CROSS: Signature scheme with restricted errors

Violetta Weger

DMV 2023

September 25, 2023

Motivation

2016

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

Motivation

2016

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

Standardized:	Signatures:	Dilithium, FALCON, SPHINCS+
	PKE/KEM:	KYBER

4th round:	PKE/KEM:	Classic McEliece, BIKE, HQC

2023

Motivation

2016

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

based on structured lattices — Hash-based

Standardized: Signatures: Dilithium, FALCON, SPHINCS+
PKE/KEM: KYBER

4th round: PKE/KEM: Classic McEliece, BIKE, HQC — Code-based

2023

Motivation

2016

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

based on structured lattices — Hash-based

Standardized: Signatures: Dilithium, FALCON, — SPHINCS+

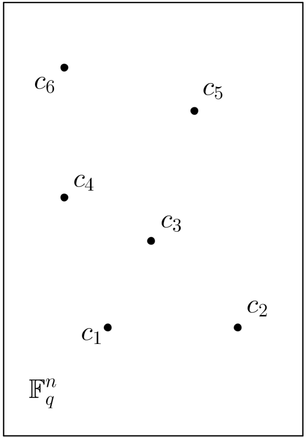
PKE/KEM: KYBER

4th round: PKE/KEM: Classic McEliece, BIKE, HQC — Code-based

2023

NIST additional call for signature schemes

Coding Theory

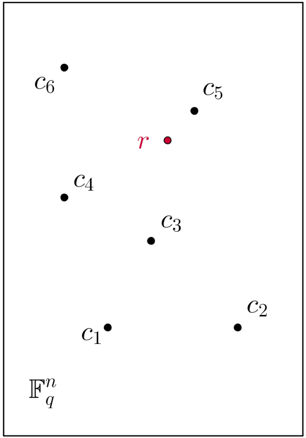


Set Up

- *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*

Coding Theory

$\boldsymbol{c} \longrightarrow \boxed{\lightning} \longrightarrow \boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$

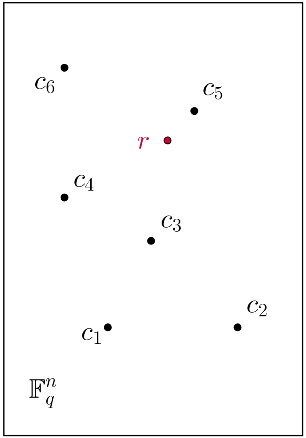


Set Up

- *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

Coding Theory

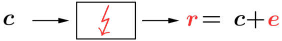
$\boldsymbol{c} \longrightarrow \boxed{\lightning} \longrightarrow \boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$

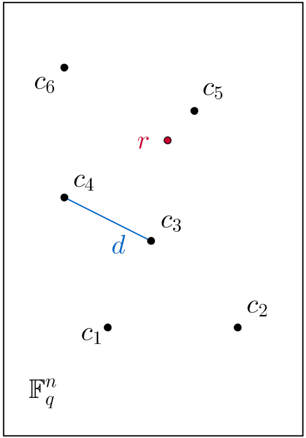


Set Up

- *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*: $d_H(x,y) = \mid \{i \mid x_i \neq y_i\} \mid$

Coding Theory





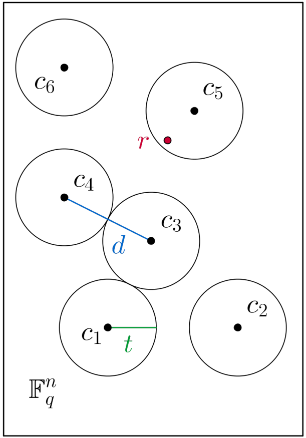
Set Up

- *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*: $d_H(x,y) = |\{i \mid x_i \neq y_i\}|$
- *minimum distance of a code*:

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

Coding Theory

$$\boldsymbol{c} \longrightarrow \boxed{\lightning} \longrightarrow \boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$$



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*: $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$
- *minimum distance of a code*:

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

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

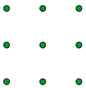
Classic Approach: McEliece

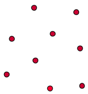
Algebraic structure

(Reed-Solomon, Goppa,..)

$\rightarrow$ efficient decoders

$\langle G \rangle$





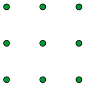
$\langle \widetilde{G} \rangle$

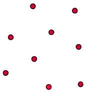
random code

$\rightarrow$ how hard to decode?

Classic Approach: McEliece

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

$\langle G \rangle$ 

 $\langle \widetilde{G} \rangle$

random code

$\rightarrow$ NP-hard

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

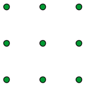
lin. constraint $\boxed{1.\ s = eH^\top}$ $\boxed{2.\ \mathrm{wt}_H(e) \leq t}$ non-lin. constraint

- SDP is NP-hard

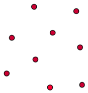
E. Berlekamp, R. McEliece, H. Van Tilborg. "On the inherent intractability of certain coding problems ", IEEE TIT, 1978.

Classic Approach: McEliece

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

$\langle G \rangle$ 

scrambling
$\xrightarrow{\varphi}$

 $\langle \widetilde{G} \rangle$

Seemingly random code
$\rightarrow$ NP-hard?

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

lin. constraint $\boxed{1.\ s = eH^\top}$ $\boxed{2.\ \mathrm{wt}_H(e) \leq t}$ non-lin. constraint

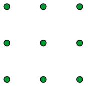
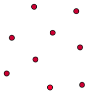
- SDP is NP-hard
- 1. code-based system

E. Berlekamp, R. McEliece, H. Van Tilborg. “On the inherent intractability of certain coding problems ”, IEEE TIT, 1978.

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

Classic Approach: McEliece

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

$\langle G \rangle$  scrambling $\xrightarrow{\varphi}$  $\langle \widetilde{G} \rangle$

Seemingly random code
$\rightarrow$ NP-hard?

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

lin. constraint $\boxed{1.\ s = eH^\top}$ $\boxed{2.\ \mathrm{wt}_H(e) \leq t}$ non-lin. constraint

- SDP is NP-hard
- 1. code-based system
- ISD: exponential time

E. Berlekamp, R. McEliece, H. Van Tilborg. “On the inherent intractability of certain coding problems ”, IEEE TIT, 1978.

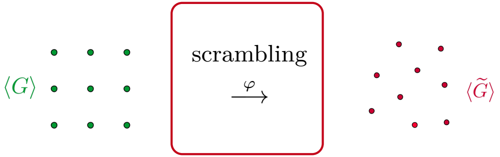
R. J. McEliece. “A public-key cryptosystem based on algebraic coding theory”, DSNP Report, 1978

E. Prange. “The use of information sets in decoding cyclic codes.”, IRE TIT, 1962.

Classic Approach: McEliece

Distinguishing Problem

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



Seemingly random code
$\to$ NP-hard?

Syndrome Decoding Problem (SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, target weight t, find $e \in \mathbb{F}_q^n$ s.t.

lin. constraint $\boxed{1.\ s = eH^\top}$ $\boxed{2.\ \mathrm{wt}_H(e) \leq t}$ non-lin. constraint

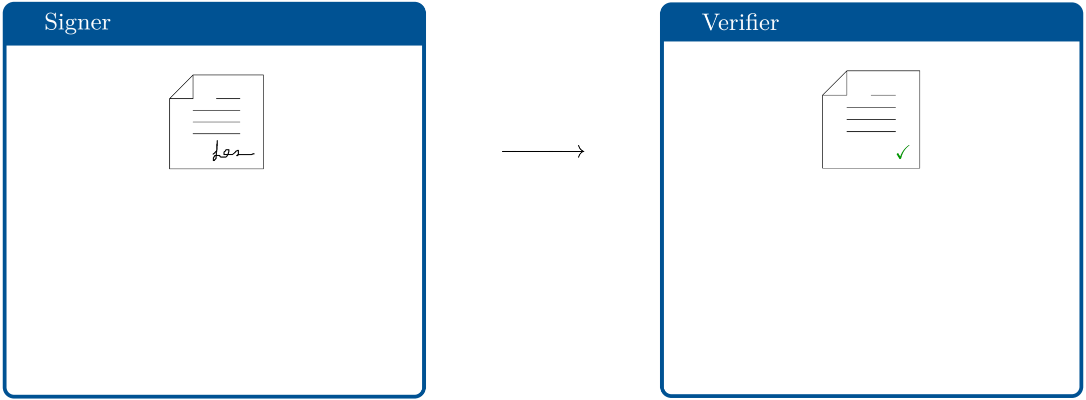
- SDP is NP-hard
- 1. code-based system
- ISD: exponential time

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

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

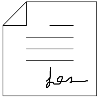
E. Prange. "The use of information sets in decoding cyclic codes.", IRE TIT, 1962.

Idea of Signature Schemes



Idea of Signature Schemes

Signer



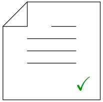
- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

$\xrightarrow{\mathcal{P}}$

$\xrightarrow{m,\ \sigma}$

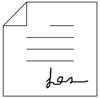
Verifier



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

Idea of Signature Schemes

Signer



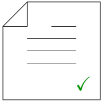
- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

$\longrightarrow$

small $\mathcal{P}$

small σ

Verifier

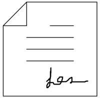


fast verification

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

Idea of Signature Schemes

Signer

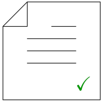


- Key Generation:
  $\mathcal{P}$ public, $\mathcal{S}$ secret
- Signing: use $\mathcal{S}$ and message m to generate signature σ

small $\mathcal{P}$

small σ

Verifier



fast verification

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

Approaches for signatures:

- Hash-and-Sign
- ZK Protocol
- ZK + MPC

Idea of ZK Protocol

Prover		**Verifier**
$\mathcal{S}$: secret key $\mathcal{P}$: 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 key $\mathcal{P}$: 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 key
$\mathcal{P}$: 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 key
$\mathcal{P}$: 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 $b = \mathrm{Hash}(m, c)$

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

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 key
$\mathcal{P}$: 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 $b = \mathrm{Hash}(m, c)$

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

Good Security:

$\rightarrow$ EUF secure

$\rightarrow$ no trapdoor

$\rightarrow$ no distinguisher

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: 1. Problem

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.

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.		
c_2: commitment to weight 2.	$\xleftarrow{b}$	$b \in \{1, 2\}$
response: transformation, e.g. permutation $r_1 = \varphi$, or transformed secret $r_2 = \varphi(e)$	$\xrightarrow{r_b}$	recover c_b from r_b and $\mathcal{P}$

SDP: given H, s, t find e s.t.

1. $s = eH^\top$ 2. $\mathrm{wt}_H(e) = t$

Code-based ZK Protocols: 1. Problem

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.

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.		
c_2: commitment to weight 2.	$\xleftarrow{b}$	$b \in \{1, 2\}$
response: transformation, e.g. permutation $r_1 = \varphi$, or transformed secret $r_2 = \varphi(e)$	$\xrightarrow{r_b}$	recover c_b from r_b and $\mathcal{P}$

1. Problem: large cheating probability $\rightarrow$ big signature sizes

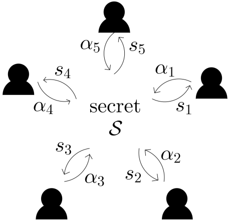
CVE $\lambda = 128$ bit security $\rightarrow$ signature size: 43 kB

1. Solution: MPC in-the-head

1.Solution: Multiparty Computation (MPC) in-the-head

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

Ingredients: ZK protocol + $(N-1)$-private MPC



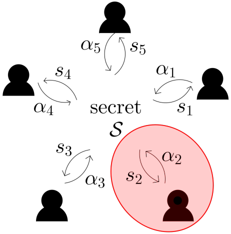
Prover		**Verifier**
Split $\mathcal{S}$ into N shares s_i		
Commitments c_i to s_i	$\xrightarrow{c_i,\alpha_i}$	Challenge
Compute $f(s_i) = \alpha_i$	$\xleftarrow{\ell}$	$\ell \in \{1, \dots, N\}$
Response: all shares but ℓ	$\xrightarrow{s_i}$	Check α_i, c_i from s_i

1. Solution: MPC in-the-head

1.Solution: Multiparty Computation (MPC) in-the-head

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

Ingredients: ZK protocol + $(N-1)$-private MPC



Prover		**Verifier**
Split $\mathcal{S}$ into N shares s_i		
Commitments c_i to s_i	$\xrightarrow{c_i,\alpha_i}$	Challenge
Compute $f(s_i) = \alpha_i$	$\xleftarrow{\ell}$	$\ell \in \{1, \ldots, N\}$
Response: all shares but ℓ	$\xrightarrow{s_i}$	Check α_i, c_i from s_i

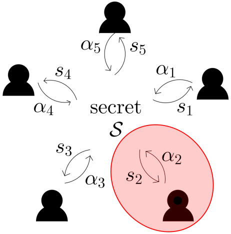
$\rightarrow$ New cheating probability: $1/N$

1. Solution: MPC in-the-head

1.Solution: Multiparty Computation (MPC) in-the-head

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

Ingredients: ZK protocol + $(N-1)$-private MPC



Prover		**Verifier**
Split $\mathcal{S}$ into N shares s_i		
Commitments c_i to s_i	$\xrightarrow{c_i, \alpha_i}$	Challenge
Compute $f(s_i) = \alpha_i$	$\xleftarrow{\ell}$	$\ell \in \{1, \ldots, N\}$
Response: all shares but ℓ	$\xrightarrow{s_i}$	Check α_i, c_i from s_i

Problem: Verification and signing is slow

Code-based ZK Protocols: 2. Problem

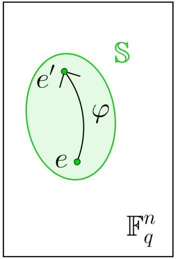
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

$\rightarrow$ acts trans. on secret space $\mathbb{S}$



Code-based ZK Protocols: 2. Problem

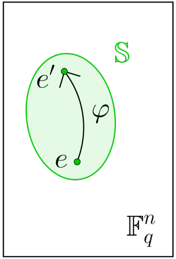
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

$\rightarrow$ acts trans. on secret space $\mathbb{S}$



$\mathbb{S} = B_H(t)$ $\rightarrow$ lin. isometry in Hamming metric $\rightarrow$ $\varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$

$\rightarrow$ Problem: Permutations are costly! $t \log_2(n(q-1))$ bits per round!

Code-based ZK Protocols: 2. Problem

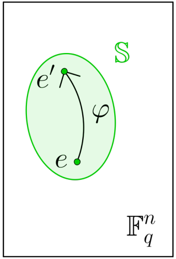
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

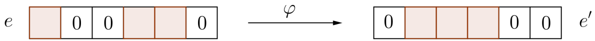
$\rightarrow$ acts trans. on secret space $\mathbb{S}$



$\mathbb{S} = B_H(t)$ $\rightarrow$ lin. isometry in Hamming metric $\rightarrow$ $\varphi \in (\mathbb{F}_q^\star)^n \rtimes S_n$

$\rightarrow$ Problem: Permutations are costly! $t\log_2(n(q-1))$ bits per round!

How to avoid permutations?



Code-based ZK Protocols: 2. Problem

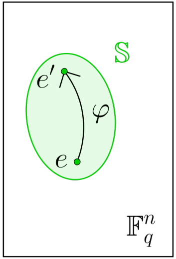
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

$\rightarrow$ acts trans. on secret space $\mathbb{S}$



e 

2. Solution: exchange $\mathbb{S} = B_H(t)$ with $\mathbb{S} = \mathbb{E}^n$

Non-lin. constraint: 2. $\mathrm{wt}_H(e) \leq t \rightarrow$ 2. $e \in \mathbb{E}^n$

Code-based ZK Protocols: 2. Problem

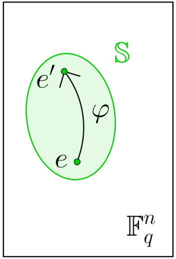
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

$\rightarrow$ acts trans. on secret space $\mathbb{S}$



e

Restricted SDP (R-SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} < \mathbb{F}_q^{\star}$, find $e \in \mathbb{F}_q^n$ s.t.

1. $s = eH^\top$
2. $e \in \mathbb{E}^n$.

Code-based ZK Protocols: 2. Problem

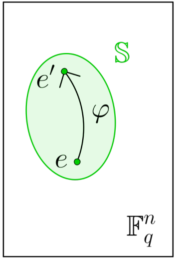
Transformations:

- allow to check lin. constraint

$\rightarrow$ linear map

- allow to check non-lin. constraint
- should not reveal info. on secret e

$\rightarrow$ acts trans. on secret space $\mathbb{S}$



e

Restricted SDP (R-SDP)

Given p.c. matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{n-k}$, $\mathbb{E} < \mathbb{F}_q^{\star}$, find $e \in \mathbb{F}_q^n$ s.t.

1. $s = eH^\top$
2. $e \in \mathbb{E}^n$.

NP-hard

Restricted Errors

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

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

Restricted Errors

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

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

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

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

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

Restricted Errors

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

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

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

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

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

Restricted Errors

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

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

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

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

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

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

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

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

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

$\rightarrow$ Smaller sizes: $n\log_2(z)$ instead of $t\log_2((q-1)n)$

$\rightarrow$ Faster arithmetic: ops. in $(\mathbb{F}_z^n,+)$ instead of $(\mathbb{F}_q^n,\cdot)$

Restricted-G SDP

Restricted Syndrome Decoding Problem

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

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

$\rightarrow (G, \star) \leq (\mathbb{E}^n, \star)$

$\rightarrow G = \langle x_1, \ldots, x_m \rangle$

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

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

Restricted-G SDP

Restricted-G Syndrome Decoding Problem

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

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

$\to (G, \star) \leq (\mathbb{E}^n, \star)$

$\to G = \langle x_1, \ldots, x_m \rangle$

$\to \; e' = \star_{i=1}^{m} x_i^{u_i} \in G$

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

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

Restricted-G SDP

Restricted-G Syndrome Decoding Problem

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

- $(\mathbb{E}^n, \star) \cong (\mathbb{F}_z^n, +)$
- $\rightarrow (G, \star) \leq (\mathbb{E}^n, \star)$
- $\rightarrow G = \langle x_1, \ldots, x_m \rangle$
- $\rightarrow \; e' = \star_{i=1}^m x_i^{u_i} \in G$
- $M_G = [\ell(x_i)] \in \mathbb{F}_z^{m\times n}$
- $\ell(e') = yM_G, \; y \in \mathbb{F}_z^m$

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

$\rightarrow$ Smaller sizes: $t\log_2((q-1)n) \;\rightarrow\;$ rest: $n\log_2(z) \;\rightarrow\;$ rest-G: $m\log_2(z)$

$\rightarrow$ Faster: ops. in $(\mathbb{F}_q^n, \cdot) \;\rightarrow\;$ rest: $(\mathbb{F}_z^n, +) \;\rightarrow\;$ rest-G: $(\mathbb{F}_z^m, \cdot)$

CROSS

Ingredients:

- ZK protocol:

CROSS

Ingredients:

- ZK protocol: CVE

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.:

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

Optimizations:

- unbalanced challenges
- Merkle trees

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

Optimizations:

- unbalanced challenges
- Merkle trees

Result:

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

Optimizations:

- unbalanced challenges
- Merkle trees

Result:

$\rightarrow$ simple

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

Optimizations:

- unbalanced challenges
- Merkle trees

Result:

$\rightarrow$ simple

$\rightarrow$ secure

CROSS

Ingredients:

- ZK protocol: CVE
- hard prob.: R- (G)-SDP

Optimizations:

- unbalanced challenges
- Merkle trees

Result:

→ simple

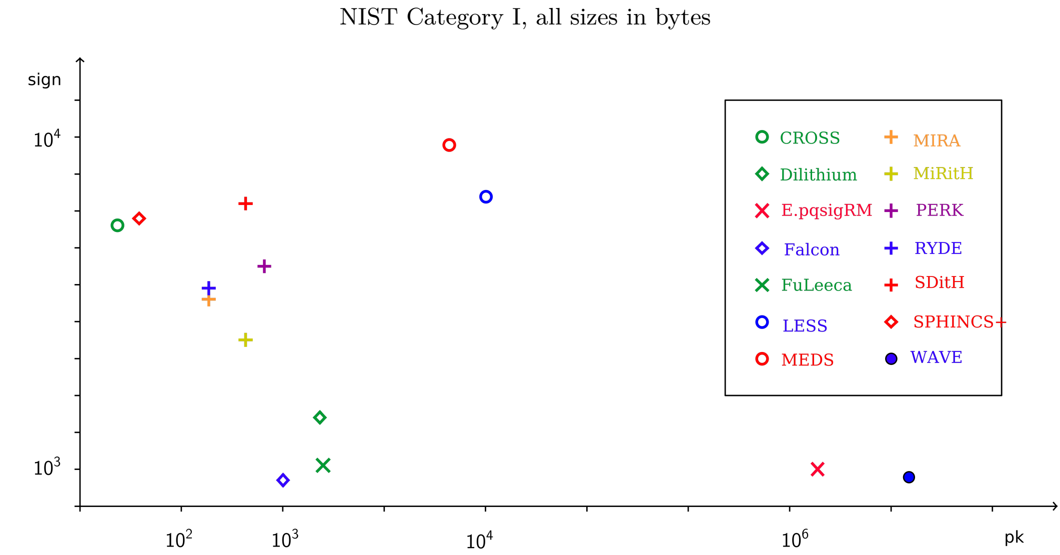
→ secure

Sizes in bytes, times in MCycles

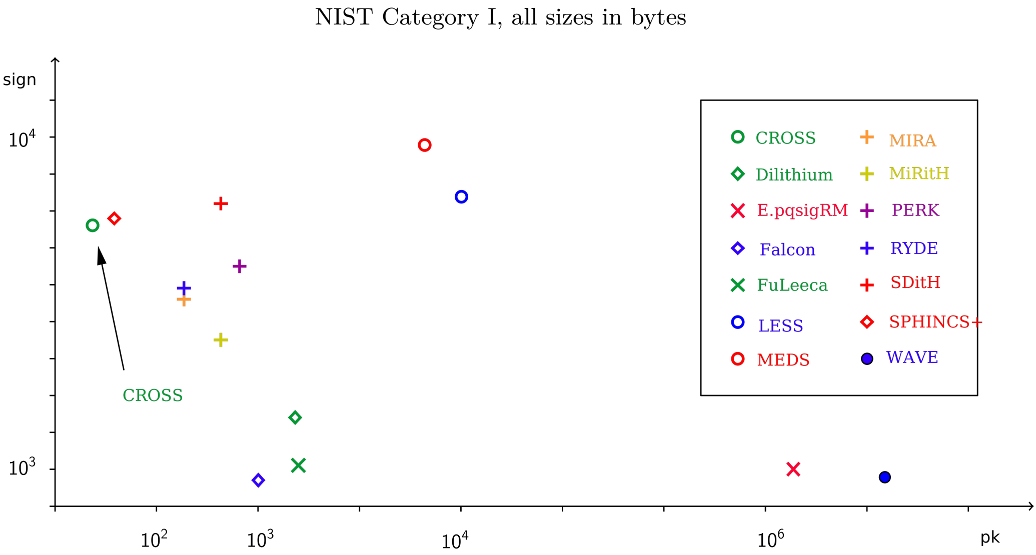
No optimized implementation

Level		$\lvert$ pk $\rvert$	$\lvert$ sign $\rvert$	t_{sign}	t_{verify}
I	fast	38	8’665	3.08	2.11
	short	38	7’625	11.04	7.81
III	fast	56	21’697	4.91	3.23
	short	56	17’429	18.06	12.24
V	fast	77	37’924	11.05	7.49
	short	77	31’696	29.08	19.44

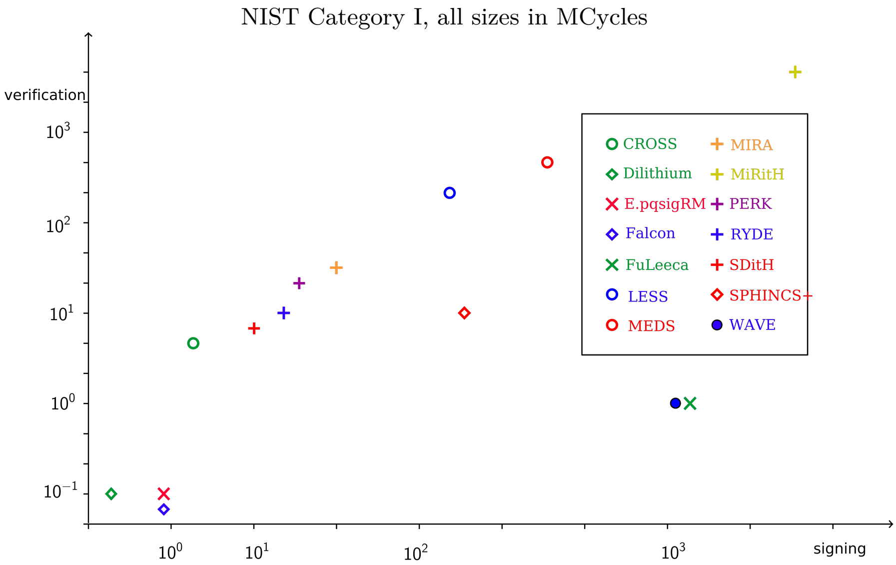
Performance



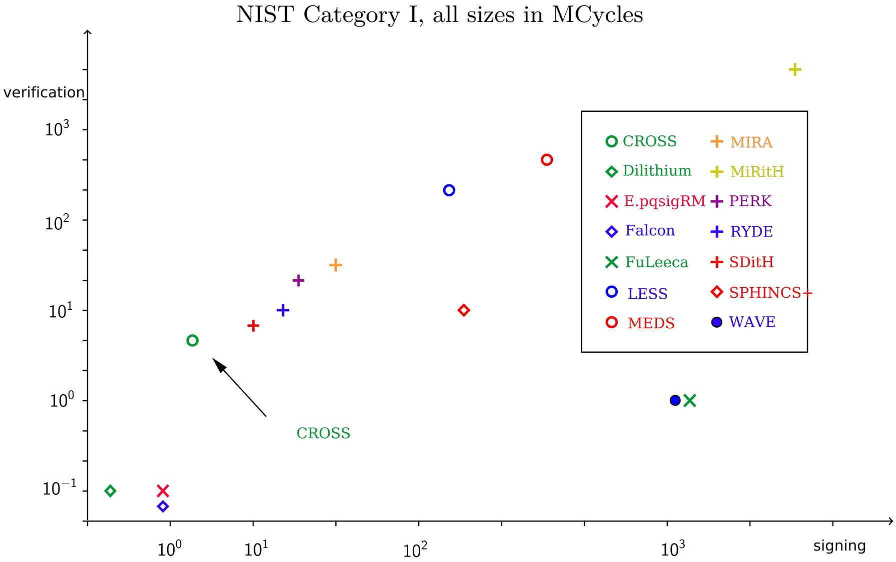
Performance



Performance



Performance



Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

CROSS

Codes & Restricted Objects Signature Scheme

`http://cross-crypto.com/`

Website

Slides

Questions?

What's next?

- Cryptanalysis continues
- Improvements?
- How many rounds?

CROSS

Codes & Restricted Objects Signature Scheme

`http://cross-crypto.com/`

Website

Slides

Thank you!

Code-Based Submissions

All sizes in bytes, times in MCycles.

Scheme	Based on	Technique	| Pk |	| Sig |	Sign	Verify
CROSS	Restricted SDP	ZK	32	7’625	11	7.4
Enh. pqsigRM	Reed-Muller	Hash & Sign	2’000’000	1’032	1.3	0.2
FuLeeca	Lee SDP	Hash & Sign	1’318	1’100	1’846	1.3
LESS	Code equiv.	ZK	13’700	8’400	206	213
MEDS	Matrix rank equiv.	ZK	9’923	9’896	518	515
MIRA	Matrix rank SDP	MPC	84	5’640	46’8	43’9
MiRitH	Matrix rank SDP	MPC	129	4’536	6’108	6’195
PERK	Permuted Kernel	MPC	150	6’560	39	27
RYDE	Rank SDP	MPC	86	5’956	23.4	20.1
SDitH	SDP	MPC	120	8’241	13.4	12.5
WAVE	Large wt $(U, U+V)$	Hash & Sign	3’677’390	822	1’160	1.23

Not all schemes have optimized implementations $\rightarrow$ Numbers may change

Hash-and-Sign: CFS

PROVER	VERIFIER
KEY GENERATION	
$\mathcal{S} = H$ parity-check matrix	
$\mathcal{P} = (t, HP)$ permuted H	
SIGNING	
Choose message m	
$s = \text{Hash}(m)$	
Find e: $s = eH^\top = eP(HP)^\top$,	
and $\text{wt}(e) \leq t$	
$\xrightarrow{m, eP}$	
	VERIFICATION
	Check if $\text{wt}(eP) \leq t$
	and $eP(HP)^\top = \text{Hash}(m)$

Hash-and-Sign: CFS

PROVER	VERIFIER
KEY GENERATION	
$\mathcal{S} = H$ parity-check matrix	
$\mathcal{P} = (t, HP)$ permuted H	
SIGNING	
Choose message m	
$s = \text{Hash}(m)$ Find e: $s = eH^\top = eP(HP)^\top$, and $\text{wt}(e) \leq t$	
$\xrightarrow{m, eP}$	
	VERIFICATION
	Check if $\text{wt}(eP) \leq t$ and $eP(HP)^\top = \text{Hash}(m)$

Problem: Distinguishability

Hash-and-Sign: CFS

PROVER		VERIFIER
KEY GENERATION		
$\mathcal{S} = H$ parity-check matrix		
$\mathcal{P} = (t, HP)$ permuted H		
SIGNING		
Choose message m		
$s = \mathrm{Hash}(m)$		
Find e: $s = eH^\top = eP(HP)^\top$, and $\mathrm{wt}(e) \leq t$		
	$\xrightarrow{m, eP}$	
		VERIFICATION
		Check if $\mathrm{wt}(eP) \leq t$ and $eP(HP)^\top = \mathrm{Hash}(m)$

Not any s is syndrome of low weight 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 $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

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 $c_2 = \mathrm{Hash}(y - z\sigma(e), \sigma(e))$

Recall SDP: (1) $s = eH^\top$ (2) $\mathrm{wt}(e) \leq t$

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

CROSS

Basis

- Restricted SDP
- ZK + Fiat-Shamir

$\rightarrow$ compact

Optimizations

- Merkle trees
- unbalanced challenges

$\rightarrow$ efficient

Security

- no trapdoor needed
- EUF-CMA security

$\rightarrow$ secure

CROSS

Basis

- Restricted SDP
- ZK + Fiat-Shamir

$\rightarrow$ compact

Optimizations

- Merkle trees
- unbalanced challenges

$\rightarrow$ efficient

Security

- no trapdoor needed
- EUF-CMA security

$\rightarrow$ secure

Sizes in bytes, times in MCycles

⚠ No optimized implementation

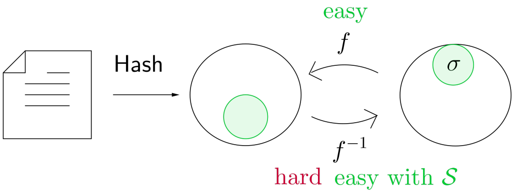
Level		$\lvert \text{pk} \rvert$	$\lvert \text{sign} \rvert$	t_{sign}	t_{verify}
I	fast	38	8'665	3.08	2.11
	short	38	7'625	11.04	7.81
III	fast	56	21'697	4.91	3.23
	short	56	17'429	18.06	12.24
V	fast	77	37'924	11.05	7.49
	short	77	31'696	29.08	19.44

Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

$\rightarrow$ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$

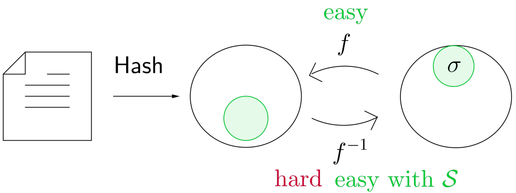


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

$\rightarrow$ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



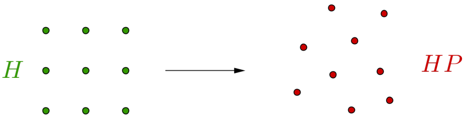
CFS: first code-based

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

- $\mathcal{S} = H$ structured code $\rightarrow \mathcal{P} = HP$

$\rightarrow$ large public key sizes

$\rightarrow$ distinguishers

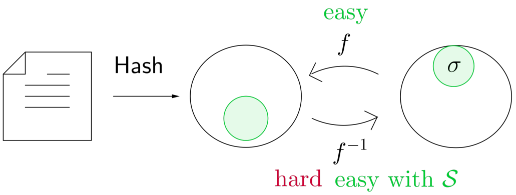


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

$\rightarrow$ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



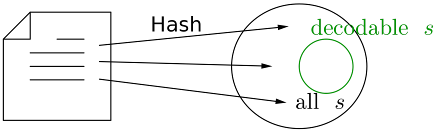
CFS: first code-based

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

- $\mathcal{S} = H$ structured code $\rightarrow \mathcal{P} = HP$
- $f(x) = x(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t \rightarrow \sigma = eP$

$\rightarrow$ slow signing

$\rightarrow$ σ not random: attacks

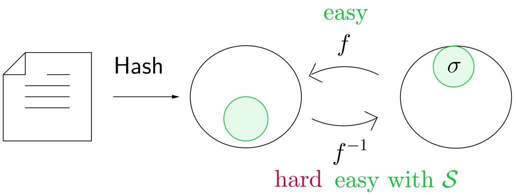


Idea of Hash-and-Sign

Ingredients:

- Secret key $\mathcal{S}$: secret code
- Trapdoor function: f

$\rightarrow$ signature: $\sigma = f^{-1}(\mathsf{Hash}(m))$



CFS: first code-based

N. Courtois, M. Finiasz, N. Sendrier. "How to achieve a McEliece-based digital signature scheme", Asiacrypt, 2001.

- $\mathcal{S} = H$ structured code $\rightarrow \mathcal{P} = HP$
- $f(x) = x(HP)^\top$
- $\mathsf{Hash}(m) = eH^\top$, $\mathrm{wt}_H(e) \leq t \rightarrow \sigma = eP$

Problems:

$\rightarrow$ large public keys

$\rightarrow$ slow signing

$\rightarrow$ security?