Secure Outsourcing in Discrete-Logarithm-Based and Pairing-Based Cryptography (Invited Talk)

Damien Vergnaud

Secure Outsourcing in Discrete-Logarithm-Based and Pairing-Based Cryptography (Invited Talk)

Damien Vergnaud[1,2]

[1] Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6
LIP6, Paris, France
[2] Institut Universitaire de France

Abstract. Cryptographic operations are performed everywhere, from standard laptop to smart cards. Some devices computational resources can be very limited and it is natural to delegate costly operations to another device capable of carrying out cryptographic algorithms. In this setting, it is obviously important to ensure the limited device that the computation is carried out correctly and that the powerful device does not learn anything about what is actually computing (including the secret inputs and outputs). We briefly review the recent advances on secure outsourcing of group exponentiation (in groups of known prime order as well as in groups of unknown order) and pairing computation.

1 Introduction

Many widely used public-key cryptographic systems and protocols relies on the (supposed) computational hardness of the discrete-logarithm or the discrete-root problems. The core operation of these cryptosystems is group exponentiation in a finite Abelian group, i.e., computing u^a from a group element u and an exponent a. Besides, since their introduction in cryptography [15, 4], *pairings* proved to be an amazingly flexible and useful tool for the construction of cryptosystems with unique features (*e.g.* efficient identity based cryptography [4]). In this setting, the core operation is the computation of pairings which is the most expensive operation in pairing-based cryptographic protocols.

We consider the problem of "outsourcing" group exponentiation and pairing computation from a weak computational device to a more powerful one. Indeed, some devices computational resources can be very limited and it is natural, as most of the devices are online or directly connected to a powerful device (like a SIM card in a smart phone) to securely delegate sensitive and costly operations to a device capable of carrying out cryptographic algorithms. Outsourcing cryptographic computations is a classical problem which was formalized in [13] by Hohenberger and Lysyanskaya. In this scenario, the powerful device[1] can, po-

[1] Hohenberger and Lysyanskaya also considered delegation protocols to two devices that are physically separated (and do not communicate) that achieve security as long as one of them is honest. Since this separation of the two devices is a strong assumption hard to be met in practice, we consider only protocols to outsource cryptographic operations to a *single* untrusted server.

tentially, be operated by a malicious adversary and it is obviously important to ensure the limited device that the computation is carried out correctly and that the powerful device does not learn anything about what is actually computing (including the secret inputs and outputs).

2 Group Exponentiation

In the last 30 years, the question of how a computationally limited device may outsource group exponentiation to another, potentially malicious, but much more computationally powerful device has been a very active research topic (*e.g.* [18, 17, 3, 26, 6, 7]). Many solutions have been proposed and then cryptanalyzed in follow-up papers (*e.g.* [23, 21, 24, 14, 22, 7]). We briefly review the recent advances on secure outsourcing of group exponentiation.

Recently, Chevalier, Laguillaumie and Vergnaud [7] proposed a taxonomy of private exponentiation delegation protocols (to a single untrusted computational resource) in groups of *known prime* order. Their taxonomy covers all the practical situations: the group element u can be secret or public, variable or fixed, the exponent a can be secret or public, and the result of the exponentiation u^a can also be either public or secret. They provided simple constructions in all different settings and proved that these protocols cannot be significantly improved if one wants to use a single untrusted computational resource and to limit the computational cost of the delegating device to a small number of (generic) group operations. Aguilar-Melchor, Deneuville, Gaborit, Lepoint and Ricosset later showed [1] that using homomorphic encryption, it is sometimes possible to reduce the computational costs for privately delegating elliptic-curve operations (but at the cost of a very large communication complexity).

Another important use case is the setting of RSA exponentiation: a device wants to delegate the computation of a signature given a public key (N, e), a public message (or hash value of a message) m and the secret signing exponent d. By outsourcing some exponentiations to a powerful device, the delegation protocol outputs a (public) signature $\sigma = m^d \bmod N$. Most proposed protocols are variants of two protocols (named RSA-S1 and RSA-S2) that were proposed by Matsumoto, Kato and Imai in 1988 [18]. Both schemes use a random linear decomposition of the RSA private exponent d. Several attacks were proposed on the protocols RSA-S1 and its variants (*e.g.* [23]). Recently, Mefenza and Vergnaud [19] proposed an improved lattice-based attack on RSA-S1 and a simple variant of this protocol that provides better efficiency for the same security level. They also presented the first attacks on the protocol RSA-S2.

A cryptographic delegation protocol that does not ensure verifiability may cause severe security problems (in particular if the computation occurs in the verification algorithm of some authentication protocol). Di Crescenzo, Khodjaeva, Kahrobaei and Shpilrain [10] proposed recently private and verifiable protocols in a large class of cyclic groups. In the presented protocols, the probability that a cheating server convinces the client of an incorrect computation result can

be proved to be exponentially small (whereas previous best results could only achieve a constant probability). Their protocols need some pre-computation depending on the base u and cannot be used easily in practice if this group element is variable. The different proposals for verifiable group exponentiation where pre-computation does not depend on the base u are very inefficient and it is actually better in practice to directly perform the computation on the restricted device rather than using these solutions. A challenging problem is to study secure and verifiable outsourcing protocols for group exponentiation that covers all the practical situations as in [7].

3 Pairings

Pairings (or bilinear maps) were introduced in cryptography in 2000 by Joux [15] and Boneh-Franklin [4]. A pairing is a bilinear, non-degenerate and computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where, in practice, $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups (of prime-order r) of the group of points of an elliptic curve defined over a finite field $\mathbb{F}_q$ and some finite field extension $\mathbb{F}_{q^k}$ (respectively) and the so-called *target* group $\mathbb{G}_T$ is the order r subgroup of $\mathbb{F}_{q^k}$. The pairing computation is more resource consuming compared to a scalar multiplication on the elliptic curve $E(\mathbb{F}_q)$.

In 2005, Girault and Lefranc [11] introduced the first secure pairing delegation protocol via the notion of *Server-Aided Verification*, which consists in speeding up the verification step of an authentication/signature scheme. Chevallier-Mames, Coron, McCullagh, Naccache and Scott [8, 9] introduced the security notions of verifiable pairing delegation protocol and proposed the first verifiable pairing delegation protocol. Later in 2014, Canard, Devigne and Sanders [5] improved their construction and proposed a much more efficient verifiable delegation protocol. Canard, Devigne and Sanders showed that their construction is more efficient for the client than computing a pairing himself on the so-called KSS-18 curve [16]. Later, Guillevic and Vergnaud [12] showed that Canard, Devigne and Sanders protocol is actually less efficient than computing a pairing for the state-of-the-art optimal Ate pairing on a Barreto-Naehrig curve [2] and it remains open to propose an efficient verifiable delegation protocol for pairing computation on these curves.

Due to the inefficiency of the known protocols for delegation of a unique pairing, another approach is to propose efficient protocols when the client wants to compute several pairings at the same time. In 2007, Tsang, Chow and Smith [25] introduced the security notion of *batch* pairing delegation protocols and propose the first verifiable batch pairing delegation protocols when the client wants to compute several pairings $e(P_i, Q_i)$ where $P_i \in \mathbb{G}_1$ and $Q_i \in \mathbb{G}_2$ for $i \in \{1, \ldots, n\}$ and $n \geq 2$. In [20], Mefenza and Vergnaud recently proposed four new efficient batch pairing delegation protocols in different settings but it remains open to construct a generic verifiable batch pairing delegation protocol when both inputs of the pairing are variable and secret. Another interesting open problem is to provide lower bounds on the efficiency of verifiable pairing delegation protocols (as it was done in [7] for private delegation of group exponentiation).

Acknowledgments. The author would like to thank his co-authors on this active and interesting research area: Céline Chevalier, Aurore Guillevic, Fabien Laguillaumie and Thierry Mefenza. The author is supported in part by the French ANR ALAMBIC project (ANR16-CE39-0006) and the French ANR IDFIX project (ANR-16-CE39-0004).

References

1. Carlos Aguilar Melchor, Jean-Christophe Deneuville, Philippe Gaborit, Tancrède Lepoint, and Thomas Ricosset. Delegating elliptic-curve operations with homomorphic encryption. In *2018 IEEE Conference on Communications and Network Security, CNS 2018*, pages 1–9. IEEE, 2018.
2. Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Heidelberg, August 2006.
3. Philippe Béguin and Jean-Jacques Quisquater. Fast server-aided RSA signatures secure against active attacks. In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 57–69. Springer, Heidelberg, August 1995.
4. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, August 2001.
5. Sébastien Canard, Julien Devigne, and Olivier Sanders. Delegating a pairing can be both secure and efficient. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *ACNS 14*, volume 8479 of *LNCS*, pages 549–565. Springer, Heidelberg, June 2014.
6. Bren Cavallo, Giovanni Di Crescenzo, Delaram Kahrobaei, and Vladimir Shpilrain. Efficient and secure delegation of group exponentiation to a single server. In Stefan Mangard and Patrick Schaumont, editors, *RFIDsec 2015*, volume 9440 of *LNCS*, pages 156–173. Springer, 2015.
7. Céline Chevalier, Fabien Laguillaumie, and Damien Vergnaud. Privately outsourcing exponentiation to a single server: Cryptanalysis and optimal constructions. In Ioannis G. Askoxylakis, Sotiris Ioannidis, Sokratis K. Katsikas, and Catherine A. Meadows, editors, *ESORICS 2016, Part I*, volume 9878 of *LNCS*, pages 261–278. Springer, Heidelberg, September 2016.
8. Benoît Chevallier-Mames, Jean-Sébastien Coron, Noel McCullagh, David Naccache, and Michael Scott. Secure delegation of elliptic-curve pairing. Cryptology ePrint Archive, Report 2005/150, 2005. `http://eprint.iacr.org/2005/150`.
9. Benoît Chevallier-Mames, Jean-Sébastien Coron, Noel McCullagh, David Naccache, and Michael Scott. Secure delegation of elliptic-curve pairing. In Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors, *CARDIS 2010*, *LNCS*, pages 24–35. Springer, 2010.
10. Giovanni Di Crescenzo, Matluba Khodjaeva, Delaram Kahrobaei, and Vladimir Shpilrain. Practical and secure outsourcing of discrete log group exponentiation to a single malicious server. In Bhavani M. Thuraisingham, Ghassan Karame, and Angelos Stavrou, editors, *CCSW@CCS 2017, Dallas, TX, USA, November 3, 2017*, pages 17–28. ACM, 2017.
11. Marc Girault and David Lefranc. Server-aided verification: Theory and practice. In Bimal K. Roy, editor, *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 605–623. Springer, Heidelberg, December 2005.

12. Aurore Guillevic and Damien Vergnaud. Algorithms for outsourcing pairing computation. In Marc Joye and Amir Moradi, editors, *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*, volume 8968 of *Lecture Notes in Computer Science*, pages 193–211. Springer, 2014.
13. Susan Hohenberger and Anna Lysyanskaya. How to securely outsource cryptographic computations. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 264–282. Springer, Heidelberg, February 2005.
14. Markus Jakobsson and Susanne Wetzel. Secure server-aided signature generation. In Kwangjo Kim, editor, *PKC 2001*, volume 1992 of *LNCS*, pages 383–401. Springer, Heidelberg, February 2001.
15. Antoine Joux. A one round protocol for tripartite diffie-hellman. In *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, pages 385–394, 2000.
16. Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 126–135. Springer, Heidelberg, September 2008.
17. Chi-Sung Laih, Sung-Ming Yen, and Lein Harn. Two efficient server-aided secret computation protocols based on the addition sequence. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *ASIACRYPT'91*, volume 739 of *LNCS*, pages 450–459. Springer, Heidelberg, November 1993.
18. Tsutomu Matsumoto, Koki Kato, and Hideki Imai. Speeding up secret computations with insecure auxiliary devices. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 497–506. Springer, Heidelberg, August 1990.
19. Thierry Mefenza and Damien Vergnaud. Cryptanalysis of server-aided RSA protocols with private-key splitting. in submission, 2017.
20. Thierry Mefenza and Damien Vergnaud. Verifiable outsourcing of pairing computations. in submission, 2018.
21. Johannes Merkle. Multi-round passive attacks on server-aided RSA protocols. In S. Jajodia and P. Samarati, editors, *ACM CCS 00*, pages 102–107. ACM Press, November 2000.
22. Johannes Merkle and Ralph Werchner. On the security of server-aided RSA protocols. In Hideki Imai and Yuliang Zheng, editors, *PKC'98*, volume 1431 of *LNCS*, pages 99–116. Springer, Heidelberg, February 1998.
23. Phong Q. Nguyen and Igor Shparlinski. On the insecurity of a server-aided RSA protocol. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 21–35. Springer, Heidelberg, December 2001.
24. Birgit Pfitzmann and Michael Waidner. Attacks on protocols for server-aided RSA computation. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 153–162. Springer, Heidelberg, May 1993.
25. Patrick P. Tsang, Sherman S. M. Chow, and Sean W. Smith. Batch pairing delegation. In Atsuko Miyaji, Hiroaki Kikuchi, and Kai Rannenberg, editors, *IWSEC 07*, volume 4752 of *LNCS*, pages 74–90. Springer, Heidelberg, October 2007.
26. Yujue Wang, Qianhong Wu, Duncan S. Wong, Bo Qin, Sherman S. M. Chow, Zhen Liu, and Xiao Tan. Securely outsourcing exponentiations with single untrusted program for cloud storage. In Miroslaw Kutylowski and Jaideep Vaidya, editors, *ESORICS 2014, Part I*, volume 8712 of *LNCS*, pages 326–343. Springer, Heidelberg, September 2014.