The simple roots problem

Dominic Bucerzan, Vlad Dragoi, Tania Richmond

THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

THE SIMPLE ROOTS PROBLEM

Dominic Bucerzan*, Vlad Dragoi**, Tania Richmond***

*Aurel Vlaicu University of Arad Department of Mathematics and Computer Science Romania, 310330 Arad, Elena Dragoi, 2
** Laboratoire LITIS - EA 4108 Université de Rouen Normandie - UFR Sciences et Techniques, 76800 Saint Etienne du Rouvray, France
*** Laboratoire IMATH, EA 2134, Avenue de lUniversité , BP 20132, 83957 La Garde Cedex, France
Corresponding author: Xxxx XXXXXXXX, E-mail: xxxx@xxxx.xxx

Abstract: The simple roots problem is a natural question related to the structure of the error locator polynomial, which is one of the key objects in the decoding algorithms for Alternant codes. Finding the roots of this polynomial enables the error positions and thus the decoding solution for this family of codes. Hence, we propose here to study the structure of the error locator polynomial, denoted $\sigma(x)$. We prove that when the degree of $\sigma(x)$ is sub-linear in the length of the code, the probability that all the coefficients of $\sigma(x)$ are different from zero is extremely high.
Key words: The simple roots problem, Goppa codes, McEliece scheme.

1 Introduction

Finding a practical solution for quantum resistant cryptography became an urgent issue, due to two major facts: firstly the existence of a quantum polynomial time algorithm [Sho94] that breaks the actual RSA and ECC solutions and secondly the improvements of classical algorithms against discrete logarithm in small characteristic [BGJT14]. NIST's [1] appeal for post-quantum cryptography is one among many recent initiatives to find alternative solutions. In the cryptographic community, quantum resistant schemes is probably one of the hottest topics these days and that is one of the reasons many scientific projects and conferences started to integrate this field in their program.

Code-based cryptography is a promising solutions for post-quantum cryptography [BBD09]. It is also the oldest quantum resistant public key encryption schemes thanks to McEliece's idea [McE78] to use a family of error correcting codes that admits an efficient decoding algorithm. In the original paper, McEliece proposed to use binary Goppa codes, which are still unbroken up to nowadays. Other families of algebraic codes were proposed like Generalized Reed-Solomon (GRS) code [Nie86], Reed-Muller (RM) codes [Sid94], algebraic geometry (AG) codes [JM96], Polar codes

[1] http://csrc.nist.gov/groups/ST/post-quantum-crypto/

[SK14, HSEA14] etc. But they were successfully cryptanalyzed, mainly due to their algebraic structure (GRS - [SS92], RM - [MS07], AG - [CMCP14], Polar - [BCD$^+$16]). Another promising family of codes is the QC-MDPC variant [MTSB13], mainly due to the "random"-like structure of the codes. Nonetheless, this scheme is quite recent and needs a bit more of comprehension and analysis, fact that is mentioned in [BDLO16] where the author's exhibit the existence of weak keys.

The original McEliece scheme is one of the most studied variant. Despite their well known structure there are no efficient key recovery or decoding attacks against binary irreducible Goppa codes. A distinguisher exists in the case of high rate Goppa codes [FGO$^+$13]. But despite of this potential vulnerability there is no efficient algorithm for the moment exploiting the knowledge and properties of this distinguisher. This family of codes was also the most cryptanalyzed scheme from side-channel perspective. There are mainly two types of side-channel attacks classified by their goal:

1. Recover the secret message [STM$^+$08, AHPT11, MSSS11, Str11];
2. Recover the private key (fully or partially) [SSMS09, HMP10, Str10, Str13, PRD$^+$15, PRD$^+$16, BCDR16].

In each paper, authors propose to counter the leak and thus step towards a secure implementation of the scheme. Countermeasures and secured implementations are also proposed in [CHP12, DCCR13, BCS13]. In several articles the weakness comes from the *error locator polynomial* which is mainly used by all the decoders for the Alternant codes. Hence understanding the structure of this polynomial is a crucial step for securing the McEliece cryptosystem. Our goal here is to study the error locator polynomial, from a practical point of view in timing attacks context and from a theorical point of view as a mathematical problem.

Our contribution is to study the error locator polynomial. We analyze the probability that the aforementioned polynomial is rather dense or sparse. We formally define the *simple roots problem* that is the probability that a simple roots polynomial defined over an extension field of $\mathbb{F}_2$ has all coefficients different from zero. This paper is a natural extension of the work done in [DCCR13, Ric16] and hence our work completes this topic by answering the remaining questions and proposing an asymptotic analysis of the results.

For that we give a simple formula for the first elementary symmetric function and compare the case of dependent variables with the independent case. Moreover, we provide asymptotic analysis for the usual cryptographic scenario, namely the Hamming weight of the error, is sub-linear in the code length. We prove that when $t = o(2^m)$ with $m \to \infty$, the probability that a simple roots polynomial of degree t over $\mathbb{F}_{2^m}$ has only non zero coefficients equals $1 - ct/n + O(t^2/n^2)$, where c is a constant that we compute. Even thought our results are really sharp in the sub-linear case ($t = o(2^m)$), they need improvement for the linear case.

Regardless of the impact of our results in cryptography, it represents in itself an application in the field of discrete probability and enumerative combinatorics. On the other hand for the asymptotic behavior we notice that other techniques inspired by the work of Flajolet et Sedgewick in the field of asymptotic combinatorics [FS09] might be alternative solutions to the study of such objects. It would also be interesting to see whether closed formulae exist for the distribution of the rest of the coefficient, not only the roots sum.

Another remark is that our results might also be seen from a geometric point of view. Indeed, each symmetric function that equals to zero can be seen as an hypersurface since it is the solution to an algebraic equation in t unknowns over an extension field of $\mathbb{F}_2$. Thus it becomes a classical geometry problem of estimating the number of points on a curve from which asymptotics might be deduced. Nonetheless, estimating the number of points in the intersections of two surfaces seems rather difficult to compute, for which our technique is able to give a solution to this question.

2 Background

Since the background on coding theory is not really relevant for understanding the results and the motivation in our work, we only give some details concerning the original McEliece scheme and binary Goppa codes. Nevertheless we address interested readers in coding theory to [MS86].

2.1 Goppa codes

Definition 2.1 (Binary Goppa code)**.** *Let $g(x)$ be a polynomial over $\mathbb{F}_{2^m}[x]$ with $\deg(g) = t$ and $\mathcal{L} = \{\alpha_1, \alpha_1, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_{2^m}$ s.t. $g(\alpha_i) \neq 0$.*

We define the syndrome polynomial associated to any vector $c \in \mathbb{F}_2^n$ by $\mathcal{S}_c(x) = \sum_{i=1}^{n} \frac{c_i}{x \oplus \alpha_i}$.

Now given $g(x), \mathcal{L}$ and $\mathcal{S}_c(x)$ the binary Goppa code is defined as:

$$\mathbf{\Gamma}(\mathcal{L}, g) = \{c \in \mathbb{F}_2^n \mid \mathcal{S}_c(x) \equiv 0 \mod g(x)\}.$$

Among the most important properties that a Goppa code satisfies we recall the followings.

Proposition 2.2 ([MS86])**.** *A Goppa code $\mathbf{\Gamma}(\mathcal{L}, g)$ is a linear code over $\mathbb{F}_2$. Its length is given by $n = |\mathcal{L}|$, its dimension is $k \geq n - mt$, where $t = \deg(g)$ and its minimun distance $d \geq t + 1$. The syndrome polynomial $\mathcal{S}_c(x)$ satisfies the following property:*

$$\mathcal{S}_c(x) = \frac{\omega(x)}{\sigma(x)} \mod g(x),$$

where $\sigma(x) = \prod_{i=1}^{t}(x \oplus a_i)$ is called the error locator polynomial (ELP) and the elements $a_i \in \mathcal{L}$, $\forall i \in \{1, \ldots, t\}$, are the error positions.

Alternant decoders For the (irreducible) binary Goppa codes, we can use (at least) three different decoding algorithms, namely the extended Euclidean algorithm (EEA), the Berlekamp-Massey algorithm and the Patterson algorithm. The *Extended Euclidean Algorithm (EEA)* can correct up to $\frac{t}{2}$ errors. The error-correction capacity can be increased up to t errors for irreducible binary Goppa codes by using the syndrome associated to g^2 instead of g. Unfortunately, the corresponding parity-check matrix has twice more rows. The *Berlekamp-Massey algorithm (BMA)* has to use g^2, similarly to the EEA, in order to decode up to t errors. The advantage of this algorithm is that it is not vulnerable to several existing timing attacks and it allows a fast and constant-time computation [BCS13]. *The Patterson algorithm* offers another solution for the syndrome decoding. The decryption described in [Pat75] permits to correct up to t errors by using the syndrome associated to g (and not to g^2). That leads to smaller keys to correct the same amount of errors than EEA or BMA with g^2.

2.2 The McEliece Cryptosystem

The McEliece public key encryption scheme [McE78] is composed of three algorithms: *key generation* (KeyGen), *encryption* (Encrypt) and *decryption* (Decrypt).

The first step is the key generation algorithm, see Figure 1. It takes as inputs the integers n, k, t such that $k < n$ and $t < n$, and outputs the public key/private key pair $(\mathsf{pk}, \mathsf{sk})$. In order to encrypt a message $\boldsymbol{m} \in \mathbb{F}_2^k$ one applies the $\mathsf{Encrypt}(\boldsymbol{m}, \mathsf{pk})$ function, see Figure 2. The last step is the decryption function, see Figure 3. It takes as input a ciphertext $\boldsymbol{z}$ and the private key sk, and outputs the corresponding message $\boldsymbol{m}$.

1. Pick a generator matrix $\boldsymbol{G}$ of a $[n,k]$-binary Goppa code $\boldsymbol{\Gamma}(\mathcal{L},g)$ that can corrects up to t errors.
2. Randomly pick a $(k\times k)$-invertible matrix $\boldsymbol{S}$ and a $(n\times n)$-permutation matrix $\boldsymbol{P}$.
3. Compute $\boldsymbol{G}_{\text{pub}} \stackrel{\text{def}}{=} \boldsymbol{SGP}$.
4. Return
$$\mathsf{pk} = (\boldsymbol{G}_{\text{pub}}, t) \text{ and } \mathsf{sk} = (\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P}).$$

Figure 1: The Key Generation function of the original McEliece scheme - $\mathsf{KeyGen}(n,k,t) = (\mathsf{pk},\mathsf{sk})$

1. Generate a random error-vector $\boldsymbol{e}\in\mathbb{F}_2^n$ of Hamming weight $\mathsf{wt}(\boldsymbol{e})\leq t$.
2. Return $\boldsymbol{z} = \boldsymbol{m}\boldsymbol{G}_{\text{pub}} \oplus \boldsymbol{e}$.

Figure 2: The Encryption function of the original McEliece scheme - $\mathsf{Encrypt}(\boldsymbol{m},\mathsf{pk}) = \boldsymbol{z}$

1. Compute a parity-check matrix $\boldsymbol{H}$ of $\boldsymbol{\Gamma}(\mathcal{L},g)$ thanks to $\boldsymbol{G}$.
2. Compute $\boldsymbol{z}^* = \boldsymbol{z}\boldsymbol{P}^{-1}$ and $\boldsymbol{m}^* = \mathcal{D}ecode(\boldsymbol{z}^*,\boldsymbol{H})$.
3. Return $\boldsymbol{m}^*\boldsymbol{S}^{-1}$.

Figure 3: The Decryption function of the original McEliece scheme - $\mathsf{Decrypt}(\boldsymbol{z},\mathsf{sk}) = \boldsymbol{m}$

Here $\mathcal{D}ecode(.,.)$ is an efficient decoding algorithm for $\boldsymbol{\Gamma}(\mathcal{L},g)$. Notice that multiplying the error vector by a permutation does not change the weight of the vector. One can easily verify the correctness of the scheme by checking

$$\mathsf{Decrypt}(\mathsf{Encrypt}(\boldsymbol{m},\mathsf{pk}),\mathsf{sk}) = \boldsymbol{m}.$$

1. Compute the syndrome polynomial of $\boldsymbol{z}^*$ using the parity-check matrix $\boldsymbol{H}$.
2. Solve the so-called key-equation $\mathcal{S}_{\boldsymbol{z}^*}(x) = \frac{\omega(x)}{\sigma(x)} \mod g(x)$ to find $\sigma(x)$.
3. Find all roots of $\sigma(x)$ by evaluating it over $\mathcal{L}$.
4. Correct $\boldsymbol{z}^*$ to the codeword $\boldsymbol{z}^* + \boldsymbol{e}\boldsymbol{P}^{-1}$.
5. Return $\boldsymbol{m}^* = \boldsymbol{m}\boldsymbol{S}$.

Figure 4: The Decode function in the McEliece decryption - $\mathcal{D}ecode(\boldsymbol{z}^*,\boldsymbol{H}) = \boldsymbol{m}^*$

By looking inside the $\mathcal{D}ecode(.,.)$ function, described in Figure 4, we can easily notice that the evaluation of the error locator polynomial (step 3) is not depending on the decoder chosen to solve the key-equation (step 2, see Alternant decoders in Subsection 2.1). That is why we analyze the structure of the error locator polynomial and how it can influence the evualation of this polynomial. We call that the simple roots problem because by definition the error locator polynomial has only simple roots over $\mathcal{L}\subseteq\mathbb{F}_{2^m}$.

3 The simple roots problem

3.1 Preliminaries

Definition 3.1. *Let t and m be two strictly positive integers and $n \stackrel{def}{=} 2^m$. Let $\mathbb{A}_t \stackrel{def}{=} \{(\alpha_1,\ldots,\alpha_t)\in (\mathbb{F}_{2^m})^t \,:\, 1\leq i<j\leq t, \alpha_i\neq\alpha_j\}$ be the set of t-tuples with pairwise distinct elements.*

- *Let $(a_1, \ldots, a_t)$ be a random uniform variable defined over $\mathbb{A}_t$ with*

$$\mathsf{prob}((a_1, \ldots, a_t) = (\alpha_1, \ldots, \alpha_t)) = 1/\left|\mathbb{A}_t\right|,$$

where $|\mathbb{A}_t| = n(n-1)\ldots(n-t+1)$ is known as the number of "arrangements" or the number of injections from $\{1, 2, \ldots, t\}$ to $\{1, 2, \ldots, n\}$.

- *We define the random variables $S_{k,t}$ over $\mathbb{F}_{2^m}$ such that*

$$S_{k,t} \stackrel{def}{=} \begin{cases} 1 & , \quad k = 0 \\ \sum\limits_{1 \le j_1 < j_2 < \cdots < j_k \le t} a_{j_1} \ldots a_{j_k} & , \quad 1 \le k \le t \\ 0 & , \quad k > t \end{cases}$$

The $S_{k,t}$ are the so-called elementary symmetric functions.

- *We define the simple roots polynomial as*

$$\sigma(x) \stackrel{def}{=} \prod_{i=1}^{t}(x \oplus a_i) \stackrel{def}{=} \sum_{i=0}^{\infty} S_{i,t} x^{t-i}.$$

Definition 3.2 (The simple roots problem)**.** *Let m and t be two integers and $\sigma(x)$ be a simple roots polynomial with coefficient $S_{k,t}$ as defined in Definition 3.1.*

The simple roots problem *is then defined as the probability that all the coefficients of $\sigma(x)$ are different from zero, namely:*

$$\mathrm{SRP}(\mathbb{F}_2, m, t) \stackrel{def}{=} \mathsf{prob}(\forall\ 1 \le k \le t,\ S_{k,t} \neq 0).$$

Remark 3.3. *This model is known in the literature as a urn process without replacement. Indeed we remark that sampling a random uniform variable $(a_1, \ldots, a_t)$ from the set $\mathbb{A}_t$ is equivalent to sampling t random dependent uniform variables from $\mathbb{F}_{2^m}$. For example $S_{1,t} \stackrel{def}{=} a_1 + \ldots a_t$ is the sum of t dependent uniform random variables over $\mathbb{F}_{2^m}$.*
When we consider independent random uniform variables over $(\mathbb{F}_{2^m})^t$ we will use the usual notation, namely $(u_1, \ldots, u_t)$ where

$$\forall(\alpha_1, \ldots, \alpha_t) \in (\mathbb{F}_{2^m})^t, \quad \mathsf{prob}((u_1, \ldots, u_t) = (\alpha_1, \ldots, \alpha_t)) = 1/n^t.$$

Furthermore we recall some known properties from the urn process models. The next proposition is a direct consequence of [Ric16, Theorem 8.2].

Proposition 3.4. *Let $(a_1, \ldots, a_t)$ be a random uniform variable defined over $\mathbb{A}_t$ and $(\alpha_1, \ldots, \alpha_t) \in \mathbb{A}_t$. Then we have that $(a_1, \ldots, a_t)$ is exchangeable:*

$$\forall \pi \in \mathfrak{S}_t \quad , \quad \mathsf{prob}((a_1, \ldots, a_t) = (\alpha_1, \ldots, \alpha_t)) = \mathsf{prob}((a_{\pi(1)}, \ldots, a_{\pi(t)}) = (\alpha_1, \ldots, \alpha_t)).$$

Furthermore we deduce Corollary 3.5 and a more general case in Corollary 3.6.

Corollary 3.5. *Let $(a_1, \ldots, a_t)$ be a random uniform variable defined over $\mathbb{A}_t$ and $\alpha \in \mathbb{F}_{2^m}$. Then we have that*

$$\forall 1 \le k \le t\ ,\ \mathsf{prob}(a_k = \alpha) = \mathsf{prob}(a_1 = \alpha) = 1/n,$$

which is exactly the probability $\mathsf{prob}(u_k = \alpha)$. So the probability of extracting α at the k^{th} position is given regardless of the independence condition.

Corollary 3.6. *Let $(a_1, \ldots, a_t)$ be a random uniform variable defined over $\mathbb{A}_t$ and X be a random variable defined over $\mathbb{F}_{2^m}$ as a function $X \stackrel{def}{=} f(a_1, \ldots, a_t)$ that is symmetric in all the variables, more exactly X satisfies the condition: for any $\pi \in \mathfrak{S}_t$, $f(a_1, \ldots, a_t) = f(a_{\pi(1)} \ldots, a_{\pi(t)})$.*
Then we have that

$$\forall 1 \le i < j \le t\ ,\ \mathsf{prob}(a_i = X) = \mathsf{prob}(a_j = X).$$

3.2 General properties

From this subsection we consider that $m \geq 2$ and $t \geq 3$. In the Appendix (Remark 5) we give the results in the case of $1 \leq t \leq 3$. Many properties that we give here can be found in [Ric16].

Notation 3.7. *We denote by* $A_t^* \stackrel{def}{=} A_t \cap (\mathbb{F}_{2^m}^*)^t$ *the set of* t*-tuples with pairwise distinct elements that are different from zero and for any* $1 \leq k \leq t$ *denote by* $S_{k,t}^*$ *the restriction of* $S_{k,t}$ *to* A_t^*.

Let t_1 *and* t_2 *denote two strictly positive integers. Then for any* k *and* i *such that* $1 \leq k \leq t_1$ *and* $1 \leq i \leq t_2$ *we denote*

$$\begin{array}{ll} \mathsf{prob}_{k,t_1} & \stackrel{def}{=} \mathsf{prob}(S_{k,t_1} = 0) \\ \mathsf{prob}^*_{k,t_1} & \stackrel{def}{=} \mathsf{prob}(S^*_{k,t_1} = 0) \\ \mathcal{E}^{i,t_2}_{k,t_1} & \stackrel{def}{=} \mathsf{prob}(S_{k,t_1} = 0\ ,\ S_{i,t_2} = 0) \\ \mathcal{E}^{\overline{i,t_2}}_{k,t_1} & \stackrel{def}{=} \mathsf{prob}(S_{k,t_1} = 0\ ,\ S_{i,t_2} \neq 0). \end{array}$$

In the next paragraph we recall the recurrence relation between the symmetric functions and give the first properties related to $\mathsf{prob}_{t,t}$ and $\mathcal{E}^{k,t}_{t,t}$.

Properties 3.8 ([Ric16, Property 8.5])**.** *Let* $(a_1, \ldots, a_t)$ *be a random uniform variable defined over* $\mathbb{A}_t$ *and for* $1 \leq k \leq t$, $S_{k,t}$ *be the elementary symmetric functions. Then we have that*

$$\forall 1 \leq k \leq t \quad S_{k,t} = S_{k,t-1} + a_t S_{k-1,t-1}.$$

Using basic probability identities we deduce from 3.8 the following relations.

Corollary 3.9. *Let* $(a_1, \ldots, a_t)$ *be a random uniform variable defined over* $\mathbb{A}_t$ *and for* $1 \leq k \leq t$, $S_{k,t}$ *be the elementary symmetric functions. Then we have that*

1. $S_{k,t} = 0 \quad \Leftrightarrow \quad S_{k,t-1} = a_t S_{k-1,t-1}$.
2. $\mathsf{prob}_{t,t} = \frac{t}{n}$ *and* $\mathsf{prob}^*_{t,t} = 0$.
3. $\forall\ 1 \leq k \leq t-1, \quad \mathcal{E}^{k,t}_{t,t} = \mathsf{prob}^*_{k,t-1} \times \frac{t}{n}$ *and* $\mathcal{E}^{t-1,t}_{t,t} = 0$.
4. $\forall\ 2 \leq k \leq t-1, \quad \mathcal{E}^{k-1,t-1}_{k,t} = \mathsf{prob}_{k,t-1}\mathsf{prob}_{k-1,t-1}$ *and* $\mathcal{E}^{0,t-1}_{1,t} = 0$.

The first identities in Corollary 3.9 are also given in [Ric16, Property 8.3] and [Ric16, Lemma 8.1]. The next result is a generalization of [Ric16, Lemma 8.2].

Lemma 3.10. *Let* $(a_1, \ldots, a_t)$ *be a random uniform variable defined over* $\mathbb{A}_t$ *and* X *be a random variable defined over* $\mathbb{F}_{2^m}$ *as* $X \stackrel{def}{=} f(a_1, \ldots, a_{t-1})$*, such that for any* $\pi \in \mathfrak{S}_t$*,* $f(a_1, \ldots, a_{t-1}) = f(a_{\pi(1)} \ldots, a_{\pi(t-1)})$*. Then we have*

$$\mathsf{prob}(a_t = X) = \frac{1}{n-t+1} \times \Big(1 - (t-1) \times \mathsf{prob}(a_{t-1} = X)\Big).$$

Proof. Let us begin by splitting the probability into two different probabilities.

$$\begin{aligned}\mathsf{prob}(a_t = X) &= \underbrace{\mathsf{prob}(a_t = X\ ,\ \exists i \in \{1,\dots,t-1\}; a_i = X)}_{=0} \\ &+\ \mathsf{prob}(a_t = X\ ,\ \ \forall\, i \in \{1,\dots,t-1\}, a_i \neq X)\end{aligned}$$

$$\begin{aligned}\Rightarrow \mathsf{prob}(a_t = X) &= \mathsf{prob}(a_t = X\ ,\ \ \forall i \in \{1,\dots,t-1\}, a_i \neq X) \\ &= \sum_{(\alpha_1,\dots,\alpha_t)\in\mathbb{A}_t} \mathsf{prob}(a_t = \alpha_t\ ,\ X = \alpha_t, a_{t-1} = \alpha_{t-1}, \dots, a_1 = \alpha_1) \\ &= \sum_{(\alpha_1,\dots,\alpha_t)\in\mathbb{A}_t} \mathsf{prob}(a_t = \alpha_t \mid X = \alpha_t, a_{t-1} = \alpha_{t-1}, \dots, a_1 = \alpha_1) \\ &\times \mathsf{prob}(X = \alpha_t, a_{t-1} = \alpha_{t-1}, \dots, a_1 = \alpha_1) \\ &= \frac{1}{n-t+1} \times \sum_{(\alpha_1,\dots,\alpha_t)\in\mathbb{A}_t} \mathsf{prob}(X = \alpha_t, a_{t-1} = \alpha_{t-1}, \dots, a_1 = \alpha_1) \\ &= \frac{1}{n-t+1} \times \mathsf{prob}(\ \forall i \in \{1,\dots,t-1\}, a_i \neq X) \\ &= \frac{1}{n-t+1} \times (1 - \mathsf{prob}(\ \exists i \in \{1,\dots,t-1\}; a_i = X))\end{aligned}$$

Using the definition of the random variables a_i, we get that $\mathsf{prob}(a_i = X, a_j = X) = 0$ for any pair of integers (i, j) such that $1 \leq i < j \leq t-1$. Thus the probability

$$\mathsf{prob}(\ \exists i \in \{1,\dots,t-1\};\ a_i = X) = \sum_{i=1}^{t-1} \mathsf{prob}(a_i = X).$$

Since the random variable $X \stackrel{\text{def}}{=} f(a_1,\dots,a_{t-1})$ satisfies the conditions in Corollary 3.6 we obtain the wanted result.

□

3.3 The distribution of the first symmetric function

This subject was already studied in [Ric16] where a closed formula was given for $\mathsf{prob}_{1,t}$ (see [Ric16, Proposition 8.2]). However this formula is really difficult to analyze from a asymptotic point of view. It is also hard to visualize the difference between the odd and even cases for t, for which we give here an elegant one, that can easily be analyzed.

Proposition 3.11. *Let $(a_1,\dots,a_t)$ be a random uniform variable defined over $\mathbb{A}_t$. Then*

For even t

$$\mathsf{prob}_{1,t} = \frac{1}{n} + (-1)^{t/2}\left(1 - \frac{1}{n}\right)\frac{\binom{n/2}{t/2}}{\binom{n}{t}}.$$

For odd t

$$\mathsf{prob}_{1,t} = \frac{1}{n}.$$

Proof. Using Proposition 3.4 and Lemma 3.10 applied to a_t and $S_{1,t-1}$ we deduce the following equation

$$\mathsf{prob}_{1,t} = \frac{1}{n-t+1} - \frac{t-1}{n-t+1} \times \mathsf{prob}_{1,t-2}\ ,\ \text{ with }\ \mathsf{prob}_{1,1} = \frac{1}{n} \text{ and } \mathsf{prob}_{1,2} = 0. \tag{1}$$

The solution to Equation (1) is

$$\mathsf{prob}_{1,t} = \begin{cases} \frac{1}{n} & \text{for } t \textit{ odd}, \\ \frac{-2\Gamma(\frac{3}{2}-\frac{n}{2})\Gamma(\frac{t}{2}+\frac{1}{2})}{n\sqrt{\pi}\Gamma(\frac{t-n}{2}+\frac{1}{2})} + \frac{1}{n} & \text{for } t \textit{ even}. \end{cases}$$

For odd t, we just have to check that $\frac{1}{n} - \frac{1}{n-t+1} + \frac{t-1}{n-t+1} \times \frac{1}{n} = 0$ in order to obtain the result in this case.

For even t, we begin by transforming the relation for $\mathsf{prob}_{1,t}$ using the following identity for the Gamma function

$$\Gamma(1-\frac{n-1}{2})\Gamma(\frac{n-1}{2}) = \pi/\sin(\frac{\pi}{2}(n-1)).$$

Since in our case $n = 2^m$ we have that $n - 1 = -1 \mod 4$ for any $m \geq 2$ and thus obtain $\Gamma(1-\frac{n-1}{2})\Gamma(\frac{n-1}{2}) = -\pi$.

We use the same technique for the second function and thus obtain $\Gamma(1-\frac{n-t+1}{2})\Gamma(\frac{n-t+1}{2}) = \frac{\pi}{(-1)^{t/2}}$. Hence, using the definition for the Gamma function, the probability when t is even becomes

$$\begin{aligned} \mathsf{prob}_{1,t} &= \frac{1}{n} + \frac{2(-1)^{t/2}}{\sqrt{\pi}n} \frac{\Gamma(\frac{t+1}{2})\Gamma(\frac{n-t+1}{2})}{\Gamma(\frac{n-1}{2})} \\ &= \frac{1}{n} + (-1)^{t/2} \frac{n-1}{n} \frac{\binom{n/2}{t/2}}{\binom{n}{t}}. \end{aligned}$$

The last step is to verify that the result verifies the Equation (1), that can be easily computed by injecting the formula for $\mathsf{prob}_{1,t-2}$ in (1). □

In the next paragraph we generalize our result to any value $\alpha \in \mathbb{F}_{2^m}$. We obtain the same probability when t is odd and a slightly different formula for even t.

Proposition 3.12. *Let $(a_1, \ldots, a_t)$ be a random uniform variable defined over $\mathbb{A}_t$. Then for any $\alpha \in \mathbb{F}_{2^m}^*$ we have*

For even t

$$\mathsf{prob}(S_{1,t} = \alpha) = \frac{1}{n} + (-1)^{t/2+1} \frac{1}{n} \frac{\binom{n/2}{t/2}}{\binom{n}{t}}.$$

For odd t

$$\mathsf{prob}(S_{1,t} = \alpha) = \frac{1}{n}.$$

Proof. Using the same technique as in Proposition 3.11, we obtain the following recurrence relation

$$\mathsf{prob}(S_{1,t} = \alpha) = \frac{1}{n-t+1} - \frac{t-1}{n-t+1} \times \mathsf{prob}(S_{1,t-2} = \alpha).$$

As for the first terms of the recurrence, we have $\mathsf{prob}(S_{1,1} = \alpha) = \mathsf{prob}(a_1 = \alpha) = 1/n$ and for the second one, we can use Lemma 3.10 and obtain:

$$\begin{aligned} \mathsf{prob}(S_{1,2} = \alpha) &= \mathsf{prob}(a_1 + a_2 = \alpha) \\ &= \mathsf{prob}(a_2 = a_1 + \alpha) \\ &\overset{3.10}{=} \frac{1}{n-1} \left(1 - \mathsf{prob}(a_1 = a_1 + \alpha)\right) \\ &= \frac{1}{n-1}. \end{aligned}$$

The solution to this equation is quite similar to the first case

$$\mathsf{prob}_{1,t} = \begin{cases} \frac{1}{n} & \text{for } t \textit{ odd}, \\ \frac{-\Gamma(\frac{1}{2}-\frac{n}{2})\Gamma(\frac{t}{2}+\frac{1}{2})}{n\sqrt{\pi}\Gamma(\frac{t-n}{2}+\frac{1}{2})} + \frac{1}{n} & \text{for } t \textit{ even}. \end{cases}$$

Using the same technique we obtain the wanted result. □

Remark 3.13. *Let $(u_1, \ldots, u_t)$ be a sequence of independent random variables, each one uniformly distributed on $\mathbb{F}_{2^m}$. Then we have:*

$$\forall \alpha \in \mathbb{F}_{2^m},\ \mathsf{prob}\left(\sum_{i=1}^{t} u_i = \alpha\right) = 1/n.$$

But from Proposition 3.12 and 3.11, we get that:

$$\forall \alpha \in \mathbb{F}_{2^m},\ \lim_{n\to\infty} \left| \mathsf{prob}\left(\sum_{i=1}^{t} a_i = \alpha\right) - \mathsf{prob}\left(\sum_{i=1}^{t} u_i = \alpha\right) \right| = 0.$$

This result represents a natural consequence of the fact that when the size of the samples goes to infinity the urn process without replacement becomes a urn process with replacement. This is also analogue to the convergence of the Hypergeometric distribution to the binomial distribution.

Details on the asymptotic expansion of $\mathsf{prob}_{1,t}$ in function of t when n goes to infinity are given in Section 4.

3.4 Bounds on the rest of the coefficients

In order to achieve our goal, we need to prove two important lemmas. The first one, Lemma 3.14, is a slightly better result than [Ric16, Lemma 8.3].

Lemma 3.14. *For any $2 \leq k \leq t-1$, we have*

$$\mathcal{E}_{k,t}^{k-1,t} \leq \frac{2(k-1)}{(n-t+1)(n-t+k)}.$$

We prove this lemma in Appendix 5.

Proposition 3.15 ([Ric16, Proposition 8.3])**.** *Let $(a_1, \ldots, a_t)$ be $\mathbb{F}_{2^m}$-valued random exchangeable variables. Then for any $2 \leq k \leq t-1$, we have:*

$$\left| \mathsf{prob}_{k,t} - \frac{1}{n-t+1} \right| \leq \frac{2t}{(n-t+1)^2}.$$

In order to complete the results, one last result is needed, namely the probability that two coefficients $S_{i,t}$ and $S_{k,t}$ equal to zero at the same time. This result was not obtained in [Ric16] and numerical simulations showed that this quantity was negligible compared to $\mathsf{prob}_{k,t}$. So here we give an upper bound for the wanted probabilities and thus complete the proofs.

Lemma 3.16. *For any $1 \leq i < k \leq t-1$ s.t. $k > i+1$, we have:*

$$\mathcal{E}_{k,t}^{i,t} \leq \frac{4}{(n-t+1)^2} + \frac{8t}{(n-t+1)^3} + \frac{8t^2}{(n-t+1)^4}.$$

Proof.

$$\begin{aligned}
\mathcal{E}_{k,t}^{i,t} &= \mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0\ ,\ S_{k-1,t-1}=0\ ,\ S_{i-1,t-1}=0) && (2)\\
&+\ \mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0\ ,\ S_{k-1,t-1}=0\ ,\ S_{i-1,t-1}\neq 0) && (3)\\
&+\ \mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0\ ,\ S_{k-1,t-1}\neq 0\ ,\ S_{i-1,t-1}=0) && (4)\\
&+\ \mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0\ ,\ S_{k-1,t-1}\neq 0\ ,\ S_{i-1,t-1}\neq 0) && (5)
\end{aligned}$$

We remark that the sum of Probability (2) and Probability (3) is upper bounded by $\mathcal{E}_{k,t}^{k-1,t-1}$. Moreover the third probability, namely (4), can be upper bounded by $\mathcal{E}_{i,t}^{i-1,t-1}$. So we obtain that:

$$\begin{aligned}
\mathcal{E}_{k,t}^{i,t} &\leq \mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0 \mid S_{k-1,t-1}\neq 0\ ,\ S_{i-1,t-1}\neq 0)\\
&+\ \mathcal{E}_{k,t}^{k-1,t-1}+\mathcal{E}_{i,t}^{i-1,t-1}
\end{aligned}$$

Using the relation between the coefficients from Corollary 3.9, we obtain that $\mathsf{prob}(S_{k,t}=0\ ,\ S_{i,t}=0 \mid S_{k-1,t-1}\neq 0\ ,\ S_{i-1,t-1}\neq 0) = \mathsf{prob}(a_t = S_i^{t-1}/S_{i-1,t-1} = S_{k,t-1}/S_{k-1,t-1})$, which can also be bounded by

$$1/(n-t+1)\mathsf{prob}(S_{i,t-1}/S_{i-1,t-1} = S_{k,t-1}/S_{k-1,t-1}). \tag{6}$$

If we develop the relation $S_{i,t-1}/S_{i-1,t-1} = S_{k,t-1}/S_{k-1,t-1}$, we have as before an equation of degree two in a_{t-1}, from which we deduce that Probability (6) can be upper bounded by $1/(n-t+1)\times 2/(n-t+1)$. Furthermore we use the result from Corollary 3.9, more exactly $\mathcal{E}_{k,t}^{k-1,t-1} = \mathsf{prob}_{k,t-1}\times \mathsf{prob}_{k-1,t-1}$, and the upper bound for $\mathsf{prob}_{k,t}$ from Proposition 3.15 to finally obtain

$$\mathcal{E}_{k,t}^{i,t} \leq 2\left(\frac{1}{n-t+1}+\frac{2t}{(n-t+1)^2}\right)^2+\frac{2}{(n-t+1)^2}.$$

□

In Figure 5 we recall all the results we have obtained for the probabilities involved in the study of the simple roots problem.

From those results, we extract upper and lower bounds for the simple roots problem (SRP) for a polynomial of degree t over $\mathbb{F}_{2^m}$, problem denoted $SRP(\mathbb{F}_2, m, t)$ in this paper.

3.5 The simple roots problem

Theorem 3.17. *Let $(a_1,\ldots,a_t)$ be a random uniform variable defined over $\mathbb{A}_t$ and*

- $\mathsf{lb} = 1-\left(\frac{t}{n}+\frac{t-2}{n-t+1}+\frac{2t(t-2)}{(n-t+1)^2}+\mathsf{prob}_{1,t}\right)$,
- $\mathsf{ub} = \mathsf{lb}+\frac{t-2}{(n-t+1)^2}\left(4+7(t-1)+\frac{8t(t-1)}{n-t+1}+\frac{8t^2(t-1)}{(n-t+1)^2}\right)$,

where

$$\mathsf{prob}_{1,t} = \frac{1}{n}+\begin{cases}(-1)^{t/2}\left(1-\frac{1}{n}\right)\dfrac{\binom{n/2}{t/2}}{\binom{n}{t}} & \text{for}\quad t\equiv 0 \pmod 2,\\ 0 & \text{for}\quad t\equiv 1 \pmod 2.\end{cases}$$

Then we have

$$\mathsf{lb} \leq \mathrm{SRP}(\mathbb{F}_2, m, t) \leq \min(\mathsf{ub}, 1-t/n).$$

Probability	Formula	Reference
$\mathbf{prob_{1,t}}$	$\frac{1}{n}+(-1)^{t/2}\frac{n-1}{n}\frac{\binom{n/2}{t/2}}{\binom{n}{t}}$ (*for even t*) $\frac{1}{n}$ (*for odd t*)	Proposition 3.11
$\mathbf{prob_{k,t}}$	$\geq \frac{1}{n-t+1}-\frac{2t}{(n-t+1)^2}$ $\leq \frac{1}{n-t+1}+\frac{2t}{(n-t+1)^2}$	Corollary 3.15
$\mathbf{prob_{t,t}}$	$\frac{t}{n}$	Proposition 3.9
$\boldsymbol{\mathcal{E}_{k,t}^{i,t}}$	$\leq \frac{4}{(n-t+1)^2}+\frac{8t}{(n-t+1)^3}+\frac{8t^2}{(n-t+1)^4}$	Lemma 3.16
$\boldsymbol{\mathcal{E}_{k,t}^{k-1,t}}$	$\leq \frac{2(k-1)}{(n-t+1)^2}$	Lemma 3.14

Figure 5: Bounds on probabilities

Proof. For the lower bound, we have:

$$\begin{aligned}\mathrm{SRP}(\mathbb{F}_2,m,t) &= 1-\mathsf{prob}\left(\exists i\in\{1,\ldots,n\};\ S_{i,t}=0\right)\\ &\stackrel{\text{def}}{=} 1-\sum_{i=1}^{t}\mathsf{prob}_{i,t}\\ &\geq 1-\left(\frac{t}{n}+\frac{t-2}{n-t+1}+\frac{2t\,(t-2)}{(n-t+1)^2}+\mathsf{prob}_{1,t}\right).\end{aligned}$$

For the upper bound, we have$\mathrm{SRP}(\mathbb{F}_2,m,t)\leq \min\limits_{1\leq i\leq t}\left(\mathsf{prob}(S_{i,t}\neq 0)\right)=1-t/n$. Nonetheless, we prefer to compute a finer approximation. Therefore we use the Bonferroni inequality

$$\mathsf{prob}\left(\exists i\in\{1,\ldots,n\};\ S_{i,t}=0\right)\geq\sum_{i=1}^{t}\mathsf{prob}_{i,t}-\sum_{1\leq j<k\leq t}\mathcal{E}_{j,t}^{k,t}$$

and obtain

$$\begin{aligned}\mathrm{SRP}(\mathbb{F}_2,m,t) &= 1-\mathsf{prob}\left(\exists i\in\{1,\ldots,n\};\ S_{i,t}=0\right)\\ &\leq 1-\sum_{i=1}^{t}\mathsf{prob}\left(S_{i,t}=0\right)+\sum_{1\leq j<k\leq t}\mathcal{E}_{j,t}^{k,t}\\ &\leq \mathsf{lb}+\frac{4t(t-2)}{(n-t+1)^2}+\frac{(t-1)(t-2)}{(n-t+1)^2}\\ &+\frac{(t-2)(t-1)}{2}\left(\frac{4}{(n-t+1)^2}+\frac{8t}{(n-t+1)^3}+\frac{8t^2}{(n-t+1)^4}\right).\end{aligned}$$

□

4 Asymptotic behavior and numerical values

4.1 Discussion on the upper bound

Since $1 - t/n$ is an absolute upper bound to the simple roots problem we analyze the regime on t for which ub is better that $1 - t/n$. To do so, we simplify a bit the inequalities, and by that we mean that we loose the constant factors in the expressions. For example we consider the fraction $t^2/(n-t)^2$ instead of $t(t-2)/(n-t+1)^2$. Hence, we have to analyze the regime of values for t for which

$$1 - \frac{t}{n} - \frac{t}{n-t} + \left(\frac{t}{n-t}\right)^2 \left[5 + 4\frac{t}{n-t} + 4\left(\frac{t}{n-t}\right)^2\right] \leq 1 - \frac{t}{n}. \tag{7}$$

Proposition 4.1. *Let n be an integer that goes to infinity. Then for $t > 0.14n$, we have $\mathsf{ub} \geq 1 - t/n$.*

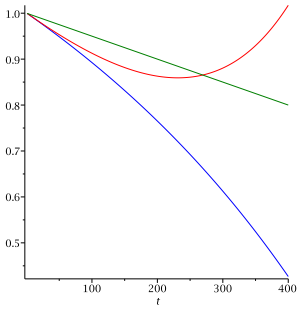
Proof. Computing the difference between ub and $1 - t/n$ implies from Equation (7) solving the following equation in $x \in (0, 1)$

$$4x^4 + 4x^3 + 5x^2 - x = 0, \tag{8}$$

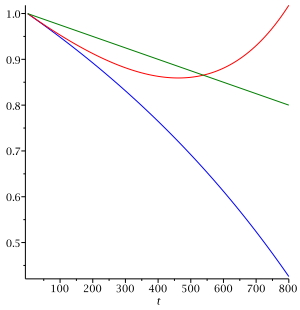
where $x = (n/t - 1)^{-1}$. So solving Equation(8) gives the range of values for t in function of n for which ub becomes grater than $1 - t/n$, namely $n > 6.8t$, which implies the wanted result.

□

Figure 6 plots the evolution of the three bounds, namely the lower bound lb in blue, the upper bound ub in red and $1 - t/n$ in green, when $n = 2000$ (Figure 6a) and $n = 4000$ (Figure 6b). If we compute the value of t for which $1 - t/n$ becomes smaller than ub (intersection between red and green curves), we obtain $t = 280$ for $n = 2000$ (Figure 6a), respectively $t = 560$ for $n = 4000$ (Figure 6b).



(a) $n = 2000$



(b) $n = 4000$

Figure 6: The lower bound in blue, the upper bound in red and $1 - t/n$ in green

Proposition 4.1 states that for $t \geq 0.14n$ our approximation for ub becomes too large. The main reason comes from the approximation that we make on $\mathsf{prob}\left(S_{j,t} = 0, S_{k,t} = 0\right)$. Nonetheless, in a sub-linear regime for t, the bounds become sharp enough, fact that we analyze in the next subsection.

4.2 Asymptotic expansion

We begin here by the study of the probability $\mathsf{prob}_{1,t}$, since in this case we have a closed formula. The next proposition gives the asymptotic equivalence for $\mathsf{prob}_{1,t}$ when t is sub-linear in n as well as linear.

Proposition 4.2. *Let $h(\cdot)$ denote the binary entropy function. Then for even t we have*

$$\mathsf{prob}_{1,t} = \frac{1}{n} + \begin{cases} O\left(\frac{1}{n^{t/2}}\right) & for \quad t = O(1), \\ O\left(\frac{1}{(e\sqrt{n})^{\sqrt{n}}}\right) & for \quad t = O(\sqrt{n}), \\ O\left(\frac{1}{2^{h(c)n/2}}\right) & for \quad t = cn, \text{ with } c \text{ a constant.} \end{cases}$$

Proof. Use the Stirling formula for factorials to deduce for $t = cp$ with c constant

$$\binom{n}{t} = 2^{h(c)n}\sqrt{\frac{1}{2\pi c(1-c)n}}\left(1 - \frac{1}{12n}\left(\frac{1}{c} + \frac{1}{1-c} - 1\right) + O\left(\frac{1}{n^2}\right)\right).$$

Since $t/2 = cn/2$ use the same approximation and deduce the wanted result for $t = cn$.

For the other cases we have

$$\tbinom{n}{t} = \begin{cases} \frac{n^t}{t!}\left(1 + O(\frac{1}{n})\right) & \text{if } t = O(1), \\ \frac{n^t}{t!}e^{-c}\left(1 + O(\frac{1}{\sqrt{n}})\right) & \text{if } \frac{t^2}{2n} = c + O(\frac{1}{\sqrt{n}}). \end{cases}$$

Use the later approximations to obtain the results. □

Next we analyze the difference between the ub and lb when t is sub-linear in n.

Proposition 4.3. *Let $t = o(n)$ when $n \to \infty$. Then we have*

$$\mathsf{lb} = 1 - \begin{cases} \frac{2c-1}{n} + O\left(\frac{1}{n^2}\right) & for \quad t = c, \text{ with } c \text{ a constant}, \\ \frac{2}{\sqrt{n}} - \frac{2}{n} + O\left(\frac{1}{n^{3/2}}\right) & for \quad t = \sqrt{n}, \\ 2\sqrt{\frac{\log n}{n}} + \frac{1}{n} - 3\frac{\log n}{n} + O\left(\frac{\log n}{n}^{3/2}\right) & for \quad t = \sqrt{n\log n}. \end{cases}$$

Then $\mathsf{ub} - \mathsf{lb}$ is given by:

$$\mathsf{ub} - \mathsf{lb} = \begin{cases} \frac{3(c-1)^2}{n^2} + O\left(\frac{1}{n^3}\right) & for \quad t = c, \text{ with } c \text{ a constant}, \\ \frac{3}{n} + \frac{4}{n^{3/2}} + O\left(\frac{1}{n^2}\right) & for \quad t = \sqrt{n}, \\ 3\frac{\log n}{n} + O\left(\frac{\log n}{n}^{3/2}\right) & for \quad t = \sqrt{n\log n}. \end{cases}$$

Proof. Develop the series for the formulae of ub and lb and obtain the wanted results. □

Proposition 4.3 states that for a sub-linear t in n, the upper and the lower bound converge to the same limit, fact that we illustrate through the following figures. In Figure 7a we plot the lower bound in blue, the upper bound in red and $1 - t/n$ in green for $n = t^2$. In Figure 7b we plot the same functions but when $n = t^3$. We notice that when $t = n^{1/3}$ the difference between ub and lb converges much faster to zero than for $t = n^{1/2}$.

(a) $n = t^2$ (b) $n = t^3$

Figure 7: The lower bound in blue, the upper bound in red and $1 - t/n$ in green

4.3 Numerical values

Numerical simulations were conducted using the Monte Carlo method for estimating several quantities. We executed our simulations in PariGP, a free software mainly known for its library in number theory and finite fields. In practice we tested several range of values for n and t but we recall here only the most relevant for the McEliece scheme. Hence, in Figure 8 we choose to fix $n = 1024$ and consider $3 \leq t \leq 200$. Our algorithm chooses t different elements in $\mathbb{F}_{2^{10}}$ and computes the polynomial $\sigma(x)$. We repeat this procedure $3 \cdot 10^6$ times and compute the mean number of polynomials $\sigma(x)$ with non zero coefficients. Finally we plot in black the experimental result as well as the lb in blue, the ub in red and $1 - t/n$ in green. The figure 8 is a fine illustration of the theoretic results obtained in the later section.

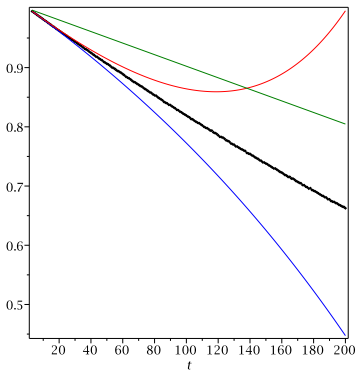


Figure 8: The experimental results in black, the lower bound in blue, the upper bound in red and $1 - t/n$ in green for $n = 1024$ and $3 \leq t \leq 200$.

5 Conclusion

In this paper we study the simple roots problem, that is a probability problem related to the error locator polynomial. Our results prove that when the degree of the error locator polynomial ($\sigma(x)$) is sub-linear in the length of the code, we have a sharp asymptotic approximation for the probability that all the coefficients of $\sigma(x)$ are different from zero. A direct application of our results is a natural countermeasure against timing attacks on the decoding algorithm in the McEliece cryptosystem using any family of codes belonging to the Alternant codes.

We also give an elegant closed formula for the first coefficient of $\sigma(x)$, more exactly for the sum of σ's roots, which represents a nice combinatorial result. We point out that for a linear regime

in the code length of the $\deg(\sigma)$, the results here are no longer sharp enough and other techniques have to be considered.

References

[AHPT11] Roberto Avanzi, Simon Hoerder, Dan Page, and Michael Tunstall. Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *J. Cryptographic Engineering*, 1(4):271–281, 2011.

[BBD09] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer-Verlag, 2009.

[BCD+16] Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich. Cryptanalysis of the McEliece public key cryptosystem based on polar codes. In *Post-Quantum Cryptography2016*, Lecture Notes in Comput. Sci., Fukuoka, Japan, February 2016.

[BCDR16] Dominic Bucerzan, Pierre-Louis Cayrel, Vlad Dragoi, and Tania Richmond. Improved timing attacks against the secret permutation in the McEliece PKC. *International Journal of Computers Communications & Control*, 12(1):7–25, 2016.

[BCS13] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. Mcbits: Fast constant-time code-based cryptography. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, volume 8086 of *Lecture Notes in Comput. Sci.*, pages 250–272. Springer, 2013.

[BDLO16] Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani. Weak keys for the quasi-cyclic MDPC public key encryption scheme. In *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, pages 346–367, 2016.

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Comput. Sci.*, pages 1–16, Copenhagen, Denmark, May 2014. Springer.

[Che82] Chin-Long Chen. Formulas for the solutions of quadratic equations over $GF(2^m)$(corresp.). *IEEE Transactions on Information Theory*, 28(5):792–794, September 1982.

[CHP12] Pierre-Louis Cayrel, Gerhard Hoffmann, and Eduardo Persichetti. Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes. In *Public-Key Cryptography - PKC 2012*, volume 7293 of *Lecture Notes in Comput. Sci.*, pages 138–155. Springer, 2012.

[CMCP14] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2014*, pages 1446–1450, June 2014.

[DCCR13] Vlad Dragoi, Pierre-Louis Cayrel, Brice Colombier, and Tania Richmond. Polynomial structures in code-based cryptography. In *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*, pages 286–296, 2013.

[FGO+13] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high rate McEliece cryptosystems. *IEEE Trans. Inform. Theory*, 59(10):6830–6844, October 2013.

[FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.

[HMP10] Stefan Heyse, Amir Moradi, and Christof Paar. Practical power analysis attacks on software implementations of McEliece. In Nicolas Sendrier, editor, *Post-Quantum Cryptography 2010*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 108–125. Springer, 2010.

[HSEA14] R Hooshmand, M Koochak Shooshtari, T Eghlidos, and MR Aref. Reducing the key length of McEliece cryptosystem using polar codes. In *2014 11th International ISC Conference on Information Security and Cryptology (ISCISC)*, pages 104–108. IEEE, 2014.

[JM96] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Des. Codes Cryptogr.*, 8(3):293–307, 1996.

[McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[MS86] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North–Holland, Amsterdam, fifth edition, 1986.

[MS07] Lorenz Minder and Amin Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 347–360, Barcelona, Spain, 2007.

[MSSS11] H. Gregor Molter, Marc Stöttinger, Abdulhadi Shoufan, and Falko Strenzke. A simple power analysis attack on a McEliece cryptoprocessor. *Journal Cryptographic Engineering*, 1(1):29–36, 2011.

[MTSB13] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2069–2073, 2013.

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[Pat75] N. Patterson. The algebraic decoding of Goppa codes. *IEEE Trans. Inform. Theory*, 21(2):203–207, 1975.

[PRD+15] Martin Petrvalský, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel, and Viktor Fischer. Countermeasure against the SPA attack on an embedded McEliece cryptosystem. In *Radioelektronika (RADIOELEKTRONIKA), 2015 25th International Conference*, pages 462–466. IEEE, April 2015.

[PRD+16] Martin Petrvalský, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel, and Viktor Fischer. Differential power analysis attack on the secure bit permutation in the McEliece cryptosystem. *RadioElektronika 2016*, pages 132–137, April 2016.

[Ric16] Tania Richmond. *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs*. PhD thesis, Université Jean Monnet, Saint-Étienne, October 2016.

[Sho94] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In S. Goldwasser, editor, *FOCS*, pages 124–134, 1994.

[Sid94] Vladimir Michilovich Sidelnikov. A public-key cryptosytem based on Reed-Muller codes. *Discrete Math. Appl.*, 4(3):191–207, 1994.

[SK14] Sujan Raj Shrestha and Young-Sik Kim. New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pages 368–372. IEEE, 2014.

[SS92] Vladimir Michilovich Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.*, 1(4):439–444, 1992.

[SSMS09] Abdulhadi Shoufan, Falko Strenzke, H. Gregor Molter, and Marc Stöttinger. A timing attack against patterson algorithm in the McEliece PKC. In *Information, Security and Cryptology - ICISC 2009, 12th International Conference*, volume 5984 of *Lecture Notes in Comput. Sci.*, pages 161–175, Seoul, Korea, December 2009. Springer.

[STM+08] Falko Strenzke, Erik Tews, H. Gregor Molter, Raphael Overbeck, and Abdulhadi Shoufan. Side channels in the McEliece PKC. In Johannes Buchmann and Jintai Ding, editors, *Post-Quantum Cryptography 2008*, volume 5299 of *Lecture Notes in Comput. Sci.*, pages 216–229. Springer, 2008.

[Str10] Falko Strenzke. A Timing Attack against the Secret Permutation in the McEliece PKC. In Nicolas Sendrier, editor, *Post-Quantum Cryptography 2010*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 95–107. Springer, 2010.

[Str11] Falko Strenzke. Message-aimed side channel and fault attacks against public key cryptosystems with homomorphic properties. *J. Cryptographic Engineering*, 1(4):283–292, 2011.

[Str13] Falko Strenzke. Timing attacks against the syndrome inversion in code-based cryptosystems. In *Post-Quantum Cryptography 2013*, volume 7932 of *Lecture Notes in Comput. Sci.*, pages 217–230, Limoges, France, June 2013. Springer.

Appendix

A. The simple roots problem for $1 \leq t \leq 3$

- for $t = 1$, we have $P(x) = x - a_1$ and thus

$$\mathrm{SRP}(\mathbb{F}_2, m, 1) \stackrel{\text{def}}{=} \mathsf{prob}(a_1 \neq 0) = 1 - 1/n.$$

- for $t = 2$, we have $P(x) = x^2 - (a_1 + a_2)x + a_1 a_2$ and thus

$$\mathrm{SRP}(\mathbb{F}_2, m, 2) \stackrel{\text{def}}{=} \mathsf{prob}(a_1 a_2 \neq 0\ ,\ a_1 + a_2 \neq 0).$$

  Since $a_1 + a_2$ is different from zero for any values of the tuple (a_1, a_2), we have that

$$\mathrm{SRP}(\mathbb{F}_2, m, 2) = \mathsf{prob}(a_1 a_2 \neq 0) = 1 - 2/n = 1 - 1/2^{m-1}.$$

- for $t = 3$, we have $P(x) = x^3 - (a_1 + a_2 + a_3)x^2 + (a_1 a_2 + a_1 a_3 + a_2 a_3)x - a_1 a_2 a_3$. In order to give the probability, we detail each coefficient separately:

– $\mathsf{prob}(a_1a_2a_3 = 0) = 3 \times \mathsf{prob}(a_1 = 0) = 3/n$ (here we use the fact that (a_1, a_2, a_3) is exchangeable).

– $\mathsf{prob}(a_1a_2a_3 = 0\ ,\ a_1a_2 + a_1a_3 + a_2a_3 = 0) = 0$ because of the fact that a_1, a_2, a_3 are pairwise distinct. Indeed if we replace the values of $a_1a_2a_3$ and $a_1a_2 + a_1a_3 + a_2a_3$ into $P(x)$, we obtain $P(x) = x^2(x - a_1 - a_2 - a_3)$ which is impossible since $P(x)$ is a simple roots polynomial.

–

$$\begin{aligned}\mathsf{prob}(a_1 + a_2 + a_3 = 0) &= \mathsf{prob}(a_3 = a_1 + a_2\ ,\ \forall 1 \le i \le 2,\ a_i \ne a_1 + a_2)\\ &= \mathsf{prob}(a_3 = a_1 + a_2 \mid \forall 1 \le i \le 2,\ a_i \ne a_1 + a_2)\\ &\times \mathsf{prob}(\forall 1 \le i \le 2\ a_i \ne a_1 + a_2)\\ &= \frac{1}{n-2} \times (1 - \mathsf{prob}(\exists\ 1 \le i \le 2;\ \ a_i = a_1 + a_2)).\end{aligned}$$

Using the fact that (a_1, a_2) is exchangeable, we deduce that

$$\mathsf{prob}(\exists\ 1 \le i \le 2;\ a_i = a_1 + a_2) = 2 \times \mathsf{prob}(a_1 = a_1 + a_2) = 2 \times \mathsf{prob}(a_2 = 0).$$

So we have that

$$\mathsf{prob}(a_1 + a_2 + a_3 = 0) = 1/n.$$

– Using the same argument for the second coefficient we obtain

$$\begin{aligned}\mathsf{prob}(a_1a_2 + a_1a_3 + a_2a_3 = 0) &= \mathsf{prob}(a_3 = a_1a_2/(a_1 + a_2))\\ &= \frac{1}{n-2} \times (1 - \mathsf{prob}(\exists 1 \le i \le 2;\ a_i = a_1a_2/(a_1 + a_2))\\ &= \frac{1}{n-2} \times (1 - 2 \times \mathsf{prob}(a_2 = a_1a_2/(a_1 + a_2))\\ &= \frac{1}{n-2} \times (1 - 2 \times \mathsf{prob}(a_2^2 = 0))\\ &= 1/n.\end{aligned}$$

– The last quantity to examine is

$$\mathsf{prob}(a_1 + a_2 + a_3 = 0\ ,\ a_1a_2 + a_1a_3 + a_2a_3 = 0\ ,\ a_1a_2a_3 \ne 0).$$

First we develop the equations. We obtain that $a_3 = a_1 + a_2$ and $a_3 = a_1a_2/(a_1 + a_2)$, since $a_1 + a_2 \ne 0$. This implies that $a_1^2 + a_2^2 = a_1a_2$. Since $(\mathbb{F}_{2^m}^*, \times)$ is a cyclic group we can put $a_1 = \theta^i$ and $a_2 = \theta^{i+j}$ with $j \ne 0$ and θ a generator of the cyclic group. We develop the equation and obtain $\theta^{2i} + \theta^{2i+2j} + \theta^{2i+j} = 0$. We multiply the equation by θ^{-2i} and obtain a second degree equation in θ^j, namely

$$\theta^{2i} + \theta^i + 1 = 0, \tag{9}$$

which turns out to have no solution if m is odd and two solutions when m is even.

Figure 9 synthesizes these results and gives the probability $\mathrm{SRP}(\mathbb{F}_2, m, 3) = 1 - 5/n$ when m is odd.

$a_1+a_2+a_3$	$a_1a_2+a_1a_3+a_2a_3$	$a_1a_2a_3$	prob
0	0	0	0
$\neq$	0	0	0
0	$\neq$	0	0
0	0	$\neq$	0
$\neq$	$\neq$	0	$3/n$
0	$\neq$	$\neq$	$1/n$
$\neq$	0	$\neq$	$1/n$
$\neq$	$\neq$	$\neq$	$1-5/n$

Figure 9: The probability for $t=3$ when m is odd.

B. Proof of Lemma 3.14

Lemma (3.14)**.** *For any $2 \leq k \leq t-1$, we have*

$$\mathcal{E}_{k,t}^{k-1,t} \leq \frac{2(k-1)}{(n-t+1)(n-t+k)}.$$

Proof. Let's start by giving the recurrence relation for each variable involved in the equation:

$$\begin{array}{rcl} S_{k-1,t} = 0 & \Leftrightarrow & S_{k-2,t-1} \times a_t = S_{k-1,t-1} \\ S_{k,t} = 0 & \Leftrightarrow & S_{k-1,t-1} \times a_t = S_{k,t-1} \end{array}$$

1. In the first time, we find a recurrence relation for $\mathcal{E}_{k,t}^{k-1,t}$ and begin by splitting it into two different probabilities such that:

$$\begin{aligned} \mathcal{E}_{k,t}^{k-1,t} = & \underbrace{\mathsf{prob}\left(S_{k-1,t}=0\ ,\ S_{k,t}=0\ ,\ S_{k-2,t-1}=0\right)}_{\leq \mathcal{E}_{k-1,t-1}^{k-2,t-1}} \\ & + \mathsf{prob}\left(S_{k-1,t}=0\ ,\ S_{k,t}=0\ ,\ S_{k-2,t-1}\neq 0\right). \end{aligned}$$

So we obtain the following inequality:

$$\begin{aligned} \mathcal{E}_{k,t}^{k-1,t} - \mathcal{E}_{k-1,t-1}^{k-2,t-1} &\leq \mathsf{prob}\left(S_{k-1,t}=0\ ,\ S_{k,t}=0\ ,\ S_{k-2,t-1}\neq 0\right) \\ &= \mathsf{prob}\left(S_{k-1,t}=0\ ,\ S_{k,t}=0 \mid S_{k-2,t-1}\neq 0\right) \times \mathsf{prob}\left(S_{k-2,t-1}\neq 0\right) \\ &= \mathsf{prob}\left(S_{k,t}=0 \mid S_{k-1,t}=0\ ,\ S_{k-2,t-1}\neq 0\right) \\ &\times \mathsf{prob}\left(S_{k-1,t}=0 \mid S_{k-2,t-1}\neq 0\right) \times \left(1-\mathsf{prob}_{k-2,t-1}\right). \end{aligned}$$

We detail a part the two probabilities involved in the inequality and begin by considering

$$\mathsf{prob}\left(S_{k-1,t}=0 \mid S_{k-2,t-1}\neq 0\right) = \mathsf{prob}\left(a_t = \frac{S_{k-1,t-1}}{S_{k-2,t-1}}\right)$$

Since $S_{k-1,t-1}/S_{k-2,t-1}$ verifies Lemma 3.10, we upper bound this probability by $1/(n-t+1)$.

We also analyze the second probability involved in the relation, more exactly:

$$\mathsf{prob}\left(S_{k,t}=0 \mid S_{k-1,t}=0\ ,\ S_{k-2,t-1}\neq 0\right).$$

We notice that given $S_{k-1,t}=0$ and $S_{k-2,t-1}\neq 0$, and using Corollary 3.9, we have that $S_{k,t}=0 \Leftrightarrow {S_{k-1,t-1}}^2 = S_{k-2,t-1} \times S_{k,t-1}$. If we develop this equality, we have:

$$\begin{array}{lll} & \left((S_{k-2,t-2})^2 + S_{k-3,t-2} \times S_{k-1,t-2}\right) & a_{t-1}^2 \\ + & (S_{k-3,t-2} \times S_{k,t-2} + S_{k-1,t-2} \times S_{k-2,t-2}) & a_{t-1} \\ + & (S_{k-1,t-2})^2 + S_{k-2,t-2} \times S_{k,t-2} & \\ \hline = & 0 & \end{array}$$

But this is a second degree equation in a_{t-1} over $\mathbb{F}_{2^m}$. So the number of solutions in a_{t-1} is at most two and in some cases zero [Che82]. This implies that the probability can be bounded by

$$\mathsf{prob}(S_{k,t} = 0 \mid S_{k-1,t} = 0\ ,\ S_{k-2,t-1} \neq 0) \leq \frac{2}{n-t+2}.$$

Putting all those relations together, we obtain the following inequality:

$$\begin{aligned} \mathcal{E}_{k,t}^{k-1,t} - \mathcal{E}_{k-1,t-1}^{k-2,t-1} &\leq \frac{1}{n-t+1} \times \frac{2}{n-t+2} \times (1 - \mathsf{prob}_{k-2,t-1}) \\ &\leq \frac{2}{(n-t+1)(n-t+2)} \\ &= 2\left(\frac{1}{n-t+1} - \frac{1}{n-t+2}\right). \end{aligned}$$

2. In order to finish the proof of Lemma 3.14, one last step remains, more exactly to give the final relation using induction. As $S_{0,t} = 1$, we have that $\mathcal{E}_{1,t}^{0,t} = 0, \quad \forall\ t < n$. We also know that $\mathcal{E}_{t,t}^{t-1,t} = 0$, fact proved in Corollary 3.9. Thus we have:

$$\begin{array}{ll} \mathcal{E}_{k,t}^{k-1,t} - \mathcal{E}_{k-1,t-1}^{k-2,t-1} & \leq 2\left(\frac{1}{n-(t-1)} - \frac{1}{n-(t-2)}\right) \\ \cdots & \cdots \\ \mathcal{E}_{2,t-k+2}^{1,t-k+2} - \underbrace{\mathcal{E}_{1,t-k+1}^{0,t-k+1}}_{=0} & \leq 2\left(\frac{1}{n-(t-k+1)} - \frac{1}{n-(t-k)}\right) \end{array}$$

So we obtain the following inequality:

$$\forall k \in \{2, \ldots, t-1\}, \quad \mathcal{E}_{k,t}^{k-1,t} \leq 2\left(\frac{1}{n-t+1} - \frac{1}{n-t+k}\right) = \frac{2(k-1)}{(n-t+1)(n-t+k)}.$$

□