKP10, ABB10a, ABB10b], achieving selective or adaptive security in the standard model.

There exist generic conversions from a selectively secure/anonymous IBE scheme to an adaptively secure/anonymous IBE scheme, either in the random oracle model or when the size of the space of identities is small [BB04a]. However, in general there is a separation between the two models. For example, Galindo proved [Gal06] a separation result regarding semantic security: any IBE scheme which has selective semantic security can be transformed into another scheme which also has selective semantic security, but does not even enjoy one-wayness against adaptive attacks. The idea of this transformation is to choose a special identity id^* in the setup phase, and add the secret key for id^* in the public parameters.

Similar separation results can be easily proven for the case of anonymity. However, note that the transformation by Galindo leads to a quite artificial IBE scheme, which in particular is not anonymous against adaptive attacks, because ciphertexts addressed to id^* can be easily told apart from the rest of ciphertexts. This observation motivates this work. We want to investigate the relation between selective and adaptive semantic security (respectively, anonymity) for IBE schemes which are not so artificial, for example because they also enjoy some anonymity (respectively, semantic security) property. It is interesting to note that the existing identity-based encryption schemes in the literature which enjoy both semantic security and anonymity have either both properties proved in the selective setting [BW06, BW07, Duc10, ABB10a] or both properties proved in the adaptive setting [Gen06, CKRS09, DIP10].

We provide both negative and positive results, which are summarised in Table 2.1. On the negative side, we prove that an IBE scheme which is at the same time semantically secure and anonymous in front of selective attacks is not necessarily semantically secure nor anonymous in front of adaptive attacks. Then, we prove that there is a separation between selective anonymity and adaptive anonymity even for IBE schemes which are fully (i.e. adaptively) semantically secure. On the positive side, we prove that the symmetric situation is different: for IBE schemes which are fully (i.e. adaptively) anonymous, the notions of selective and adaptive semantic security are equivalent.

2.2.1 Security of Identity-based Encryption

We recall here the security definition we are interested in. To simplify, We give the definitions and describe our results for chosen-plaintext attacks.

Semantic Security.

Definition 3 (IND-CPA) *Let* $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encrypt}, \mathsf{Decrypt})$ *be an identity-based encryption scheme. Let* $k \in \mathbb{N}$ *and let* $\mathcal{ID} = \mathcal{ID}(k)$ *be a set of identities. Let* $\mathcal{A} = (\mathcal{A}_f, \mathcal{A}_g)$

Anonymity / Indistinguishability	ANO-sID-CPA	ANO-CPA
IND-sID-CPA	$\not\Rightarrow$ IND-CPA (Thm. 10), $\not\Rightarrow$ ANO-CPA (Thm. 11)	$\Rightarrow$ IND-CPA (Thm. 12), $\Rightarrow$ ANO-CPA (trivial)
IND-CPA	$\not\Rightarrow$ ANO-CPA (Thm. 11), $\Rightarrow$ IND-CPA (trivial)	$\Rightarrow$ ANO-CPA (trivial), $\Rightarrow$ IND-CPA (trivial)

Table 2.1 – Taxonomy of the notions of IND-sID-CPA, IND-CPA, ANO-sID-CPA and ANO-CPA for IBE.

$\underline{\mathbf{Exp}^{\text{ind-cpa}}_{\Pi,\mathcal{A}}(k,\mathcal{ID})}$
$(\mathsf{params},\mathsf{msk}) \leftarrow \Pi.\mathsf{Setup}(1^k)$
$(m_0,m_1,\mathsf{id}_{\mathsf{ch}},st) \leftarrow \mathcal{A}_f^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,\mathsf{params})$
$b \xleftarrow{\$} \{0,1\}$
$c \leftarrow \Pi.\mathsf{Encrypt}(1^k,\mathsf{params},\mathsf{id}_{\mathsf{ch}},m_b)$
$b' \leftarrow \mathcal{A}_g^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,c,st)$
Return $(b'=b)$

(a) IND-CPA

$\underline{\mathbf{Exp}^{\text{ind-sid-cpa}}_{\Pi,\mathcal{A}}(k,\mathcal{ID})}$
$(\mathsf{id}_{\mathsf{ch}},st) \leftarrow \mathcal{A}_{init}(1^k,\mathcal{ID})$
$\mathsf{params} \leftarrow \mathsf{IBE.Setup}(1^k)$
$(m_0,m_1,st') \leftarrow \mathcal{A}_f^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,st)$
$b \xleftarrow{\$} \{0,1\}$
$c \leftarrow \Pi.\mathsf{Encrypt}(1^k,\mathsf{params},\mathsf{id}_{\mathsf{ch}},m_b)$
$b' \leftarrow \mathcal{A}_g^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,c,st')$
Return $(b'=b)$

(b) IND-sID-CPA

Figure 2.1 – Random Experiments for Semantic Security

be an adversary that runs in two stages with access to an extraction oracle $\mathcal{O}_{Extract}(\cdot)$. *We consider the random experiments (a) from Figure 2.1.*

During the two stages, $\mathcal{A}_f$ *and* $\mathcal{A}_g$ *run under the restriction that they do not query their extraction oracle on* id_{ch}. *The* advantage *of* $\mathcal{A}$ *is defined as*

$$Adv^{ind\text{-}cpa}_{\Pi,\mathcal{A}}(k,\mathcal{ID}) = \left|\Pr\left[\boldsymbol{Exp}^{ind\text{-}cpa}_{\Pi,\mathcal{A}}(k,\mathcal{ID}) = 1\right] - \frac{1}{2}\right|.$$

The scheme Π *is said to be* indistinguishable under a chosen plaintext attack *if the function* $Adv^{ind\text{-}cpa}_{\Pi,\mathcal{A}}$ *is negligible for any adversary* $\mathcal{A}$ *whose time complexity is polynomial in* k.

The notion of IND-CPA security for identity-based encryption schemes can be weakened, by forcing the adversary to *select* the challenge identity $\mathsf{id}_{\mathsf{ch}} \in \mathcal{ID}$ at the first stage of the previous experiment. In some sense, the adversary commits to the identity he will try to attack in the future.

Definition 4 (IND-sID-CPA) *Let* $\Pi = (Setup, Extract, Encrypt, Decrypt)$ *be an identity-based encryption scheme. Let* $k \in \mathbb{N}$. *Let* $\mathcal{A} = (\mathcal{A}_{init}, \mathcal{A}_f, \mathcal{A}_g)$ *be an adversary that runs in three stages with access to an extraction oracle* $\mathcal{O}_{Extract}(\cdot)$. *We consider the random experiments (b) from Figure 2.1.*

During the two stages, $\mathcal{A}_f$ *and* $\mathcal{A}_g$ *run under the restriction that they do not query their extraction oracle on* id_{ch}. *The* advantage *of* $\mathcal{A}$ *is defined as*

$$Adv^{ind\text{-}sid\text{-}cpa}_{\Pi,\mathcal{A}}(k,\mathcal{ID}) = \left|\Pr\left[\boldsymbol{Exp}^{ind\text{-}sid\text{-}cpa}_{\Pi,\mathcal{A}}(k,\mathcal{ID}) = 1\right] - \frac{1}{2}\right|.$$

The scheme Π *is said to be* indistinguishable under a chosen plaintext attack for selective identity *if the function* $Adv^{ind\text{-}sid\text{-}cpa}_{\Pi,\mathcal{A}}$ *is negligible for any adversary* $\mathcal{A}$ *whose time complexity is polynomial in* k.

In contrast to this weakened *selective* security notion for identity-based encryption, we will sometimes refer to the standard IND-CPA security notion as *full* security.

Anonymity.

Definition 5 (ANO-CPA) *Let* $\Pi = (Setup, Extract, Encrypt, Decrypt)$ *be an identity-based encryption scheme. Let* $k \in \mathbb{N}$ *and let* $\mathcal{ID} = \mathcal{ID}(k)$ *be a set of identities. Let* $\mathcal{D} = (\mathcal{D}_f, \mathcal{D}_g)$ *be an adversary that runs in two stages with access to an extraction oracle* $\mathcal{O}_{Extract}(\cdot)$. *We consider the random experiments (a) from Figure 2.2.*

During the two stages, $\mathcal{D}_f$ *and* $\mathcal{D}_g$ *run under the restriction that they do not query their extraction oracle on* id_0, id_1. *The* advantage *of* $\mathcal{D}$ *is defined as*

$$Adv^{ano\text{-}cpa}_{\Pi,\mathcal{D}}(k,\mathcal{ID}) = \left|\Pr\left[\boldsymbol{Exp}^{ano\text{-}cpa}_{\Pi,\mathcal{D}}(k,\mathcal{ID}) = 1\right] - \frac{1}{2}\right|.$$

The scheme Π *is said to be* anonymous under a chosen plaintext attack *if the function* $Adv^{ano\text{-}cpa}_{\Pi,\mathcal{D}}$ *is negligible for any adversary* $\mathcal{D}$ *whose time complexity is polynomial in* k.

Again, this notion of adaptive (or full) anonymity, ANO-CPA, can be weakened if the adversary is forced to select the two challenge identities at the first stage of the attack. The resulting notion of *selective anonymity* is formally defined as follows.

$\underline{\mathbf{Exp}^{\text{ano-cpa}}_{\Pi,\mathcal{D}}(k,\mathcal{ID})}$
$(\mathsf{params},\mathsf{msk}) \leftarrow \Pi.\mathsf{Setup}(1^k)$
$(m,\mathsf{id}_0,\mathsf{id}_1,st) \leftarrow \mathcal{D}_f^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,\mathsf{params})$
$\tilde{b} \xleftarrow{\$} \{0,1\}$
$c \leftarrow \Pi.\mathsf{Encrypt}(1^k,\mathsf{params},\mathsf{id}_{\tilde{b}},m)$
$\tilde{b}' \leftarrow \mathcal{D}_g^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,c,st)$
Return $(\tilde{b}' = \tilde{b})$

(a) ANO-CPA

$\underline{\mathbf{Exp}^{\text{ano-sid-cpa}}_{\Pi,\mathcal{D}}(k,\mathcal{ID})}$
$(\mathsf{id}_0,\mathsf{id}_1,st) \leftarrow \mathcal{D}_{init}(1^k,\mathcal{ID})$
$\mathsf{params} \leftarrow \mathsf{IBE.Setup}(1^k)$
$(m,st') \leftarrow \mathcal{D}_f^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,st)$
$\tilde{b} \xleftarrow{\$} \{0,1\}$
$c \leftarrow \Pi.\mathsf{Encrypt}(1^k,\mathsf{params},\mathsf{id}_{\tilde{b}},m)$
$\tilde{b}' \leftarrow \mathcal{D}_g^{\mathcal{O}_{\mathsf{Extract}}(\cdot)}(1^k,c,st')$
Return $(\tilde{b}' = \tilde{b})$

(b) ANO-sID-CPA

Figure 2.2 – Random Experiments for Anonymity

Definition 6 (ANO-sID-CPA) *Let $\Pi = (Setup, Extract, Encrypt, Decrypt)$ be an identity-based encryption scheme. Let $k \in \mathbb{N}$. Let $\mathcal{D} = (\mathcal{D}_{init}, \mathcal{D}_f, \mathcal{D}_g)$ be an adversary that runs in three stages with access to an extraction oracle $\mathcal{O}_{Extract}(\cdot)$. We consider the random experiments (b) from Figure 2.2.*

During the two last stages, $\mathcal{D}_f$ and $\mathcal{D}_g$ run under the restriction that they do not query their extraction oracle on id_0, id_1. The advantage *of $\mathcal{D}$ is defined as*

$$Adv^{ano\text{-}sid\text{-}cpa}_{\Pi,\mathcal{D}}(k,\mathcal{ID}) = \left|\Pr\left[\boldsymbol{Exp}^{ano\text{-}sid\text{-}cpa}_{\Pi,\mathcal{D}}(k,\mathcal{ID}) = 1\right] - \frac{1}{2}\right|.$$

The scheme Π is said to be anonymous under a selective identity chosen plaintext attack *if the function $Adv^{ano\text{-}sid\text{-}cpa}_{\Pi,\mathcal{D}}$ is negligible for any adversary $\mathcal{D}$ whose time complexity is polynomial in k.*

We assume that the size of $\mathcal{ID}$ (the set of possible identities) is at least exponential in k because otherwise adaptive and selective scenario are actually equivalent.

2.2.2 Relations among IND-sID-CPA, IND-CPA, ANO-sID-CPA and ANO-CPA

Again, we describe our results in the scenario of chosen-plaintext attackers who cannot make decryption queries for ciphertexts of their choice, but our results extend directly to a chosen-ciphertext attack scenario. The same results are also valid for hierarchical identity-based encryption, as well.

Negative Results

The first of the following results state that an IBE scheme which is at the same time semantically secure and anonymous against selective attacks is not necessarily semantically secure nor anonymous against adaptive attacks. The other one proves that there is a separation between selective and adaptive anonymity even for schemes which enjoy adaptive semantic security.

Theorem 10 ([HLR11], Theorem 1) *There exist identity-based encryption schemes that are secure under* IND-sID-CPA *and* ANO-sID-CPA *attacks, but are not secure under* IND-CPA *attacks.*

Theorem 11 ([HLR11], Theorem 2) *There exist identity-based encryption schemes that are secure under* IND-CPA *and* ANO-sID-CPA *attacks, but are not secure under* ANO-CPA *attacks.*

To prove the theorem, the idea is to explicitly exhibit the scheme that is claimed to exist. The constructions are ad-hoc and serve only to state these separations. For instance, the scheme of Theorem 10 is built from a scheme Π secure in the sense IND-sID-CPA and ANO-sID-CPA as follows: a specific identity $\mathsf{id}^\star$ is added to the global parameters, and the encryption of a message is regularly done with Π.Encrypt for any identity different from $\mathsf{id}^\star$, and the bit 0 is concatenated to the ciphertext. For the identity $\mathsf{id}^\star$, the encryption consists in given the plaintext concatenated to the bit 1. This new scheme essentially inherits the security of Π, but is clearly not IND-CPA.

Theorem 11 gives a stronger result, since even if we strengthen the semantic security, a scheme does not necessary benefit from a stronger anonymity. The construction is quite similar to the previous one: the idea is still to distinguish an encryption to a specific identity $\mathsf{id}^\star$ from an encryption to any other. An attacker in the stronger model will choose this identity for its attack.

Positive Results

Eventually, we prove, in a game-based proof, that if we strengthen the anonymity notion, from ANO-sID-CPA to ANO-CPA, then the weaker (selective) indistinguishability notion of IND-sID-CPA becomes equivalent to the adaptive notion of IND-CPA.

Theorem 12 ([HLR11], Theorem 3) *Let k be an integer and let $\mathcal{ID} = \mathcal{ID}(k)$ be a set of possible identities. For any IND-CPA adversary $\mathcal{A}$ against an identity based encryption scheme Π, there exists an IND-sID-CPA adversary $\mathcal{A}'$ and an ANO-CPA adversary $\mathcal{D}$ such that*

$$Adv^{ind\text{-}cpa}_{\Pi,\mathcal{A}}(k,\mathcal{ID}) \leq \frac{q_E+1}{\#\mathcal{ID}} + 2\cdot Adv^{ano\text{-}cpa}_{\Pi,\mathcal{D}}(k,\mathcal{ID}) + Adv^{ind\text{-}sid\text{-}cpa}_{\Pi,\mathcal{A}'}(k,\mathcal{ID})$$

where q_E denotes $\mathcal{A}$'s number of queries to its extraction oracle, and $\#\mathcal{ID}$ is the cardinality of the set $\mathcal{ID}$.

2.2.3 Conclusion and Perspectives

We provide a theoretical study of the relations between selective and adaptive security properties for identity-based encryption schemes which enjoy at the same time some level of anonymity and semantic security.

The security analysis of the anonymous identity-based encryption schemes that exist in the literature seem to suggest that proving adaptive anonymity is as hard as proving adaptive semantic security. Indeed, either semantic security and anonymity are both proved in the selective model [BW06, BW07, SKOS09, Duc10, ABB10a] or they are both proved in the adaptive model [Gen06, CKRS09, DIP10]. This probably responds to the fact that similar

challenges appear when proving full anonymity and full semantic security, namely the problem that the partition strategy (which is really useful in the selective case) is much harder to apply in the adaptive case.

Our study suggests that another approach to proving that a scheme is fully anonymous and fully secure is possible. Once adaptive anonymity is proved for a scheme, then semantic security can be proved in a selective scenario. We believe that these theoretical relations may have an impact in the design or in the analysis of anonymous (hierarchical) identity-based encryption schemes.

Our positive result may be useful to simplify the proofs of some existing (H)IBE schemes that are adaptively secure. For instance, it is interesting to study whether it can help to get a simpler proof or scheme in the case of [DIP10]. Therein, De Caro *et al.* use the dual system encryption technique of Waters to obtain a fully secure and fully anonymous HIBE. Using our approach, if one could argue independently that the scheme is IND-sID-CPA secure, full anonymity would imply full security. Potentially this could result in a scheme based on less computational assumptions, although arguably this would depend on the hypothesis needed to prove selective security.

The same argument could be applied if, for instance, the HIBE scheme of Boyen-Waters [BW06], which is only selectively anonymous and selectively semantically secure, could be proven anonymous against an adaptive adversary, for example using the new dual encryption techniques of Waters [Wat09].

2.3 Constant Size Ciphertexts in Attribute-Based Encryption

We propose in this section, the first collusion-resistant ABE scheme which produces constant size ciphertexts and which admits reasonably expressive decryption policies. Our scheme is inspired by the dynamic threshold (identity-based) encryption scheme from [DP08], in which the ciphertext's size was constant as well. As we have just said, this scheme directly leads to a weak ABE scheme, without the collusion resistance property. The challenge was to modify this scheme in order to achieve collusion resistance without losing the other security and efficiency properties, in particular that of constant size ciphertexts. The resulting scheme works for threshold policies: the sender chooses ad-hoc a set S of attributes and a threshold t, and only users who hold at least t of the attributes in S can decrypt. An extension is possible in order to support also weighted threshold policies.

Our new scheme achieves security against selective chosen plaintext attacks (sCPA), in the standard model, under the assumption that the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) problem is hard to solve. This is essentially the same level of security that was proved for the scheme in [DP08].

2.3.1 Definitions

We capture the notions of ciphertext-policy attribute-based encryption by providing definition and security notion for *functional encryption* with public index ([BSW11]).

SYNTAX. Let $R : \Sigma_K \times \Sigma_E \to \{0,1\}$ be a Boolean function where Σ_K and Σ_E denote "key index" and "ciphertext index" spaces. A functional encryption (FE) scheme for the relation R consists of algorithms:

$\mathsf{Setup}(k, \mathrm{des}) \to (\mathsf{mpk}, \mathsf{msk})$**:** The setup algorithm takes as input a security parameter k and a scheme description des and outputs a master public key mpk and a master secret key msk.

$\mathsf{KeyGen}(\mathsf{msk}, X) \to \mathsf{sk}_X$**:** The key generation algorithm takes the master secret key msk and a key index $X \in \Sigma_K$ as inputs. It outputs a private key sk_X.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, Y) \to C$**:** This algorithm takes as input a public key mpk, the message M, and a ciphertext index $Y \in \Sigma_E$. It outputs a ciphertext C.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_X, X, C, Y) \to \mathsf{M}$ or $\perp$**:** The decryption algorithm takes the public parameters mpk, a private key sk_X for the key index X and a ciphertext C for the ciphertext index Y as inputs. It outputs the message M or a symbol $\perp$ indicating that the ciphertext is not in a valid form.

Correctness mandates that, for all k, all $(\mathsf{mpk}, \mathsf{msk})$ produced by $\mathsf{Setup}(k, \mathrm{des})$, all $X \in \Sigma_K$, all keys sk_X returned by $\mathsf{KeyGen}(\mathsf{msk}, X)$ and all $Y \in \Sigma_E$,

- If $R(X, Y) = 1$, then $\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_X, X, \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, Y), Y) = \mathsf{M}$.
- If $R(X, Y) = 0$, then $\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_X, X, \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}, Y), Y) = \perp$.

SECURITY NOTION. We now give the standard security definition for functional encryption schemes. Constructions satisfying this security property are sometimes called *payload hiding* in the literature.

A stronger property, called *attribute-hiding*, guarantees that ciphertexts additionally hide their underlying attributes Y and it will not be considered here. To date, this property has only been obtained (e.g., [KSW08]) for access policies that are less expressive than those considered here. We henceforth consider FE systems with public index (according to the terminology of [BSW11]), where ciphertext attributes Y are public.

Definition 7 *A FE scheme for relation R is fully secure (or payload-hiding) if no probabilistic polynomial time (PPT) adversary $\mathcal{A}$ has non-negligible advantage in this game:*

Setup. *The challenger runs $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(k, \mathrm{des})$ and gives mpk to $\mathcal{A}$.*

Phase 1. *On polynomially-many occasions, the adversary $\mathcal{A}$ chooses a key index X and obtains a private key $\mathsf{sk}_X = \mathsf{Keygen}(\mathsf{msk}, X)$. Such queries can be adaptive in that each one may depend on the information gathered so far.*

Challenge. *$\mathcal{A}$ chooses messages $\mathsf{M}_0, \mathsf{M}_1$ and a ciphertext index $Y^\star$ such that $R(X, Y^\star) = 0$ for all key indexes X that have been queried at step 2. Then, the challenger flips a fair binary coin $b \in \{0, 1\}$, generates a ciphertext $C^\star = \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{M}_b, Y^\star)$, and hands it to the adversary.*

Phase 2. *$\mathcal{A}$ is allowed to make more key generation queries for any key index X such that $R(X, Y^\star) = 0$.*

Guess. *$\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$ and wins if $b' = b$.*

The advantage of the adversary $\mathcal{A}$ is measured by $\mathbf{Adv}(k) := |\Pr[b' = b] - \frac{1}{2}|$ where the probability is taken over all coin tosses.

A weaker notion of selective security can also be defined as in the above game with the exception that the adversary $\mathcal{A}$ has to choose the challenge ciphertext index $Y^\star$ before the setup phase but private key queries $X_1, \ldots, X_q$ can still be adaptive. A dual notion called co-selective security [AL10], in contrast, requires $\mathcal{A}$ to declare q key queries for key indexes

$X_1, \ldots, X_q$ before the setup phase, but $\mathcal{A}$ can adaptively choose the target challenge ciphertext index $Y^\star$.

CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION. In a ciphertext-policy attribute-based encryption scheme, ciphertexts are associated with access structures over the subsets of at most n attributes of the space of attributes, for some specified $n \in \mathbb{N}$. Decryption works only if the attribute set ω associated to a certain secret key is authorised in the access structure $\mathbb{A}$ (*i.e.*, $\omega \in \mathbb{A}$). We formally define it as an instance of FE as follows.

Definition 8 (CP-ABE) *Let U be an attribute space. Given some $n \in \mathbb{N}$, let $\mathcal{AS}$ be any collection of access structures over U such that for any $\mathbb{A} \in \mathcal{AS}$, there exists some subset $B \subset U$ with $|B| \leq n$ and such that every minimal set ω of $\mathbb{A}$ satisfies that $\omega \subset B$. A ciphertext-policy attribute-based encryption (CP-ABE) for the collection $\mathcal{AS}$ is a functional encryption for $R^{\mathsf{CP}} : 2^U \times \mathcal{AS} \to \{0,1\}$ defined by $R^{\mathsf{CP}}(\omega, \mathbb{A}) = 1$ iff $\omega \in \mathbb{A}$ (for any $\omega \subseteq U$ and $\mathbb{A} \in \mathcal{AS}$). Furthermore, the description* des *consists of the attribute universe U and the bound n, whereas $\Sigma_K^{\mathsf{CP}} = 2^U$ and $\Sigma_E^{\mathsf{CP}} = \mathcal{AS}$.*

Our construction is only for threshold access structures, i.e. when each access structure $\mathbb{A}$ in the collection $\mathcal{AS}$ is of the threshold type, and admits also some weighted threshold access structures, as we discuss in subsection 2.3.4. We describe our new scheme in the next paragraph.

2.3.2 Description of The Scheme

Let us describe hereafter our ciphertext-policy attribute-based encryption scheme, which supports threshold decryption policies.

In the decryption process, we will use the algorithm Aggregate of [DPP07, DP08]. Given a list of values $\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq n}$, where $r, \gamma \in (\mathbb{Z}/p\mathbb{Z})^\star$ are unknown and $x_i \neq x_j$ if $i \neq j$, the algorithm computes the value

$$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma+x_i}}, x_i\}_{1\leq i\leq n}) = g^{\frac{r}{\prod_{i=1}^{n}(\gamma+x_i)}}.$$

using $O(n^2)$ exponentiations.

Although the algorithm Aggregate of [DPP07, DP08] is given for elements in $\mathbb{G}_T$, it is immediate to see that it works in any group of prime order. Running Aggregate for elements in $\mathbb{G}$ results in our case in a more efficient decryption algorithm.

Concretely, the algorithm proceeds by defining $\Lambda_{0,\eta} = g^{r/(\gamma+x_\eta)}$ for each $\eta \in \{1, \ldots, n\}$ and observing that, if we define

$$\Lambda_{j,\eta} = g^{\frac{r}{(\gamma+x_\eta)\cdot\prod_{i=1}^{j}(\gamma+x_i)}} \qquad \text{with} \quad 1 \leq j < \eta \leq n,$$

these values satisfy the recursion formula

$$\Lambda_{j,\eta} = \Big(\frac{\Lambda_{j-1,j}}{\Lambda_{j-1,\eta}}\Big)^{1/(x_\eta - x_j)}. \tag{2.1}$$

Therefore, as long as elements $x_1, \ldots, x_n$ are pairwise distinct, (2.1) allows sequentially computing $\Lambda_{j,\eta}$ for $j = 1$ to $n-1$ and $\eta = j+1$ to n in order to finally obtain $\Lambda_{n-1,n} = g^{\frac{r}{\prod_{i=1}^{n}(\gamma+x_i)}}$.

DESCRIPTION.

– $\mathsf{Setup}(k, U, n)$: the trusted setup algorithm chooses a suitable encoding $\tau : U \to (\mathbb{Z}/p\mathbb{Z})^\star$ sending each of the m attributes $\mathsf{at} \in U$ onto a (different) element $\tau(\mathsf{at}) \in (\mathbb{Z}/p\mathbb{Z})^\star$. It also chooses groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^k$ with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and generators $g, h \xleftarrow{\$} \mathbb{G}$. Then, it chooses a set $\mathcal{D} = \{d_1, \ldots, d_{n-1}\}$ consisting of $n-1$ pairwise different elements of $(\mathbb{Z}/p\mathbb{Z})^\star$, which must also be different to the values $x = \tau(\mathsf{at})$, for all $\mathsf{at} \in U$. For any integer i lower or equal to $n-1$, we denote as $\mathcal{D}_i$ the set $\{d_1, \ldots, d_i\}$. Next, the algorithm picks at random $\alpha, \gamma \in (\mathbb{Z}/p\mathbb{Z})^\star$ and sets $u = g^{\alpha\gamma}$ and $v = e(g^\alpha, h)$. The master secret key is then $\mathsf{msk} = (g, \alpha, \gamma)$ and the public parameters are

$$\mathsf{params} = \left(U, n, u, v, \left\{h^{\alpha\gamma^i}\right\}_{i=0,\ldots,2n-1}, \mathcal{D}, \tau\right).$$

– $\mathsf{Keygen}(\mathsf{msk}, \omega)$: to generate a key for the attribute set $\omega \subset U$, pick $r, z \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}^*$ and compute the private key

$$\mathsf{sk}_\omega = \left(\left\{g^{\frac{r}{\gamma+\tau(\mathsf{at})}}\right\}_{\mathsf{at}\in\omega}, \left\{h^{r\gamma^i}\right\}_{i=0,\ldots,n-2}, h^{\frac{r-z}{\gamma}}, z\right).$$

– $\mathsf{Encrypt}(\mathsf{params}, S, t, \mathsf{M})$: given a subset $S \subset U$ with $s = |S|$ attributes, $s \leq n$, a threshold t satisfying $1 \leq t \leq s$, and a message $\mathsf{M} \in \mathbb{G}_T$, the sender picks at random $\kappa \in (\mathbb{Z}/p\mathbb{Z})^\star$ and computes

$$\begin{cases} C_1 &= u^{-\kappa}, \\ C_2 &= h^{\kappa\cdot\alpha^{\cdot\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))}\prod_{d\in\mathcal{D}_{n+t-1-s}}(\gamma+d)}, \\ K &= v^\kappa = e(g^\alpha, h)^\kappa. \end{cases}$$

The value C_2 is computed from the set $\{h^{\alpha\gamma^i}\}_{i=0,\ldots,2n-1}$ that can be found in the public parameters. The ciphertext is then $C = (C_1, C_2, C_3)$, where $C_3 = K \cdot \mathsf{M}$.

– $\mathsf{Decrypt}(\mathsf{params}, \mathsf{sk}_\omega, \omega, C, (S, t))$: given $C = (C_1, C_2, C_3) \in \mathbb{G}^2 \times \mathbb{G}_T$, any user with a set of attributes ω such that $|\omega \cap S| \geq t$ can use the secret key sk_ω to decrypt the ciphertext, as follows. Let ω_S be any subset of $\omega \cap S$ with $|\omega_S| = t$. The user computes, from all $\mathsf{at} \in \omega_S$, the value

$$\mathsf{Aggregate}(\{g^{\frac{r}{\gamma+\tau(\mathsf{at})}}, \tau(\mathsf{at})\}_{\mathsf{at}\in\omega_S}) = g^{\frac{r}{\prod_{\mathsf{at}\in\omega_S}(\gamma+\tau(\mathsf{at}))}}.$$

With the output of the algorithm $\mathsf{Aggregate}$, the decryption algorithm also computes

$$\chi = e(g^{\frac{r}{\prod_{\mathsf{at}\in\omega_S}(\gamma+\tau(\mathsf{at}))}}, C_2) = e(g,h)^{\kappa\cdot\alpha\cdot r\cdot\prod_{\mathsf{at}\in S\setminus\omega_S}(\gamma+\tau(\mathsf{at}))\prod_{d\in\mathcal{D}_{n+t-1-s}}(\gamma+d)}.$$

For simplicity, let $\tau(d) = d$ for all $d \in \mathcal{D}$ and define $P_{(\omega_S,S)}(\gamma)$ as

$$P_{(\omega_S,S)}(\gamma) = \frac{1}{\gamma}\left(\prod_{y\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\omega_S}(\gamma+\tau(y)) - \prod_{y\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\omega_S}\tau(y)\right).$$

The crucial point is that, since $|\omega_S| \geq t$, the degree of the polynomial $P_{(\omega_S,S)}(X)$ is lower or equal to $n-2$. Therefore, from the values included in sk_ω, the user can compute $h^{rP_{(\omega_S,S)}(\gamma)}$.

After that, the user calculates

$$e(C_1, h^{rP_{(\omega_S,S)}(\gamma)}) \cdot \chi = e(g,h)^{\kappa\cdot\alpha\cdot r\cdot\prod_{y\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\omega_S}\tau(y)} \tag{2.2}$$

and

$$e(C_1, h^{\frac{r-z}{\gamma}}) = e(g,h)^{-\kappa\cdot\alpha\cdot r}\cdot e(g,h)^{\kappa\cdot\alpha\cdot z} \tag{2.3}$$

From Equation (2.2), the decryption algorithm obtains

$$e(g,h)^{\kappa\cdot\alpha\cdot r} = \Big(e(C_1, h^{rP_{(\omega_S,S)}(\gamma)})\cdot\chi\Big)^{1/\prod_{y\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\omega_S}\tau(y)}$$

and multiplies this value in Equation (2.3). The result of this multiplication leads to $e(g,h)^{\kappa\cdot\alpha\cdot z}$. This value is raised to z^{-1} to obtain $K = e(g,h)^{\kappa\cdot\alpha}$. Finally, the plaintext is recovered by computing $\mathsf{M} = C_3/K$.

2.3.3 Security Result

Our new scheme achieves security against selective chosen plaintext attacks, in the standard model. This security relies on the hardness of a problem that we call the *augmented multi-sequence of exponents decisional Diffie-Hellman problem* - aMSE-DDH (see [HLR10]), which is a slight modification of the multi-sequence of exponents decisional Diffie-Hellman problem considered in [DP08]. The generic complexity of these two problems is covered by the analysis in [BBG05], because the problems fit their general Diffie-Hellman exponent problem framework. Using well-known techniques, it is possible to obtain security against chosen ciphertext attacks (CCA), in the random oracle model.

Theorem 13 ([HLR10], Theorem 1) *Let k be an integer. For any adversary $\mathcal{A}$ against the selective security of our CP-ABE scheme, for a universe U of m attributes and maximal size $n \geq |\tilde{S}|$ for any decryption policy $(\tilde{S},\tilde{t})$, there exists a solver $\mathcal{B}$ of the $(\tilde{\ell},\tilde{m},\tilde{t})$-aMSE-DDH problem such that*

$$\mathbf{Adv}_{\mathcal{B}}^{aMSE\text{-}DDH}(k) \;\geq\; \frac{1}{n^2}\cdot\mathbf{Adv}_{\mathcal{A}}^{ABE\text{-}sCPA}(k).$$

2.3.4 Further Improvements and Perspectives

MORE GENERAL POLICIES. Our scheme can support another family of access structures, namely the *weighted threshold* ones. A family $\mathbb{A}\subset 2^U$ is a weighted threshold access structure if there exist a threshold t and an assignment of weights $\mathrm{wt}: U\to\mathbb{Z}^+$ such that $\omega\in\mathbb{A}\iff\sum_{\mathsf{at}\in\omega}\mathrm{wt}(\mathsf{at})\geq t$. Of course, there are many access structures which are not weighted threshold, for example $\mathbb{A}=\{\{\mathsf{at}_1,\mathsf{at}_2\},\{\mathsf{at}_2,\mathsf{at}_3\},\{\mathsf{at}_3,\mathsf{at}_4\}\}$ in the set $U=\{\mathsf{at}_1,\mathsf{at}_2,\mathsf{at}_3,\mathsf{at}_4\}$. The same extension proposed in [DP08] works for our threshold ABE scheme. Let K be an upper bound for $\mathrm{wt}(\mathsf{at})$, for all $\mathsf{at}\in U$ and for all possible assignments of weights that realise weighted threshold decryption policies. During the setup of the ABE scheme, the new universe of attributes will be $U'=\{\mathsf{at}_1||1,\mathsf{at}_1||2,\ldots,\mathsf{at}_1||K,\ldots,\mathsf{at}_m||1,\ldots,\mathsf{at}_m||K\}$. During the secret key request phase, if an attribute at belongs to the requested subset $\omega\subset U$, the secret key sk_ω will contain the elements $g^{\frac{r}{\gamma+\tau(\mathsf{at}^{(j)})}}$ corresponding to $\mathsf{at}^{(j)}=\mathsf{at}||j$, for all $j=1,\ldots,K$.

Later, suppose a sender wants to encrypt a message for a weighted threshold decryption policy $\mathbb{A}$, defined on a subset of attributes $S=\{\mathsf{at}_1,\ldots,\mathsf{at}_s\}$ (without loss of generality). Let

t and $\mathrm{wt} : S \to \mathbb{Z}^+$ be the threshold and assignment of weights that realise $\mathbb{A}$. The sender can use the threshold ABE encryption routine described previously, with threshold t, but applied to the set of attributes $S' = \{\mathsf{at}_1||1, \ldots, \mathsf{at}_1||\mathrm{wt}(\mathsf{at}_1), \ldots, \mathsf{at}_s||1, \ldots, \mathsf{at}_s||\mathrm{wt}(\mathsf{at}_s)\}$. In this way, if a user holds a subset of attributes $\omega \in \mathbb{A}$, he will have $\mathrm{wt}(\mathsf{at})$ valid elements in his secret key, for each attribute $\mathsf{at} \in \omega$. In total, he will have $\sum_{\mathsf{at}\in\omega} \mathrm{wt}(\mathsf{at}) \geq t$ valid elements, so he will be able to run the decryption routine of the threshold ABE scheme and decrypt the ciphertext.

DELEGATIONS OF KEYS. Our attribute-based encryption scheme admits delegation of secret keys: from a valid secret key $\mathsf{sk}_\omega = \left(\left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in\omega}, \left\{ h^{r\gamma^i} \right\}_{i=0,\ldots,n-2}, h^{\frac{r-z}{\gamma}}, z \right)$ it is possible to compute a valid secret key $\mathsf{sk}_{\omega'}$ for any subset $\omega' \subset \omega$, as follows: take $\rho \in (\mathbb{Z}/p\mathbb{Z})^\star$ at random and compute

$$\mathsf{sk}_{\omega'} = \left(\left\{ \left(g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right)^\rho \right\}_{\mathsf{at}\in\omega'}, \left\{ \left(h^{r\gamma^i} \right)^\rho \right\}_{i=0,\ldots,n-2}, \left(h^{\frac{r-z}{\gamma}} \right)^\rho, z \cdot \rho \right).$$

Our ABE scheme can be therefore viewed as a hierarchical ABE scheme with the natural hierarchy: a user holding attributes ω is over a user holding attributes ω', if $\omega' \subset \omega$. Then, the techniques developed in [CHK04] can be applied to transform our hierarchical ABE scheme, which enjoys selective security under chosen plaintext attacks, into an ABE scheme which enjoys selective security under chosen ciphertext attacks, in the standard model. The price to pay is an increase in the size of the secret keys sk_ω, that must contain $2l$ additional elements, where l is the bit-length of the verification keys of a (one-time) signature scheme that is used in the transformation. The size of the ciphertexts remains constant.

OPEN PROBLEMS. Many directions can be investigated concerning attribute-based encryption, and more generally functional encryption, with as target the triptych efficiency/expressivity/security. It would be interesting to maintain the short size of the ciphertexts while the decryption policy describes attribute set satisfying more complex Boolean formulae specified by an access structure. Very expressive ABE schemes with constant-size ciphertexts and full security are still missing. Even though this might be achieved at the expense of more complex underlying algorithmic assumptions, the simplification of these assumptions is an interesting and important problem regarding both security and efficiency. The fact that the security relies on an ad-hoc problem like the augmented multi-sequence of exponents decisional Diffie-Hellman problem is not satisfactory. Providing weaker assumptions for the security is an interesting issue. A possible way to answer this question is to design lattice-based attribute-based schemes: some attempts have been done in [A+11, AFV11], which are good starting points, but they need many improvements to become practical.

2.4 Short Attribute-Based Signatures for Threshold Predicates

We describe the first two threshold ABS schemes featuring constant-size signatures and with security in the selective-predicate setting (*i.e.,* as opposed to the *full* security setting) in the standard model. The new schemes are built (non-generically) on two different constant-size attribute-based encryption schemes. In both schemes, n denotes the maximum size of the admitted signing predicates.

– Our first scheme supports (weighted) threshold predicates for small [1] universes of attributes. Its design relies on the constant-size ciphertext-policy ABE scheme from Section 2.3, in the sense that the signer implicitly proves his ability to decrypt a ciphertext by using the Groth-Sahai proof systems [GS08], and by binding the signed message (and the corresponding predicate) to the signature using a technique suggested by Malkin, Teranishi, Vahlis and Yung [MTVY11]. The signature consists of 15 group elements, and the secret key of a user holding a set Ω of attributes has $|\Omega| + n$ elements. Our scheme is selective-predicate and adaptive-message unforgeable under chosen message attacks if the augmented multi-sequence of exponents computational Diffie-Hellman assumption [HLR10] and the Decision Linear assumption [BBS04] hold. The privacy of the attributes used to sign is proved in the computational sense under the Decision Linear assumption [BBS04].

– The second scheme supports threshold predicates (as well as compartmented and hierarchical predicates) for *large* universes of attributes, which can be obtained by hashing arbitrary strings. It is built upon a key-policy ABE scheme proposed by Attrapadung, Libert and de Panafieu [ALP11] and has signatures consisting of *only* 3 group elements. The secret keys are longer than in the first scheme, as they include $(2n + 2) \times (|\Omega| + n)$ group elements. On the other hand, its selective-predicate and adaptive-message unforgeability relies on the more classical n-Diffie-Hellman exponent assumption. Moreover, the scheme protects the privacy of the involved attributes unconditionally.

2.4.1 Background and Definitions

NOTATIONS. We will treat a vector as a column vector. For any $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n)^\top \in \mathbb{Z}/p\mathbb{Z}^n$, and any element g of a group $\mathbb{G}$, $g^{\overrightarrow{\alpha}}$ stands for $(g^{\alpha_1}, \ldots, g^{\alpha_n})^\top \in \mathbb{G}^n$. The inner product of $\overrightarrow{a}, \overrightarrow{z} \in \mathbb{Z}/p\mathbb{Z}^n$ is denoted as $\langle \overrightarrow{a}, \overrightarrow{z} \rangle = \overrightarrow{a}^\top \overrightarrow{z}$. Given $g^{\overrightarrow{a}}$ and $\overrightarrow{z}$, $(g^{\overrightarrow{a}})^{\overrightarrow{z}} := g^{\langle \overrightarrow{a}, \overrightarrow{z} \rangle}$ is computable without knowing $\overrightarrow{a}$. For equal-dimension vectors $\overrightarrow{A}$ and $\overrightarrow{B}$ of exponents or group elements, $\overrightarrow{A} \cdot \overrightarrow{B}$ stands for their component-wise product. We denote by I_n the identity matrix of size n. For any set U, we define $2^U = \{S \mid S \subseteq U\}$. Given a set $S \subset \mathbb{Z}/p\mathbb{Z}$, and some $i \in S$, the i-th Lagrange basis polynomial is $\Delta_i^S(X) = \prod_{j \in S \setminus \{i\}} (X - j)/(i - j)$.

SETTING. Our two schemes work in the setting of bilinear groups. That is, we use a pair of multiplicative groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order p with an efficiently computable and non-degenerate pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

The security of our first scheme is partially based on the hardness of the computational version of the problem previously mentioned in Section 2.3.3 under the name of *augmented multi-sequence of exponents decisional Diffie-Hellman problem* (see [HLR10] for its precise definition). The security analysis of our first scheme also appeals to the (now classical) *Decision Linear assumption*, described below.

Definition 9 (DLIN – [BBS04]) *In a group $\mathbb{G}$ of order p, the* Decision Linear Problem *(DLIN) is to distinguish the distributions $(g, g^a, g^b, g^{a \cdot \delta_1}, g^{b \cdot \delta_2}, g^{\delta_1 + \delta_2})$ and $(g, g^a, g^b, g^{a \cdot \delta_1}, g^{b \cdot \delta_2}, g^{\delta_3})$, with $a, b, \delta_1, \delta_2, \delta_3 \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$.*

1. *i.e.* polynomial in the security parameter, which is sufficient for many applications.

This problem is to decide if vectors $\overrightarrow{g_1} = (g^a, 1, g)^\top$, $\overrightarrow{g_2} = (1, g^b, g)^\top$ and $\overrightarrow{g_3} = (g^{a\delta_1}, g^{b\delta_2}, g^{\delta_3})^\top$ are linearly dependent in the $(\mathbb{Z}/p\mathbb{Z})^\star$-module $\mathbb{G}^3$ formed by entry-wise multiplication.

The security of our second scheme is based on a non-interactive and falsifiable [Nao03] assumption, the hardness of n-Diffie-Hellman Exponent problem, proven to hold in generic groups in [BBG05].

Definition 10 (n-DHE – [BGW05]) *In a group $\mathbb{G}$ of prime order p, the n-Diffie-Hellman Exponent (n-DHE) problem is, given a tuple $(g, g^\gamma, g^{\gamma^2}, \ldots, g^{\gamma^n}, g^{\gamma^{n+2}}, \ldots, g^{\gamma^{2n}})$ where $\gamma \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$, $g \xleftarrow{\$} \mathbb{G}$, to compute $g^{\gamma^{n+1}}$.*

GROTH-SAHAI PROOF SYSTEMS. Our first scheme uses Groth-Sahai proofs based on the DLIN assumption and symmetric pairings, although instantiations based on the symmetric external Diffie-Hellman assumption are also possible. In the DLIN setting, the Groth-Sahai proof systems [GS08] use a common reference string comprising vectors $\overrightarrow{g_1}, \overrightarrow{g_2}, \overrightarrow{g_3} \in \mathbb{G}^3$, where $\overrightarrow{g_1} = (g_1, 1, g)^\top$, $\overrightarrow{g_2} = (1, g_2, g)^\top$ for some $g_1, g_2, g \in \mathbb{G}$. To commit to $X \in \mathbb{G}$, one sets $\overrightarrow{C} = (1, 1, X)^\top \cdot \overrightarrow{g_1}^r \cdot \overrightarrow{g_2}^s \cdot \overrightarrow{g_3}^t$ with $r, s, t \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$. In the soundness setting (*i.e.*, when proofs should be perfectly sound), $\overrightarrow{g_3}$ is set as $\overrightarrow{g_3} = \overrightarrow{g_1}^{\xi_1} \cdot \overrightarrow{g_2}^{\xi_2}$ with $\xi_1, \xi_2 \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}^*$. Commitments $\overrightarrow{C} = (g_1^{r+\xi_1 t}, g_2^{s+\xi_2 t}, X \cdot g^{r+s+t(\xi_1+\xi_2)})^\top$ are then Boneh-Boyen-Shacham (BBS) ciphertexts [BBS04] that can be decrypted using $a = \log_g(g_1)$, $b = \log_g(g_2)$.

In contrast, defining $\overrightarrow{g_3} = \overrightarrow{g_1}^{\xi_1} \cdot \overrightarrow{g_2}^{\xi_2} \cdot (1, 1, g^{-1})^\top$ gives linearly independent $\{\overrightarrow{g_1}, \overrightarrow{g_2}, \overrightarrow{g_3}\}$ and $\overrightarrow{C}$ is a perfectly hiding commitment. Moreover, proofs are perfectly witness indistinguishable (WI) in that two proofs generated using any two distinct witnesses are perfectly indistinguishable. Under the DLIN assumption, the WI and the soundness setting are computationally indistinguishable.

To prove that committed group elements satisfy certain relations, the Groth-Sahai techniques require one commitment per variable and one proof element (made of a constant number of group elements) per relation. Such proofs are available for pairing-product relations, which are of the type

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T, \tag{2.4}$$

for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$ and constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in (\mathbb{Z}/p\mathbb{Z})^\star$, for $i, j \in \{1, \ldots, n\}$.

At some additional cost (typically, auxiliary variables have to be introduced), pairing-product equations admit non-interactive zero-knowledge (NIZK) proofs (this is the case when the target element t_T has the special form $t_T = \prod_{i=1}^{t} e(S_i, T_i)$, for constants $\{(S_i, T_i)\}_{i=1}^{t}$ and some $t \in \mathbb{N}$): on a simulated common reference string (CRS), prepared for the WI setting, a trapdoor makes it possible to simulate proofs without knowing the witnesses. Linear pairing product equations (where $a_{ij} = 0$ for all i, j in (2.4)) consist of only 3 group elements and we only need linear equations here.

SYNTAX OF THRESHOLD ATTRIBUTE-BASED SIGNATURES AND THEIR SECURITY. We describe the syntax and security model of attribute-based signatures with respect to *threshold*

signing predicates $\Gamma = (t, S)$, but the algorithms and security model for more general signing predicates can be described in a very similar way. In the threshold case, every message Msg is signed for a subset S of the universe of attributes and a threshold t such that $1 \leq t \leq |S|$ of the sender's choice.

An *attribute-based signature scheme*

$$\mathsf{ABS} = (\mathsf{ABS.TSetup}, \mathsf{ABS.MSetup}, \mathsf{ABS.Keygen}, \mathsf{ABS.Sign}, \mathsf{ABS.Verify})$$

consists of five probabilistic polynomial-time (PPT) algorithms:

- $\mathsf{TSetup}(\lambda, \mathcal{P}, n)$: is the randomised *trusted setup* algorithm taking as input a security parameter λ, an attribute universe $\mathcal{P}$ and an integer $n \in \mathsf{poly}(\lambda)$ which is an upper bound on the size of threshold policies. It outputs a set of public parameters params (which contains λ, $\mathcal{P}$ and n). An execution of this algorithm is denoted as $\mathsf{params} \leftarrow \mathsf{ABS.TSetup}(1^\lambda, \mathcal{P}, n)$.
- $\mathsf{MSetup}(\mathsf{params})$: is the randomised *master setup* algorithm, that takes as input params and outputs a master secret key msk and the corresponding master public key mpk. We write $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{ABS.MSetup}(\mathsf{params})$ to denote an execution of this algorithm.
- $\mathsf{Keygen}(\mathsf{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$: is a *key extraction* algorithm that takes as input the public parameters params, the master keys mpk and msk, and an attribute set $\Omega \subset \mathcal{P}$. The output is a private key SK_Ω. We write $SK_\Omega \leftarrow \mathsf{ABS.Keygen}(\mathsf{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$ to denote an execution of this algorithm.
- $\mathsf{Sign}(\mathsf{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma)$: is a randomised *signing* algorithm which takes as input the public parameters params, the master public key mpk, a secret key SK_Ω, a message Msg and a threshold signing policy $\Gamma = (t, S)$ where $S \subset \mathcal{P}$ and $1 \leq t \leq |S| \leq n$. It outputs a signature σ. We denote the action taken by the signing algorithm as $\sigma \leftarrow \mathsf{ABS.Sign}(\mathsf{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma)$.
- $\mathsf{Verify}(\mathsf{params}, \mathsf{mpk}, \mathsf{Msg}, \sigma, \Gamma)$: is a deterministic *verification* algorithm taking as input the public parameters params, a master public key mpk, a message Msg, a signature σ and a threshold predicate $\Gamma = (t, S)$. It outputs 1 if the signature is deemed valid and 0 otherwise. We write $b \leftarrow \mathsf{ABS.Verify}(\mathsf{params}, \mathsf{mpk}, \mathsf{Msg}, \sigma, \Gamma)$ to refer to an execution of the verification protocol.

For correctness, it is required that for any $\lambda \in \mathbb{N}$, any integer $n \in \mathsf{poly}(\lambda)$, any universe $\mathcal{P}$, any set of public parameters $\mathsf{params} \leftarrow \mathsf{ABS.TSetup}(1^\lambda, \mathcal{P}, n)$, any master key pair $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{ABS.MSetup}(\mathsf{params})$, any subset $\Omega \subset \mathcal{P}$ and any threshold policy $\Gamma = (t, S)$ where $1 \leq t \leq |S|$, then

$$\mathsf{ABS.Verify}\big(\mathsf{params}, \mathsf{mpk}, \mathsf{Msg}, \mathsf{ABS.Sign}(\mathsf{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma), \Gamma\big) = 1$$

whenever $SK_\Omega \leftarrow \mathsf{ABS.Keygen}(\mathsf{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$ and $|\Omega \cap S| \geq t$.

Unforgeability and privacy are the typical requirements for attribute-based signature schemes.

Unforgeability. An ABS scheme must satisfy the usual property of unforgeability, even against a group of colluding users that pool their secret keys. We consider a relaxed notion where the attacker *selects* the signing policy $\Gamma^\star = (t^\star, S^\star)$ that he wants to attack at the

beginning of the game. However, the message $\mathsf{Msg}^\star$ whose signature is eventually forged is not selected in advance. The attacker can ask for valid signatures for messages and signing policies of his adaptive choice. The resulting property of *selective-predicate and adaptive-message unforgeability under chosen message attacks* (sP-UF-CMA, for short) is defined by considering the following game.

Definition 11 *Let λ be an integer. Consider the following game between a probabilistic polynomial time (PPT) adversary $\mathcal{F}$ and its challenger.*

Initialisation. *The challenger begins by specifying a universe of attributes $\mathcal{P}$ as well as an integer $n \in \mathsf{poly}(\lambda)$, which are sent to $\mathcal{F}$. Then, $\mathcal{F}$ selects a subset $S^\star \subset \mathcal{P}$ of attributes such that $|S^\star| \leq n$ and a threshold $t^\star \in \{1, \ldots, |S^\star|\}$. These define a threshold predicate $\Gamma^\star = (t^\star, S^\star)$.*

Setup. *The challenger runs the setup algorithm $\mathit{params} \leftarrow \mathit{ABS.TSetup}(1^\lambda, \mathcal{P}, n)$ and $(\mathsf{mpk}, \mathit{msk}) \leftarrow \mathit{ABS.MSetup}(\mathit{params})$, and sends $\mathit{params}, \mathsf{mpk}$ to the forger $\mathcal{F}$.*

Queries. *$\mathcal{F}$ can interleave private key and signature queries.*

- ***Private key queries.*** *$\mathcal{F}$ adaptively chooses a subset of attributes $\Omega \subset \mathcal{P}$ under the restriction that $|\Omega \cap S^\star| < t^\star$ and must receive $SK_\Omega \leftarrow \mathit{ABS.Keygen}(\mathit{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$ as the answer.*
- ***Signature queries.*** *$\mathcal{F}$ adaptively chooses a pair (Msg, Γ) consisting of a message Msg and a threshold predicate $\Gamma = (t, S)$ such that $1 \leq t \leq |S| \leq n$. The challenger chooses an arbitrary attribute set $\Omega \subset \mathcal{P}$ such that $|\Omega \cap S| \geq t$, runs $SK_\Omega \leftarrow \mathit{ABS.Keygen}(\mathit{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$ and computes[2] a signature $\sigma \leftarrow \mathit{ABS.Sign}(\mathit{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma)$ which is returned to $\mathcal{F}$.*

Forgery. *At the end of the game, $\mathcal{F}$ outputs a pair $(\mathsf{Msg}^\star, \sigma^\star)$. We say that $\mathcal{F}$ is successful if:*

- *$\mathit{ABS.Verify}(\mathit{params}, \mathsf{mpk}, \mathsf{Msg}^\star, \sigma^\star, \Gamma^\star) = 1$, and*
- *$\mathcal{F}$ has not made any signature query for the pair $(\mathsf{Msg}^\star, \Gamma^\star)$.*

The forger's advantage in breaking the sP-UF-CMA security is defined as $\mathsf{Succ}^{\text{sP-UF-CMA}}_{\mathcal{F},\mathit{ABS}}(\lambda) = \Pr[\mathcal{F}\ \mathit{wins}]$. A threshold attribute-based signature scheme ABS is said to be selective-predicate adaptive-message unforgeable (or sP-UF-CMA unforgeable) *if, for any PPT adversary $\mathcal{F}$, $\mathsf{Succ}^{\text{sP-UF-CMA}}_{\mathcal{F},\mathit{ABS}}(\lambda)$ is a negligible function of λ.*

Privacy (of Involved Attributes). This property ensures that a signature leaks nothing about the attributes that have been used to produce it beyond the fact that they satisfy the signing predicate. Privacy must hold even against attackers that control the master entity and is defined *via* a game between an adversary $\mathcal{D}$ and its challenger. Depending on the resources allowed to $\mathcal{D}$ and on its success probability, we can define computational privacy and perfect (unconditional) privacy.

2. Since a given attribute set Ω may have many valid private keys SK_Ω, a generalisation of the definition could allow $\mathcal{F}$ to obtain many signatures from the same private key SK_Ω. However, due to the signer privacy requirement, which is formalised hereafter, this does not matter.

Definition 12 *Let $\lambda \in \mathbb{N}$ and consider this game between a distinguisher $\mathcal{D}$ and its challenger.*

Setup. *The adversary $\mathcal{D}$ specifies a universe of attributes $\mathcal{P}$ and an integer $n \in \mathsf{poly}(\lambda)$, that are sent to the challenger. The challenger runs $\mathit{params} \leftarrow \mathit{ABS.TSetup}(1^\lambda, \mathcal{P}, n)$ and sends params to $\mathcal{D}$. The adversary $\mathcal{D}$ runs $(\mathsf{mpk}, \mathit{msk}) \leftarrow \mathit{ABS.MSetup}(\mathit{params})$ and sends $(\mathsf{mpk}, \mathit{msk})$ to the challenger (who must verify consistency of this master key pair).*

Challenge. *$\mathcal{D}$ outputs a tuple $(\Gamma, \Omega_0, \Omega_1, \mathsf{Msg})$, where $\Gamma = (t, S)$ is a threshold predicate such that $1 \leq t \leq |S| \leq n$ and Ω_0, Ω_1 are attribute sets satisfying $|\Omega_b \cap S| \geq t$ for each $b \in \{0,1\}$. The challenger picks a random bit $\beta \xleftarrow{\$} \{0,1\}$, runs $SK_{\Omega_\beta} \leftarrow \mathit{ABS.Keygen}(\mathit{params}, \mathsf{mpk}, \mathsf{msk}, \Omega_\beta)$ and computes the challenge signature $\sigma^\star \leftarrow \mathit{ABS.Sign}(\mathit{params}, \mathsf{mpk}, SK_{\Omega_\beta}, \mathsf{Msg}, \Gamma)$, which is sent as a challenge to $\mathcal{A}$.*

Guess. *$\mathcal{D}$ outputs a bit $\beta' \in \{0,1\}$ and wins if $\beta' = \beta$.*

The advantage of $\mathcal{D}$ is measured in the usual way, as the distance $\mathit{Adv}^{\mathit{Priv}}_{\mathcal{D},\mathit{ABS}}(\lambda) := |\Pr[\beta' = \beta] - \frac{1}{2}|$.

A threshold attribute-based signature scheme ABS is said computationally private *if $\mathit{Adv}^{\mathit{Priv}}_{\mathcal{D},\mathit{ABS}}(\lambda)$ is a negligible function of λ for any PPT distinguisher $\mathcal{D}$ and it is said* perfectly/unconditionally private *if $\mathit{Adv}^{\mathit{Priv}}_{\mathcal{D},\mathit{ABS}}(\lambda) = 0$ for any (possibly computationally unbounded) distinguisher $\mathcal{D}$.*

2.4.2 A First Short Attribute-Based Signature Scheme

We present here our first scheme to produce attribute-based signatures with constant size, for threshold predicates. The secret key sk_Ω for a user holding a set of attributes Ω contains $|\Omega| + n$ elements, where n is the maximum size of the attribute set for any signing policy. This construction is for "small" universes of attributes $\mathcal{P} = \{\mathtt{at}_1, \ldots, \mathtt{at}_\eta\}$, for some integer $\eta \in \mathbb{N}$, as public parameters have linear size in η; therefore, η must be polynomial in the security parameter of the scheme. Attributes $\{\mathtt{at}_i\}_{i=1}^{\eta}$ are arbitrary strings which some encoding function ς maps to $\mathbb{Z}_p^*$. Since the scheme is a small universe construction, we may set $n = \eta$ in the description hereafter.

The construction is based on the ABE scheme described in Section 2.3. The intuition is to have the signer implicitly prove his ability to decrypt a ciphertext corresponding to that ABE scheme. This non-interactive proof is generated using the Groth-Sahai proof systems [GS08], by binding the signed message (and the corresponding predicate) to the non-interactive proof using a technique suggested by Malkin *et al.* [MTVY11]. In some sense, this technique can be seen as realising signatures of knowledge in the standard model: it consists in embedding the message to be signed in the Groth-Sahai CRS by calculating part of the latter as a "hash value" of the message. As noted in [MTVY11], Waters' hash function [Wat05] is well-suited to this purpose since, in the security proof, it makes it possible to answer signing queries using simulated NIZK proofs. At the same time, with non-negligible probability, adversarially-generated signatures are produced using a perfectly sound Groth-Sahai CRS and they thus constitute real proofs, from which witnesses can be extracted.

In [MTVY11], the above technique was applied to an instantiation of Groth-Sahai proofs

based on the Symmetric eXternal Diffie-Hellman assumption (and thus asymmetric pairings). In this section, we adapt this technique so as to get it to work with symmetric pairings and the linear assumption.

In the notations of the verification algorithm, when $\overrightarrow{C} = (C_1, C_2, C_3)^\top \in \mathbb{G}^3$ is a vector of group elements and if $g \in \mathbb{G}$, we denote by $E(g, \overrightarrow{C})$ the vector of pairing values $\big(e(g, C_1), e(g, C_2), e(g, C_3)\big)^\top$.

DESCRIPTION.

– $\mathsf{TSetup}(\lambda, \mathcal{P}, n)$: the trusted setup algorithm conducts the following steps.

1. Choose groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with an efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Select generators $g, h \xleftarrow{\$} \mathbb{G}$ and also choose a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^k$, for some $k \in \mathsf{poly}(\lambda)$.

2. Define a suitable injective encoding ς sending each one of the n attributes $\mathsf{at} \in \mathcal{P}$ onto an element $\varsigma(\mathsf{at}) = x \in \mathbb{Z}/p\mathbb{Z}^\star$. Choose a set $\mathcal{D} = \{d_1, \ldots, d_{n-1}\}$ consisting of $n-1$ pairwise different elements of $\mathbb{Z}/p\mathbb{Z}^*$, which must also be different from the encoding of any attribute in $\mathcal{P}$. For any integer i lower or equal to $n-1$, we denote as $\mathcal{D}_i$ the set $\{d_1, \ldots, d_i\}$.

3. Generate Groth-Sahai reference strings by choosing random generators $g_1, g_2 \xleftarrow{\$} \mathbb{G}$ and defining vectors $\overrightarrow{g_1} = (g_1, 1, g)^\top \in \mathbb{G}^3$ and $\overrightarrow{g_2} = (1, g_2, g)^\top \in \mathbb{G}^3$. Then, for each $i \in \{0, \ldots, k\}$, pick $\xi_{i,1}, \xi_{i,2} \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ at random and define a vector $\overrightarrow{g_{3,i}} = \overrightarrow{g_1}^{\xi_{i,1}} \cdot \overrightarrow{g_2}^{\xi_{i,2}} = \big(g_1^{\xi_{i,1}}, g_2^{\xi_{i,2}}, g^{\xi_{i,1}+\xi_{i,2}}\big)^\top$. Exponents $\{(\xi_{i,1}, \xi_{i,2})\}_{i=0}^k$ can then be discarded as they are no longer needed.

The resulting public parameters are

$$\mathsf{params} = \Big(\mathcal{P},\ n,\ \lambda,\ \mathbb{G},\ \mathbb{G}_T,\ g,\ h,\ \overrightarrow{g_1},\ \overrightarrow{g_2},\ \{\overrightarrow{g_{3,i}}\}_{i=0}^k,\ H,\ \varsigma,\ \mathcal{D}\Big).$$

– $\mathsf{MSetup}(\mathsf{params})$: picks at random $\alpha, \gamma \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}^*$ and sets $u = g^{\alpha\gamma}$ and $v = e(g^\alpha, h)$. The master secret key is $\mathsf{msk} = (\alpha, \gamma)$ and the master public key consists of

$$\mathsf{mpk} = \Big(\ u,\ v,\ g^\alpha,\ \Big\{h^{\alpha\gamma^i}\Big\}_{i=0,\ldots,2n-1}\Big).$$

$\mathsf{Keygen}(\mathsf{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$: given an attribute set Ω and $\mathsf{msk} = (\alpha, \gamma)$, pick $r \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}^*$ and compute

$$SK_\Omega = \Big(\ \Big\{g^{\frac{r}{\gamma+\varsigma(\mathsf{at})}}\Big\}_{\mathsf{at}\in\Omega}, \Big\{h^{r\gamma^i}\Big\}_{i=0,\ldots,n-2}, h^{\frac{r-1}{\gamma}}\Big). \tag{2.5}$$

– $\mathsf{Sign}(\mathsf{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma)$: to sign $\mathsf{Msg} \in \{0,1\}^*$ w.r.t. the policy $\Gamma = (t, S)$, where $S \subset \mathcal{P}$ is an attribute set of size $s = |S| \leq n$ and $1 \leq t \leq s \leq n$, the algorithm returns $\perp$ if $|\Omega \cap S| < t$. Otherwise, it first parses SK_Ω as in (2.5) and conducts the following steps.

1. Let Ω_S be any subset of $\Omega \cap S$ with $|\Omega_S| = t$. From all $\mathsf{at} \in \Omega_S$, compute the value

$$A_1 = \mathsf{Aggregate}(\{g^{\frac{r}{\gamma+\varsigma(\mathsf{at})}}, \varsigma(\mathsf{at})\}_{\mathsf{at}\in\Omega_S}) = g^{\frac{r}{\prod_{\mathsf{at}\in\Omega_S}(\gamma+\varsigma(\mathsf{at}))}}$$

using the algorithm Aggregate of [DP08]. From A_1, compute

$$T_1 = A_1^{\frac{1}{\prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\Omega_S}\varsigma(\mathsf{at})}}.$$

2. Define the value $P_{(\Omega_S,S)}(\gamma)$ as

$$P_{(\Omega_S,S)}(\gamma) = \frac{1}{\gamma}\left(\prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\Omega_S}(\gamma+\varsigma(\mathsf{at})) - \prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\Omega_S}\varsigma(\mathsf{at})\right).$$

Since $|\Omega_S| = t$, the degree of $P_{(\Omega_S,S)}(X)$ is $n-2$. Therefore, from the private key SK_Ω, one can compute $h^{r\cdot P_{(\Omega_S,S)}(\gamma)/(\prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\Omega_S}\varsigma(\mathsf{at}))}$ and multiply it with the last element $h^{\frac{r-1}{\gamma}}$ of SK_Ω to obtain

$$T_2 = h^{\frac{r-1}{\gamma}} \cdot h^{r\frac{P_{(\Omega_S,S)}(\gamma)}{\prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})\setminus\Omega_S}\varsigma(\mathsf{at})}}.$$

Note that the obtained values $T_1, T_2 \in \mathbb{G}$ satisfy the equality

$$e(T_2, u^{-1}) \cdot e\Big(T_1, h^{\alpha\cdot\prod_{\mathsf{at}\in(S\cup\mathcal{D}_{n+t-1-s})}(\gamma+\varsigma(\mathsf{at}))}\Big) = e(g^\alpha, h) \tag{2.6}$$

and that, in the terms in the left-hand-side of equality (2.6), the second argument of each pairing is publicly computable using params and mpk.

3. Compute $M = m_1 \ldots m_k = H(\mathsf{Msg}, \Gamma) \in \{0,1\}^k$ and use M to form a message-specific Groth-Sahai CRS $\mathbf{g}_M = (\overrightarrow{g_1}, \overrightarrow{g_2}, \overrightarrow{g}_{3,M})$. Namely, for $i = 0$ to k, parse $\overrightarrow{g_{3,i}}$ as $(g_{X,i}, g_{Y,i}, g_{Z,i})^\top \in \mathbb{G}^3$. Then, define the vector

$$\overrightarrow{g}_{3,M} = \Big(g_{X,0}\cdot\prod_{i=1}^{k} g_{X,i}^{m_i},\ g_{Y,0}\cdot\prod_{i=1}^{k} g_{Y,i}^{m_i},\ g_{Z,0}\cdot\prod_{i=1}^{k} g_{Z,i}^{m_i}\Big)^\top.$$

4. Using the newly defined $\mathbf{g}_M = (\overrightarrow{g_1}, \overrightarrow{g_2}, \overrightarrow{g}_{3,M})$, generate Groth-Sahai commitments to T_1 and T_2. Namely, pick $r_1, s_1, t_1, r_2, s_2, t_2 \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ and compute

$$\overrightarrow{C}_{T_j} = (1, 1, T_j)^\top \cdot \overrightarrow{g_1}^{r_j} \cdot \overrightarrow{g_2}^{s_j} \cdot \overrightarrow{g}_{3,M}^{\,t_j}$$

for $j \in \{1,2\}$. Then, generate a NIZK proof that committed variables (T_1, T_2) satisfy the pairing-product equation (2.6). To this end, we introduce an auxiliary variable $\Theta \in \mathbb{G}$ (with its own commitment $\overrightarrow{C}_\Theta = (1,1,\Theta)^\top \cdot \overrightarrow{g_1}^{r_\theta} \cdot \overrightarrow{g_2}^{s_\theta} \cdot \overrightarrow{g}_{3,M}^{\,t_\theta}$, for $r_\theta, s_\theta, t_\theta \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$), which takes on the value $\Theta = h$, and actually prove that

$$e(T_1, H_S) = e(g^\alpha, \Theta)\cdot e(T_2, u) \tag{2.7}$$
$$e(g, \Theta) = e(g, h), \tag{2.8}$$

where $H_S = h^{\alpha \cdot \prod_{\mathsf{at} \in (S \cup \mathcal{D}_{n+t-1-s})} (\gamma + \varsigma(\mathsf{at}))}$. The proofs for relations (2.7) and (2.8) are called $\overrightarrow{\pi_1}$ and $\overrightarrow{\pi_2}$, respectively, and they are given by

$$\begin{aligned} \overrightarrow{\pi}_1 &= (\pi_{1,1}, \pi_{1,2}, \pi_{1,3})^\top = \left(H_S^{r_1} \cdot (g^\alpha)^{-r_\theta} \cdot u^{-r_2},\ H_S^{s_1} \cdot (g^\alpha)^{-s_\theta} \cdot u^{-s_2},\ H_S^{t_1} \cdot (g^\alpha)^{-t_\theta} \cdot u^{-t_2}\right)^\top \\ \overrightarrow{\pi}_2 &= (\pi_{2,1}, \pi_{2,2}, \pi_{2,3})^\top = \left(g^{r_\theta},\ g^{s_\theta},\ g^{t_\theta}\right)^\top. \end{aligned}$$

Finally, output the signature $\sigma = \left(\overrightarrow{C}_{T_1}, \overrightarrow{C}_{T_2}, \overrightarrow{C}_\theta, \overrightarrow{\pi}_1, \overrightarrow{\pi_2}\right) \in \mathbb{G}^{15}$.

– $\mathsf{Verify}(\mathsf{params}, \mathsf{mpk}, \mathsf{Msg}, \sigma, \Gamma)$: it first parses Γ as a pair (t, S) and σ as

$$\left(\overrightarrow{C}_{T_1}, \overrightarrow{C}_{T_2}, \overrightarrow{C}_\theta, \overrightarrow{\pi}_1, \overrightarrow{\pi_2}\right).$$

It computes $M = m_1 \ldots m_k = H(\mathsf{Msg}, \Gamma) \in \{0,1\}^k$ and forms the corresponding vector

$$\overrightarrow{g}_{3,M} = \left(g_{X,0} \cdot \prod_{i=1}^{k} g_{X,i}^{m_i},\ g_{Y,0} \cdot \prod_{i=1}^{k} g_{Y,i}^{m_i},\ g_{Z,0} \cdot \prod_{i=1}^{k} g_{Z,i}^{m_i}\right)^\top \in \mathbb{G}^3.$$

Then, parse the proofs $\overrightarrow{\pi_1}$ and $\overrightarrow{\pi_2}$ as vectors $(\pi_{1,1}, \pi_{1,2}, \pi_{1,3})^\top$ and $(\pi_{2,1}, \pi_{2,2}, \pi_{2,3})^\top$, respectively. Define $H_S = h^{\alpha \cdot \prod_{\mathsf{at} \in (S \cup \mathcal{D}_{n+t-1-s})} (\gamma + \varsigma(\mathsf{at}))}$ and return 1 if and only if these relations are both satisfied:

$$\begin{aligned} E(H_S, \overrightarrow{C_{T_1}}) &= E(g^\alpha, \overrightarrow{C_\theta}) \cdot E(u, \overrightarrow{C_{T_2}}) \cdot E(\pi_{1,1}, \overrightarrow{g_1}) \cdot E(\pi_{1,2}, \overrightarrow{g_2}) \cdot E(\pi_{1,3}, \overrightarrow{g}_{3,M}) \quad (2.9) \\ E(g, \overrightarrow{C_\theta}) &= E\left(g, (1,1,h)\right) \cdot E(\pi_{2,1}, \overrightarrow{g_1}) \cdot E(\pi_{2,2}, \overrightarrow{g_2}) \cdot E(\pi_{2,3}, \overrightarrow{g}_{3,M}). \quad (2.10) \end{aligned}$$

SECURITY RESULTS. This first scheme is selective-predicate and adaptive-message unforgeable by reduction to the hardness of the $(\tilde{\ell}, \tilde{m}, \tilde{t})$-aMSE-CDH. It enjoys a computational privacy under the DLIN assumption.

Theorem 14 ([HLLR11], Theorem 1) *The scheme is selective-predicate and adaptive-message unforgeable under chosen-message attacks assuming that (1) H is a collision-resistant hash function; (2) the DLIN assumption holds in $\mathbb{G}$; (3) the $(\tilde{\ell}, \tilde{m}, \tilde{t})$-aMSE-CDH assumption holds in $(\mathbb{G}, \mathbb{G}_T)$.*

Theorem 15 ([HLLR11], Theorem 2) *This scheme has computational privacy, assuming that DLIN holds in $\mathbb{G}$.*

2.4.3 A Second Short Attribute-Based Signature Scheme

The idea of our second scheme is that a (threshold) attribute-based signature can be computed only if the signer holds t attributes in S which, combined with $n - t$ dummy attributes, lead to n attributes at such that $P_S(\mathsf{at}) = 0$ for a certain polynomial $P_S(Z)$. This makes it possible to interpolate a polynomial $Q_\Omega(X)$ with degree $n - 1$ whose constant term is a secret α of the authority, recover in some way the value g^α (also known only by the authority) and produce a valid signature, by manipulating polynomials "in the exponent".

The main advantage of our second ABS scheme over the previous one is that signatures are much shorter, since they have only three group elements. This comes at the cost of longer

secret keys sk_Ω, containing $(2n+2) \times (|\Omega| + n)$ group elements. Another advantage is that the size of the considered universe of attributes may be much larger, even exponential in the security parameter λ; we only need that all attributes in the universe $\mathcal{P}$ as different elements of $\mathbb{Z}/p\mathbb{Z}^*$.

DESCRIPTION.

- $\mathsf{TSetup}(\lambda, \mathcal{P}, n)$: chooses a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^k$, for some integer $k \in \mathsf{poly}(\lambda)$, as well as bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. It also picks $u_0, u_1, \ldots, u_k \xleftarrow{\$} \mathbb{G}$ and sets $\overrightarrow{U} = (u_0, u_1, \ldots, u_k)^\top$. It finally chooses a set $\mathcal{D} = \{d_1, \ldots, d_n\}$ of n distinct elements of $\mathbb{Z}/p\mathbb{Z}$ that will serve as dummy attributes.
  The resulting public parameters are $\mathsf{params} = \Big(\mathcal{P},\ n,\ \lambda,\ \mathbb{G},\ \mathbb{G}_T, g,\ \overrightarrow{U},\ \mathcal{D},\ H\Big)$.
- $\mathsf{MSetup}(\mathsf{params})$: randomly chooses $\alpha, \alpha_0 \xleftarrow{\$} \mathbb{Z}_p$, $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_N)^\top \xleftarrow{\$} \mathbb{Z}_p^N$, where $N = 2n+1$. It then computes $e(g,g)^\alpha$, $h_0 = g^{\alpha_0}$, $\overrightarrow{H} = (h_1, \ldots, h_N)^\top = g^{\overrightarrow{\alpha}}$.
  The master secret key is defined to be $\mathsf{msk} = g^\alpha$ and the master public key is $\mathsf{mpk} = \Big(e(g,g)^\alpha,\ h_0,\ \overrightarrow{H}\Big)$.
- $\mathsf{Keygen}(\mathsf{params}, \mathsf{mpk}, \mathsf{msk}, \Omega)$: to generate a key for the attribute set Ω, the algorithm picks a polynomial $Q_\Omega[X] = \alpha + \beta_1 X + \cdots + \beta_{n-1} X^{n-1}$ where $\beta_1, \ldots, \beta_{n-1} \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$. Then, it proceeds as follows.

  1. For each attribute $\omega \in \Omega$, choose a random exponent $r_\omega \xleftarrow{\$} \mathbb{Z}_p$ and generate a key component $\mathsf{sk}_\omega = (D_{\omega,1}, D_{\omega,2}, K_{\omega,1}, \ldots, K_{\omega,N-1})$ where
  $$D_{\omega,1} = g^{Q_\Omega(\omega)} \cdot h_0^{r_\omega}, \quad D_{\omega,2} = g^{r_\omega}, \quad \Big\{K_{\omega,i} = \big(h_1^{-\omega^i} \cdot h_{i+1}\big)^{r_\omega}\Big\}_{i=1,\ldots,N-1}. \tag{2.11}$$
  2. For each $d \in \mathcal{D}$, generate a private key component $\mathsf{sk}_d = (D_{d,1}, D_{d,2}, K_{d,1}, \ldots, K_{d,N-1})$ in the same way as in (2.11), by choosing a fresh random value $r_d \in \mathbb{Z}/p\mathbb{Z}$ and computing
  $$D_{d,1} = g^{Q_\Omega(d)} \cdot h_0^{r_d}, \quad D_{d,2} = g^{r_d}, \quad \Big\{K_{d,i} = \big(h_1^{-w^i} \cdot h_{i+1}\big)^{r_d}\Big\}_{i=1,\ldots,N-1}. \tag{2.12}$$

  The private key finally consists of $SK_\Omega = \big(\{\mathsf{sk}_\omega\}_{\omega\in\Omega}, \{\mathsf{sk}_d\}_{d\in\mathcal{D}}\big)$.

- $\mathsf{Sign}(\mathsf{params}, \mathsf{mpk}, SK_\Omega, \mathsf{Msg}, \Gamma)$: to sign $\mathsf{Msg} \in \{0,1\}^*$ w.r.t. the policy $\Gamma = (t, S)$, where S is an attribute set of size $s = |S| \leq n$ and $t \in \{1, \ldots, s\}$, the algorithm first computes $M = H(\mathsf{Msg}, \Gamma) \in \{0,1\}^k$ and parses the private key SK_Ω as $\big(\{\mathsf{sk}_\omega\}_{\omega\in\Omega}, \{\mathsf{sk}_d\}_{d\in\mathcal{D}}\big)$.

  1. It considers the subset $\mathcal{D}_{n-t} \subset \mathcal{D}$ containing the $n-t$ first attributes of $\mathcal{D}$ (chosen in some pre-specified lexicographical order). It also chooses an arbitrary subset $S_t \subset \Omega \cap S$ such that $|S_t| = t$ and defines $\overrightarrow{Y} = (y_1, \ldots, y_N)^\top$ as the vector containing the coefficients of the polynomial
  $$P_S(Z) = \sum_{i=1}^{n-t+s+1} y_i Z^{i-1} = \prod_{\omega\in S}(Z - \omega) \cdot \prod_{d\in\mathcal{D}_{n-t}} (Z - d). \tag{2.13}$$

Since $n - t + s + 1 \leq 2n + 1 = N$, the coordinates $y_{n-t+s+2}, \ldots, y_N$ are all set to 0.

2. For each $\omega \in S_t$, use $\mathsf{sk}_\omega = (D_{\omega,1}, D_{\omega,2}, \{K_{\omega,i}\}_{i=1}^{N-1})$ to compute

$$D'_{\omega,1} = D_{\omega,1} \cdot \prod_{i=1}^{N-1} K_{\omega,i}^{y_{i+1}} = g^{Q_\Omega(\omega)} \cdot \big(h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}\big)^{r_\omega}. \tag{2.14}$$

The last equality comes from the fact that $P_S(\omega) = 0$ for all $\omega \in S$.

3. Likewise, for each dummy attribute $d \in \mathcal{D}_{n-t}$, use $\mathsf{sk}_d = (D_{d,1}, D_{d,2}, \{K_{d,i}\}_{i=1}^{N-1})$ to compute

$$D'_{d,1} = D_{d,1} \cdot \prod_{i=1}^{N-1} K_{d,i}^{y_{i+1}} = g^{Q_\Omega(d)} \cdot \big(h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}\big)^{r_d}. \tag{2.15}$$

4. Using $\{D'_{\omega,1}\}_{\omega \in S_t}$ and $\{D'_{d,1}\}_{d \in \mathcal{D}_{n-t}}$ and the corresponding $D_{\omega,2} = g^{r_w}$, $D_{d,2} = g^{r_d}$, compute

$$D_1 = \prod_{\omega \in S_t} {D'_{\omega,1}}^{\Delta_\omega^{S_t \cup \mathcal{D}_{n-t}}(0)} \cdot \prod_{d \in \mathcal{D}_{n-t}} {D'_{d,1}}^{\Delta_d^{S_t \cup \mathcal{D}_{n-t}}(0)} = g^\alpha \cdot (h_0 \cdot \prod_{i=1}^{N} h_i^{y_i})^r \tag{2.16}$$

$$D_2 = \prod_{\omega \in S_t} D_{\omega,2}^{\Delta_\omega^{S_t \cup \mathcal{D}_{n-t}}(0)} \cdot \prod_{d \in \mathcal{D}_{n-t}} D_{d,2}^{\Delta_d^{S_t \cup \mathcal{D}_{n-t}}(0)} = g^r, \tag{2.17}$$

where $r = \sum_{\omega \in S_t} \Delta_\omega^{S_t \cup \mathcal{D}_{n-t}}(0) \cdot r_\omega + \sum_{d \in \mathcal{D}_{n-t}} \Delta_d^{S_t \cup \mathcal{D}_{n-t}}(0) \cdot r_d$.

5. Parse $M \in \{0,1\}^k$ as a string $m_1 \ldots m_k$ where $m_j \in \{0,1\}$ for $j = 1, \ldots, k$. Then, choose $z, w \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ and compute

$$\sigma_1 = D_1 \cdot \big(h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}\big)^w \cdot \big(u_0 \cdot \prod_{j=1}^{k} u_j^{m_j}\big)^z, \qquad \sigma_2 = D_2 \cdot g^w, \qquad \sigma_3 = g^z.$$

Return the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{G}^3$.

– $\mathsf{Verify}(\mathsf{params}, \mathsf{mpk}, \mathsf{Msg}, \sigma, \Gamma)$: it parses Γ as a pair (t, S). It computes $M = H(\mathsf{Msg}, \Gamma) \in \{0,1\}^k$ and considers the subset $\mathcal{D}_{n-t} \subset \mathcal{D}$ containing the $n - t$ first dummy attributes of $\mathcal{D}$. Then, it defines the vector $\overrightarrow{Y} = (y_1, \ldots, y_N)^\top$ from the polynomial $P_S(Z)$ as per (2.13). The algorithm accepts the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ as valid and thus outputs 1 if and only if

$$e(g,g)^\alpha = e(\sigma_1, g) \cdot e\big(\sigma_2, h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}\big)^{-1} \cdot e\big(\sigma_3, u_0 \cdot \prod_{j=1}^{k} u_j^{m_j}\big)^{-1}. \tag{2.18}$$

The correctness of the scheme follows from the property that for each attribute $\omega \in S_t \subset S \cap \Omega$, the vector $\overrightarrow{X}_\omega^N = (1, \omega, \omega^2, \ldots, \omega^{N-1})$ is orthogonal to $\overrightarrow{Y}$, so that we have

$$D'_{\omega,1} = D_{\omega,1} \cdot \prod_{i=1}^{N-1} K_{\omega,i}^{y_{i+1}} = g^{Q_\Omega(\omega)} \cdot \Big(h_0 \cdot h_1^{-(\langle \overrightarrow{X}_\omega^N, \overrightarrow{Y} \rangle - y_1)} \prod_{i=2}^{N} h_i^{y_i}\Big)^{r_\omega} = g^{Q_\Omega(\omega)} \cdot \Big(h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}\Big)^{r_\omega},$$

which explains the second equality of (2.14) and the same holds for (2.15). In addition, the values (D_1, D_2) obtained as per (2.16)-(2.17) satisfy $e(D_1, g) = e(g, g)^{\alpha} \cdot e(h_0 \cdot \prod_{i=1}^{N} h_i^{y_i}, D_2)$, which easily leads to the verification equation (2.18).

SECURITY RESULTS. This second scheme is selective-predicate and adaptive-message unforgeable by reduction to the hardness of the n-Diffie-Hellman Exponent (n-DHE) problem. This scheme also enjoys unconditional privacy, which is another advantage over our first scheme.

Theorem 16 ([HLLR11], Theorem 3) *The scheme is selective-predicate and adaptive-message unforgeable under chosen-message attacks if H is collision-resistant and if the $(2n+1)$-DHE assumption holds in $\mathbb{G}$, where n is the maximal number of attributes in the set S.*

Theorem 17 ([HLLR11], Theorem 4) *This second ABS scheme enjoys perfect privacy.*

2.4.4 Extensions and Perspectives

The first signature scheme, as the encryption scheme of Section 2.3, can support weighted threshold predicates. Furthermore, since the final form of the signatures is that of a Groth-Sahai non-interactive proof, one could consider signing predicates which are described by a monotone formula (OR / AND gates) over threshold clauses. The Groth-Sahai proof would be then a proof of knowledge of some values that satisfy a monotone formula of equations. The size of such a proof (and therefore, the size of the resulting attribute-based signatures) would be linear in the number of threshold clauses in the formula. We stress that this is still better than having size linear in the number of involved attributes, as in all previous constructions.

Concerning the second scheme, we can use similar ideas for other families of predicates which are realised with a secret sharing scheme with properties which resemble those of Shamir's. The ideas underlying this extension are quite related to those in [DHMR10], where dummy attributes were used to design attribute-based encryption schemes for general decryption predicates. For instance, we could achieve hierarchical threshold predicates (following [Tas07]) and compartmented access structures (defined in [Bri89]). The resulting ciphertexts are not constant size anymore, but their size is less than linear in the number of involved attributes, and thus, in this aspect the resulting schemes still outperform previous constructions.

Like encryption schemes, attribute-based signatures must achieve the best possible expressivity, the highest security while being efficient, in terms of signature size or computational complexity. In any case, if the expressivity is very high, compressing signatures (or ciphertexts in the case of ABE) will imply longer secret keys. Our results may inspire ideas leading to the design of fully secure ABS schemes with constant-size signatures and supporting more expressive predicates. The scheme from [EHM11] is the example of a fully-secure scheme with general signing policies, but its efficiency is not satisfactory: it uses Groth-Sahai proof system, composite order bilinear groups and the size of the signatures grows with the size of the signing policy. The construction form [OT11] has also long signatures. Interesting ideas are contained in this paper, and adaptations in the lattice world could be possible.

Bibliography

[A+08] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi. *Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions.* J. Cryptology, 21(3), 350–391 (2008)

[AM94] L. M. Adleman and K. S. McCurley. *Open problems in number theoretic complexity, II.* Proc. of ANTS-I, Springer LNCS Vol. 877, 291–322 (1994)

[ABB10a] S. Agrawal, D. Boneh and X. Boyen. *Efficient Lattice (H)IBE in the Standard Model*. Proc. of Eurocrypt 2010, Springer LNCS Vol. 6110, 553–572 (2010)

[ABB10b] S. Agrawal, D. Boneh and Xavier Boyen. *Lattice Basis Delegation in Fixed Dimension and Shorter Ciphertext Hierarchical IBE.* Proc. of Crypto 2010, Springer LNCS Vol. 6223, 98–115 (2010)

[A+11] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris and H. Wee. *Fuzzy Identity Based Encryption from Lattices*. Preprint, `http://eprint.iacr.org/2011/414` (2011)

[AFV11] S. Agrawal, D. M. Freeman and V. Vaikuntanathan. *Predicate Encryption for Inner Products from LWE*. Preprint, `http://eprint.iacr.org/2011/410` (2011)

[ACGL11] C. Aguilar Melchor, P.-L. Cayrel, P. Gaborit and F. Laguillaumie *A New Efficient Threshold Ring Signature Scheme based on Coding Theory*. . IEEE Transactions on Information Theory, Vol. 57(7) 4833–4842 (2011)

[AG09] G. Ateniese and P. Gasti. *Universally Anonymous Ibe Based on the Quadratic Residuosity Assumption*. Proc. of CT-RSA 2009, Springer LNCS Vol. 5473, 32–47 (2009)

[AL10] N. Attrapadung, B. Libert. *Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation*. Proc. of PKC 2010, Springer LNCS Vol. 6056, 384–402 (2010)

[ALP11] N. Attrapadung, B. Libert and E. de Panafieu. *Expressive Key-Policy Attribute-based Encryption with Constant-Size Ciphertexts*. Proc. of PKC 2011, Springer LNCS Vol. 6571 , 90–108 (2011)

[BK98] R. Balasubramanian and N. Koblitz. *The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes–Okamoto–Vanstone Algorithm*. J. Cryptology 11(2), 141–145 (1998)

[BGOS07] P. S. L. M. Barreto, S. D. Galbraith, C. O'Eigeartaigh and M. Scott. *Efficient pairing computation on supersingular Abelian varieties*. Des. Codes Cryptography 42(3), 239–271 (2007)

[BLS03] P. S. L. M. Barreto, B. Lynn and M. Scott. *On the Selection of Pairing-Friendly Groups*. Proc. of SAC 2003, Springer LNCS Vol. 3006, 17–25 (2003)

[BN06] P. S. L. M. Barreto and M. Naehrig. *Pairing-friendly elliptic curves of prime order*. Proc. of SAC 2005, Springer LNCS Vol. 3897, 319–331 (2006)

[BBDP01] M. Bellare, A. Boldyreva, A. Desai and D. Pointcheval. *Key-Privacy in Public-Key Encryption.* Proc. of Asiacrypt 2001, Springer LNCS Vol. 2248, 566–582 (2001)

[Ben94] J. Benaloh. *Dense probabilistic encryption.* Proc. of SAC 94, 129–128, (1994)

[BG10] A. Bernard and N. Gama. *Smallest Reduction Matrix of Binary Quadratic Forms*. Proc. of ANTS-IX, Springer LNCS Vol. 6197, 32–49 (2010)

[BL] D. Bernstein and T. Lange. *Explicit-Formulas Database*, `http://www.hyperelliptic.org/EFD/`

[BSW07] J. Bethencourt, A. Sahai and B. Waters. *Ciphertext-Policy Attribute-based Encryption.* Proc. of IEEE Symposium on Security and Privacy, IEEE Society Press, 321–334 (2007)

[BHL07] R. Bhaskar, J. Herranz and F. Laguillaumie. *Aggregate Designated Verifier Signatures and Application to Secure Routing*. International Journal of Security and Networks, Special Issue on Cryptography in Networks, Vol. 1 (1/2/3), 192–201 (2007)

[BPT04] I. Biehl, S. Paulus and T. Takagi. *Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders*. Des. Codes Cryptography 31(2), 99–123 (2004)

[BMX06] I. F. Blake, V. K. Murty and G. Xu. *Refinements of Miller's algorithm for computing the Weil/Tate pairing*. J. Algorithms, 58(2), 134–149 (2006)

[BB04a] D. Boneh and X. Boyen. *Efficient Selective-ID Secure Identity based Encryption Without Random Oracles*. Proc. of Eurocrypt 2004, Springer LNCS Vol. 3027, 223–238 (2004)

[BB04b] D. Boneh and X. Boyen. *Secure Identity based Encryption Without Random Oracles. Proc. of Crypto 2004, Springer LNCS Vol. 3152*, 443–459 (2004)

[BBG05] D. Boneh, X. Boyen and E.-J. Goh. *Hierarchical Identity-based Encryption with Constant Size Ciphertext.* Proc. of Eurocrypt 2005, Springer LNCS Vol. 3494, 440–456 (2005)

[BBS04] D. Boneh, X. Boyen and H. Shacham. *Short group signatures.* Proc. of Crypto 2004, Springer LNCS Vol. 3152, 41–55 (2004)

[BCOP04] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano. *Public Key Encryption with Keyword Search.* Proc. of Eurocrypt 2004, Springer LNCS Vol. 3027, 506–522 (2004)

[BDH99] D. Boneh, G. Durfee and N. Howgrave-Graham. *Factoring $N = p^r q$ for large r.* Proc. of Crypto'99, Springer LNCS Vol. 1666, 326–337 (1999)

[BF03] D. Boneh and M. Franklin. *Identity based Encryption from the Weil Pairing*. SIAM J. of Computing, 32(3), 586–615 (2003)

[BGW05] D. Boneh, C. Gentry and B. Waters. *Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys.* Proc. of Crypto 2005, Springer LNCS Vol. 3621, 258–275 (2005)

[BGN05] D. Boneh, E.-J. Goh and K. Nissim. *Evaluating 2-DNF Formulas on Ciphertexts*. Proc. of TCC 2005. Springer LNCS Vol. 3378, 325–341 (2005)

[BSW11] D. Boneh, A. Sahai and B. Waters. *Functional Encryption: Definitions and Challenges*. Proc. of TCC 2011, Springer LNCS Vol. 6597, 253–273 (2011)

[BW07] D. Boneh and B. Waters. *Conjunctive, Subset, and Range Queries on Encrypted Data*. Proc. of TCC 2007, Springer LNCS Vol. 4392, 535–554 (2007)

[BGS07] A. Bostan, P. Gaudry and É. Schost. *Linear Recurrences with Polynomial Coefficients and Application to Integer Factorization and Cartier-Manin Operator*. SIAM J. Comput., 36(6), 1777–1806 (2007)

[Boy07] X. Boyen. *Mesh Signatures*. Proc. of Eurocrypt 2007, Springer LNCS Vol. 4515, 210–227 (2007)

[BW06] X. Boyen and B. Waters. *Anonymous Hierarchical Identity-based Encryption (Without Random Oracles)*. Proc. of Crypto 2006, Springer LNCS Vol. 4117, 290–307 (2006)

[BELL10] J. Boxall, N. El Mrabet, F. Laguillaumie and D.-P. Le. *A Variant of Miller's Formula and Algorithm*. Proc. of Pairing 2010, Springer LNCS Vol. 6487, 417–434 (2010)

[BSS02] E. Bresson, J. Stern and M. Szydlo. *Threshold Ring Signatures and Applications to ad-hoc Groups*. Proc. of Crypto 2002, Springer LNCS Vol. 2442, 465–480 (2002)

[Bri89] E.-F. Brickell. *Some Ideal Secret Sharing Schemes*. Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 9, 105–113 (1989)

[BLS11] R. Bröker, K. Lauter and A. V. Sutherland. *Modular polynomials via isogeny volcanoes*. To appear in Math. Comp. (2011)

[BST02] J. Buchmann, K. Sakurai and T. Takagi. *An IND-CCA2 Public-Key Cryptosystem with Fast Decryption*. Proc. of ICISC'01, Springer LNCS Vol. 2288, 51–71 (2002)

[BTV04] J. Buchmann, T. Takagi and U. Vollmer. *Number Field Cryptography*. High Primes & Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, van der Poorten and Stein, eds., vol. 41 of Fields Institute Communications, AMS 111–125 (2004)

[BTW95] J. Buchmann, C. Thiel and H. C. Williams. *Short Representation of Quadratic Integers*. Proc. of CANT'92, Math. Appl. 325, Kluwer Academic Press, 159–185 (1995)

[BV07] J. Buchmann and U. Vollmer. *Binary Quadratic Forms. An Algorithmic Approach*. Springer (2007)

[BW88] J. Buchmann and H. C. Williams. *A Key-Exchange System based on Imaginary Quadratic Fields*. J. Cryptology, 1, 107–118 (1988)

[CKRS09] J. Camenisch, M. Kohlweiss, A. Rial and C. Sheedy. *Blind and Anonymous Identity-based Encryption and Authorised Private Searches on Public Key Encrypted Data*. Proc. of PKC 2009, Spinger LNCS Vol. 5443, 196-214 (2009)

[C+09] S. Canard, C. Delerablée, E. Hufschmitt, A. Gouget, F. Laguillaumie, H. Sibert, J. Traoré and D. Vergnaud. *Fair E-cash: Be Compact, Spend Faster*. Proc. of ISC 2009, Springer LNCS Vol. 5735, 294–309 (2009)

[CDL11] S. Canard, J. Devigne and F. Laguillaumie. *Improving the Security of an Efficient Unidirectional Proxy Re-Encryption Scheme*. Journal of Internet Services and Information Security, Vol. 1(2/3), 140–160 (2011)

[CLM08] S. Canard, F. Laguillaumie, M. Milhau. *Trapdoor Sanitizable Signatures and their Application to Content Protection*. Proc. of ACNS 2008, Springer LNCS Vol. 5037, 256–276 (2008)

[CHK04] R. Canetti, S. Halevi, J. Katz. *Chosen-Ciphertext Security from Identity-based Encryption*. Proc. of Eurocrypt 2004, Springer LNCS Vol. 3027, 207–222 (2004)

[DIP10] A. De Caro, V. Iovino, and G. Persiano. *Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts*. Proc. of Pairing 2010, Springer LNCS Vol. 6487, 347–366 (2010)

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert. *Bonsai Trees, or How to Delegate a Lattice Basis.* Proc. of Eurocrypt 2010, Springer LNCS Vol. 6110, 523–552 (2010)

[Cas06] G. Castagnos. *Quelques schémas de cryptographie asymétrique probabiliste.* Thèse de l'Université de Limoges (2006)

[CJLN09] G. Castagnos, A. Joux, F. Laguillaumie, P. Q. Nguyen. *Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses*. Proc. of Asiacrypt'09. Springer LNCS Vol. 5912, 469-486 (2009)

[CL09] G. Castagnos, F. Laguillaumie. *On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis*. Proc. of Eurocrypt'09. Springer LNCS Vol. 5479, 260-277 (2009)

[CS05] S. Chatterjee and P. Sarkar. *Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model*. Proc. of ICISC 2005, Springer LNCS Vol. 3935, 424–440 (2006)

[CGRW11] K.H.F. Cheng, R.K. Guy, R. Scheidler and H.C. Williams. *Classification And Symmetries Of A Family Of Continued Fractions With Bounded Period Length*. Preprint (2011).

[CW05] K.H.F. Cheng and H.C. Williams. *Some Results Concerning Certain Periodic Continued Fractions.* Acta Arith. 117, 247–264 (2005)

[CN07] L. Cheung and C. Newport. *Provably Secure Ciphertext Policy ABE*. Proc. of ACM-CCS 2007, ACM, 456–465 (2007)

[Chi89] A. L. Chistov. *The complexity of constructing the ring of integers of a global field*. Dolk. Akad. Nauk. SSSR, 306, 1063–1067 (1989). English translation: Soviet. Math. Dolk. 39, 597–600 (1989)

[Coc01] C. Cocks. *An Identity-based Encryption Scheme based on Quadratic Residues*. Proc. of IMA Cryptography and Coding 2001, Springer LNCS Vol. 2260, 360–363 (2001)

[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer (2000)

[CL84] H. Cohen and H.W. Lenstra, Jr. *Heuristics on class groups*. Springer LNM Vol. 1052, 26–36 (1984)

[CHBNW09] C. Costello, H. Hisil, C. Boyd, J. M. G. Nieto and K. K.-H. Wong. *Faster Pairings on Special Weierstrass Curves.* Proc. of Pairing 2009; Springer LNCS Vol. 5671, 89–101 (2009)

[CLN10] C. Costello, T. Lange and M. Naehrig. *Faster Pairing Computations on Curves with High-Degree Twists*. Proc. of PKC 2010, Springer LNCS Vol. 6056, 224–242 (2010)

[Cox99] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons (1999)

[CP01] R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective*. Springer (2001)

[DJ01] I. Damgård and M. J. Jurik. *A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System*, Proc. of PKC' 01, Springer LNCS Vol. 1992, 119–136 (2001)

[DHMR07] V. Daza, J. Herranz, P. Morillo and C. Ràfols. *CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts*. Proc. of ProvSec'07, Springer LNCS Vol. 4784, 35–50 (2007)

[DHMR10] V. Daza, J. Herranz, P. Morillo and C. Ràfols. *Extensions of access structures and their cryptographic applications. Applicable Algebra in Engineering, Communication and Computing*, 21(4), 257–284 (2010)

[DPP07] C. Delerablée, P. Paillier, D. Pointcheval. *Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys*. Proc. of Pairing 2007, Springer LNCS Vol. 4575, 39–59 (2007)

[DP08] C. Delerablée and D. Pointcheval. *Dynamic Threshold Public-Key Encryption*. Proc. of Crypto 2008, Springer LNCS Vol. 5157, 317–334 (2008)

[Duc10] L. Ducas. *Anonymity from Asymmetry: New Constructions for Anonymous HIBE*. Proc. of CT-RSA 2010, Springer LNCS Vol. 5985, 148–164 (2010)

[Elg85] T. Elgamal. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.*, IEEE Transactions on Information Theory, Vol. 31(4), 469–472, (1985)

[EMN09] K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi. *A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length.* Proc. of ISPEC 2009, Springer LNCS Vol. 5451, 13–23 (2009)

[EHM11] A. Escala, J. Herranz and P. Morillo. *Revocable Attribute-based Signatures with Adaptive Security in the Standard Model.* Proc. of Africacrypt 2011, Springer LNCS Vol. 6737, 224–241 (2011)

[GPS08] S. D. Galbraith, K. G. Paterson and N. P. Smart. *Pairings for Cryptographers*. Discrete Applied Mathematics, Vol. 156(16), 3113–3121 (2008)

[Gal06] D. Galindo. *A Separation Between Selective and Full-Identity Security Notions for Identity-based Encryption*. Proc. of ICCSA 2006, Springer LNCS Vol. 3982, 318–326 (2006)

[Gen06] C. Gentry. *Practical Identity-based Encryption Without Random Oracles*. Proc. of Eurocrypt 2006, Springer LNCS Vol. 4004, 445–464 (2006)

[Gjo04] K. Gjøsteen. *Subgroup membership problems and public key cryptosystems*. Ph.D. dissertation, Norwegian University of Science and Technology (2004). Available at http://ntnu.diva-portal.org/smash/get/diva2: 121977/FULLTEXT01

[GM84] S. Goldwasser and S. Micali. *Probabilistic Encryption*. J. Comput. Syst. Sci., Vol. 28(2), 270–299 (1984)

[GJPS08] V. Goyal, A. Jain, O. Pandey, and A. Sahai. *Bounded Ciphertext Policy Attribute-based Encryption*. Proc. of ICALP'08, Springer LNCS Vol. 5126, 579–591 (2008)

[GPSW06] V. Goyal, O. Pandey, A. Sahai and B. Waters. *Attribute-based encryption for fine-grained access control of encrypted data.* Proc. of Computer and Communications Security, CCS'06, ACM, 89–98 (2006)

[GW08] J. E. Gower and S. S. Wagstaff, Jr. *Square form factorization.* Math. Comput. 77(261), 551-588 (2008)

[GS08] J. Groth and A. Sahai. *Efficient Non-Interactive Proof Systems for Bilinear Groups.* Proc. of Eurocrypt 2008, Springer LNCS Vol. 4965, 415–432 (2008)

[Hal05] S. Halevi. *A sufficient condition for key-privacy*. Cryptology ePrint Archive, Report 2005/005 (2005).

[HPT99] M. Hartmann, S. Paulus and T. Takagi. *NICE - New Ideal Coset Encryption*. Proc. of CHES'99, Springer LNCS Vol. 1717, 328–339 (1999)

[HL08] J. Herranz and F. Laguillaumie. *Blind Ring Signatures Secure under the Chosen Target CDH Assumption.* Proc. of ISC 2006, Springer LNCS Vol. 4176, 117–130 (2006)

[HLLR11] J. Herranz, F. Laguillaumie, B. Libert and C. Ràfols. Submitted, `http://hal.archives-ouvertes.fr/hal-00611651/fr/` (2011)

[HLR10] J. Herranz, F. Laguillaumie and C. Ràfols. *Constant Size Ciphertexts in Threshold Attribute-Based Encryption.* Proc. of PKC 2010, Springer LNCS Vol. 6056, 19-34 (2010)

[HLR11] J. Herranz, F. Laguillaumie and C. Ràfols. *Relations between Semantic Security and Anonymity in Identity Based Encryption.* Information Processing Letters, 111(10), 453–460 (2011)

[Hes08] F. Heß. *Pairing Lattices*. Proc. of Pairing 2008, Springer LNCS Vol. 5209, 18–38 (2008)

[HSV06] F. Heß, N. P. Smart and F. Vercauteren. *The Eta Pairing Revisited.* IEEE Transactions on Information Theory 52(10), 4595–4602 (2006)

[Huh00] D. Hühnlein. *Efficient Implementation of Cryptosystems based on Non-Maximal Imaginary Quadratic Orders*. Proc. of SAC'99, Springer LNCS Vol. 1756, 150–167 (2000)

[Huh01] D. Hühnlein. *Faster Generation of NICE-Schnorr-Type Signatures.* Proc. of RSA-CT'01, Springer LNCS Vol. 2020, 1–12 (2001)

[HJPT98] D. Hühnlein, M. Jacobson, Jr., S. Paulus and T. Takagi. *A Cryptosystem Based on Non-Maximal Imaginary Quadratic Orders with Fast Decryption.* Proc. of Eurocrypt'98, Springer LNCS Vol. 1403, 294–307 (1998)

[HM00] D. Hühnlein and J. Merkle. *An Efficient NICE-Schnorr-Type Signature Scheme*. Proc. of PKC'00, Springer LNCS Vol. 1751, 14–27 (2000)

[IJ08] S. Ionica and A. Joux. *Another Approach to Pairing Computation in Edwards Coordinates*. Proc. of Indocrypt 2008, Springer LNCS Vol. 5365, 400–413 (2008)

[IJ10] S. Ionica and A. Joux. *Pairing the Volcano*. Proc. of ANTS-IX, Springer LNCS Vol. 6197, 201–218 (2010)

[JLW95] M. J. Jacobson Jr., R. F. Lukes and H. C. Williams. *An investigation of bounds for the regulator of quadratic fields.* Experimental Mathematics, 4(3), 211–225, 1995

[JSW08] M. J. Jacobson Jr., R. Scheidler and D. Weimer. *An Adaptation of the NICE Cryptosystem to Real Quadratic Orders.* Proc. of Africacrypt'08, Springer LNCS Vol. 5023, 191-208 (2008)

[JJ00] É. Jaulmes and A. Joux. *A NICE Cryptanalysis*. Proc. of Eurocrypt'00, Springer LNCS Vol. 1807, 382–391 (2000)

[Jou00] A. Joux. *A One Round Protocol for Tripartite Diffie-Hellman*. Proc. of ANTS-IV, Springer LNCS Vol. 1838, 385–394 (2000)

[KSW08] J. Katz, A. Sahai and B. Waters. *Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products*. Proc. of Eurocrypt 2008, Springer LNCS Vol. 4965, 146–162 (2008)

[LLQ06] F. Laguillaumie, B. Libert, J.-J. Quisquater. *Universal Designated Verifier Signatures Without Random Oracles or Non Black Box Assumptions*. Proc. of SCN 2006. Springer LNCS Vol. 4116, 63–77 (2006)

[LV05] F. Laguillaumie, D. Vergnaud. *Short Undeniable Signatures Without Random Oracles: the Missing Link*. Proc. of Indocrypt 2005, Springer LNCS Vol. 3797, 283–296 (2005)

[LV10] F. Laguillaumie, D. Vergnaud. *Time-Selective Convertible Undeniable Signatures with Short Conversion Receipts*. Inf. Sci., 180(12), 2458–2475 (2010)

[LPV05] F. Laguillaumie, P. Paillier, D. Vergnaud. *Universally Convertible Directed Signatures*. Proc. of Asiacrypt 2005, Springer LNCS Vol. 3788, 682–701 (2005).

[LO+10] A. Lewko, T. Okamoto, A. Sahai, K. Takashima and B. Waters. *Fully Secure Functional Encryption: Attribute-based Encryption and (Hierarchical) Inner Product Encryption*. Proc. of Eurocrypt 2010, Springer LNCS Vol. 6110, 62–91 (2010)

[LW10] A. B. Lewko and B. Waters. *New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts*. Proc. of TCC 2010, Springer LNCS Vol. 5978, 455–479 (2010)

[L+10] J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren. *Attribute-based Signature and its Applications*. Proc. of *ASIACCS'10*, ACM Press, 60–69 (2010)

[LK10] J. Li and K. Kim. *Hidden Attribute-based Signatures without Anonymity Revocation*. Information Sciences, 180(9), 1681–1689 (2010)

[MTVY11] T. Malkin, I. Teranishi, Y. Vahlis and M. Yung. *Signatures Resilient to Continual Leakage on Memory and Computation*. Proc. of TCC 2011, Springer LNCS Vol. 6597, 89–106 (2011)

[MPR08] H.K. Maji, M. Prabhakaran and M. Rosulek. *Attribute-based Signatures*. Proc. of CT-RSA 2011, Springer LNCS Vol. 6558, 376–392 (2011)

[MKHO09] S. Matsuda, N. Kanayama, F. Heßand E. Okamoto. *Optimised Versions of the Ate and Twisted Ate Pairings*. IEICE Transactions 92-A(7), 1660–1667 (2009)

[McK99] J. McKee. *Speeding Fermat's factoring method*. Math. Comput. 68(228), 1729–1737 (1999)

[Mil07] J. Milan. *Factoring Small Integers: An Experimental Comparison*. INRIA report available at `http://hal.inria.fr/inria-00188645/en/` (2007)

[Mil04] V. S. Miller. *The Weil Pairing, and Its Efficient Calculation*. J. Cryptology 17(4), 235–261 (2004)

[Nac07] D. Naccache. *Secure and* Practical *Identity-based Encryption*. Information Security, IET 1(2), 59–64 (2007)

[NS98] D. Naccache and J. Stern. *A New Public Key Cryptosystem Based on Higher Residues*. Proc. of CCS'98, 546–560 (1998)

[Nao03] M. Naor. *On Cryptographic Assumptions and Challenges*. Proc. of Crypto 2003, Springer LNCS Vol. 2729, 96–109 (2003)

[NV09] *The LLL Algorithm*. P. Q. Nguyen, B. Vallée (Eds.), Springer Series Information Security and Cryptography (2009)

[Oka90] T. Okamoto. *A fast signature scheme based on congruential polynomial operations*. IEEE Transactions on Information Theory 36(1), 47–53 (1990)

[OT08] T. Okamoto and K. Takashima. *Homomorphic Encryption and Signatures from Vector Decomposition*. Proc. of Pairing 2008, Springer LNCS Vol. 5209, 57–74 (2008)

[OT11] T. Okamoto and K. Takashima. *Efficient Attribute-based Signatures for Non-Monotone Predicates in the Standard Model*. Proc. of PKC 2011, Springer LNCS Vol. 6571, 35–52 (2011)

[OU98] T. Okamoto and S. Uchiyama. *A New Public-Key Cryptosystem as Secure as Factoring*. Proc. of Eurocrypt'98, Springer LNCS Vol. 1403, 308–318 (1998)

[Pai99] P. Paillier. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*. Proc. of Eurocrypt'99, Springer LNCS Vol. 1592, 223–238 (1999)

[PT99] S. Paulus and T. Takagi. *A generalization of the Diffie-Hellman problem and related cryptosystems allowing fast decryption*. Proc. of ICISC'98, 211–220 (1999)

[PT00] S. Paulus and T. Takagi. *A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time*. J. Cryptology, 13(2), 263–272 (2000)

[Per01] R. Peralta. *Elliptic curve factorization using a "partially oblivious" function*. Cryptography and computational number theory, Progr. Comput. Sci. Appl. Logic. 20. Birkhäuser, 123–128 (2001).

[PO96] R. Peralta and E. Okamoto. *Faster Factoring of Integers of a Special Form*. IEICE Trans. Fundamentals, E79-A, 4, 489–493 (1996).

[RSA78] R. Rivest, A. Shamir, L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Comm. ACM, Vol. 21 (2), 120–126 (1978)

[RST01] R. L. Rivest, A. Shamir and Y. Tauman. *How to Leak a Secret*. Proc. of Asiacrypt 2001, Springer LNCS Vol. 2248, 552–565 (2001)

[SW05] A. Sahai and B. Waters. *Fuzzy Identity-based Encryption*. Proc. of Eurocrypt 2005, Springer LNCS Vol. 3494, 457–473 (2005)

[Sch82] R. Schoof. *Quadratic fields and factorization*. Computational Methods in Number Theory, MC-Tracts 154/155, 235–286 (1982)

[SKOS09] J. H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki. *Anonymous Hierarchical Identity-based Encryption with Constant Size Ciphertexts*. Proc. of PKC 2009, Spinger LNCS Vol. 5443, 215–234 (2009)

[SS09] S.F. Shahandashti and R. Safavi-Naini. *Threshold Attribute-based Signatures and their Application to Anonymous Credential Systems*. Proc. of Africacrypt 2009, Springer LNCS Vol. 5580, 198–216 (2009)

[Sha84] A. Shamir. *Identity-Based Cryptosystems and Signature Schemes*. Proc. of Crypto 1984, Springer LNCS Vol. 196, 47–53 (1984)

[Ver09] F. Vercauteren. *Optimal Pairings*. IEEE Transactions of Information Theory 56(1), 455–461 (2009)

[Tak98] T. Takagi. *Fast RSA-Type Cryptosystem Modulo $p^k q$*. Proc. of Crypto'98, Springer LNCS Vol. 1462, 318–326 (1998)

[Tas07] T. Tassa. *Hierarchical Threshold Secret Sharing*. J. Cryptology, 20(2), 237–264 (2007)

[Wat05] B. Waters. *Efficient Identity-Based Encryption Without Random Oracles*. Proc. of Eurocrypt 2005, Springer LNCS Vol. 3494, 114–127 (2005)

[Wat09] B. Waters. *Dual System Encryption: Realizing Fully Secure IBE And HIBE under Simple Assumptions*. Proc. of Crypto 2009, Springer LNCS Vol. 5677, 619–636 (2009)

[Wat11] B. Waters. *Ciphertext-Policy Attribute-based Encryption: an Expressive, Efficient, and Provably Secure Realization*. Proc. of PKC 2011, Springer LNCS Vol. 6571, 53–70 (2011)

[Wei04] D. Weimer. *An Adaptation of the NICE Cryptosystem to Real Quadratic Orders.* Master's thesis, Technische Universität Darmstadt (2004)