Code-based cryptography: 101

Class 2

Gustavo Banegas

Inria and Laboratoire d'Informatique de l'Ecole polytechnique, France
gustavo@cryptme.in
https://www.cryptme.in

June 1, 2022

Outline

McEliece vs Niederreiter

Signatures

Code-based cryptography 101

Recap of McEliece...

- Let C be a length-n binary Goppa code Γ of dimension k with minimum distance $2t+1$ where $t \approx (n-k)/\log_2(n)$; original parameters (1978) $n = 1024$, $k = 524$, $t = 50$.
- The McEliece secret key consists of a generator matrix G for Γ, an efficient t-error correcting decoding algorithm for Γ; an $n \times n$ permutation matrix P and a nonsingular $k \times k$ matrix S.
- n, k, t are public; but Γ. P, S are randomly generated secrets.
- The McEliece public key is $k \times n$ matrix $G' = SGP$.

Niederreiter cryptosystem

Niederreiter

- Use $n \times n$ permutation matrix P and $(n-k) \times (n-k)$ invertible matrix S.
- Generate the parity matrix H, for a linear code (usually Binary Goppa Code). The public key is $K = SHP$. The private key is (S, H, P)

Niederreiter cryptosystem

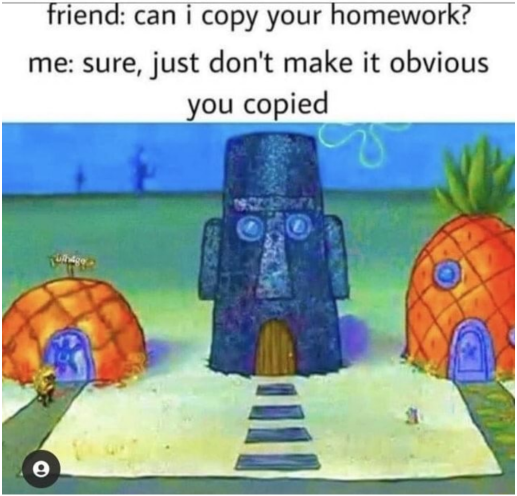
Niederreiter

Basically, Niederreiter did the following:

Niederreiter cryptosystem

Niederreiter

Basically, Niederreiter did the following:



Niederreiter cryptosystem

Niederreiter

Originally, Niederreiter proposed in 1986 the scheme with Reed-Solomon codes. However, it was broken in 1992[1].

[1] V. M. Sidelnikov & S. O. Shestakov (1992). "On the insecurity of cryptosystems based on generalized Reed-Solomon codes". Discrete Mathematics and Applications.

Niederreiter cryptosystem

Niederreiter

Originally, Niederreiter proposed in 1986 the scheme with Reed-Solomon codes. However, it was broken in 1992[1]. The proposal to make Niederreiter secure again was ...

[1] V. M. Sidelnikov & S. O. Shestakov (1992). "On the insecurity of cryptosystems based on generalized Reed-Solomon codes". Discrete Mathematics and Applications.

Niederreiter cryptosystem

Niederreiter

Originally, Niederreiter proposed in 1986 the scheme with Reed-Solomon codes. However, it was broken in 1992[1]. The proposal to make Niederreiter secure again was ... **use Binary Goppa codes**.

[1] V. M. Sidelnikov & S. O. Shestakov (1992). "On the insecurity of cryptosystems based on generalized Reed-Solomon codes". Discrete Mathematics and Applications.

Attacks against code-based

Attacks!

- Information Set Decoding: [Prange, 62]
- Relax the weight profile: [Lee & Brickell, 88]
- Compute sums on partial columns first: [Leon, 88]
- Use the birthday attack: [Stern, 89], [Dumer, 91]
- First "real" implementation: [Canteaut & Chabaud, 98]
- Initial McEliece parameters broken: [Bernstein, Lange, & Peters, 08]
- Lower bounds: [Finiasz & Sendrier, 09]

Attacks against code-based

Attacks!!

- Asymptotic exponent improved [May, Meurer, & Thomae, 11]
- Decoding one out of many [Sendrier, 11]
- Even better asymptotic exponent [Becker, Joux, May, & Meurer, 12]
- "Nearest Neighbor" variant [May & Ozerov, 15]
- Sublinear error weight [Canto Torres & Sendrier, 16]
- McEliece needs a Break – Solving McEliece-1284 and Quasi-Cyclic-2918 with Modern ISD [Esser, May, & Zweydinger, 21]

McEliece vs Niederreiter cryptosystem

Niederreiter

- McEliece:
  - Created in 1978;
  - It uses Binary Goppa Codes;
  - **Public Key:** $(k \times n)$ matrix $G' = SGP$;
  - **Private Key:** Γ, P, S.
- Niederreiter:
  - Created in 1986;
  - Originally, it uses Generalized Reed-Solomon codes (but it was broken)
  - For security, it uses Binary Goppa Codes;
  - **Public Key:** $((n - k) \times n)$ matrix $H' = SHP$;
  - **Private Key:** H, P, S.

SPOILER ALERT!

SPOILER ALERT!

This is the scenario in code-based signatures:

Digital Signatures

Digital Signatures

The main idea in a signature scheme is:

- Take the hash of a message m, such as $h = H(m)$;
- Sign h with a private key sk;
- Publish h and pk. Anyway can verify that m was properly signed, and it is valid.

Digital Signatures

Digital Signatures

The main idea of a Hash-and-Sign scheme is:

- Take the hash of a message m, such as $h = H(m)$;
- Sign h with a private key sk;
- Publish h and pk. Anyway can verify that m was properly signed, and it is valid.

Digital Signatures

Digital Signatures

How it is possible to do it in Code-based?
Let $H \in \mathbb{F}_2^{r \times n}$ a parity check matrix of a t-error correcting Goppa code.

Digital Signatures

Digital Signatures

How it is possible to do it in Code-based?
Let $H \in \mathbb{F}_2^{r \times n}$ a parity check matrix of a t-error correcting Goppa code. Signing:

- Hash the message m into $h(m) = s \in \mathbb{F}_2^r$;
- Find e of minimal weight such that $eH^T = s$;
- Use e as a signature.

Verification:

- hash the message m into $h(m) = s \in \mathbb{F}_2^r$;
- verify if $eH^T \stackrel{?}{=} s$.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[2] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$.

[2] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[2] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536

[2] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[2] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536 ($\approx 1.2Mb$).
Another problem is that it can only allows $t = 9$. So, the security is not the highest.

[2] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[2] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536 ($\approx 1.2Mb$).
Another problem is that it can only allows $t = 9$. So, the security is not the highest. In 2003/2004 Bleichenbacher's "Decoding One Out of Many"-type attack (unpublished) reduces the security to $\frac{1}{3}tm$.

[2] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[3] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$.

[3] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[3] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536

[3] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[3] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536 ($\approx 1.2Mb$).
Another problem is that it can only allows $t = 9$. So, the security is not the highest.

[3] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

CFS Signatures

In 2001, N. Courtois, Finiasz and Sendrier (CFS) published "How to achieve a McEliece-based digital signature scheme".[3] The parameters were:
$n = 2^m = 2^{16}$, $t = 9$, $r = n - k = tm = 144$. The public key H has size 144×65536 ($\approx 1.2Mb$).
Another problem is that it can only allows $t = 9$. So, the security is not the highest. In 2003/2004 Bleichenbacher's "Decoding One Out of Many"-type attack (unpublished) reduces the security to $\frac{1}{3}tm$.
** All this was using binary Goppa Codes **.

[3] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 157–174. Springer, 2001.

RankSign

RankSign

Besides the Goppa codes, there is Low Rank Parity Check (LRPC) codes. It doesn't use the "Hamming" metric, it uses rank metric. In 2017, RankSign was published as a signature[4].

[4] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Z'emor. RankSign - a signature proposal for the NIST's call. NIST PQC Call for Proposals, 2017. Round 1 Submission.

RankSign

RankSign

Besides the Goppa codes, there is Low Rank Parity Check (LRPC) codes. It doesn't use the "Hamming" metric, it uses rank metric. In 2017, RankSign was published as a signature[4].It is similar to CFS but it uses different codes. Guess what happened?

[4] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Z'emor. RankSign - a signature proposal for the NIST's call. NIST PQC Call for Proposals, 2017. Round 1 Submission.

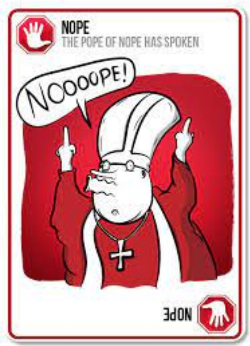
RankSign

RankSign

Besides the Goppa codes, there is Low Rank Parity Check (LRPC) codes. It doesn't use the "Hamming" metric, it uses rank metric. In 2017, RankSign was published as a signature. It is similar to CFS but it uses different codes. Guess what happened?

In 2018, it was broken. [a]

[a] T. Debris-Alazard and J.-P. Tillich. Two attacks on rank metric code-based schemes: RankSign and an IBE scheme. In International Conference on the Theory and Application of Cryptology and Information Security, pages 62–92. Springer, 2018.



Signature in Code-based

Signature in Code-based

All broken signatures in code-based:
CFS, RankSign, RaCCos, pqsigRM, LXY, KKS, and goes on...

Signature in Code-based

Signature in Code-based

All broken signatures in code-based:
CFS, RankSign, RaCCos, pqsigRM, LXY, KKS, and goes on...
'Safe' signature (so far): Wave, Durandal, and LESS.

Wave Code-based

Wave signature

Wave signature is a hash-and-sign. It was presented in 2019 at Asiacrypt.
The Wave trapdoor is built from two random linear codes U and V of length $n/2$ and dimensions k_U and k_V, respectively, over $\mathbb{F}_q$.
The codes U and V are combined to form a code W of length n, and dimension $k = k_U + k_V$.

Wave Code-based

Wave signature

The public key is a parity-check matrix $H \in \mathbb{F}_q^{(n-k \times n)}$ for the code W;

The private key consists of U, V, and data allowing us to map decoding problems into U and V;

Wave Code-based

Wave signature

The public key is a parity-check matrix $H \in \mathbb{F}_q^{(n-k \times n)}$ for the code W;

The private key consists of U, V, and data allowing us to map decoding problems into U and V; The parameters are the following:

Parameters	λ	q	n	w	$k = k_U + k_V$	d
Supertubos	128	3	8492	7980	$5605 = 3558 + 2047$	81

Wave Code-based

Wave signature

Wave works in $\mathbb{F}_3$. So, the arithmetic is not "boolean" any more. Also, can someone name a hash function that works in $\mathbb{F}_3$?

[5] Troika: a ternary cryptographic hash function

Wave Code-based

Wave signature

Wave works in $\mathbb{F}_3$. So, the arithmetic is not “boolean” any more. Also, can someone name a hash function that works in $\mathbb{F}_3$? There is one but it is slow (Troika[5]).

[5] Troika: a ternary cryptographic hash function

Wave Code-based

Wave signature in a Nutshell

Key Generation:

- Generate the SK, that is, subspace code of V and U;
- Generate the PK K that is the combination of V and U;

Wave Code-based

Wave signature in a Nutshell

Key Generation:

- Generate the SK, that is, subspace code of V and U;
- Generate the PK K that is the combination of V and U;

Signing:

- Hash the message m using a ternary hash function $s = H(m)$;
- Generate the error e using two decoders;
  - First generate an error e_v for the subspace V;
  - Then generate an error e_u for the subspace U;
  - return $e = e_v + e_u$.

Wave Code-based

Wave signature in a Nutshell

Key Generation:

- Generate the SK, that is, subspace code of V and U;
- Generate the PK K that is the combination of V and U;

Signing:

- Hash the message m using a ternary hash function $s = H(m)$;
- Generate the error e using two decoders;
  - First generate an error e_v for the subspace V;
  - Then generate an error e_u for the subspace U;
  - return $e = e_v + e_u$.

Verification:

- Hash the message m using a ternary hash function $s = H(m)$;
- Check the weight of $wt(e) \stackrel{?}{=} w$, abort if it is different;
- Check if $s \stackrel{?}{=} eK^T$, abort if it is different.

Wave Code-based

Wave signature

Pros and cons of Wave signature:

- Wave has the smallest signatures in code-based: 930 b;
- It has fast verification.

Wave Code-based

Wave signature

Pros and cons of Wave signature:

- Wave has the smallest signatures in code-based: 930 b;
- It has fast verification.

Cons:

- The public key has size around 4 Mb;
- Key generation and signature are slower than others;
  - It needs to compute the entire Gauss elimination: $O(n^3)$ (constant-time version);

Questions

Thank you for your attention.
Questions?
gustavo@cryptme.in