UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Code-based digital signatures: state of the art and open challenges

Marco Baldi

Università Politecnica delle Marche
Ancona, Italy

m.baldi@univpm.it

25th International Symposium on
Mathematical Theory of Networks and Systems (MTNS 2022)
Invited Session on "Applications of Coding Theory in Security"

September 12, 2022

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

UNIVERSITÀ POLITECNICA DELLE MARCHE

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

UNIVERSITÀ POLITECNICA DELLE MARCHE

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

UNIVERSITÀ POLITECNICA DELLE MARCHE

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

UNIVERSITÀ POLITECNICA DELLE MARCHE

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

UNIVERSITÀ POLITECNICA DELLE MARCHE

The NIST post-quantum standardization process

- In 2016 **NIST** has initiated a process for the development and standardization of one or more post-quantum public-key cryptographic algorithms.
  - 69 submissions in the 1° round
  - 26 admitted to the 2° round
  - 7 finalists and 8 alternates in the 3° round

Selected for standardization

Public-Key Encryption/KEMs:
- CRYSTALS-KYBER

Digital Signatures:
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

- PKE/KEMs admitted to the 4° round: BIKE, Classic McEliece, HQC, SIKE
- Just a few days after its admission to the fourth round, SIKE has been attacked[1].
- Rainbow has been the subject of a destructive key recovery attack although it had been admitted to the third round[2].

[1] https://eprint.iacr.org/2022/975
[2] https://eprint.iacr.org/2022/214

Post-quantum digital signatures

- **Dustin Moody**, NIST PQC team, 5 July 2022:

  ...NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023.

- NIST is going to issue a new Call for Proposals.
- NIST is looking for an alternative to lattice-based signatures.

Post-quantum digital signatures

- **Dustin Moody**, NIST PQC team, 5 July 2022:

  ...NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023.

- NIST is going to issue a new Call for Proposals.
- NIST is looking for an alternative to lattice-based signatures.

Post-quantum digital signatures

- **Dustin Moody**, NIST PQC team, 5 July 2022:

  ...NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023.

- NIST is going to issue a new Call for Proposals.
- NIST is looking for an alternative to lattice-based signatures.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Linear codes

- A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of length n and dimension k is a linear k-dimensional subspace of $\mathbb{F}_q^n$.

- Code parameters:
  - n: code length;
  - k: code dimension;
  - $r = n - k$: code redundancy;
  - $R = k/n$: code rate.
- Representations of a linear code:
  - generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, s.t. $\mathscr{C} = \{\mathbf{u}\mathbf{G} | \mathbf{u} \in \mathbb{F}_q^k\}$;
  - parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$, s.t. $\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{H}\mathbf{c}^\top = \mathbf{0}_r\}$.
- Hamming weight: $\mathrm{wt}(\mathbf{a}) = |\{i \text{ s.t. } a_i \neq 0\}|$.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Linear codes

- A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of length n and dimension k is a linear k-dimensional subspace of $\mathbb{F}_q^n$.

- Code parameters:
  - n: code length;
  - k: code dimension;
  - $r = n - k$: code redundancy;
  - $R = k/n$: code rate.

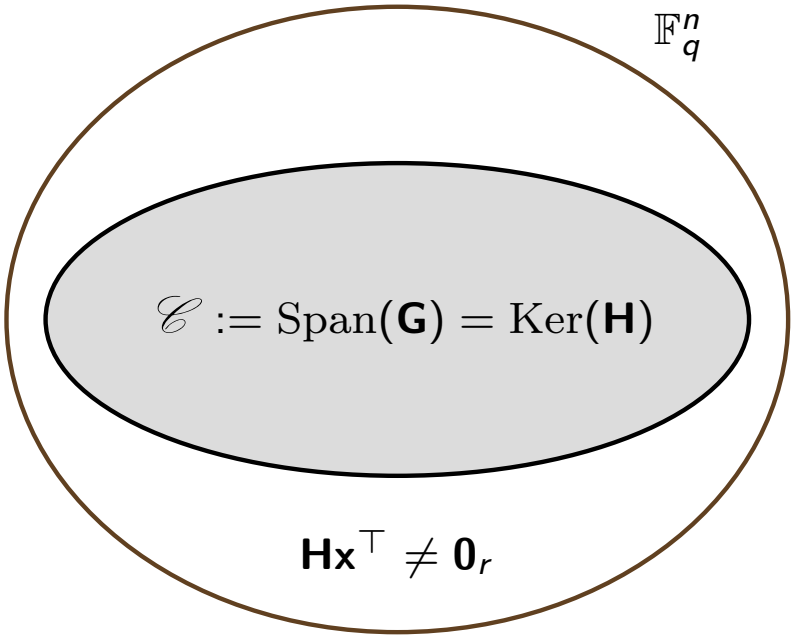
- Representations of a linear code:
  - generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, s.t. $\mathscr{C} = \{\mathbf{u}\mathbf{G} | \mathbf{u} \in \mathbb{F}_q^k\}$;
  - parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$, s.t. $\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{H}\mathbf{c}^\top = \mathbf{0}_r\}$.

- Hamming weight: $\mathrm{wt}(\mathbf{a}) = |\{i \text{ s.t. } a_i \neq 0\}|$.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Linear codes

- A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of length n and dimension k is a linear k-dimensional subspace of $\mathbb{F}_q^n$.

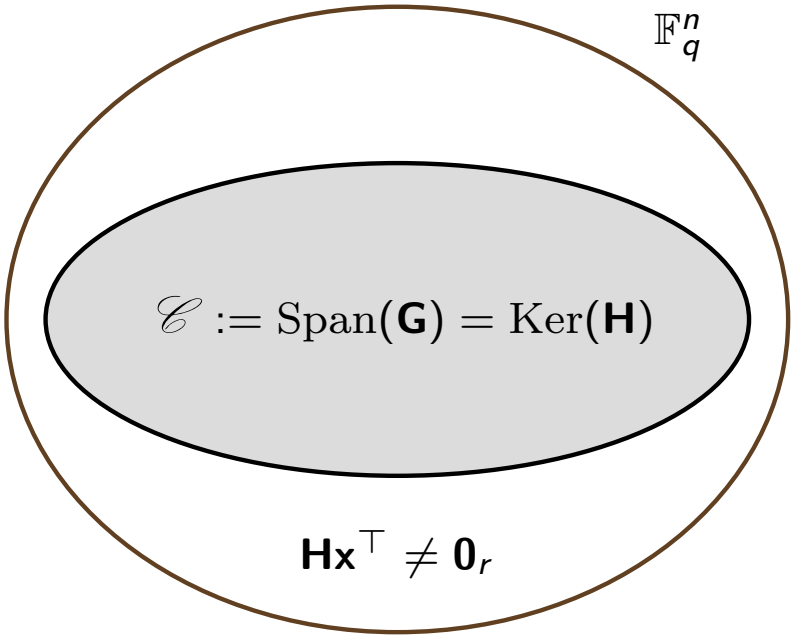


- Code parameters:
  - n: code length;
  - k: code dimension;
  - $r = n - k$: code redundancy;
  - $R = k/n$: code rate.
- Representations of a linear code:
  - generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, s.t. $\mathscr{C} = \{\mathbf{u}\mathbf{G} | \mathbf{u} \in \mathbb{F}_q^k\}$;
  - parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$, s.t. $\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{H}\mathbf{c}^\top = \mathbf{0}_r\}$.
- Hamming weight: $\mathrm{wt}(\mathbf{a}) = |\{i \text{ s.t. } a_i \neq 0\}|$.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Linear codes

- A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of length n and dimension k is a linear k-dimensional subspace of $\mathbb{F}_q^n$.



- Code parameters:
  - n: code length;
  - k: code dimension;
  - $r = n - k$: code redundancy;
  - $R = k/n$: code rate.

- Representations of a linear code:
  - generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, s.t. $\mathscr{C} = \{\mathbf{u}\mathbf{G} | \mathbf{u} \in \mathbb{F}_q^k\}$;
  - parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$, s.t. $\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{H}\mathbf{c}^\top = \mathbf{0}_r\}$.

- Hamming weight: $\mathrm{wt}(\mathbf{a}) = |\{i \text{ s.t. } a_i \neq 0\}|$.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Syndrome Decoding Problem

- **Syndrome Decoding Problem (SDP)**: given an arbitrary parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ and $\mathbf{s} \in \mathbb{F}_q^r$, find $\mathbf{e}$ with weight $\leq t$ such that $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$.
- For the Hamming metric, SDP is NP-hard.
- For the binary case (i.e., $q = 2$), when t is sub-linear in n the best solver is Information Set Decoding (ISD), with running time

$$T_{ISD} = \mathcal{O}\left(2^{t \cdot \alpha(R)}\right), \quad \alpha(R) = -\log_2(1-R)$$

- Quantum solver: Grover + ISD, complexity is still exponential in t:

$$\widetilde{T}_{ISD} = \mathcal{O}\left(2^{t \cdot \frac{\alpha(R)}{2}}\right)$$

Other choices are possible

SDP is hard also for different metrics (rank, Lee ...) and/or weight constraints (large weight ...).

- E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384-386, May 1978.
- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Syndrome Decoding Problem

- **Syndrome Decoding Problem (SDP)**: given an arbitrary parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ and $\mathbf{s} \in \mathbb{F}_q^r$, find $\mathbf{e}$ with weight $\leq t$ such that $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$.
- For the Hamming metric, SDP is NP-hard.
- For the binary case (i.e., $q = 2$), when t is sub-linear in n the best solver is Information Set Decoding (ISD), with running time

$$T_{ISD} = \mathcal{O}\left(2^{t \cdot \alpha(R)}\right), \quad \alpha(R) = -\log_2(1-R)$$

- Quantum solver: Grover + ISD, complexity is still exponential in t:

$$\widetilde{T}_{ISD} = \mathcal{O}\left(2^{t \cdot \frac{\alpha(R)}{2}}\right)$$

Other choices are possible

SDP is hard also for different metrics (rank, Lee ...) and/or weight constraints (large weight ...).

- E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384-386, May 1978.
- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Syndrome Decoding Problem

- **Syndrome Decoding Problem (SDP)**: given an arbitrary parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ and $\mathbf{s} \in \mathbb{F}_q^r$, find $\mathbf{e}$ with weight $\leq t$ such that $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$.
- For the Hamming metric, SDP is NP-hard.
- For the binary case (i.e., $q = 2$), when t is sub-linear in n the best solver is Information Set Decoding (ISD), with running time

$$T_{ISD} = \mathcal{O}\left(2^{t \cdot \alpha(R)}\right), \quad \alpha(R) = -\log_2(1-R)$$

- Quantum solver: Grover + ISD, complexity is still exponential in t:

$$\widetilde{T}_{ISD} = \mathcal{O}\left(2^{t \cdot \frac{\alpha(R)}{2}}\right)$$

Other choices are possible

SDP is hard also for different metrics (rank, Lee ...) and/or weight constraints (large weight ...).

- E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384-386, May 1978.
- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Syndrome Decoding Problem

- **Syndrome Decoding Problem (SDP)**: given an arbitrary parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ and $\mathbf{s} \in \mathbb{F}_q^r$, find $\mathbf{e}$ with weight $\leq t$ such that $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$.
- For the Hamming metric, SDP is NP-hard.
- For the binary case (i.e., $q = 2$), when t is sub-linear in n the best solver is Information Set Decoding (ISD), with running time

$$T_{ISD} = \mathcal{O}\left(2^{t \cdot \alpha(R)}\right), \quad \alpha(R) = -\log_2(1-R)$$

- Quantum solver: Grover + ISD, complexity is still exponential in t:

$$\widetilde{T}_{ISD} = \mathcal{O}\left(2^{t \cdot \frac{\alpha(R)}{2}}\right)$$

Other choices are possible

SDP is hard also for different metrics (rank, Lee ...) and/or weight constraints (large weight ...).

- E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384-386, May 1978.
- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Syndrome Decoding Problem

- **Syndrome Decoding Problem (SDP)**: given an arbitrary parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ and $\mathbf{s} \in \mathbb{F}_q^r$, find $\mathbf{e}$ with weight $\leq t$ such that $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$.
- For the Hamming metric, SDP is NP-hard.
- For the binary case (i.e., $q = 2$), when t is sub-linear in n the best solver is Information Set Decoding (ISD), with running time

$$T_{ISD} = \mathcal{O}\left(2^{t \cdot \alpha(R)}\right), \quad \alpha(R) = -\log_2(1-R)$$

- Quantum solver: Grover + ISD, complexity is still exponential in t:

$$\widetilde{T}_{ISD} = \mathcal{O}\left(2^{t \cdot \frac{\alpha(R)}{2}}\right)$$

Other choices are possible

SDP is hard also for different metrics (rank, Lee ...) and/or weight constraints (large weight ...).

- E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 384-386, May 1978.
- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Quantum vs signatures

- Quantum computers will endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (lattice-based and hash-based signatures).
- Code-based digital signatures are quantum-safe...
- But finding efficient code-based solutions is still a challenge!

Two main approaches to code-based signatures

- Hash-and-sign
- Derived from identification schemes

- G. Kabatianskii, E. Krouk, B. Smeets, "A digital signature scheme based on random error-correcting codes", in IMA International Conference on Cryptography and Coding (pp. 161–167). Springer, Berlin, Heidelberg, 1997.
- N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Quantum vs signatures

- Quantum computers will endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (lattice-based and hash-based signatures).
- Code-based digital signatures are quantum-safe...
- But finding efficient code-based solutions is still a challenge!

Two main approaches to code-based signatures

- Hash-and-sign
- Derived from identification schemes

- G. Kabatianskii, E. Krouk, B. Smeets, "A digital signature scheme based on random error-correcting codes", in IMA International Conference on Cryptography and Coding (pp. 161–167). Springer, Berlin, Heidelberg, 1997.
- N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Quantum vs signatures

- Quantum computers will endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (lattice-based and hash-based signatures).
- Code-based digital signatures are quantum-safe...
- But finding efficient code-based solutions is still a challenge!

Two main approaches to code-based signatures

- Hash-and-sign
- Derived from identification schemes

- G. Kabatianskii, E. Krouk, B. Smeets, "A digital signature scheme based on random error-correcting codes", in IMA International Conference on Cryptography and Coding (pp. 161–167). Springer, Berlin, Heidelberg, 1997.
- N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Quantum vs signatures

- Quantum computers will endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (lattice-based and hash-based signatures).
- Code-based digital signatures are quantum-safe...
- But finding efficient code-based solutions is still a challenge!

Two main approaches to code-based signatures

- Hash-and-sign
- Derived from identification schemes

- G. Kabatianskii, E. Krouk, B. Smeets, "A digital signature scheme based on random error-correcting codes", in IMA International Conference on Cryptography and Coding (pp. 161–167). Springer, Berlin, Heidelberg, 1997.
- N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

Quantum vs signatures

- Quantum computers will endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (lattice-based and hash-based signatures).
- Code-based digital signatures are quantum-safe...
- But finding efficient code-based solutions is still a challenge!

Two main approaches to code-based signatures

- Hash-and-sign
- Derived from identification schemes

- G. Kabatianskii, E. Krouk, B. Smeets, "A digital signature scheme based on random error-correcting codes", in IMA International Conference on Cryptography and Coding (pp. 161–167). Springer, Berlin, Heidelberg, 1997.
- N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute **s** = Hash(m) and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top$ = Hash(m).

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute **s** = Hash(m) and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top$ = Hash(m).

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute $\mathbf{s} = \text{Hash(m)}$ and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top = \text{Hash(m)}$.

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

▶ N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute $\mathbf{s} = \text{Hash(m)}$ and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top = \text{Hash(m)}$.

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

▶ N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute **s** = Hash(m) and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top = \text{Hash(m)}$.

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

▶ N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Hash-and-sign code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix **H** of $\mathscr{C}$.
  - **Signature generation**: compute **s** = Hash(m) and decode **s** into low weight vector **e**;
  - **Signature verification**: check that **e** has low weight and $\mathbf{He}^\top$ = Hash(m).

- However, finding a decodable syndrome is not easy!
  - Number of possible syndromes: $N_s = q^r$.
  - Every two vectors with weight $\leq t$ have distinct syndromes.
  - Number of decodable syndromes: $N_d = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - Probability to pick a decodable syndrome is N_d/N_s: normally, $N_s \gg N_d$.

- Example with Goppa codes: $q = 2$, $r = mt$, $n = 2^m \Rightarrow N_s = n^t$.
  $N_d \approx \frac{n^t}{t!}$.
  Probability of picking a decodable syndrome $= \frac{N_d}{N_s} \approx \frac{1}{t!}$.
- However, small t requires large k: public key size increases.
- Small t and large k imply high code rate: Goppa code distinguishers become efficient.

▶ N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

Evolution of hash-and-sign code-based signatures

- **1997**: Kabatianskii-Krouk-Smeets (KKS) scheme
  - does not require Goppa codes and can use random codes
  - uses two nested codes without needing decoding
  - has a very large region of weak parameters
- **2001**: Courtois-Finiasz-Sendrier (CFS) scheme
  - uses high rate Goppa codes
  - very large public-keys and long signature times
  - security issues due to distinguishers for high rate Goppa codes
- **2013**: Baldi-Bianchi-Chiaraluce-Rosenthal-Schipani (BBCRS) scheme
  - based on low density generator matrix (LDGM) codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage due to correlations
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - exploits the hardness of decoding large-weight errors over $\mathbb{F}_q$
  - based on generalized $(U; U + V)$ codes
  - requires information-set decoding for signature generation (slow)
  - public key size in the order of 4 MB for 128-bit security

Evolution of hash-and-sign code-based signatures

- **1997**: Kabatianskii-Krouk-Smeets (KKS) scheme
  - does not require Goppa codes and can use random codes
  - uses two nested codes without needing decoding
  - has a very large region of weak parameters
- **2001**: Courtois-Finiasz-Sendrier (CFS) scheme
  - uses high rate Goppa codes
  - very large public-keys and long signature times
  - security issues due to distinguishers for high rate Goppa codes
- **2013**: Baldi-Bianchi-Chiaraluce-Rosenthal-Schipani (BBCRS) scheme
  - based on LDGM codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage due to correlations
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - exploits the hardness of decoding large-weight errors over $\mathbb{F}_q$
  - based on generalized $(U; U + V)$ codes
  - requires information-set decoding for signature generation (slow)
  - public key size in the order of 4 MB for 128-bit security

Evolution of hash-and-sign code-based signatures

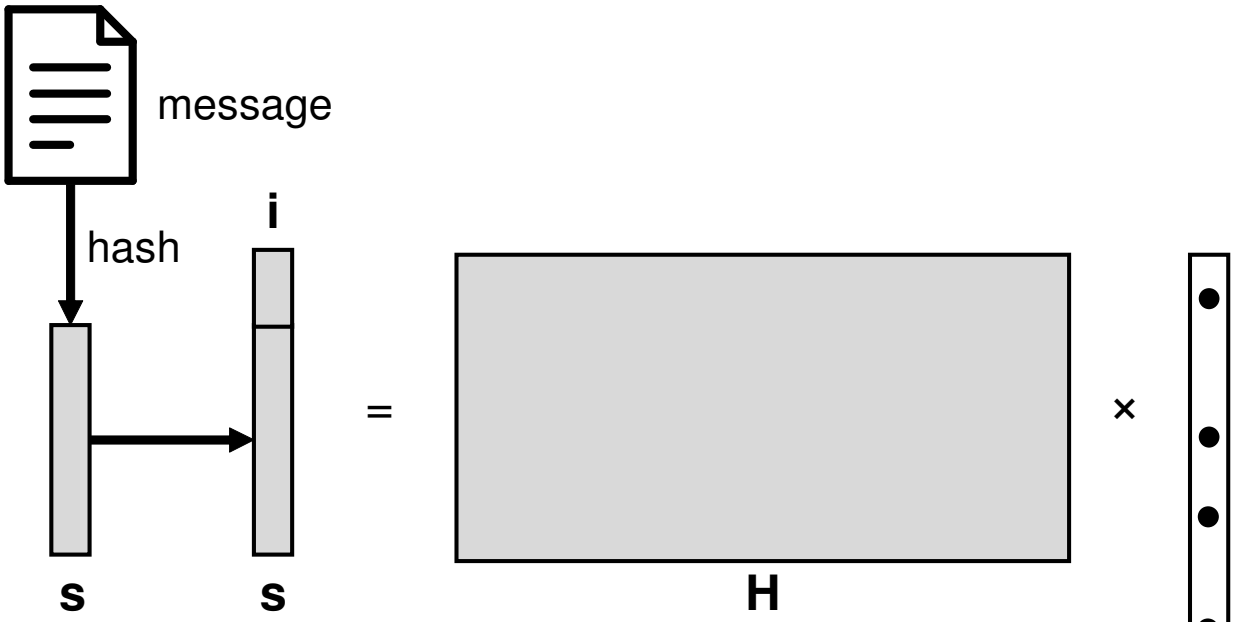
- **1997**: Kabatianskii-Krouk-Smeets (KKS) scheme
  - does not require Goppa codes and can use random codes
  - uses two nested codes without needing decoding
  - has a very large region of weak parameters
- **2001**: Courtois-Finiasz-Sendrier (CFS) scheme
  - uses high rate Goppa codes
  - very large public-keys and long signature times
  - security issues due to distinguishers for high rate Goppa codes
- **2013**: Baldi-Bianchi-Chiaraluce-Rosenthal-Schipani (BBCRS) scheme
  - based on LDGM codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage due to correlations
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - exploits the hardness of decoding large-weight errors over $\mathbb{F}_q$
  - based on generalized $(U; U + V)$ codes
  - requires information-set decoding for signature generation (slow)
  - public key size in the order of 4 MB for 128-bit security

Evolution of hash-and-sign code-based signatures

- **1997**: Kabatianskii-Krouk-Smeets (KKS) scheme
  - does not require Goppa codes and can use random codes
  - uses two nested codes without needing decoding
  - has a very large region of weak parameters
- **2001**: Courtois-Finiasz-Sendrier (CFS) scheme
  - uses high rate Goppa codes
  - very large public-keys and long signature times
  - security issues due to distinguishers for high rate Goppa codes
- **2013**: Baldi-Bianchi-Chiaraluce-Rosenthal-Schipani (BBCRS) scheme
  - based on LDGM codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage due to correlations
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - exploits the hardness of decoding large-weight errors over $\mathbb{F}_q$
  - based on generalized $(U; U + V)$ codes
  - requires information-set decoding for signature generation (slow)
  - public key size in the order of 4 MB for 128-bit security

UNIVERSITÀ POLITECNICA DELLE MARCHE

CFS

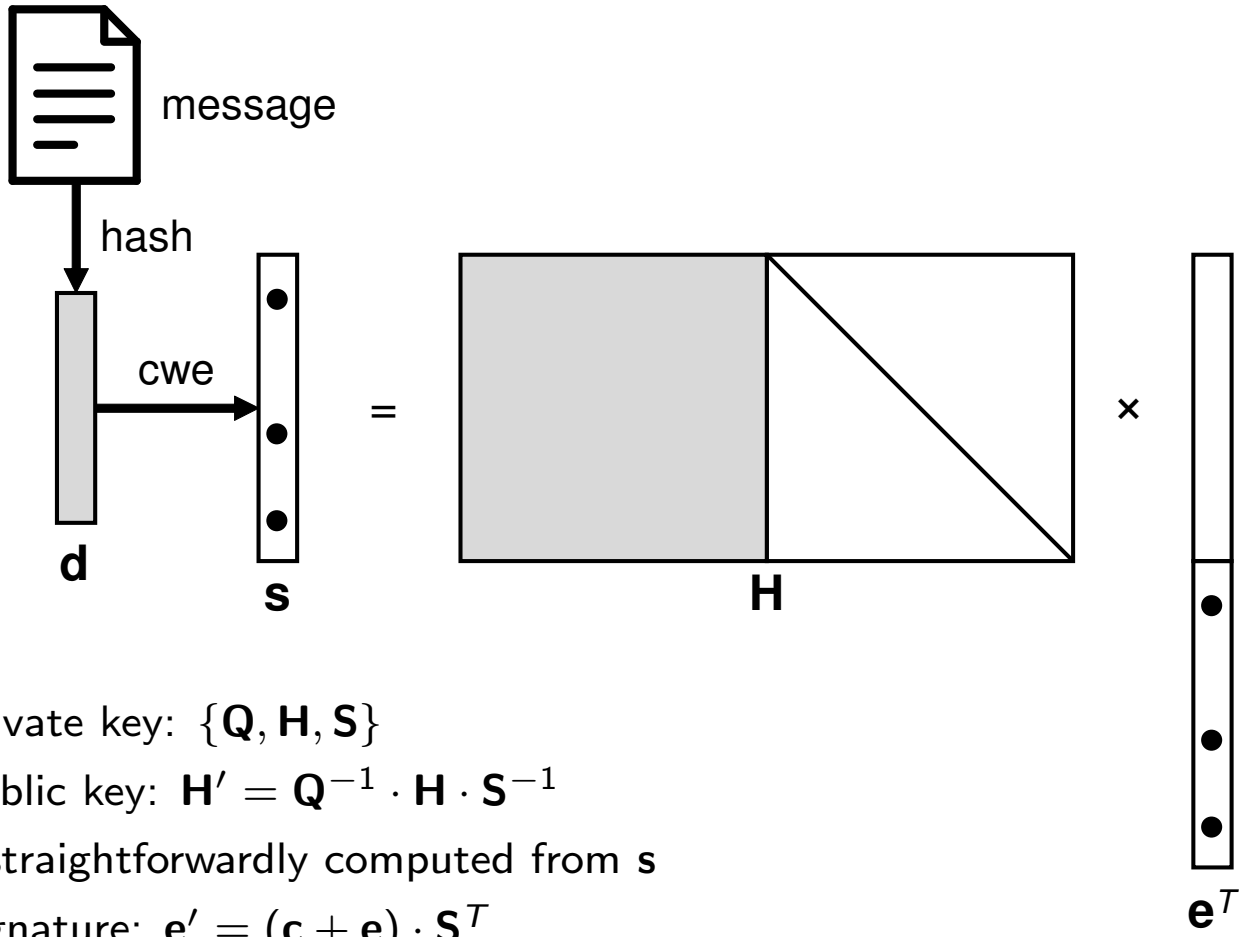


- Private key: $\{\mathbf{V}, \mathbf{H}, \mathbf{P}\}$
- Public key: $\mathbf{H}' = \mathbf{V} \cdot \mathbf{H} \cdot \mathbf{P}$
- Vary the syndrome by appending a counter $\mathbf{i}$
- $\mathbf{e}$ found through decoding of $[\mathbf{i}|\mathbf{s}]$
- Signature: $\mathbf{e}' = \mathbf{e} \cdot \mathbf{P}$
- Verification: $[\mathbf{i}|\mathbf{s}] \stackrel{?}{=} \mathbf{H}' \cdot \mathbf{e}'^T$

▶ N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Proc. ASIACRYPT 2001, vol. 2248 of Springer LNCS, pp. 157–174, 2001.

UNIVERSITÀ POLITECNICA DELLE MARCHE

BBCRS (PQCrypto 2013)



- Private key: $\{\mathbf{Q}, \mathbf{H}, \mathbf{S}\}$
- Public key: $\mathbf{H}' = \mathbf{Q}^{-1} \cdot \mathbf{H} \cdot \mathbf{S}^{-1}$
- $\mathbf{e}$ straightforwardly computed from $\mathbf{s}$
- Signature: $\mathbf{e}' = (\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$
- Verification: $\mathbf{s} \stackrel{?}{=} \mathbf{H}' \cdot \mathbf{e}'^T$

▶ M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, "Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures," Proc. PQCrypto 2013, vol. 7932 of Springer LNCS, pp. 1–15, 2013.

BBCRS - rationale

- The sparsity of $\mathbf{s}$ and the systematic form of $\mathbf{H}$ allow trivially deriving a sparse $\mathbf{e}$ without decoding
- The random codeword $\mathbf{c}$ adds noise to $\mathbf{e}$ and makes the signature stochastic
- If $\mathbf{S}$ is sparse then the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ is sparse too

Pro

Very fast signature generation (no decoding)

Con

To make the decoding problem hard for low-weight vectors we need sparse signatures and hence:

- a sparse codeword $\mathbf{c}$ (easy to find using LDGM codes)
- a sparse $\mathbf{S}$

BBCRS - rationale

- The sparsity of $\mathbf{s}$ and the systematic form of $\mathbf{H}$ allow trivially deriving a sparse $\mathbf{e}$ without decoding
- The random codeword $\mathbf{c}$ adds noise to $\mathbf{e}$ and makes the signature stochastic
- If $\mathbf{S}$ is sparse then the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ is sparse too

Pro

Very fast signature generation (no decoding)

Con

To make the decoding problem hard for low-weight vectors we need sparse signatures and hence:

- a sparse codeword $\mathbf{c}$ (easy to find using LDGM codes)
- a sparse $\mathbf{S}$

BBCRS - rationale

- The sparsity of $\mathbf{s}$ and the systematic form of $\mathbf{H}$ allow trivially deriving a sparse $\mathbf{e}$ without decoding
- The random codeword $\mathbf{c}$ adds noise to $\mathbf{e}$ and makes the signature stochastic
- If $\mathbf{S}$ is sparse then the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ is sparse too

Pro

Very fast signature generation (no decoding)

Con

To make the decoding problem hard for low-weight vectors we need sparse signatures and hence:

- a sparse codeword $\mathbf{c}$ (easy to find using LDGM codes)
- a sparse $\mathbf{S}$

BBCRS - cryptanalysis

- In the BBCRS scheme all the components of the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ are sparse and binary
- The signature is obtained as the sum of a few rows of $\mathbf{S}^T$
- As a result, the structure of each row of $\mathbf{S}^T$ is still visible in the signature

Attack

- Collect many signatures (100'000)
- Look at correlations (covariance) between pairs of signature entries
- Recover the rows of $\mathbf{S}^T$ by collecting correlated entries

BBCRS - cryptanalysis

- In the BBCRS scheme all the components of the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ are sparse and binary
- The signature is obtained as the sum of a few rows of $\mathbf{S}^T$
- As a result, the structure of each row of $\mathbf{S}^T$ is still visible in the signature

Attack

- Collect many signatures (100'000)
- Look at correlations (covariance) between pairs of signature entries
- Recover the rows of $\mathbf{S}^T$ by collecting correlated entries

BBCRS - cryptanalysis

- In the BBCRS scheme all the components of the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ are sparse and binary
- The signature is obtained as the sum of a few rows of $\mathbf{S}^T$
- As a result, the structure of each row of $\mathbf{S}^T$ is still visible in the signature

Attack

- Collect many signatures (100'000)
- Look at correlations (covariance) between pairs of signature entries
- Recover the rows of $\mathbf{S}^T$ by collecting correlated entries

BBCRS - cryptanalysis

- In the BBCRS scheme all the components of the signature $(\mathbf{c} + \mathbf{e}) \cdot \mathbf{S}^T$ are sparse and binary
- The signature is obtained as the sum of a few rows of $\mathbf{S}^T$
- As a result, the structure of each row of $\mathbf{S}^T$ is still visible in the signature

Attack

- Collect many signatures (100'000)
- Look at correlations (covariance) between pairs of signature entries
- Recover the rows of $\mathbf{S}^T$ by collecting correlated entries

▶ A. Phesso, JP. Tillich, "An Efficient Attack on a Code-Based Signature Scheme," Proc. PQCrypto 2016, vol. 9606 of Springer LNCS, pp. 86–103, 2016.

UNIVERSITÀ POLITECNICA DELLE MARCHE

From BBCRS to SPANSE

How to avoid the attack against BBCRS?

- Restrict to one-time use (at least for the moment ☺)
- Possibly avoid sparsity of signatures, but how?
  - Replace the sparse binary $\mathbf{S}$ with a dense one over $\mathbb{F}_q$
  - Rely on the hardness of large-weight vector decoding over $\mathbb{F}_q$

Zero-concentrated S

$\mathbf{S}$ no longer sparse, but dense with the constraint of having small-valued entries taken from $\mathbb{F}_q$.

- d_i: fraction of entries equal to $i, i = 0, 1, 2, \ldots, q-1$, in each row of $\mathbf{S}$.
- $d(x) = \sum_{i=0}^{q-1} d_i x^i$, with $\sum_{i=0}^{q-1} d_i = 1$: polynomial describing the density of the symbols of $\mathbb{F}_q$ in each row of $\mathbf{S}$.
- If $d(x)$ has decreasing coefficients we say it is zero-concentrated.
- The matrix $\mathbf{Q}$ is no longer needed to disguise the secret key, because of the density of $\mathbf{S}$, and can be replaced with a simple permutation matrix $\mathbf{P}$.

▶ M. Baldi, F. Chiaraluce, P. Santini, " SPANSE: combining sparsity with density for efficient one-time code-based digital signatures," CoRR, abs/2205.12887, https://arxiv.org/abs/2205.12887.

UNIVERSITÀ POLITECNICA DELLE MARCHE

From BBCRS to SPANSE

How to avoid the attack against BBCRS?

- Restrict to one-time use (at least for the moment ☺)
- Possibly avoid sparsity of signatures, but how?
  - Replace the sparse binary $\mathbf{S}$ with a dense one over $\mathbb{F}_q$
  - Rely on the hardness of large-weight vector decoding over $\mathbb{F}_q$

Zero-concentrated S

$\mathbf{S}$ no longer sparse, but dense with the constraint of having small-valued entries taken from $\mathbb{F}_q$.

- d_i: fraction of entries equal to $i, i = 0, 1, 2, \ldots, q-1$, in each row of $\mathbf{S}$.
- $d(x) = \sum_{i=0}^{q-1} d_i x^i$, with $\sum_{i=0}^{q-1} d_i = 1$: polynomial describing the density of the symbols of $\mathbb{F}_q$ in each row of $\mathbf{S}$.
- If $d(x)$ has decreasing coefficients we say it is zero-concentrated.
- The matrix $\mathbf{Q}$ is no longer needed to disguise the secret key, because of the density of $\mathbf{S}$, and can be replaced with a simple permutation matrix $\mathbf{P}$.

▶ M. Baldi, F. Chiaraluce, P. Santini, " SPANSE: combining sparsity with density for efficient one-time code-based digital signatures," CoRR, abs/2205.12887, https://arxiv.org/abs/2205.12887.

From BBCRS to SPANSE

How to avoid the attack against BBCRS?

- Restrict to one-time use (at least for the moment ☺)
- Possibly avoid sparsity of signatures, but how?
  - Replace the sparse binary $\mathbf{S}$ with a dense one over $\mathbb{F}_q$
  - Rely on the hardness of large-weight vector decoding over $\mathbb{F}_q$

Zero-concentrated S

$\mathbf{S}$ no longer sparse, but dense with the constraint of having small-valued entries taken from $\mathbb{F}_q$.

- d_i: fraction of entries equal to $i, i = 0, 1, 2, \ldots, q-1$, in each row of $\mathbf{S}$.
- $d(x) = \sum_{i=0}^{q-1} d_i x^i$, with $\sum_{i=0}^{q-1} d_i = 1$: polynomial describing the density of the symbols of $\mathbb{F}_q$ in each row of $\mathbf{S}$.
- If $d(x)$ has decreasing coefficients we say it is zero-concentrated.
- The matrix $\mathbf{Q}$ is no longer needed to disguise the secret key, because of the density of $\mathbf{S}$, and can be replaced with a simple permutation matrix $\mathbf{P}$.

▶ M. Baldi, F. Chiaraluce, P. Santini, " SPANSE: combining sparsity with density for efficient one-time code-based digital signatures," CoRR, abs/2205.12887, https://arxiv.org/abs/2205.12887.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Security level and key size

- Public key size: $K_s = 2436.6$ kB
- Number of different signatures: $N_s = 2^{263.9}$
- Number of different codewords: $N_c = 2^{133.8}$
- ISD work factor: 2^{132}
- PGE+SS work factor: $2^{131.6}$

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Another approach to code-based signatures

Hash-and-sign code-based digital signatures

- Classic approach (McEliece)
- Rely on a trapdoor based on some hidden structure
- Key recovery attacks may target such a hidden structure

Code-based signatures derived from ID schemes

- Alternative approach
- Start from an interactive identification scheme
- Do not require any trapdoor
- Structural attacks are avoided
- Must be rendered non-interactive through suitable transforms

Identification schemes

Phase 1

The prover randomly generates a pair $(\mathsf{sk}, \mathsf{pk})$

Phase 2

The prover exchanges messages with the verifier, who is only equipped with pk, with the goal of demonstrating knowledge of sk

Decision

The verifier decides whether to accept the prover or not

Properties:

1. zero-knowledge: no information about the secret key is revealed during the identification process
2. completeness: an honest prover always gets accepted
3. soundness: an impersonator has only a small probability of being accepted

Identification schemes

Phase 1

The prover randomly generates a pair $(\mathsf{sk}, \mathsf{pk})$

Phase 2

The prover exchanges messages with the verifier, who is only equipped with pk, with the goal of demonstrating knowledge of sk

Decision

The verifier decides whether to accept the prover or not

Properties:

1. zero-knowledge: no information about the secret key is revealed during the identification process
2. completeness: an honest prover always gets accepted
3. soundness: an impersonator has only a small probability of being accepted

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes

- A **prover** (holding sk) wants to prove their identity to a **verifier** (holding pk), without revealing information about the secret key.
- Single round interaction between prover and verifier:

- The honest prover can always reply correctly, an adversary is able to reply with some **cheating probability** δ. With N rounds, the cheating probability gets reduced to δ^N.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes

- A **prover** (holding sk) wants to prove their identity to a **verifier** (holding pk), without revealing information about the secret key.
- Single round interaction between prover and verifier:

PROVER		VERIFIER
Prepare commitment c		
	$\xrightarrow{c}$	
	$\longleftarrow$ Exchange additional messages $\longrightarrow$	
		Choose random challenge b
	$\xleftarrow{b}$	
Compute reply f		
	$\xrightarrow{f}$	
		Verify validity of f

- The honest prover can always reply correctly, an adversary is able to reply with some **cheating probability** δ. With N rounds, the cheating probability gets reduced to δ^N.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes

- A **prover** (holding sk) wants to prove their identity to a **verifier** (holding pk), without revealing information about the secret key.
- Single round interaction between prover and verifier:

PROVER		VERIFIER
Prepare commitment c		
	$\xrightarrow{c}$	
	$\xleftarrow{\text{Exchange additional messages}}$	
	$\xrightarrow{\text{Exchange additional messages}}$	
		Choose random challenge b
	$\xleftarrow{b}$	
Compute reply f		
	$\xrightarrow{f}$	
		Verify validity of f

- The honest prover can always reply correctly, an adversary is able to reply with some **cheating probability** δ. With N rounds, the cheating probability gets reduced to δ^N.

Code-based identification schemes

- **Stern**'s scheme:
  - random binary codes
  - 3 passes
  - cheating probability $= 2/3$
- **Veron**'s scheme:
  - dual version of Stern's scheme
  - lower communication cost
- **CVE** scheme:
  - random codes over $\mathbb{F}_q$
  - 5 passes
  - cheating probability $= \frac{q-1}{2q}$
- **AGS** scheme:
  - random binary quasi-cyclic codes
  - 5 passes
  - cheating probability $\approx 1/2$
  - compression of communications

- J. Stern, "A new identification scheme based on syndrome decoding," in Advances in Cryptology - CRYPTO' 93, D. R. Stinson, Ed. Springer Berlin Heidelberg, 1994, pp. 13–21.
- P. Véron, "Improved identification schemes based on error-correcting codes," Applicable Algebra in Engineering, Communication and Computing, vol. 8, no. 1, pp. 57–69, 1997.
- P.-L. Cayrel, P. Véron, and S. M. El Yousfi Alaoui, "A zero-knowledge identification scheme based on the q-ary syndrome decoding problem," in Selected Areas in Cryptography. Springer Berlin Heidelberg, 2011, pp. 171–186.
- C. Aguilar, P. Gaborit, and J. Schrek, "A new zero-knowledge code based identification scheme with reduced communication," in 2011 IEEE Information Theory Workshop (ITW), Paraty, Brazil, Oct 2011, pp. 648–652.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Signatures from identification schemes

- Identification schemes can be rendered non-interactive
- The **Fiat-Shamir** transformation obtains a signature scheme as the transcript of one execution of a 3-pass identification scheme
- This requires fixing the list of challenges by deriving them from some sort of seed
- **Dagdelen et al.** generalize this approach to n-pass identification schemes, including 5-pass code-based identification schemes
- The resulting signature scheme has very compact keys
- The signature is the transcript of the identification protocol and can result large

- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.
- O. Dagdelen, D. Galindo, P. Véeron, S. M. El Yousfi Alaoui, and P. Cayrel, "Extended security arguments for signature schemes," Des. Codes Cryptogr., vol. 78, no. 2, pp. 441–461, 2016.

Examples of signatures from ID schemes

- Security level: $\lambda = 128$ bits
- Cheating probability: 2^{-128}
- Signature size = communication cost of the underlying identification scheme

	CVE	AGS	R-CVE
Number of rounds	129	128	135
Public key size (bits)	832	1574	305
Average signature size (kB)	43.263	41.040	23.201
Max signature size (kB)	51.261	56.992	22.484

- These schemes follow the classical approach and can be optimized with several modern tricks (e.g., MPC-in-the-head, seed trees), which do not affect security.
- They allow further reductions of the signature size.

- M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, "A New Path to Code-based Signatures via Identification Schemes with Restricted Errors," arXiv preprint 2008.06403, August 2020.
- S. Gueron, E. Persichetti, P. Santini, "Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup," Cryptography, 6(1):5, 2022.
- T. Feneuil, A. Joux, M. Rivain, "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs," Cryptology ePrint Archive, Paper 2022/188, 2022.
- L. Bidoux, P. Gaborit, M. Kulkarni and N. Sendrier, "Quasi-Cyclic Stern Proof of Knowledge," 2022 IEEE International Symposium on Information Theory (ISIT), 2022, pp. 1459-1464.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Examples of signatures from ID schemes

- Security level: $\lambda = 128$ bits
- Cheating probability: 2^{-128}
- Signature size = communication cost of the underlying identification scheme

	CVE	AGS	R-CVE
Number of rounds	129	128	135
Public key size (bits)	832	1574	305
Average signature size (kB)	43.263	41.040	23.201
Max signature size (kB)	51.261	56.992	22.484

- These schemes follow the classical approach and can be optimized with several modern tricks (e.g., MPC-in-the-head, seed trees), which do not affect security.
- They allow further reductions of the signature size.

- M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, "A New Path to Code-based Signatures via Identification Schemes with Restricted Errors," arXiv preprint 2008.06403, August 2020.
- S. Gueron, E. Persichetti, P. Santini, "Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup," Cryptography, 6(1):5, 2022.
- T. Feneuil, A. Joux, M. Rivain, "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs," Cryptology ePrint Archive, Paper 2022/188, 2022.
- L. Bidoux, P. Gaborit, M. Kulkarni and N. Sendrier, "Quasi-Cyclic Stern Proof of Knowledge," 2022 IEEE International Symposium on Information Theory (ISIT), 2022, pp. 1459-1464.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Examples of signatures from ID schemes

- Security level: $\lambda = 128$ bits
- Cheating probability: 2^{-128}
- Signature size = communication cost of the underlying identification scheme

	CVE	AGS	R-CVE
Number of rounds	129	128	135
Public key size (bits)	832	1574	305
Average signature size (kB)	43.263	41.040	23.201
Max signature size (kB)	51.261	56.992	22.484

- These schemes follow the classical approach and can be optimized with several modern tricks (e.g., MPC-in-the-head, seed trees), which do not affect security.
- They allow further reductions of the signature size.

- M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, "A New Path to Code-based Signatures via Identification Schemes with Restricted Errors," arXiv preprint 2008.06403, August 2020.
- S. Gueron, E. Persichetti, P. Santini, "Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup," Cryptography, 6(1):5, 2022.
- T. Feneuil, A. Joux, M. Rivain, "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs," Cryptology ePrint Archive, Paper 2022/188, 2022.
- L. Bidoux, P. Gaborit, M. Kulkarni and N. Sendrier, "Quasi-Cyclic Stern Proof of Knowledge," 2022 IEEE International Symposium on Information Theory (ISIT), 2022, pp. 1459-1464.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes based on code equivalence

- **Code Equivalence Problem (CEP)**: given $\mathscr{C}$ and $\mathscr{C}'$, find an isometry τ such that $\mathscr{C}' = \tau(\mathscr{C})$.
- Hard-to-solve instances exist:
  - permutations and self dual codes;
  - monomials and random codes over $\mathbb{F}_q$ with $q \geq 5$.
- LESS: first cryptographic scheme based on code equivalence:
  - 3-pass code-based ID scheme;
  - soundness error is $1/2$;
- LESS-FM: follow-up, improved version of LESS:
  - updated and secure parameters;
  - optimized underlying ID scheme;
  - tunable features (e.g., 5.3 kB signatures with 20.5 kB public keys, or 10.4 kB signatures with 11.6 kB publick keys).
- Possibility of advanced functionalities, such as ring signatures.

- N. Sendrier, D. E. Simos, "The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography", in Proc. International Workshop on Post-Quantum Cryptography, Springer, Berlin, 2013, pp. 203–216.
- J. F. Biasse, G. Micheli, E. Persichetti, P. Santini, "LESS is more: Code-based signatures without syndromes", in Proc. International Conference on Cryptology in Africa, Springer, Cham, 2020, pp. 45–65.
- A. Barenghi, J. F. Biasse, E. Persichetti, P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem", in Proc. International Conference on Post-Quantum Cryptography, Springer, Cham, 2021, pp. 23–43.
- A. Barenghi, J. F. Biasse, T. Ngo, E. Persichetti, P. Santini, "Advanced signature functionalities from the code equivalence problem", in International Journal of Computer Mathematics: Computer Systems Theory 7.2, pp. 112–128, 2022.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes based on code equivalence

- **Code Equivalence Problem (CEP)**: given $\mathscr{C}$ and $\mathscr{C}'$, find an isometry τ such that $\mathscr{C}' = \tau(\mathscr{C})$.
- Hard-to-solve instances exist:
  - permutations and self dual codes;
  - monomials and random codes over $\mathbb{F}_q$ with $q \geq 5$.
- LESS: first cryptographic scheme based on code equivalence:
  - 3-pass code-based ID scheme;
  - soundness error is $1/2$;
- LESS-FM: follow-up, improved version of LESS:
  - updated and secure parameters;
  - optimized underlying ID scheme;
  - tunable features (e.g., 5.3 kB signatures with 20.5 kB public keys, or 10.4 kB signatures with 11.6 kB publick keys).
- Possibility of advanced functionalities, such as ring signatures.

- N. Sendrier, D. E. Simos, "The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography", in Proc. International Workshop on Post-Quantum Cryptography, Springer, Berlin, 2013, pp. 203–216.
- J. F. Biasse, G. Micheli, E. Persichetti, P. Santini, "LESS is more: Code-based signatures without syndromes", in Proc. International Conference on Cryptology in Africa, Springer, Cham, 2020, pp. 45–65.
- A. Barenghi, J. F. Biasse, E. Persichetti, P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem", in Proc. International Conference on Post-Quantum Cryptography, Springer, Cham, 2021, pp. 23–43.
- A. Barenghi, J. F. Biasse, T. Ngo, E. Persichetti, P. Santini, "Advanced signature functionalities from the code equivalence problem", in International Journal of Computer Mathematics: Computer Systems Theory 7.2, pp. 112–128, 2022.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes based on code equivalence

- **Code Equivalence Problem (CEP)**: given $\mathscr{C}$ and $\mathscr{C}'$, find an isometry τ such that $\mathscr{C}' = \tau(\mathscr{C})$.
- Hard-to-solve instances exist:
  - permutations and self dual codes;
  - monomials and random codes over $\mathbb{F}_q$ with $q \geq 5$.
- LESS: first cryptographic scheme based on code equivalence:
  - 3-pass code-based ID scheme;
  - soundness error is $1/2$;
- LESS-FM: follow-up, improved version of LESS:
  - updated and secure parameters;
  - optimized underlying ID scheme;
  - tunable features (e.g., 5.3 kB signatures with 20.5 kB public keys, or 10.4 kB signatures with 11.6 kB publick keys).
- Possibility of advanced functionalities, such as ring signatures.

- N. Sendrier, D. E. Simos, "The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography", in Proc. International Workshop on Post-Quantum Cryptography, Springer, Berlin, 2013, pp. 203–216.
- J. F. Biasse, G. Micheli, E. Persichetti, P. Santini, "LESS is more: Code-based signatures without syndromes", in Proc. International Conference on Cryptology in Africa, Springer, Cham, 2020, pp. 45–65.
- A. Barenghi, J. F. Biasse, E. Persichetti, P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem", in Proc. International Conference on Post-Quantum Cryptography, Springer, Cham, 2021, pp. 23–43.
- A. Barenghi, J. F. Biasse, T. Ngo, E. Persichetti, P. Santini, "Advanced signature functionalities from the code equivalence problem", in International Journal of Computer Mathematics: Computer Systems Theory 7.2, pp. 112–128, 2022.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Identification schemes based on code equivalence

- **Code Equivalence Problem (CEP)**: given $\mathscr{C}$ and $\mathscr{C}'$, find an isometry τ such that $\mathscr{C}' = \tau(\mathscr{C})$.
- Hard-to-solve instances exist:
  - permutations and self dual codes;
  - monomials and random codes over $\mathbb{F}_q$ with $q \geq 5$.
- LESS: first cryptographic scheme based on code equivalence:
  - 3-pass code-based ID scheme;
  - soundness error is $1/2$;
- LESS-FM: follow-up, improved version of LESS:
  - updated and secure parameters;
  - optimized underlying ID scheme;
  - tunable features (e.g., 5.3 kB signatures with 20.5 kB public keys, or 10.4 kB signatures with 11.6 kB publick keys).
- Possibility of advanced functionalities, such as ring signatures.

- N. Sendrier, D. E. Simos, "The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography", in Proc. International Workshop on Post-Quantum Cryptography, Springer, Berlin, 2013, pp. 203–216.
- J. F. Biasse, G. Micheli, E. Persichetti, P. Santini, "LESS is more: Code-based signatures without syndromes", in Proc. International Conference on Cryptology in Africa, Springer, Cham, 2020, pp. 45–65.
- A. Barenghi, J. F. Biasse, E. Persichetti, P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem", in Proc. International Conference on Post-Quantum Cryptography, Springer, Cham, 2021, pp. 23–43.
- A. Barenghi, J. F. Biasse, T. Ngo, E. Persichetti, P. Santini, "Advanced signature functionalities from the code equivalence problem", in International Journal of Computer Mathematics: Computer Systems Theory 7.2, pp. 112–128, 2022.

Identification schemes based on code equivalence

- **Code Equivalence Problem (CEP)**: given $\mathscr{C}$ and $\mathscr{C}'$, find an isometry τ such that $\mathscr{C}' = \tau(\mathscr{C})$.
- Hard-to-solve instances exist:
  - permutations and self dual codes;
  - monomials and random codes over $\mathbb{F}_q$ with $q \geq 5$.
- LESS: first cryptographic scheme based on code equivalence:
  - 3-pass code-based ID scheme;
  - soundness error is $1/2$;
- LESS-FM: follow-up, improved version of LESS:
  - updated and secure parameters;
  - optimized underlying ID scheme;
  - tunable features (e.g., 5.3 kB signatures with 20.5 kB public keys, or 10.4 kB signatures with 11.6 kB publick keys).
- Possibility of advanced functionalities, such as ring signatures.

- N. Sendrier, D. E. Simos, "The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography", in Proc. International Workshop on Post-Quantum Cryptography, Springer, Berlin, 2013, pp. 203–216.
- J. F. Biasse, G. Micheli, E. Persichetti, P. Santini, "LESS is more: Code-based signatures without syndromes", in Proc. International Conference on Cryptology in Africa, Springer, Cham, 2020, pp. 45–65.
- A. Barenghi, J. F. Biasse, E. Persichetti, P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem", in Proc. International Conference on Post-Quantum Cryptography, Springer, Cham, 2021, pp. 23–43.
- A. Barenghi, J. F. Biasse, T. Ngo, E. Persichetti, P. Santini, "Advanced signature functionalities from the code equivalence problem", in International Journal of Computer Mathematics: Computer Systems Theory 7.2, pp. 112–128, 2022.

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones

UNIVERSITÀ POLITECNICA DELLE MARCHE

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones

UNIVERSITÀ POLITECNICA DELLE MARCHE

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones

UNIVERSITÀ POLITECNICA DELLE MARCHE

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones

UNIVERSITÀ POLITECNICA DELLE MARCHE

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones

Conclusion

- New post-quantum digital signature schemes are needed
- Lattice-based solutions apparently are the first choice, but diversity is required
- Code-based signatures are post-quantum
- Two main approaches: hash-and-sign and identification-based
- Some promising schemes already exists
- Research is needed to make them (at least) as efficient as lattice-based ones