Recent progress in code-based cryptography

Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhard Hoffmann,
Mohammed Meziani and Robert Niebuhr

Abstract

The last three years have witnessed tremendous progress in the understanding of code-based cryptography. One of its most promising applications is the design of cryptographic schemes with exceptionally strong security guarantees and other desirable properties. In contrast to number-theoretic problems typically used in cryptography, the underlying problems have so far resisted subexponential time attacks as well as quantum algorithms. This paper will survey the more recent developments. Keywords: *Post-quantum cryptography, coding-based cryptography, encryption, digital signatures, identification, secret-key.*

Introduction

Code-based cryptography is one of the most promising candidates for post-quantum cryptography, i.e. cryptosystems that resist attacks by quantum computers. Examples are the McEliece and the Niederreiter encryption schemes [12, 14]. The underlying problem, the Syndrome Decoding problem, has been proven NP-complete in [1]. In 2008, Overbeck and Sendrier [70] published a comprehensive state-of-the-art of code-based cryptography. In the last three years, there have been many new publications in various areas of cryptography.

Our contribution

In this paper, we provide a state-of-the-art of code-based cryptography. We present the publications since 2008 in several areas of this field, including encryption and identification schemes, digital signatures, secret-key cryptography, and cryptanalysis.

Organization of the paper

In Section 1, we present the recent improvements in the design of encryption schemes attempting to reduce the public key sizes. In Section 2, we detail the recent results in zero-knowledge identification schemes. Section 3 deals with the new improvements of code-based signature schemes and Section 4 presents the new results in code-based secret-key cryptography. The subsequent Section 5 details the latest results in cryptanalysis. We conclude in Section 6.

1 Encryption

In code-based cryptography there are at least three encryption schemes: the McEliece [12], the Niederreiter [14] encryption schemes, and, more recently, the HyMES [9] (Hybrid

McEliece encryption scheme). All those schemes have already been described in [78] pages 97–100 and 127–129.

The McEliece encryption scheme never caught the attention like e.g. RSA, mostly because of the relatively large size of the public generator matrix. Things changed when it turned out that the scheme is unscathed by quantum-computer attacks, and several contributions have been made in the last few years [5, 7, 48, 65, 11].

1.1 Reducing the key size of the McEliece cryptosystem

Since [10], the idea of using compact representations of the public matrix used in the McEliece encryption scheme has been investigated. After several cryptanalyses, Berger et al. [48] and Misoczki and Barreto [65] proposed to use QC alternant codes and QD Goppa codes respectively to reduce the public key size from several hundred thousands bits (500 Kbits for the original proposal) to only 20 Kbits. The idea of those constructions is to generate the whole matrix via permutations of the first row. Furthermore, those constructions allow to encrypt the message without computing the whole matrix but by using the first row only. After several attacks (see Section 5), the binary parameters are still secure in both cases.

1.2 Implementation on different platforms

Due to a lack of space we will not detail the section in this version of the paper.

2 Identification

In the last few years there were many attempts to build secure identification schemes based on error-correcting codes. Such schemes allow a prover holding a secret key to prove his/her identity to a verifier holding the corresponding public key without revealing any additional information that might be used by an impersonator. At Crypto'93, Stern [20] presented the first identification scheme based on the SD problem. This scheme is a multiple-rounds zero-knowledge protocol, where each round is a three-pass interaction between the prover and the verifier, and for which the success probability for a cheater is 2/3. The number of rounds depends on the security level needed; for 80 bits security level, one needs about 150 rounds (the norm ISO/IEC-9798-5 proposes the two cheat probabilities 2^{-16} and 2^{-32} for which one needs 28 resp. 56 rounds).

2.1 Quasi-cyclic Stern

Due to the usual drawback of code-based cryptosystems, the large public key size, Gaborit and Girault proposed in 2007 [17] a way to reduce this disadvantage. The idea consists in using QC codes instead of random codes.
Using this class of codes, Cayrel et al. proposed in [15] an efficient implementation of Stern's protocol on a smart-card. For a security level of 80 bits, they obtained an authentication in 6 seconds and a signature in 24 seconds without cryptographic co-processor. This is a promising result when compared to an RSA implementation which would take more than 30 seconds in a similar context.

2.2 Cayrel et al.'s identification scheme

Recently, Cayrel et al. presented in [16] an identification scheme using q-ary codes instead of binary codes which constitutes an improvement of the Stern and Véron constructions. This scheme is a five-pass protocol for which the success probability of a cheater is bounded by 1/2 per round. In addition to the new way to calculate the commitments, this protocol uses another improvement which is inspired by [18, 19]. It consists of sending a random challenge value from $\mathbb{F}_q$ by the verifier after receiving the two commitments from the sender, who sends back the secret key scrambled by a random vector, a random permutation and the random challenge.

3 Signature

In code-based cryptography, there have been many attempts to design signature schemes using linear codes. Some proposals like [22, 30, 21] have been proved to be insecure; however, the two following schemes remain secure. The first one, by Kabatianskii, Krouk, and Smeets (KKS) [31] in 1997, is based on random codes and claimed to be secure. However, [26] showed that a passive attacker intercepting just a few signatures can efficiently find the private key. The second one, introduced by Courtois, Finiasz and Sendrier (CFS) in 2001, is the first code-based signature scheme with a security reduction [27] to two NP-complete problems: the SD and the GD problem. This latter has lately been shown to be solvable, but only under very specific parameter constraints (see Section 5).

3.1 Quasi-dyadic-CFS

Motivated by the drawback of having large memory requirement, Barreto et al. [23] proposed an improved version of CFS using QD Goppa codes instead of the standard Goppa codes. This class of codes is mentioned earlier in Section 1. This modification allows to reduce the key size by a factor of 4 in practice and to speed-up the computation by using the QD structure.

3.2 Parallel-CFS

In view of Bleichenbacher's attack described in [59], the preliminary parameters of the CFS had to be increased. This leads to an increase of the public key size or of the signature cost by an exponential factor in parameters m or t, where 2^m the code length and t the degree of the Goppa polynomial, respectively.

Recently, Finiasz suggested in [28] a way to increase the security of the CFS while keeping the parameters as small as possible. The idea of his proposal consists in performing a parallel complete decoding to generate two CFS signatures using two different hash-functions for the same message. In this case, an attacker has to produce two forgeries for the same message, which makes the decoding attack much harder compared with the regular CFS.

3.3 Barreto et. al's OTS

In 2010, Barreto et al. [24] developed a syndrome-based one-time signature scheme (BMS-OTS) by combining the idea of Schnorr [32] and KKS [31]. The security of their proposal is based on the hardness of decoding random binary codes, which is believed to be hard on average [25].

4 Secret key code-based cryptography

Until 2006, only two results have been proposed in code-based cryptography in the area of hash functions and stream ciphers. Regarding stream ciphers, Fischer and Stern [42] (FS) presented the first pseudo-random generator at Eurocrypt 1996, whose security stems from the intractability of the SD problem for random binary linear codes.

In context of hashing, two different versions have been proposed following the Merkle-Damgård [45, 41] design principle: the first one is the Syndrome Based hash function (SB) in 2003 [34] whose compression function uses a random binary matrix and the algorithm from [44] for embedding data in a constant weight word. However, this algorithm is the most time-consuming part of the scheme. That is why a second and faster variant of SB, called Fast Syndrome Based hash function (FSB) [47], has been developed in 2005 by replacing the latter encoding function by a faster one called regular encoding. This algorithm embeds data into a regular word. This word is composed of a number of equal-sized blocks, each of which contains exactly one non-zero entry.

4.1 FSB SHA-3 proposal

The first round SHA3-submission FSB due to Augot et al. [33] is an enhanced variant of FSB with two main features: It uses truncated QC codes to reduce the storage capacity and it provides a security reduction to the SD problem. It is designed following the well-known Merkle-Damgård transform [45, 41] and parameterized by four positive integers. Each set of these parameters defines a unique compression function, which is a composition of an encoding function and a syndrome mapping. This mapping is based on a parity check matrix derived from digits of π (about 2 million bits) by circular shifting a number of vectors of the same length.

So far, the FSB SHA-3 proposal is secure. It can be proven that breaking it (finding collisions or preimages) is at least as difficult as solving certain problems introduced and proved NP-complete in [47]: the RSD and the 2-RNSD problem. The complexity of solving the latter problem is less than that of the conventional SD as demonstrated lately in [39] (see Section 5). Despite this feature, FSB suffers from the drawback of having a long initialization time and handling large states, and therefore it remains far slower than widely-used hash functions like the SHA-2 family (which is a SHA-3 candidate as well).

4.2 RFSB

Motivated by the inefficiency of FSB, Bernstein et al. [40] proposed a further improved variant of FSB in 2011, named RFSB (stands for Really Fast Syndrome-Based hashing), also following the Merkle–Damgård construction [45, 41]. Its design is inspired by the Set Hash due to Zobrist [46] (and other related works [41, 36, 37]). In order to compute a hash value, the message is first broken into small pieces, each passed through a random function and finally combined using the bitwise XOR operator. The random function can be described by a random binary matrix. Unlike FSB, no encoding algorithm is used here and the matrix is not quasi cyclic, smaller than the FSB-matrix and defined as follows. Each entry is created by first encrypting a number of 16-bytes strings using the AES algorithm and then rotating the results certain times depending on the block position of the message.

4.3 SYND stream cipher

This cipher, proposed by Gaborit el al. [43] in 2007, is an improved variant of the Fisher-Stern pseudo-random generator [42] with two main improvements. Firstly, replacing a random matrix by a random QC matrix decreases the storage requirements without diminishing the hardness of the SD, as shown in [48]. Secondly, using the regular encoding technique instead of the algorithms proposed in [42] speeds up the encoding process.

5 Cryptanalysis

The two main types of attacks in code-based cryptography are structural and decoding attacks. The former exploit the structure of the underlying code, and usually they attempt to recover the secret key. The latter can be used independently of the code structure and are thus also called generic attacks.
This section details the recent cryptanalytic improvements and corresponds to Sections 3.4 and 4.3 in [78].

5.1 Structural attacks

In the past, most structural attacks against code-based cryptosystems have targeted specific classes of codes. They exploited the code structure in order to break cryptosystems which use these codes. Examples include the Sidelnikov-Shestakov attack against the Niederreiter PKC using GRS (Generalized Reed-Solomon) codes [74], Overbeck's attack against rank-metric codes [69], and cryptanalysis of Reed-Muller codes using Stern's algorithm [75].

Since a large public key size is one of the drawbacks of code-based cryptography, there have been many proposals attempting to reduce the key size, as presented in Sections 1 and 3. Often, the authors used highly structured codes which can be stored more efficiently. Examples include QC [48] and QD [65] codes, as well as LDPC codes. In recent years, there have been several publications on structural attacks against such highly structured codes.
Otmani et al. [68] cryptanalyzed a McEliece cryptosystem based on QC LDPC codes. The attack exploits the QC structure to find a punctured version of the secret key, and then uses Stern's algorithm to reconstruct the entire secret key.
In [60], Gauthier and Leander presented an attack against QC and QD codes. The attack is based on an attack framework which exploits linear redundancies in subfield subcodes of GRS codes. While the attack breaks several codes over larger fields $\mathbb{F}_q$, binary codes remain secure against it.
Faugère et al. presented an algebraic attack against the McEliece cryptosystem using

non-binary QC and QD codes at Eurocrypt 2010 [57], and an extention of this work at SCC 2010 [58]. The attacker sets up a system of algebraic equations, the solution of which will be an alternant decoder for the underlying code. While this system cannot be solved efficiently for the original McEliece cryptosystem, the additional QC or QD structure allows to significantly reduce the number of unknowns of this system. Additionally, improved Gröbner basis techniques further decrease the attack complexity. With this approach, the authors were able to break several non-binary parameters presented in [48] and [65]. Again, binary parameters remain secure. In [53], Bernstein et al. described how to improve ISD-based algorithms if the target codeword is a 2-regular word (a vector consisting of blocks, each having Hamming weight zero or two). The attack is an improvement over a previous attack against 2-regular words described in [47] and achieves an exponential speedup.
Wieschebrink presented a new attack [77] against the Berger-Loidreau public-key cryptosystem. In 2010, Faugère et al. presented a Goppa code distinguisher [56]. The algorithm allows to distinguish Goppa codes from random codes, provided that the code rate (code dimension divided by code length) is very high. While the paper does not attack a specific cryptosystem, it is an important result for past and future security proofs. Overbeck presented a security analysis of the Gabidulin version of the McEliece cryptosystem [69].

5.2 Decoding attacks

Information-set decoding (ISD) and the generalized birthday algorithm (GBA) are the two most important types of generic attacks against code-based cryptosystems. The basic ISD algorithm is due to Prange [72], with major improvements by Leon [63], Lee-Brickell [62], Stern [75], and Canteaut-Chabaud [54].
Wagner [76] generalized the well-known birthday algorithm to more than two lists which greatly improved the algorithm efficiency.

In [51], Bernstein et al. proposed several techniques to speed up ISD-based attacks, e.g. by re-using pivot values to speed up the matrix inversion step. These improvements reduce the cost to attack the original McEliece parameters $(1024, 524, 50)$ to $2^{60.5}$ binary operations. Together with van Tilborg, the above authors presented a comparison of different generic decoding algorithms [55]. Using upper and lower bounds for the cost of these algorithms, they also compared the asymptotic behaviour. While the analyzed decoding algorithms (asymptotically) save a non-constant factor compared with Lee-Brickell, they only save a factor of $1 + o(1)$ compared with Stern's algorithm.
In [59], Finiasz and Sendrier proposed lower bounds for the complexity of birthday, ISD and GBA attacks against code-based cryptosystems. The approach is to define a generic model for each attack, identify the essential steps, and use only the cost of these steps to compute the attack complexity.

In [71], Peters generalized Stern's and Lee-Brickell's algorithms (both are variants of ISD) to $\mathbb{F}_q$. Based on this generalization, the author provided an estimation of the cost of these algorithms.
Bernstein et al. published an improved ISD-algorithm in [52]. This algorithm manages to decrease the complexity slightly below the corresponding lower bound from [59]. Note that the improved algorithm does not fit into the generic model used in [59], so this result did not invalidate the lower bound formula.
Niebuhr et al. [67] generalized these lower bounds to $\mathbb{F}_q$.

While Wagner's GBA has improved the time complexity compared with previous birthday algorithms, the lists used by the algorithm can be very large. Minder and Sinclair [64] proposed a more flexible algorithm that allows to trade off time vs. memory efficiency. The modified algorithm allows to limit the list size to arbitrary values, including the size of the input lists. The drawback is a decreased time efficiency.
In [66], Niebuhr et al. showed how to increase the efficiency of GBA when attacking structured matrices. Covered by the improvement are all matrices where each row is a permutation of the first. The improvement allows to increase the time and memory efficiency by a factor of r, the co-dimension of the code. A basic problem on which several code-based cryptosystems are based is the SD problem. It was proved to be NP-complete in 1978. In most cases, however, the cryptosystems rely on specific instances of this problem that are subject to additional constraints. While code-based cryptography is assumed to be secure against quantum computer attacks, a modification of the parameters will nonetheless be required. The conventional wisdom is that Shor's algorithm [73] requires a twofold increase in the key size of these cryptosystems. In [49], Bernstein analyzed the impact of Grover's algorithm [61]. Using this algorithm to speed up specialized attacks like ISD will require a quadrupling of the McEliece key size, for instance. While this effect is smaller than the worst-case assumption of a square-root speedup in all attacks, it is greater than some more optimistic assumptions, e.g. in [70, Section 3.5].

6 Conclusion

In this paper, we have described the recent results in code-based cryptography. These results include the new improvements in several different areas of cryptography (encryption, identification, signature, secret-key and cryptanalysis). This paper provides a comprehensive state-of-the-art and an extension of the chapter ”Code-based cryptography” of the book [78]. The study of code-based cryptosystems needs still more work to obtain efficient and secure schemes, but also schemes with additional properties like identity-based encryption, batch-identification, blind signature or block cipher.

Encryption References

[1] E. Berlekamp, R. McEliece, and H. van Tilborg. On the Inherent Intractability of Certain Coding Problems. *IEEE Transactions on Information Theory*, IT-24(3), 1978.

[2] R. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory. The Deep Space Network Progress Report, DSN PR 42–44, 1978. `http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF`.

[3] H. Niederreiter. Knapsack-type Cryptosystems and Algebraic Coding Theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[4] R. Overbeck and N. Sendrier. *Code-Based Cryptography*, pages 95–146. Springer, 2008.

Identification References

[5] P. S. L. M. Barreto, R. Lindner, and R. Misoczki. Decoding Square-Free Goppa Codes over $\mathbb{F}_p$. Cryptology ePrint Archive, Report 2010/372, 2010. `http://eprint.iacr.org/`.

[6] T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Progress in Cryptology – Africacrypt'2009*, volume 5580 of *LNCS*, pages 77–97. Springer, 2009.

[7] D. J. Bernstein. List Decoding for Binary Goppa Codes. Preprint, 2008. `http://cr.yp.to/papers.html#goppalist`.

[8] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*. Springer, 2008.

[9] B. Biswas and N. Sendrier. Mceliece Cryptosystem Implementation: Theory and Practice. In *PQCrypto*, pages 47–62, 2008.

[10] P. Gaborit. Shorter Keys for Code-based Cryptography. In *International Workshop on Coding and Cryptography – WCC'2005*, pages 81–91, Bergen, Norway, 2005. ACM Press.

[11] P. Loidreau. Designing a rank metric based McEliece cryptosystem. 6061:142–152, 2010.

[12] R. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory. The Deep Space Network Progress Report, DSN PR 42–44, 1978. `http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF`.

[13] R. Misoczki and P. S. L. M. Barreto. Compact McEliece Keys from Goppa Codes. Preprint, 2009. `http://eprint.iacr.org/2009/187.pdf`.

[14] H. Niederreiter. Knapsack-type Cryptosystems and Algebraic Coding Theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

Signature References

[15] P.-L. Cayrel, P. Gaborit P., and E. Prouff. Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices. *CARDIS*, 2008.

[16] P.-Louis Cayrel, P. Véron, and S. M. Y. Alaoui. A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In *Selected Areas in Cryptography*, pages 171–186, 2010.

[17] P. Gaborit and M. Girault. Lightweight Code-based Authentication and Signature. In *IEEE International Symposium on Information Theory – ISIT'2007*, pages 191–195, Nice, France, 2007. IEEE.

[18] A. Shamir. An Efficient Identification Scheme Based on Permuted Kernels. In *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '89, pages 606–609, London, UK, 1990. Springer-Verlag.

[19] J. Stern. Designing Identification Schemes with Keys of Short Size. In *Advances in Cryptology – Proceedings of CRYPTO '94*, volume 839, pages 164–173, 1994.

[20] J. Stern. A New Identification Scheme Based on Syndrome Decoding. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, pages 13–21, New York, NY, USA, 1994. Springer-Verlag New York, Inc.

Secret Key References

[21] M. Alabbadi and S. B. Wicker. Security of Xinmei Digital Signature Scheme, 1992.

[22] M. Alabbadi and S. B. Wicker. Digital Signature Scheme Based on Error-Correcting Codes. In *IEEE International Symposium on Information Theory*, pages 9–19. IEEE, 1993.

[23] P. S. L. M. Barreto, P.-L. Cayrel, R. Misoczki, and R. Niebuhr. Quasi-dyadic CFS signatures. In *Inscrypt 2010*, volume 6584 of *LNCS*. Springer, Oct 2010.

[24] P. S. L. M. Barreto, R. Misoczki, and M. A. Simplício Jr. One-Time Signature Scheme from Syndrome Decoding over Generic Error-Correcting Codes. *Journal of Systems and Software*, 84(2):198–204, 2011.

[25] E. Berlekamp, R. McEliece, and H. van Tilborg. On the Inherent Intractability of Certain Coding Problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[26] P.-L. Cayrel, A. Otmani, and D. Vergnaud. On Kabatianskii-Krouk-Smeets Signatures. *WAIFI 2007*, Springer C. Carlet and B. Sunar LNCS:237–251, 2007.

[27] L. Dallot. Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme. Proceedings of WEWoRC 2007, Bochum, Germany, 2007. `http://users.info.unicaen.fr/~ldallot/download/articles/CFSProof-dallot.pdf`.

[28] M. Finiasz. Parallel-CFS: Strengthening the CFS Mc-Eliece-Based Signature Scheme. In A. Biryukov, G. Gong, and D. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *LNCS*, pages 159–170. Springer, 2010.

[29] M. Finiasz and N. Sendrier. Security Bounds for the Design of Code-based Cryptosystems. In *To appear in Advances in Cryptology – Asiacrypt'2009*, 2009. `http://eprint.iacr.org/2009/414.pdf`.

[30] L. Harn and D. C. Wang. Cryptoanalysis and Modification of Digital Signature Scheme Based on Error-Correcting Codes, 1992.

[31] G. Kabatianskii, E. Krouk, and B. J. M. Smeets. A Digital Signature Scheme Based on Random Error-Correcting Codes. *IMA Int. Conf.*, LNCS 1355:161–167, 1997.

[32] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *Advances in Cryptology – CRYPTO '89*, LNCS, pages 239–252. Springer, 1989.

Cryptanalysis References

[33] D. Augot, M. Finiasz, P. Gaborit, S. Manuel, and N. Sendrier. SHA-3 Proposal: FSB. Submission to the SHA-3 NIST Competition, 2008.

[34] D. Augot, M. Finiasz, and N. Sendrier. A Fast Provably Secure Cryptographic Hash Function. Cryptology ePrint Archive, Report 2003/230, 2003. `http://eprint.iacr.org/`.

[35] D. Augot, M. Finiasz, and N. Sendrier. A Family of Fast Syndrome Based Cryptographic Hash Functions. In *In E. Dawson and S. Vaudenay (Eds.), MyCrypt 2005, SpringerVerlag LNCS 3615*, pages 64–83. Springer, 2005.

[36] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental Cryptography: The Case of Hashing and Signing. In *Proc. of the 14th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '94, pages 216–233. Springer, 1994.

[37] M. Bellare and D. Micciancio. A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost. In *In Eurocrypt97*, pages 163–192. Springer, 1997.

[38] T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Progress in Cryptology – Africacrypt'2009*, volume 5580 of *LNCS*, pages 77–97. Springer, 2009.

[39] D. J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Faster 2-regular Information-Set Decoding, 2011.

[40] D. J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Really Fast Syndrome-Based Hashing. Cryptology ePrint Archive, Report 2011/074, 2011. `http://eprint.iacr.org/`.

[41] I. Damgård. A Design Principle for Hash Functions. In G. Brassard, editor, *Advances in Cryptology — CRYPTO'89, Proc.*, volume 435 of *LNCS*, pages 416–427. Springer, 1990.

[42] J.-B. Fischer and J. Stern. An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding. In *LNCS*, volume 1070 of *LNCS*, pages 245–255. Springer-Verlag, 1996.

[43] P. Gaborit, C. Laudauroux, and N. Sendrier. SYND: A Fast Code-Based Stream Cipher with a Security Reduction. In *Proceeedings of ISIT'07*, 2007.

[44] P. Guillot. Algorithmes pour le codage á poids constant. Unpublished.

[45] R. C. Merkle. One Way Hash Functions and DES. In G. Brassard, editor, *Advances in Cryptology — CRYPTO'89, Proc.*, volume 435 of *LNCS*, pages 428–446. Springer, 1990.

[46] A. L. Zobrist. A New Hashing Method with Application for Game Playing. Technical Report 88, U. Wisconsin CS Department, April 1970. `https://www.cs.wisc.edu/techreports/1970/TR88.pdf`.

Others References

[47] D. Augot, M. Finiasz, and N. Sendrier. A Family of Fast Syndrome Based Cryptographic Hash Functions. In *In E. Dawson and S. Vaudenay (Eds.), MyCrypt 2005, SpringerVerlag LNCS 3615*, pages 64–83. Springer, 2005.

[48] T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing Key Length of the McEliece Cryptosystem. In *Progress in Cryptology – Africacrypt'2009*, volume 5580 of *LNCS*, pages 77–97. Springer, 2009.

[49] D. J. Bernstein. Grover vs. McEliece. In *PQCrypto*, pages 73–80, 2010.

[50] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography.* Springer, 2008.

[51] D. J. Bernstein, T. Lange, and C. Peters. Attacking and Defending the McEliece Cryptosystem. In J. Buchmann and J. Ding, editors, *PQCrypto*, volume 5299 of *LNCS*, pages 31–46. Springer, 2008.

[52] D. J. Bernstein, T. Lange, and C. Peters. Ball-Collision Decoding. Cryptology ePrint Archive, Report 2010/585, 2010. `http://eprint.iacr.org/`.

[53] D. J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Faster 2-regular Information-Set Decoding. Cryptology ePrint Archive, Report 2011/120, 2011. `http://eprint.iacr.org/`.

[54] A. Canteaut and F. Chabaud. A New Algorithm for Finding Minimum-Weight Words in a Linear Code: Application to Primitive Narrow-Sense BCH-Codes of Length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998.

[55] C. Peters D. J. Bernstein, T. Lange and H. C. A. van Tilborg. Explicit Bounds for Generic Decoding Algorithms for Code-Based Cryptography. In *Pre-proceedings of WCC 2009*, pages 168–180, 2009.

[56] J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate mceliece cryptosystems. Cryptology ePrint Archive, Report 2010/331, 2010. `http://eprint.iacr.org/`.

[57] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In H. Gilbert, editor, *EUROCRYPT*, volume 6110 of *LNCS*, pages 279–298. Springer, 2010.

[58] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece Variants with Compact Keys – Towards a Complexity Analysis. In *SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography*, pages 45–55, RHUL, June 2010.

[59] M. Finiasz and N. Sendrier. Security Bounds for the Design of Code-based Cryptosystems. In *To appear in Advances in Cryptology – Asiacrypt'2009*, 2009. `http://eprint.iacr.org/2009/414.pdf`.

[60] V. Gauthier and G. Leander. Practical Key Recovery Attacks on Two McEliece Variants. Cryptology ePrint Archive, Report 2009/509, 2009. `http://eprint.iacr.org/`.

[61] L. K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In *STOC*, pages 212–219, 1996.

[62] P. J. Lee and E. F. Brickell. An Observation on the Security of McEliece's Public-Key Cryptosystem. *j-LECT-NOTES-COMP-SCI*, 330:275–280, 1988.

[63] J. S. Leon. A Probabilistic Algorithm for Computing Minimum Weights of Large Error-Correcting Codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, 1988.

[64] L. Minder and A. Sinclair. The Extended k-tree Algorithm. In *SODA*, pages 586–595, 2009.

[65] R. Misoczki and P. S. L. M. Barreto. Compact McEliece Keys from Goppa Codes. Preprint, 2009. `http://eprint.iacr.org/2009/187.pdf`.

[66] R. Niebuhr, P.-L. Cayrel, and J. Buchmann. Improving the Efficiency of Generalized Birthday Attacks Against Certain Structured Cryptosystems. In *WCC 2011*, Apr 2011.

[67] R. Niebuhr, P.-L. Cayrel, S. Bulygin, and J. Buchmann. On Lower Bounds for Infor-

mation Set Decoding over $\mathbb{F}_q$. In *SCC 2010, RHUL, London, UK*, 2010.

[68] A. Otmani, J.-P. Tillich, and L. Dallot. Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Preprint, 2008. `http://arxiv.org/abs/0804.0409v2`.

[69] R. Overbeck. Structural Attacks for Public Key Cryptosystems Based on Gabidulin Codes. *J. Cryptology*, 21(2):280–301, 2008.

[70] R. Overbeck and N. Sendrier. *Code-Based Cryptography*, pages 95–146. Springer, 2008.

[71] C. Peters. Information-Set Decoding for Linear Codes over $\mathbb{F}_q$. In *PQCrypto*, pages 81–94, 2010.

[72] E. Prange. The Use of Information Sets in Decoding Cyclic Codes. *IRE Transactions on Information Theory*, pages 5–9, 1962.

[73] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26:1484–1509, 1995.

[74] V. Sidelnikov and S. Shestakov. On Cryptosystems based on Generalized Reed-Solomon Codes. *Discrete Mathematics*, 4(3):57–63, 1992.

[75] J. Stern. A Method for Finding Codewords of Small Weight. In *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer-Verlag, 1988.

[76] D. Wagner. A Generalized Birthday Problem. In *LNCS*, volume 2442 of *LNCS*, pages 288–304. Springer-Verlag, 2002.

[77] C. Wieschebrink. Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. In *IEEE International Symposium on Information Theory – ISIT'2006*, pages 1733–1737, Seattle, USA, 2006. IEEE.

Conclusion References

[78] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*. Springer, 2008.