On the Use of Structured Codes in Code Based Cryptography[1]

Nicolas Sendrier[†]

[†]*INRIA, CRI Paris-Rocquencourt, Project-Team SECRET*
Email: `Nicolas.Sendrier@inria.fr`
WWW: `http://www-roc.inria.fr/secret/Nicolas.Sendrier/`

Abstract

Recent papers have considered the use of linear codes with structure (cyclic, dyadic) to reduce the public key size of code-based public key encryption schemes (McEliece, Niederreiter). We review here the security of those cryptosystems and examine what happens when structured codes are used.

1. Introduction

Following a work by Philippe Gaborit [9], several new encryption schemes, based on McEliece system [14], have been proposed [2, 15] which allow a huge reduction of the public key size (by a factor 10 or more). The question we address here is to determine on which ground the security of those new approaches is funded.

We will first review the theoretical and practical security of those systems. Once we have ascertain that there is room for interesting tradeoffs between security and key size we will examine which aspects of the security are changed by the use of structured codes. We will conclude with a few open questions.

Notations:

- $\mathbf{F}_q$ the finite field with q elements
- $\mathrm{dist}(\cdot,\cdot)$ the Hamming distance (by default over $\mathbf{F}_q$)
- $\mathrm{wt}(\cdot)$ the Hamming weight
- $\mathcal{S}_n(\mathbf{0},t)$ the sphere centered in zero of radius t of the Hamming space $\mathbf{F}_q^n$, it is the set of q-ary words of length n and Hamming weight t.

[1] Appeared in Nikova, S., Preneel, B., Storme, L., eds.: Coding Theory and Cryptography III. Contactforum. *Koninklijke Vlaamse Academie van België voor Wetenschaeppen en Kunsten* (2009), pp. 59–68

2. Code-Based Public Key Encryption

The cryptogram in McEliece public-key encryption scheme is a codeword of some public linear code to which errors are added. Only the legal user, who knows the hidden algebraic structure of the code, can remove those errors and recover the cleartext. The public key is a generator matrix of the public code and the secret key is the algebraic structure of this code (*i.e.* an algebraic decoder). In the Niederreiter scheme, the public key is a parity check matrix H of the code, the cleartext is a correctable error pattern e and the cryptogram is the syndrome eH^T. It is equivalent in term of security [12].

In the most general setting we consider a family of linear codes $\mathcal{F}_{n,t}$ parameterized by the code length n and the number t of correctable errors. For each code in $\mathcal{F}_{n,t}$, an efficient algebraic decoding procedure correcting t errors is available. In practice for a given family (binary Goppa codes for instance) and for a fixed pair (n, t) of security parameters, the code dimension k will be the same function of n and t for all elements of $\mathcal{F}_{n,t}$ (for instance $k = n - t\lceil\log_2 n\rceil$ for Goppa codes). Finally, there is another parameter, the alphabet size q. It is implicit with the choice of the code family, we keep it that way to maintain reasonably light notations. Unless specified otherwise, the alphabet will be the finite field $\mathbf{F}_q$. The linear codes and Hamming distance will be defined over $\mathbf{F}_q^n$.

There are two main classes of public-key encryption schemes based on codes, they were proposed by McEliece in 1978 [14] and Niederreiter in 1986 [16]:

(Generalized) McEliece PKC(n, t), $C \in \mathcal{F}_{n,t}$ of dimension k
Public key: $G \in \mathbf{F}_q^{k\times n}$ a generator matrix of C.
Secret key: Ψ a t-error correcting procedure[2] for C.
Encryption: $x \mapsto xG + e$, with $x \in \mathbf{F}_q^k$ and e of Hamming weight t.
Decryption: $y \mapsto \Psi(y)G^*$, with $y \in \mathbf{F}_q^n$ and G^* a right inverse of G.

Niederreiter PKC(n, t), $C \in \mathcal{F}_{n,t}$ of codimension r
Public key: $H \in \mathbf{F}_q^{r\times n}$ a parity check matrix C.
Secret key: Ψ a t-error correcting procedure[2] for C.
Encryption: $e \mapsto eH^T$, with $e \in \mathcal{S}_n(\mathbf{0}, t)$.
Decryption: $s \mapsto sH^{*T} - \Psi(sH^{*T})$, with $s \in \mathbf{F}_q^r$ and H^* a right inverse of H.

Goppa codes. In the original description the McEliece encryption scheme is defined with irreducible binary Goppa codes of maximal length. Those codes have length $n = 2^m$, correct t errors and have dimension $k = n - tm$. It may be of interest to choose $n \leq 2^m$ to tune the parameters [3]. In practice will we assume that $n > 2^{m-1}$ and thus the t-error correcting binary Goppa codes of length n will have codimension $r = tm$ (and dimension $k = n - tm$) where $m = \lceil\log_2 n\rceil$.

[2] Ψ is t-error correcting for C if for all $z \in C$ and $y \in \mathbf{F}_q^n$, $\mathrm{dist}(z, y) \leq t$ implies $\Psi(y) = z$.

3. Security Proof

In this section we will give a reductional proof of security for the Niederreiter encryption scheme (a similar proof could be made for the McEliece system but is a bit less convenient). We will denote $\mathcal{F}_{n,t}$ the code family. We will assume that all codes of $\mathcal{F}_{n,t}$ have a codimension $r = \theta(n,t)$. We denote by $\mathcal{K}_{n,t} \subset \mathbf{F}_q^{r \times n}$ the set of corresponding public keys. We will speak for short of the $\mathcal{K}_{n,t}$-Niederreiter scheme.

3.1. Decoder, Adversary and Distinguisher

We present below idealized attack models. We fix the parameters n, t and $r = \theta(n,t)$ and the public key space $\mathcal{K}_{n,t} \subset \mathbf{F}_q^{r \times n}$. We consider the probability space Ω consisting of the sample space $\mathbf{F}_q^{r \times n} \times \mathcal{S}_n(\mathbf{0}, t)$ equipped with the uniform distribution. We denote $(H, e) \in \mathbf{F}_q^{r \times n} \times \mathcal{S}_n(\mathbf{0}, t)$ the corresponding random variables.

- A program $\mathcal{D} : \mathbf{F}_q^{r \times n} \to \{0,1\}$ is a (T, ε)-distinguisher for $\mathcal{K}_{n,t}$ if it runs in time at most T and

  $$\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t}) = \left| \Pr_{\Omega}(\mathcal{D}(H) = 1 \mid H \in \mathcal{K}_{n,t}) - \Pr_{\Omega}(\mathcal{D}(H) = 1) \right| \geq \varepsilon.$$

  The quantity $\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t})$ is called the advantage of $\mathcal{D}$ for $\mathcal{K}_{n,t}$.

  A distinguisher is efficient if the ratio T/ε is small (upper bounded by a polynomial in n and t). If there is no efficient distinguisher then the set of keys $\mathcal{K}_{n,t}$ is *pseudorandom* in the sense that there is no easy way to decide where or not a matrix in $\mathbf{F}_q^{r \times n}$ is or is not a valid public key.

- A program $\mathcal{A} : \mathbf{F}_q^{r \times n} \times \mathbf{F}_q^r \to \mathcal{S}_n(\mathbf{0}, t)$ is a (T, ε)-decoder for (n, t) if it runs in time at most T and

  $$\mathrm{Succ}(\mathcal{A}) = \Pr_{\Omega}(\mathcal{A}(H, eH^T) = e) \geq \varepsilon.$$

  A decoder is efficient if the ratio T/ε is small (upper bounded by a polynomial in n and t). The existence of an efficient decoder is related to the difficulty of the bounded decoding problem in the average case (for instance the Goppa Bounded Decoding when the Goppa codes are used for the keys).

- A program $\mathcal{A} : \mathbf{F}_q^{r \times n} \times \mathbf{F}_q^r \to \mathcal{S}_n(\mathbf{0}, t)$ is a (T, ε)-adversary against $\mathcal{K}_{n,t}$-Niederreiter if it runs in time at most T and

  $$\mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}) = \Pr_{\Omega}(\mathcal{A}(H, eH^T) = e \mid H \in \mathcal{K}_{n,t}) \geq \varepsilon.$$

  The absence of efficient adversary means that the Niederreiter scheme is difficult to break in average when the message and the key are chosen randomly and uniformly in $\mathcal{S}_n(\mathbf{0}, t) \times \mathcal{K}_{n,t}$. It exactly means that the system is a one-way encryption scheme.

3.2. Security Reduction

Proposition 3.1 *We fix the security parameters (n, t) and $r = \theta(n, t)$ and denote $\mathcal{K}_{n,t}$ the public key space. If there exists a (T, ε)-adversary against $\mathcal{K}_{n,t}$-Niederreiter, then there exists either*

- *a $(T, \varepsilon/2)$-decoder for (n, t),*
- *or a $(T + O(n^2), \varepsilon/2)$-distinguisher for $\mathcal{K}_{n,t}$.*

Proof: Let $\mathcal{A} : \mathbf{F}_q^{r\times n} \times \mathbf{F}_q^r \to \mathcal{S}_n(\mathbf{0}, t)$ be a (T, ε)-adversary against $\mathcal{K}_{n,t}$-Niederreiter. We define the following distinguisher:

```
$\mathcal{D}$: input $H \in \mathbf{F}_q^{r\times n}$
  $e \leftarrow \mathcal{S}_n(\mathbf{0}, t)$        // pick randomly and uniformly
  if ($\mathcal{A}(H, eH^T) = e$) then return 1 else return 0
```

We have

$$\begin{array}{lcl} \Pr_\Omega(\mathcal{D}(H) = 1) & = & \Pr_\Omega(\mathcal{A}(H, eH^T) = e) & = & \mathrm{Succ}(\mathcal{A}) \\ \Pr_\Omega(\mathcal{D}(H) = 1 \mid H \in \mathcal{K}_{n,t}) & = & \Pr_\Omega(\mathcal{A}(H, eH^T) = e \mid H \in \mathcal{K}_{n,t}) & = & \mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}) \end{array}$$

and thus

$$\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t}) = |\mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}) - \mathrm{Succ}(\mathcal{A})|,$$

which implies, in particular

$$\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t}) + \mathrm{Succ}(\mathcal{A}) \geq \mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}) \qquad (1)$$

Because $\mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}) \geq \varepsilon$, we either have $\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t})$ or $\mathrm{Succ}(\mathcal{A})$ (which are both positive) greater or equal to $\varepsilon/2$. Finally, the running time of $\mathcal{D}$ is equal to the running of $\mathcal{A}$ plus the cost for picking e and computing the product eH^T which cannot exceed $O(n^2)$. So either $\mathcal{A}$ is a $(T, \varepsilon/2)$-decoder for (n, t) or $\mathcal{D}$ is a $(T + O(n^2), \varepsilon/2)$-distinguisher for $\mathcal{K}_{n,t}$. □

3.3. Difficult Problems and Security Assumptions

3.3.1. Pseudo-Randomness of Goppa Codes

We consider here the problems related to the security of the public key. Given the public key of some code-based system, can it be distinguished from a random matrix of same size?

Goppa Code Distinguishing (n, t)
Instance: $H \in \{0, 1\}^{r\times n}$, where $r = t\lceil \log_2 n\rceil$
Question: Is $H \in \mathcal{K}_{n,t}$?

For the security reduction of code-based systems, we will use this distinguishing problem. For a practical attack though, a distinguisher might not be sufficient.

3.3.2. Hardness of Decoding Up to the Goppa Bound

Goppa Bounded Decoding (n, t)
Instance: $H \in \{0,1\}^{r \times n}$, $s \in \{0,1\}^r$, where $r = t\lceil \log_2 n \rceil$
Output: $e \in \{0,1\}^n$ such that $\mathrm{wt}(e) \leq t$ and $eH^T = s$

The decision problem associated to the above problem is NP-complete [8]. Informally, it states that it is difficult, in the worst case, to decode in a random code the number of errors that a Goppa code of same length and dimension would decode.

3.3.3. Assumptions and Security Statement

For the Niederreiter scheme using binary Goppa codes, we will make the following two assumptions:

- *Pseudorandomness of Goppa codes:* distinguishing parity check matrices of irreducible binary Goppa codes from random binary matrices of same size is difficult in average.

- *Hardness of decoding up to the binary Goppa bound*: decoding in a binary code as many error as a Goppa code of same parameters is difficult in average.

Those two assumptions relate to the difficult problems presented in the beginning of this section. They are usually considered to hold, more precisely it is possible to find security parameters (n, t) such that they hold simultaneously.

Finally, thanks to Proposition 3.1, it is possible to claim that, under the two above assumptions, the Niederreiter (or McEliece) encryption scheme using irreducible binary Goppa codes is secure.

4. Practical Security

We will not give here full details about the attacks on the McEliece or Niederreiter schemes, but simply report the best known attacks on the message (decoding) or on the key (distinguisher). Moreover, since this section is just meant to illustrate the gap between the best message attack and the best key attack, we will assume that binary Goppa codes are being used.

4.1. Best Known Attacks on the Message

Attacking a message consist in decoding in a random binary linear code. The best known algorithms are derived form Stern's variant of information set decoding [19, 4, 3]. We will use here lower bounds given in [7]. For decoding t errors in a binary code of length n and dimension

k ($r = n - k$ is the co-dimension) the number of binary operations is lower bounded by:

$$\min_p \frac{2\ell\binom{n}{t}}{\binom{r-\ell}{t-p}\sqrt{\binom{k+\ell}{p}}} \text{ where } \ell = \log\left(2(t-p)\sqrt{\binom{k+\ell}{p}}\right).$$

4.2. Best Known Attacks on the Public Key

Attacks on the public key are very few. To recover a binary Goppa code from the public key, the best known technique is reported in [13]. It consists essentially in running one instance of the support splitting algorithm [18] for all binary irreducible Goppa code. The cost, in binary operations, for recovering a t-error correcting Goppa code of length $n = 2^m$ from a public key is at least

$$\min(R^2, (1-R)^2)\frac{2^{tm}}{tm},$$

where $R = (n - tm)/n$ is the code transmission rate.

4.3. The Gap Between Key and Message Securities

(m,t)	sizes					security	
	McEliece		Niederreiter		public key	(in bits)	
	cipher	plain	cipher	plain	(systematic)	message	key
$(10,50)$	1024	524	500	284	32 kB	60	491
$(11,32)$	2048	1696	352	233	73 kB	86	344
$(12,40)$	4096	3616	480	320	212 kB	127	471

Table 1: Main features of Goppa code-based encryption schemes

The Table 1 presents the main features of McEliece or Niederreiter public key encryption schemes using irreducible Goppa codes. The last two columns give the number of security bits (the logarithm in base two of the cost of the best known attack) for the two above attacks and for typical parameters. It is remarkable that there is a huge gap between those two numbers. Relating this fact with the main drawback of the McEliece scheme which is the public key size leads to an obvious, important and difficult question:

Can we trade some of the key security for a reduced key size?

The end of this paper is devoted to the status of this problem in the current state of the art.

5. Using Families of Structured Codes

The pioneering work concerning the question of reducing the key size in code-based cryptosystems is due to Philippe Gaborit. He proposed in [9] to use quasi-cyclic codes in McEliece cryptosystem. Several propositions were made and weakened in turn. We present later in this section an quick survey of situation. Meanwhile we explain how the security reduction changes and which approach are the most reasonable for the cryptanalists and the designers.

5.1. Security Reduction for Structured Codes

We assume that structured codes are used in Niederreiter (or McEliece) encryption scheme. In practice, for given parameters (n, t), this means that the set of public keys $\mathcal{K}_{n,t}$ belongs to a particular subset $\mathcal{H}_{n,t}$ of $\mathbf{F}_q^{r\times n}$, where $r = \theta(n, t)$ is the codimension of the (structured) codes being used in that particular instance of the cryptosystem. This subset $\mathcal{H}_{n,t}$ consists of matrices which are, for instance, circulant by block [9, 2] or "dyadic" by block [15], and can be represented in very compact manner.

In that case the security reduction changes. We wish now to distinguish a public key from a random element in $\mathcal{H}_{n,t}$. Similarly we want the decoding to be difficult when the parity check matrix is randomly chosen in $\mathcal{H}_{n,t}$. Using the notations of §3, we redefine the advantage of a distinguisher $\mathcal{D}$ for $\mathcal{K}_{n,t}$ against $\mathcal{H}_{n,t}$ as

$$\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t}, \mathcal{H}_{n,t}) = \left|\Pr_{\Omega}(\mathcal{D}(H) = 1 \mid H \in \mathcal{K}_{n,t}) - \Pr_{\Omega}(\mathcal{D}(H) = 1 \mid H \in \mathcal{H}_{n,t})\right|.$$

Also instead of a decoder for generic linear codes, we are interested in a decoder for generic structured codes, in practice the success probability we are interested is

$$\mathrm{Succ}(\mathcal{A}, \mathcal{H}_{n,t}) = \Pr_{\Omega}(\mathcal{A}(H, eH^T) = e \mid H \in \mathcal{H}_{n,t})$$

Now if we consider the Proposition 3.1 and its proof, the inequality (1), is replaced by

$$\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{n,t}, \mathcal{H}_{n,t}) + \mathrm{Succ}(\mathcal{A}, \mathcal{H}_{n,t}) \geq \mathrm{Succ}(\mathcal{A}, \mathcal{K}_{n,t}). \tag{2}$$

In other words, we relate now the security of $\mathcal{K}_{n,t}$-Niederreiter (the right-hand term of the above inequality) to the distinguishability of the public keys against the structured matrices of $\mathcal{H}_{n,t}$ and the hardness of decoding in structured codes.

5.2. Message Security for Structured Codes

Decoding in a random quasi-cyclic code is NP-complete[3], the same probably holds for quasi-dyadic codes. As for random codes, fifty years of practice of algebraic coding theory indicates that this decoding problem is likely to be hard in the average case. Else, we could produce reasonably good codes that could be efficiently decoded by picking them randomly, which is something coding theorists have stopped dreaming of for a few decades. Restricting the random choice to quasi-cyclic or quasi-dyadic codes would lead to an even stronger statement.

In short, restricting the generic decoding problem to quasi-cyclic or quasi-dyadic codes is not going to make it significantly easier than for random codes.

[3] Matthieu Finiasz, private communication

5.3. Key Security for Structured Codes

If we consider the inequality (2) and admit that generic decoding is not much easier with structure, then only the key security really makes a difference when we consider instance of code-based cryptosystem using codes with structure. This correspond to the intuition and is exactly what was intended, that is trading key security for key size. The problem now is to quantify this security loss.

An attack of original proposal by Gaborit [9] was published recently[4] [17]. Several more resistant proposals were made in 2009 [2, 15] but were seriously weakened very recently by an algebraic cryptanalysis [21, 6]. The strongest of the mentioned proposals still resist but it is certainly advisable to fully understand the new attack class before maintaining strong security claims.

5.4. Conclusion and Open Problems

First let us remark that whenever code-based cryptography do not require a decoding trapdoor, using structured codes is likely to be safe. This was successfully use for a variant [10] of Stern's zero-knowledge identification scheme [20], for designing a stream cipher [11], or a cryptographic hash function [1].

The situation is different for the public key encryption schemes (or the signature scheme [5]). The dark side of the new cryptanalytic results is that they leave little hope for the new constructions to remain secure. The bright side is that a better understanding of the attacks can probably allow good tradeoffs. In practice, the principle of [21, 6] is to write an algebraic system whose solution reveals the hidden algebraic structure of the code. Writing this system is always possible, even for irreducible Goppa codes, but in general the number of unknown is too large. By adjusting the order of quasi-cyclicity, the number of unknowns can increase (the same thing holds for quasi-dyadic codes). Of course, doing this will not allow a key reduction of same magnitude. The question becomes:

> *Can we understand the key recovery algebraic attacks on structured codes well enough to find a satisfactory tradeoff and reduce safely the public key size of the McEliece scheme?*

References

[1] D. Augot, M. Finiasz, Ph. Gaborit, S. Manuel, and N. Sendrier. SHA-3 proposal: FSB. Submission to the SHA-3 NIST competition, 2008.

[2] T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the mceliece cryptosystem. In B. Preneel, editor, *Progress in Cryptology – AFRICACRYPT 2009*, number 5580 in LNCS, pages 77–97. Springer-Verlag, 2009.

[4] a preprint presenting this work was available since 2008

[3] D. Bernstein, T. Lange, and C. Peters. Attacking and defending the McEliece cryptosystem. In J. Buchmann and J. Ding, editors, *Post-Quantum Cryptography*, number 5299 in LNCS, pages 31–46. Springer-Verlag, 2008.

[4] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.

[5] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001*, number 2248 in LNCS, pages 157–174. Springer-Verlag, 2001.

[6] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In H. Gilbert, editor, *Eurocrypt 2010*, number 6110 in LNCS. Springer, 2010. To appear.

[7] M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, number 5912 in LNCS, pages 88–105. Springer, 2009.

[8] Matthieu Finiasz. *Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clef publique*. Thèse de doctorat, École Polytechnique, October 2004.

[9] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of WCC 2005*, pages 81–90, 2005.

[10] P. Gaborit and M. Girault. Lightweight code-based identification and signature. In *IEEE Conference, ISIT'07*, pages 191–195, Nice, France, July 2007. IEEE.

[11] P. Gaborit, C. Laudaroux, and N. Sendrier. Synd: a very fast code-based stream cipher with a security reduction. In *IEEE Conference, ISIT'07*, pages 186–190, Nice, France, July 2007. IEEE.

[12] Y. X. Li, R. H. Deng, and X. M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, January 1994.

[13] P. Loidreau and N. Sendrier. Weak keys in McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3):1207–1212, April 2001.

[14] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.,* Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, January 1978.

[15] R. Misoczki and P. Barreto. Compact McEliece keys from Goppa codes. In M. J. Jacobson Jr., V. Rijmen, and R. Safavi-Naini, editors, *Selected Areas in Cryptography*, number 5867 in LNCS, pages 276–392. Springer, 2009.

[16] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

[17] A. Otmani, J.-P. Tillich, and L. Dallot. Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140, April 2010.

[18] N. Sendrier. Finding the permutation between equivalent codes: the support splitting algorithm. *IEEE Transactions on Information Theory*, 46(4):1193–1203, July 2000.

[19] J. Stern. A method for finding codewords of small weight. In G. Cohen and J. Wolfmann, editors, *Coding theory and applications*, number 388 in LNCS, pages 106–113. Springer-Verlag, 1989.

[20] J. Stern. A new identification scheme based on syndrome decoding. In D. R. Stinson, editor, *Advances in Cryptology - CRYPTO'93*, number 773 in LNCS, pages 13–21. Springer-Verlag, 1993.

[21] V. G. Umana and G. Leander. Practical key recovery attacks on two McEliece variants. Cryptology ePrint Archive, Report 2009/509, 2009. `http://eprint.iacr.org/`.