How to Sign using Restricted Errors

Violetta Weger

Summer
Doctoral Seminar
2023

July 25, 2023

Marco Baldi, Sebastian Bitzer
Alessio Pavoni, Paolo Santini
Antonia Wachter-Zeh

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

2022 reopened NIST standardization call for signature schemes

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

2022 reopened NIST standardization call for signature schemes

→ CROSS Signature scheme with restricted errors

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

2022 reopened NIST standardization call for signature schemes

→ CROSS Signature scheme with restricted errors

→ Paolo's talk: 40 submissions, 5 code-based, 7 MPC-in-the-head

Motivation

2016 NIST standardization call for post-quantum PKE/KEM and signatures

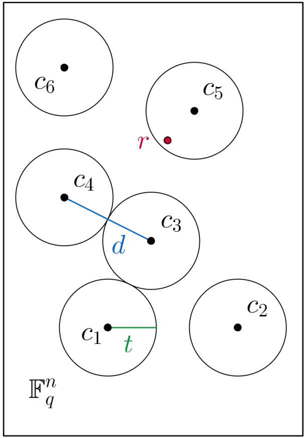
- PKE/KEM: 1 lattice-based, round 4: 3 code-based
- Signature schemes: 1 hash-based and 2 based on ideal lattices

2022 reopened NIST standardization call for signature schemes

→ CROSS Signature scheme with restricted errors

→ Paolo's talk: 40 submissions, 5 code-based, 7 MPC-in-the-head

Coding Theory



Set Up

- *Code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear k-dimensional subspace
- $c \in \mathcal{C}$ *codeword*
- $G \in \mathbb{F}_q^{k \times n}$ *generator matrix* $\mathcal{C} = \{xG \mid x \in \mathbb{F}_q^k\}$
- $H \in \mathbb{F}_q^{(n-k) \times n}$ *parity-check matrix* $\mathcal{C} = \{c \mid cH^\top = 0\}$
- $s = eH^\top$ *syndrome*
- *Decode*: find closest codeword
- *Hamming metric*: $d_H(x, y) = \mid \{i \mid x_i \neq y_i\} \mid$
- *minimum distance of a code:*

$$d(\mathcal{C}) = \min\{d_H(x, y) \mid x \neq y \in \mathcal{C}\}$$

- *error-correction capacity*: $t = \lfloor (d(\mathcal{C}) - 1)/2 \rfloor$

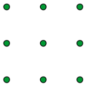
Hard Problems from Coding Theory

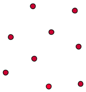
Algebraic structure

(Reed-Solomon, Goppa,..)

$\rightarrow$ efficient decoders

$\langle G \rangle$





$\langle \widetilde{G} \rangle$

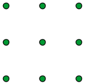
random code

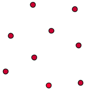
$\rightarrow$ how hard to decode?

Hard Problems from Coding Theory

Algebraic structure
(Reed-Solomon, Goppa,..)
$\rightarrow$ efficient decoders

$\langle G \rangle$





$\langle \widetilde{G} \rangle$

random code

$\rightarrow$ how hard to decode?

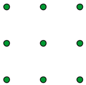
- Decoding random linear code is NP-hard

E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems ", IEEE Trans. Inf. Theory, 1978.

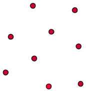
Hard Problems from Coding Theory

Algebraic structure
(Reed-Solomon, Goppa,..)
$\rightarrow$ efficient decoders

$\langle G \rangle$



scrambling
$\xrightarrow{\varphi}$



$\langle \widetilde{G} \rangle$

Seemingly random code

$\rightarrow$ how hard to decode?

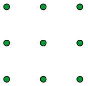
- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem

E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems ", IEEE Trans. Inf. Theory, 1978.

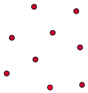
R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory", DSNP Report, 1978

Hard Problems from Coding Theory

Algebraic structure
(Reed-Solomon, Goppa,..)
$\rightarrow$ efficient decoders

$\langle G \rangle$ 

scrambling
$\xrightarrow{\varphi}$

 $\langle \widetilde{G} \rangle$

Seemingly random code

$\rightarrow$ how hard to decode?

- Decoding random linear code is NP-hard
- First code-based cryptosystem based on this problem
- Fastest solvers: ISD, exponential time

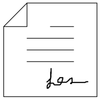
E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems ", IEEE Trans. Inf. Theory, 1978.

R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory", DSNP Report, 1978

A. Becker, A. Joux, A. May, A. Meurer "Decoding random binary linear codes in $2^{n/20}$: How 1+ 1= 0 improves information set decoding", Eurocrypt, 2012.

Idea of Signature Schemes

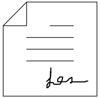
Signer



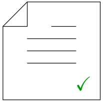
Verifier

Idea of Signature Schemes

Signer

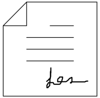


Verifier



Idea of Signature Schemes

Signer



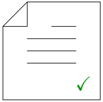
- Key Generation: $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

$\xrightarrow{\mathcal{P}}$

$\xrightarrow{m,\ \sigma}$

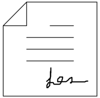
Verifier



- Verification: use $\mathcal{P}$ and message m to verify signature σ

Idea of Signature Schemes

Signer



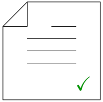
- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

small $\mathcal{P}$

small σ

Verifier

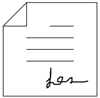


fast verification

- Verification: use $\mathcal{P}$ and message m to verify signature σ

Idea of Signature Schemes

Signer



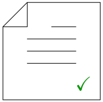
- Key Generation: $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

small $\mathcal{P}$

small σ

Verifier



fast verification

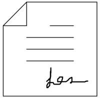
- Verification: use $\mathcal{P}$ and message m to verify signature σ

2 Approaches for signatures:

- Hash-and-Sign
- Through ZK protocol

Idea of Signature Schemes

Signer



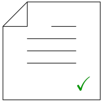
- Key Generation: $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

small $\mathcal{P}$

small σ

Verifier



fast verification

- Verification: use $\mathcal{P}$ and message m to verify signature σ

2 Approaches for signatures:

- Hash-and-Sign

Main Topic

- Through ZK protocol

Idea of ZK Protocol

Prover		**Verifier**
$\mathcal{S}$: secret		
$\mathcal{P}$: related public key	$\xrightarrow{\mathcal{P},c}$	
c: commitments to secret	$\xleftarrow{b}$	b: challenge
r_b: response to challenge b	$\xrightarrow{r_b}$	Recover c from r_b and $\mathcal{P}$

Idea of ZK Protocol

Prover		**Verifier**
$\mathcal{S}$: secret $\mathcal{P}$: related public key c: commitments to secret r_b: response to challenge b	$\xrightarrow{\mathcal{P},c}$ $\xleftarrow{b}$ $\xrightarrow{r_b}$	b: challenge Recover c from r_b and $\mathcal{P}$

Idea of ZK Protocol

Prover	Interaction	**Verifier**
$\mathcal{S}$: secret $\mathcal{P}$: related public key c: commitments to secret r_b: response to challenge b	$\xrightarrow{\mathcal{P},c}$ $\xleftarrow{b}$ $\xrightarrow{r_b}$	b: challenge Recover c from r_b and $\mathcal{P}$

Idea of ZK Protocol

Prover	Fiat-Shamir	**Verifier**
$\mathcal{S}$: secret $\mathcal{P}$: related public key c: commitments to secret b: Hash of message, c r_b: response to challenge b	$\xrightarrow{\mathcal{P},(b,r_b)}$	Recover c from r_b and $\mathcal{P}$ Verify $b = \text{Hash}(m, c)$

A. Fiat, A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems.", Proceedings on Advances in cryptology-CRYPTO, 1986.

Idea of ZK Protocol

Prover

Verifier

N

$\mathcal{S}$: secret
$\mathcal{P}$: related public key
c: commitments to secret
b: Hash of message, c
r_b: response to challenge b

$\xrightarrow{\mathcal{P},(b,r_b)}$

Recover c from r_b and $\mathcal{P}$
Verify $b = \text{Hash}(m, c)$

- α cheating probability, λ bit security level
- *Rounds*: have to repeat ZK protocol N times: $2^\lambda < (1/\alpha)^N$

A. Fiat, A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems.", Proceedings on Advances in cryptology-CRYPTO, 1986.

Code-based ZK Protocols

P.-L. Cayrel, P. Véron, S. El Yousfi Alaoui. "A zero-knowledge identification scheme based on the q-ary syndrome decoding problem", Selected Areas in Cryptography, 2011.

Syndrome Decoding Problem

Given parity-check matrix H, syndrome s, weight t, find e s.t. 1. $s = eH^\top$ 2. $\mathrm{wt}_H(e) \leq t$

Prover		**Verifier**
$\mathcal{S}$: e of weight t,		
$\mathcal{P}$: random H, $s = eH^\top$, t	$\xrightarrow{\mathcal{P}, c_1, c_2}$	
c_1: commitment to syndrome equation 1.		$b \in \{1, 2\}$
c_2: commitment to weight 2.	$\xleftarrow{b}$	
response: $r_1 = \varphi$, $r_2 = \varphi(e)$	$\xrightarrow{r_b}$	recover c_b from r_b and $\mathcal{P}$

Problem with Code-based ZK Protocols

1. Problem: Large cheating probability

$\rightarrow$ Many rounds $\rightarrow$ Large signatures

Problem with Code-based ZK Protocols

1. Problem: Large cheating probability

$\rightarrow$ Many rounds $\rightarrow$ Large signatures

Classical CVE $\lambda = 128$ bit security level

$N = 135$, $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB

Problem with Code-based ZK Protocols

1. Problem: Large cheating probability

$\rightarrow$ Many rounds $\rightarrow$ Large signatures

Classical CVE $\lambda = 128$ bit security level

$N = 135$, $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB impractical

Problem with Code-based ZK Protocols

1. Problem: Large cheating probability

→ Many rounds → Large signatures

Classical CVE $\lambda = 128$ bit security level

$N = 135$, $q = 31, n = 256, k = 204$ → signature size: 43 kB impractical

→ 1. Solution: MPC in-the-head

Problem with Code-based ZK Protocols

1. Problem: Large cheating probability

$\rightarrow$ Many rounds $\rightarrow$ Large signatures

Classical CVE $\lambda = 128$ bit security level

$N = 135,\ q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB impractical

$\rightarrow$ 1. Solution: MPC in-the-head

MPC in-the-head NIST submissions

- MIRA: 5.6 KB
- MiRith: 5.6 KB
- MQOM: 6.3 KB
- PERK: 6 KB
- RYDE: 6 KB
- SDitH: 8.2 KB

Problem with Code-Based ZK Protocols

2. Problem: Already 1 round has large communication cost

Problem with Code-Based ZK Protocols

2. Problem: Already 1 round has large communication cost

Response: transformation φ or $\varphi(e)$ $\rightarrow$ Which φ are allowed?

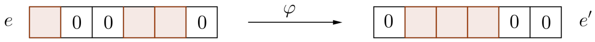
Problem with Code-Based ZK Protocols

2. Problem: Already 1 round has large communication cost

Response: transformation φ or $\varphi(e)$ $\rightarrow$ Which φ are allowed?

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}_H(e) \leq t$.



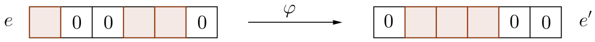
Problem with Code-Based ZK Protocols

2. Problem: Already 1 round has large communication cost

Response: transformation φ or $\varphi(e)$ $\rightarrow$ Which φ are allowed?

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}_H(e) \leq t$.



$\rightarrow \varphi$: linear isometries of Hamming metric:
permutation + scalar multiplication

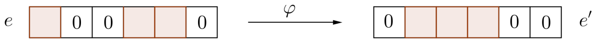
Problem with Code-Based ZK Protocols

2. Problem: Already 1 round has large communication cost

Response: transformation φ or $\varphi(e)$ $\quad\rightarrow\quad$ Which φ are allowed?

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}_H(e) \leq t$.



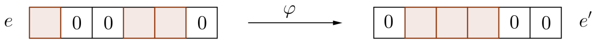
$\rightarrow$ φ : linear isometries of Hamming metric:
permutation + scalar multiplication

$\rightarrow$ size: $\varphi : n\log_2(q-1) + n\log_2(n)$ or $\varphi(e) : t\log_2(q-1) + t\log_2(n)$

Restricted Errors

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^{n}$ such that $s = eH^\top$ and $\mathrm{wt}(e) \leq t$.



Can we avoid permutations ?

Restricted Errors

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}(e) \leq t$.

$$e \quad \begin{array}{|c|c|c|c|c|c|}\hline & 0 & 0 & & & 0 \\ \hline \end{array} \xrightarrow{\varphi} \begin{array}{|c|c|c|c|c|c|}\hline 0 & & & & 0 & 0 \\ \hline \end{array} \quad e'$$

Can we avoid permutations - but keep the hardness of the problem?

$$\downarrow$$

Syndrome Decoding Problem

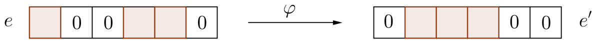
Given $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$.

$$e \quad \begin{array}{|c|c|c|c|c|c|}\hline & & & & & \\ \hline \end{array}$$

Restricted Errors

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}(e) \leq t$.



Can we avoid permutations - but keep the hardness of the problem?

$\downarrow$

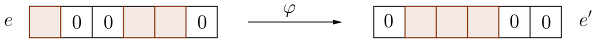
Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ such that $s = eH^\top$.

Restricted Errors

Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, weight t, find $e \in \mathbb{F}_q^n$ such that $s = eH^\top$ and $\mathrm{wt}(e) \leq t$.



Can we avoid permutations - but keep the hardness of the problem?

$$\downarrow$$

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ such that $s = eH^\top$.

$\boxed{\text{How to choose } \mathbb{E}\text{?}}$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E}, \cdot) < (\mathbb{F}_q^\star, \cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1, \ldots, z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1, 3, 9\}$$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \;\rightarrow\; g\in\mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E}=\{g^i \mid i\in\{1,\ldots,z\}\}}$$

$$q=13 \quad\rightarrow\quad g=3 \text{ order } z=3 \quad\rightarrow\quad \mathbb{E}=\{1,3,9\}$$

$$(\mathbb{E}^n,\star) \quad \xrightarrow{\ell} \quad (\mathbb{F}_z^n,+)$$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \;\to\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\to\; \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \to \quad g = 3 \text{ order } z = 3 \quad \to \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \ \rightarrow \ g \in \mathbb{F}_q^\star \text{ of prime order } z \ \rightarrow \ \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \to \mathbb{E}^n, e \mapsto e \star e'$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \ \rightarrow \ g \in \mathbb{F}_q^\star \text{ of prime order } z \ \rightarrow \ \mathbb{E} = \{g^i \mid i \in \{1,\ldots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3,9,1,3) \in \mathbb{E}^n$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1,2,0,1) \in \mathbb{F}_3^4$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \ \rightarrow\ g \in \mathbb{F}_q^\star \text{ of prime order } z \ \rightarrow\ \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3,9,1,3) \in \mathbb{E}^n$
- $\varphi(e) = e \star e' \in (\mathbb{E}^n,\star)$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1,2,0,1) \in \mathbb{F}_3^4$
- $\ell(e) + \ell(e') \in (\mathbb{F}_z^n,+)$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \;\rightarrow\; g \in \mathbb{F}_q^\star \text{ of prime order } z \;\rightarrow\; \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3,9,1,3) \in \mathbb{E}^n$
- $\varphi(e) = e \star e' \in (\mathbb{E}^n,\star)$
- $\varphi(e) = (1,9,3,3) \star (3,9,1,3)$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1,2,0,1) \in \mathbb{F}_3^4$
- $\ell(e) + \ell(e') \in (\mathbb{F}_z^n,+)$
- $(0,2,1,1) + (1,2,0,1)$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \ \rightarrow \ g \in \mathbb{F}_q^\star \text{ of prime order } z \ \rightarrow \ \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3,9,1,3) \in \mathbb{E}^n$
- $\varphi(e) = e \star e' \in (\mathbb{E}^n,\star)$
- $\varphi(e) = (1,9,3,3) \star (3,9,1,3)$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1,2,0,1) \in \mathbb{F}_3^4$
- $\ell(e) + \ell(e') \in (\mathbb{F}_z^n,+)$
- $(0,2,1,1) + (1,2,0,1)$

size of φ: old: $n\log_2((q-1)n)$ new: $n\log_2(z)$

arithmetic: old: $(\mathbb{F}_q^n,\cdot)$ new: $(\mathbb{F}_z^n,+)$

Restricted Errors

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Zero knowledge protocols and signatures from the restricted syndrome decoding problem ", Preprint, 2023

$$\boxed{(\mathbb{E},\cdot) < (\mathbb{F}_q^\star,\cdot) \ \rightarrow \ g \in \mathbb{F}_q^\star \text{ of prime order } z \ \rightarrow \ \mathbb{E} = \{g^i \mid i \in \{1,\dots,z\}\}}$$

$$q = 13 \quad \rightarrow \quad g = 3 \text{ order } z = 3 \quad \rightarrow \quad \mathbb{E} = \{1,3,9\}$$

$$(\mathbb{E}^n,\star) \qquad \xrightarrow{\ell} \qquad (\mathbb{F}_z^n,+)$$

- $e = (1,9,3,3) \in \{1,3,9\}^4$
- trans.: $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n, e \mapsto e \star e'$
- $\varphi : e' = (3,9,1,3) \in \mathbb{E}^n$
- $\varphi(e) = e \star e' \in (\mathbb{E}^n,\star)$
- $\varphi(e) = (1,9,3,3) \star (3,9,1,3)$

- $\ell(e) = (0,2,1,1) \in \mathbb{F}_3^4$
- $\ell(\varphi) \in \mathbb{F}_z^n$
- $\ell(\varphi) : \ell(e') = (1,2,0,1) \in \mathbb{F}_3^4$
- $\ell(e) + \ell(e') \in (\mathbb{F}_z^n,+)$
- $(0,2,1,1) + (1,2,0,1)$

size of φ: old: $n\log_2((q-1)n)$ new: $n\log_2(z)$

arithmetic: old: $(\mathbb{F}_q^n,\cdot)$ new: $(\mathbb{F}_z^n,+)$

Can do even better

Restricted-G SDP

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

- $(\mathbb{E}^n, \star) \cong (\mathbb{F}_z^n, +)$
- $e = (1, 9, 3, 3) \in \mathbb{E}^4 = \{1, 3, 9\}^4$

Restricted-G SDP

Restricted-G Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^{\star}$, $G = \langle x_1, \ldots, x_m \rangle \leq \mathbb{E}^n$ find $e \in G$ s.t. $s = eH^{\top}$.

- $(\mathbb{E}^n, \star) \cong (\mathbb{F}_z^n, +)$

$\rightarrow$ Subgroup $(G, \star) \leq (\mathbb{E}^n, \star)$
$G = \langle x_1, \ldots, x_m \rangle$

$\rightarrow$ $e' = \prod_{i=1}^{m} x_i^{u_i} \in G$

- $e = (1, 9, 3, 3) \notin G$

- $x_1 = (9, 1, 9, 1), x_2 = (9, 9, 1, 9), x_3 = (1, 9, 9, 3)$
- $e' = x_1^2 \star x_2^1 \star x_3^0 = (1, 9, 3, 9) \in G$

Restricted-G SDP

Restricted-G Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, $G = \langle x_1, \dots, x_m \rangle \leq \mathbb{E}^n$ find $e \in G$ s.t. $s = eH^\top$.

- $(\mathbb{E}^n, \star) \cong (\mathbb{F}_z^n, +)$

$\rightarrow$ Subgroup $(G, \star) \leq (\mathbb{E}^n, \star)$
$G = \langle x_1, \dots, x_m \rangle$

$\rightarrow$ $e' = \prod_{i=1}^m x_i^{u_i} \in G$

- $M_G = [\ell(x_i)] \in \mathbb{F}_z^{m \times n}$
- $\ell(e') = yM_G, \ y \in \mathbb{F}_z^m$

$\rightarrow$ fast arithmetic

- $e = (1, 9, 3, 3) \notin G$
- $x_1 = (9, 1, 9, 1), x_2 = (9, 9, 1, 9), x_3 = (1, 9, 9, 3)$
- $e' = x_1^2 \star x_2^1 \star x_3^0 = (1, 9, 3, 9) \in G$
- $M_G = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 2 & 2 & 0 & 2 \\ 0 & 2 & 2 & 1 \end{pmatrix}$
- $\ell(e') = (0, 2, 1, 2) = (2, 1, 0)M_G$

Restricted-G SDP

Restricted-G Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^{\star}$, $G = \langle x_1, \dots, x_m \rangle \leq \mathbb{E}^n$ find $e \in G$ s.t. $s = eH^\top$.

- $(\mathbb{E}^n, \star) \cong (\mathbb{F}_z^n, +)$

$\rightarrow$ Subgroup $(G, \star) \leq (\mathbb{E}^n, \star)$
$G = \langle x_1, \dots, x_m \rangle$

$\rightarrow$ $e' = \prod_{i=1}^m x_i^{u_i} \in G$

- $M_G = [\ell(x_i)] \in \mathbb{F}_z^{m\times n}$
- $\ell(e') = yM_G,\ y \in \mathbb{F}_z^m$

$\rightarrow$ fast arithmetic

- $e = (1, 9, 3, 3) \notin G$
- $x_1 = (9, 1, 9, 1), x_2 = (9, 9, 1, 9), x_3 = (1, 9, 9, 3)$
- $e' = x_1^2 \star x_2^1 \star x_3^0 = (1, 9, 3, 9) \in G$
- $M_G = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 2 & 2 & 0 & 2 \\ 0 & 2 & 2 & 1 \end{pmatrix}$
- $\ell(e') = (0, 2, 1, 2) = (2, 1, 0)M_G$

size: $n\log_2((q-1)n)$ $\rightarrow$ rest.: $n\log_2(z)$ $\rightarrow$ rest.-G: $m\log_2(z)$

Is this Safe?

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

Is this Safe?

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

$\rightarrow$ NP hard for $\mathbb{E} < \mathbb{F}_q^\star$

Is this Safe?

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

$\rightarrow$ NP hard for $\mathbb{E} < \mathbb{F}_q^\star$

- Restricted errors first introduced: $g = -1 \rightarrow z = 2$

M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann, E. Persichetti, P. Santini, **V.W.** "A new path to code-based signatures via identification schemes with restricted errors. ", 2020.

Is this Safe?

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^\star$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

$\rightarrow$ NP hard for $\mathbb{E} < \mathbb{F}_q^\star$

- Restricted errors first introduced: $g = -1 \rightarrow z = 2$
- several proposals for small z e.g. $z = 4, 6$

M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann, E. Persichetti, P. Santini, **V.W.** "A new path to code-based signatures via identification schemes with restricted errors. ", 2020.

J.-P. Thiers, J. Freudenberger. "Codes over Eisenstein integers for the Niederreiter cryptosystem. ", IEEE ICCE, 2021.

J.-P. Thiers, J. Freudenberger. "A new class of q-ary codes for the McEliece cryptosystem. ", Cryptography, 2021.

Is this Safe?

Restricted Syndrome Decoding Problem

Given $H \in \mathbb{F}_q^{(n-k)\times n}$, $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} \subseteq \mathbb{F}_q^{\star}$, find $e \in \mathbb{E}^n$ s.t. $s = eH^\top$.

$\rightarrow$ NP hard for $\mathbb{E} < \mathbb{F}_q^{\star}$

- Restricted errors first introduced: $g = -1 \rightarrow z = 2$
- several proposals for small z e.g. $z = 4, 6$

$\rightarrow$ Information set decoding using subset-sum solvers

M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann, E. Persichetti, P. Santini, **V.W.** "A new path to code-based signatures via identification schemes with restricted errors. ", 2020.

J.-P. Thiers, J. Freudenberger. "Codes over Eisenstein integers for the Niederreiter cryptosystem. ", IEEE ICCE, 2021.

J.-P. Thiers, J. Freudenberger. "A new class of q-ary codes for the McEliece cryptosystem. ", Cryptography, 2021.

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, **V.W.** "Generic Decoding of Restricted Errors. ", ISIT, 2023.

$\rightarrow$ a lot of additive structure on $\mathbb{E}$ not safe

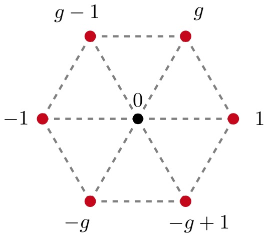
Is this Safe?

→ additive structure on $\mathbb{E}$
not safe

Is this Safe?

→ additive structure on $\mathbb{E}$ not safe

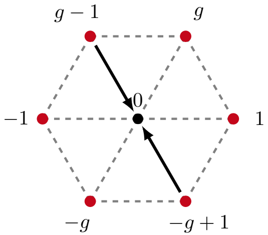
→ Sebastian's Poster



Is this Safe?

→ additive structure on $\mathbb{E}$ not safe

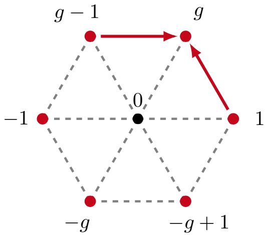
→ Sebastian's Poster



Is this Safe?

→ additive structure on $\mathbb{E}$ not safe

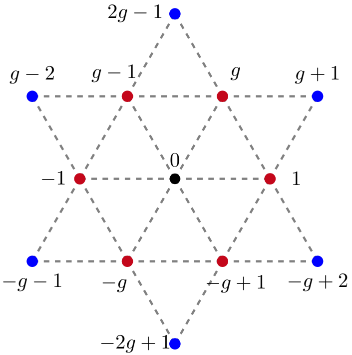
→ Sebastian's Poster



Is this Safe?

→ additive structure on $\mathbb{E}$ not safe

→ Sebastian's Poster



Is this Safe?

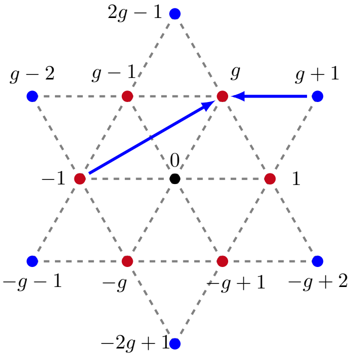
→ additive structure on $\mathbb{E}$ not safe

→ Sebastian's Poster

→ Our $\mathbb{E}$: little additive structure

- $q = 127, \ z = 7$

→ $\mathbb{E} = \{1, 2, 4, 8, 16, 32, 64\}$



Performance of Restricted-G Signatures

Restricted CVE

- classical: $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB

Performance of Restricted-G Signatures

Restricted CVE

- classical: $q = 31, n = 256, k = 204$ $\longrightarrow$ signature size: 43 kB
- rest.: $q = 127, z = 7, n = 2k = 127$ $\longrightarrow$ signature size: 10 kB

Performance of Restricted-G Signatures

Restricted CVE

- classical: $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB
- rest.: $q = 127, z = 7, n = 2k = 127$ $\rightarrow$ signature size: 10 kB
- rest.-G: $q = 509, z = 127, m = 24, n = 2k = 42$ $\rightarrow$ signature size: 7 kB

Performance of Restricted-G Signatures

Restricted CVE

- classical: $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB
- rest.: $q = 127, z = 7, n = 2k = 127$ $\rightarrow$ signature size: 10 kB
- rest.-G: $q = 509, z = 127, m = 24, n = 2k = 42$ $\rightarrow$ signature size: 7 kB

Performance of Restricted-G Signatures

Restricted CVE

- classical: $q = 31, n = 256, k = 204$ $\rightarrow$ signature size: 43 kB
- rest.: $q = 127, z = 7, n = 2k = 127$ $\rightarrow$ signature size: 10 kB
- rest.-G: $q = 509, z = 127, m = 24, n = 2k = 42$ $\rightarrow$ signature size: 7 kB

Conclusion

- Can replace SDP with Rest. SDP/ Rest.-G SDP in any code-based ZK protocol
- Achieve smaller signature sizes, smaller running times

Questions?

Scan me

CROSS

Codes & Restricted Objects Signature Scheme
`http://cross-crypto.com/`

Thank you!

Running times

Running time given in kCycles, CROSS has only PoC, no optimization, parallelization

Scheme	**Key gen.**	**Signature gen.**	**Verification**
SPHINCS	1794	5802	6506
Dilitihium	49	140	61
CROSS	19	187	184

Is this Safe?

$G = \langle x_1, \ldots, x_m \rangle$: use generators?

No: $\prod_{i=1}^{m} x_i^{u_i} H^\top = s$

$\rightarrow$ not compatible unlike $\sum_{i=1}^{m} \lambda_i x_i H^\top = s$

Solving Restricted SDP in subgroup G

- we want q, z such that $\mathbb{E}$ has no additive structure
- Publicly known: $x_1, \ldots, x_m$ generators of multiplicative group G
- $x_\ell = (g^{i_{1,\ell}}, \ldots, g^{i_{n,\ell}})$
- define $M_G \in \mathbb{F}_z^{m \times n}$ having rows $(i_{1,\ell}, \ldots, i_{n,\ell})$

$$\begin{array}{cc} & \qquad\qquad J \\ M_G = & \begin{bmatrix} i_{1,\ell} & \ldots & \boxed{} & i_{n,\ell} \end{bmatrix} \end{array}$$

$\hookrightarrow$ rank m'

$$m' \geq \min \left\{ |\, J \,|, \frac{\lambda}{\log_2(z)} \right\} \rightarrow \text{no improvement over enumerating all possible errors in these positions}$$

Comparison

Scheme	Public Key size	Signature size	Total size	Variant
SPHINCS$^+$	<0.1 <0.1	16.7 7.7	16.7 7.7	Fast Short
Falcon	0.9	0.6	1.5	-
Dilitihium	1.3	2.4	3.7	-
CROSS	0.1 0.1	7.7 7.2	7.8 7.3	Fast Short
GPS	0.1 0.1	24.0 19.8	24.1 19.9	Fast Short
FJR	0.1 0.1	22.6 16.0	22.7 16.1	Fast Short
SDItH	0.1 0.1	11.5 8.3	11.6 8.4	Fast Short
Ret. of SDitH	0.1 0.1	12.1 5.7	12.1 5.8	Fast, V3 Shortest, V3

Comparison

Scheme	**Public Key size**	**Signature size**	**Total size**	**Variant**
WAVE	3200	2.1	3202	-
Durandal	15.2	4.1	19.3	-
Ideal Rank BG	0.5	8.4	8.9	Fast
	0.5	6.1	6.6	Short
MinRank Fen	18.2	9.3	27.5	Fast
	18.2	7.1	25.3	Short
Rank SDP Fen	0.9	7.4	8.3	Fast
	0.9	5.9	6.8	Short
Beu	0.1	18.4	18.5	Fast
	0.1	12.1	12.2	Short
PKP BG	0.1	9.8	9.9	Fast
	0.1	8.8	8.9	Short
FuLeeca	1.3	1.1	2.4	-

ZKID

PROVER		VERIFIER
		VERIFICATION
commitments c_0, c_1	$\xrightarrow{c_0, c_1}$	
	$\xleftarrow{b}$	$b \in \{0, 1\}$
response r_b	$\xrightarrow{r_b}$	
		Verify c_b using $r_b, \mathcal{P}$

SIGNING		
Choose message m		
Construct signature s from $\mathcal{S}$, m		
	$\xrightarrow{m, s}$	
		VERIFICATION
		Verify signature s using $\mathcal{P}$, m

Signature Scheme

ZKID

PROVER		VERIFIER
		VERIFICATION
commitments c_0, c_1	$\xrightarrow{c_0, c_1}$	
	$\xleftarrow{b}$	$b \in \{0, 1\}$
response r_b	$\xrightarrow{r_b}$	
		Verify c_b using $r_b, \mathcal{P}$

Fiat-Shamir

SIGNING		
Choose message m		
Construct signature s from $\mathcal{S}$, m		
	$\xrightarrow{m, s}$	
		VERIFICATION
		Verify signature s using $\mathcal{P}$, m

Signature Scheme

Fiat-Shamir

PROVER		VERIFIER
KEY GENERATION		
Given $\mathcal{P}, \mathcal{S}$ of some ZKID and message m		
SIGNING		
Choose commitment c $b = \mathrm{Hash}(m, c)$ Compute response r_b Signature $s = (b, r_b)$	$\xrightarrow{m,s}$	
		VERIFICATION
		Using $r_b, \mathcal{P}$ construct c check if $b = \mathrm{Hash}(m, c)$

CVE

PROVER		VERIFIER
KEY GENERATION		
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$
		and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

CVE

PROVER		VERIFIER
KEY GENERATION		Recall SDP: (1) $s = eH^\top$ (2) $\mathrm{wt}(e) \leq t$
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$
		and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

CVE

PROVER		VERIFIER
KEY GENERATION		
Choose e with $\mathrm{wt}(e) \leq t$		
H parity-check matrix		
Compute $s = eH^\top$	$\xrightarrow{\mathcal{P}=(H,s,t)}$	
		VERIFICATION
Choose $u \in \mathbb{F}_q^n$, $\sigma \in \mathcal{S}_n$		
Set $c_1 = \mathrm{Hash}(\sigma, uH^\top)$		
Set $c_2 = \mathrm{Hash}(\sigma(u), \sigma(e))$	$\xrightarrow{c_1, c_2}$	
	$\xleftarrow{z}$	Choose $z \in \mathbb{F}_q^\times$
Set $y = \sigma(u + ze)$	$\xrightarrow{y}$	
$r_1 = \sigma$	$\xleftarrow{b}$	Choose $b \in \{1, 2\}$
$r_2 = \sigma(e)$	$\xrightarrow{r_b}$	$b = 1$: $c_1 = \mathrm{Hash}(\sigma, \sigma^{-1}(y)H^\top - zs)$
		$b = 2$: $\mathrm{wt}(\sigma(e)) = t$ and $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

Problem: big signature sizes

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost
- solution: compression technique
- do not send c_0^i, c_1^i in each round i
- before 1. round send $c = \mathrm{Hash}(c_0^1, c_1^1, \dots, c_0^N, c_1^N)$
- ith round: receiving challenge b prover sends r_b^i, c_{1-b}^i
- end: verifier checks $c = \mathrm{Hash}(c_0^1, c_1^1, \dots, c_0^N, c_1^N)$

C. Aguilar, P. Gaborit, J. Schrek. "A new zero-knowledge code based identification scheme with reduced communication", IEEE Information Theory Workshop, 2011.

Cheating Probability

- Cheating probability = Probability of impersonator getting accepted
- For security level 2^λ want cheating probability $2^{-\lambda}$
- If cheating probability δ, with N rounds $\rightarrow$ cheating probability δ^N
- might need many rounds: large communication cost
- other solution: MPC in the head
- third party: trusted helper sends commitments $\rightarrow \delta = 0$
- instead prover sends seeds of commitment: not ZK $\rightarrow$ cut and choose
- $x < N$ times send response, $N - x$ times send the seed of commitment
- to compress: use Merkle root or seed tree

T. Feneuil, A. Joux, M. Rivain. "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs", 2022.