UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Recent advances in code-based encryption and digital signatures

Paolo Santini

Università Politecnica delle Marche
Ancona, Italy
p.santini@univpm.it

November 2, 2021

Quantum computers vs public key cryptography

- **Quantum computers** pose a serious threat on public key cryptography.

  "There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031".

  Prof. **Michele Mosca**, director of the Institute for Quantum Computing at the University of Waterloo

- Currently used public key cryptography can be broken in polynomial time.

- We need new algorithms, based on different mathematical problems, with post-quantum security.

- https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf

The NIST post-quantum standardization process

- **NIST** has initiated a process for the development and standardization of one or more public-key cryptographic post-quantum algorithms.

- 69 submissions in the 1° round
- 26 admitted to the 2° round
- 7 finalists and 8 alternates in the 3° round

- One code-based finalist (Classic McEliece)
- Two code-based alternates (BIKE, HQC)

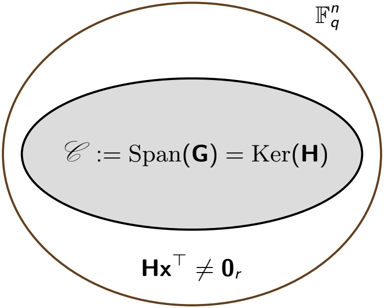
Code-based crypto is about to be standardized

Code-based cryptography is among the oldest and most understood type of public key cryptography.
It offers strong security guarantees and competitive performances.

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** $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, s.t. $\mathscr{C} = \{\mathbf{uG} | \mathbf{u} \in \mathbb{F}_q^k\}$;
  - **parity-check** $\mathbf{H} \in \mathbb{F}_q^{r\times n}$, s.t. $\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{Hc}^\top = \mathbf{0}_r\}$.

- 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., $q = 2$), the best solver is Information Set Decoding (ISD); running time is

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

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

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

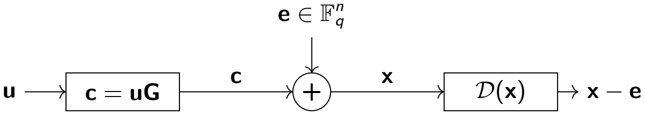
Other choices are possible

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

Error correcting codes

- Common application of codes: error correction over noisy channels.



- $\mathcal{D}$ is called decoder:
  - compute $\mathbf{s} = \mathbf{H}\mathbf{x}^\top = \mathbf{H}(\mathbf{c}+\mathbf{e})^\top = \mathbf{H}\mathbf{e}^\top$;
  - retrieve $\mathbf{e}$ from $\mathbf{s}$.
- Error correcting code: admits efficient (i.e., polynomial time) decoder $\mathcal{D}$.

How to build a trapdoor from codes

- **Secret key**: pick a code $\mathscr{C}$ with an efficient decoder $\mathcal{D}$.
- **Public key**: map $\mathscr{C}$ into a random looking code $\mathscr{C}'$.
- **Encryption**: ciphertext is a noisy codeword: $\mathbf{x} = \mathbf{c}' + \mathbf{e}$, with $\mathbf{c}' \in \mathscr{C}'$.
- **Decryption**: de-map $\mathbf{x}$ into $\mathbf{c} + \tilde{\mathbf{e}}$, with $\mathbf{c} \in \mathscr{C}$, and decode with $\mathcal{D}$.
- An adversary must decode a random looking code: best choice is ISD.

UNIVERSITÀ POLITECNICA DELLE MARCHE

The McEliece cryptosystem

- Proposed by Robert McEliece in 1978.
- Irreducible Goppa codes were used in the original proposal.
- Secret irreducible Goppa code:
  - irreducible polynomial of degree t over $GF(2^m)$,
  - length (maximum): $n = 2^m$,
  - dimension: $k \geq n - t \cdot m$,
  - correction capability: t errors,
  - efficient decoders (e.g., Patterson algorithm).

Robert J. McEliece
(May 21, 1942 – May 8, 2019)

- Secret key is $\mathbf{G}$, public key is $\mathbf{G}' = \mathbf{SGP}$, with random scrambling $\mathbf{S}$ and random permutation $\mathbf{P}$.

Trapdoor

- The public key generates a code $\mathscr{C}'$ which is indistinguishable from a random code.
- Efficient decoding can be performed only with the knowledge of $\mathscr{C}$.

▶ R. McEliece, "Public-Key System Based on Algebraic Coding Theory," DSN Progress Report 44, pp. 114–116, 1978.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Pros and Cons

Pros

- Goppa codes resisted cryptanalysis for more than 40 years.
- McEliece is faster than competing solutions.

Warnings

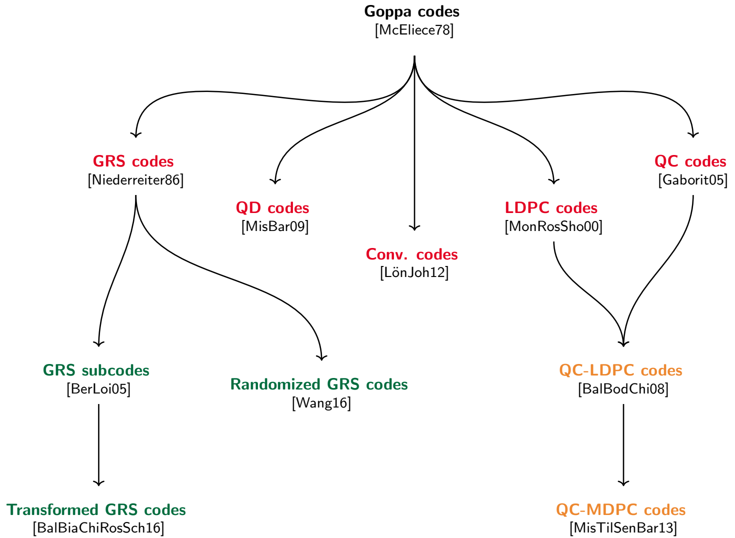
- Distinguishers prevent using high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.
- There are no NP-hard problems underlying the public key security.
- Many families of algebraic codes (other than Goppa) have been cryptanalyzed.

Cons

- It requires large public keys (260 KB or more for 128-bit security).

- J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich, "A distinguisher for high rate McEliece cryptosystems," In Proc. Information Theory Workshop 2011, pp. 282–286, Paraty, Brasil, 2011.

Alternatives to Goppa codes (Hamming metric)



LDPC codes

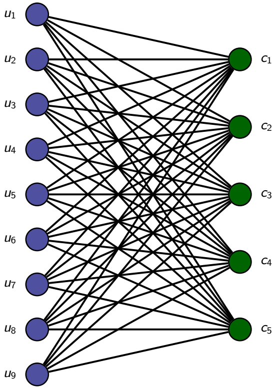
- Low-Density Parity-Check (LDPC) codes are state-of-art forward error correcting (FEC) codes.
- Introduced by Gallager in 1962 and more recently rediscovered.
- Able to approach the channel capacity under belief propagation decoding.
- Nowadays included in many applications and standards.

- R. G. Gallager, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. IT-8, pp. 21–28, Jan. 1962.
- D. J. C. MacKay and R. M. Neal, "Good codes based on very sparse matrices," in Cryptography and Coding. 5th IMA Conference, ser. Lecture Notes in Computer Science, C. Boyd, Ed. Berlin: Springer, no. 1025, pp. 100–111, 1995.
- C. Sae-Young, G. Forney, T. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," IEEE Commun. Lett., vol. 5, no. 2, pp. 58–60, Feb. 2001.

Representing LDPC codes: the Tanner graph

- **Tanner graph**: bipartite graph with n **variable nodes** $\{v_i\}_{i\in[1;n]}$ and r **check nodes** $\{c_j\}_{j\in[1;r]}$.
- Edge between v_i and c_j iff $h_{j,i}=1$.

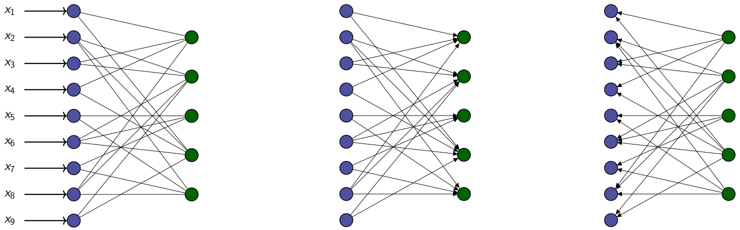
$$\mathbf{H}=\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$



- The parity-check matrix of an LDPC is sparse: majority of entries is null.
- The Tanner graph contains a small number of edges, i.e., nodes have low degree.

Decoding LDPC codes

- Efficient decoders for LDPC codes are message passing algorithms.
- Belief propagation: information spreads through the graph.



Step 0
Variable nodes store channel outputs

Step 1
From variable nodes to check nodes

Step 2
From check nodes to variable nodes

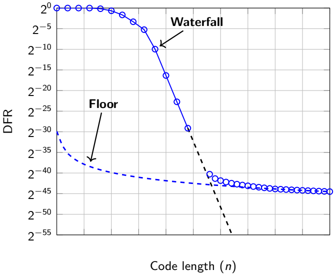
- **Iterative decoding**: steps 1 and 2 are repeated.
- Success if at some point check nodes agree, otherwise failure.

Fast decoding

Computational complexity $\approx$ number of messages.
The Tanner graph is sparse: decoding is efficient.

Decoding Failure Rate

- Decoding fails with some probability (called DFR), which is normally estimated through numerical simulations.
- Increasing n normally lowers the DFR... but be aware of floor!



- The floor may start at very low DFR, and is hardly predictable.

The "DFR" of algebraic codes

Algebraic codes (such as Goppa and GRS) do not have DFR issues: they can always correct a provable number of errors.

The Bit Flipping decoder

UNIVERSITÀ POLITECNICA DELLE MARCHE

- Bit Flipping (BF): message passing + logic operations (e.g., XOR) + threshold decision.

- From [Gallager1962]:

`The decoder computes all the parity checks and then changes any digit that is contained in more than some fixed number of unsatisfied parity-check equations. Using these new values, the parity checks are recomputed, and the process is repeated until the parity checks are all satisfied.`

- For a regular LDPC code, BF runs in time $\mathcal{O}(n)$, requires only logic operations and can be easily parallelized.

▶ R. G. Gallager, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. 8, pp. 21–28, 1962.

QC-LDPC codes

- QC code of order $n_0 \in \mathbb{N}$:
  - $n = n_0 p$, $r = r_0 p$, with $p \in \mathbb{N}$;
  - every cyclic shift of n_0 positions returns a codeword.

- A QC code can be represented by matrix formed by $p \times p$ circulant blocks:

$$\mathbf{H} = \left[\begin{array}{cccc|cccc} a_0 & b_0 & c_0 & d_0 & a_1 & b_1 & c_1 & d_1 \\ d_0 & a_0 & b_0 & c_0 & d_1 & a_1 & b_1 & c_1 \\ c_0 & d_0 & a_0 & b_0 & c_1 & d_1 & a_1 & b_1 \\ b_0 & c_0 & d_0 & a_0 & b_1 & c_1 & d_1 & a_1 \end{array}\right]$$

- A QC matrix can be represented by its first row: storage size is linear in n.

- Efficient arithmetic: circulant matrices are isomorphic to $\mathbb{F}_2[x]/(x^p + 1)$.

UNIVERSITÀ POLITECNICA DELLE MARCHE

McEliece scheme with QC-LDPC codes

- **Secret key**: parity-check matrix $\mathbf{H}$ of random QC-LDPC code $\mathscr{C}$.
- **Public key**: systematic generator matrix $\mathbf{G}$ for $\mathscr{C}$:

$$\mathbf{G} = \left[\mathbf{I}_{(n_0-1)p} \left| \begin{array}{c} \left(\mathbf{H}_{n_0}^{-1} \cdot \mathbf{H}_1\right)^\top \\ \vdots \\ \left(\mathbf{H}_{n_0}^{-1} \cdot \mathbf{H}_{n_0-1}\right)^\top \end{array} \right. \right]$$

- **Encryption**: $\mathbf{x} = \mathbf{uG} + \mathbf{e}$, where $\mathbf{e}$ has weight t.
- **Decryption**: run BF decoder on $\mathbf{x}$, retrieve $\mathbf{uG}$ and $\mathbf{e}$.

Trapdoor

- The public and private codes are the same.
- However, $\mathbf{G}$ is dense since $\mathbf{H}_{n_0}^{-1}$ is dense.
- Efficient decoding is possible only through a sparse representation of $\mathscr{C}$.

Security of public key

- SDP for the class of QC codes is yet to be proven NP-complete (is it? The question is open...): possible security issues!
- **Decoding One Of Many (DOOM)**: ISD over QC codes can receive a polynomial speed-up of $\sqrt{p} \div p$.

Practical security of QC-SDP

In practice, the problem is believed to be as hard as SDP over non QC codes.

- The dual of $\mathscr{C}$ admits $\mathbf{H}$ as generator: the rows of $\mathbf{H}$ are codewords with weight $w = n_0 v \ll n_0 p$.
- Best attack is ISD: complexity is $\mathcal{O}\left(2^{vn_0 \log_2\left(1-\frac{1}{n_0}\right)}\right)$.

Setting the density

Choose v large enough to prevent ISD.

- N. Sendrier,"Decoding one out of many," in B.-Y. Yang, editor, Post-Quantum Cryptography, volume 7071 of Lecture Notes in Computer Science, pages 51—67, Springer Verlag, 2011.

MDPC codes

- LDPC codes normally have $w = \mathcal{O}(\log(n))$, which is not enough.
- Moderate-Density Parity-Check (MDPC) codes: row weight is $w = \mathcal{O}\left(\sqrt{n}\right)$.
- MDPC codes have been formally introduced in 2009, but became "famous" only in 2013.
- Actually, MDPC codes have been used in crypto since 2007 (but were called LDPC).

Different names, same codes

An MDPC code is, simply, an LDPC with a somehow larger density.
They are decoded with LDPC decoders (e.g., BF) and have same pros and cons (e.g., high efficiency, waterfall/floor regions).

- S. Ouzan and Y. Be'ery, "Moderate-Density Parity-Check Codes," arXiv eprint 0911.3262, 2009.
- R. Misoczki, J. P. Tillich, N. Sendrier and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," Proc. IEEE ISIT 2013, Istanbul, Turkey, pp. 2069–2073.
- M. Baldi and F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes", Proc. 2007 IEEE International Symposium on Information Theory, Nice, 2007, pp. 2591-2595.
- M. Baldi, M. Bodrato, F. Chiaraluce, "A new analysis of the McEliece cryptosystem based on QC-LDPC codes", Proc. SCN 2008, vol. 5229 of LNCS, pp. 246–262, 2008.

QC-LDPC/MDPC codes in the NIST contest

- LEDAcrypt (Low-dEnsity parity-check coDe-bAsed cryptographic systems), providing:
  - A Niederreiter-based KEM with IND-CPA and ephemeral keys.
  - A Niederreiter-based KEM with IND-CCA2 and long-term keys.
  - A McEliece-based PKC with IND-CCA2.
  - Admitted to Round 1.
  - Admitted to Round 2.
  - Not admitted to Round 3 (weak keys + DFR issue).

- BIKE (Bit Flipping Key Encapsulation), providing:
  - Two McEliece/Niederreiter-based KEMs with IND-CPA and ephemeral keys.
  - Admitted to Round 1.
  - Admitted to Round 2.
  - Admitted to Round 3 as alternate candidate (DFR issue).

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt", https://www.ledacrypt.org/
- N. Aragon et al., "BIKE: Bit Flipping Key Encapsulation", https://bikesuite.org/

LEDAcrypt

- In LEDAcrypt, the secret key is $\mathbf{H} = \mathbf{H}' \cdot \mathbf{Q}$.
- $\mathbf{H}$ still has row weight $\mathcal{O}\left(\sqrt{n}\right)$: $\mathbf{H}'$ and $\mathbf{Q}$ have row weight $\mathcal{O}\left(\sqrt[4]{n}\right)$.
- Decoding complexity is reduced from $\mathcal{O}\left((v+1)n\right)$ to $\mathcal{O}\left((\sqrt{v}+1)n\right)$.
- However, $\mathbf{H}$ is more structured than purely random QC-MDPC: existence of ultra-weak keys!
- There exists a continuum of progressively less weak keys: ISD becomes gradually harder, but is always not harder than the purely random QC-MDPC case.

The fate of LEDAcrypt

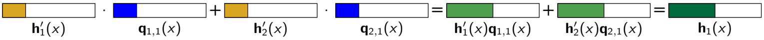
- The LEDAcrypt team proposed to choose $\mathbf{Q} = \mathbf{I}_{n_0 p}$ to avoid the attack.
- However, NIST judged this tweak as a major modification and eliminated LEDAcrypt from the competition.

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAkem: A post-quantum key encapsulation mechanism based on QC-LDPC codes", in International Conference on Post-Quantum Cryptography (pp. 3-24). Springer, Cham.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate", in Code-Based Cryptography Workshop (pp. 11-43). Springer, Cham.
- D. Apon, R. Perlner, A. Robinson, and P. Santini, "Cryptanalysis of LEDAcrypt," Proc. CRYPTO 2020, Vol. 12172 of Springer LNCS, Santa Barbara, CA, Aug. 2020.

Ultra weak keys in LEDAcrypt

- ISD searches for p positions, in a row of $\mathbf{H}$, where there are only zeros.
- Random QC-MDPC code with $n_0 = 2$: probability is $P \approx \left(\frac{1}{2}\right)^{2v} = 2^{-2v}$. Cost of ISD is $\mathcal{O}\left(1/P\right) = \mathcal{O}\left(2^{2v}\right)$.
- In LEDAcrypt: $\mathbf{H} = \begin{bmatrix} h_1(x) & h_2(x) \end{bmatrix} = \begin{bmatrix} h'_1(x) & h'_2(x) \end{bmatrix} \cdot \begin{bmatrix} q_{1,1}(x) & q_{1,2}(x) \\ q_{2,1}(x) & q_{2,2}(x) \end{bmatrix}$
  If all $h'_i(x)$ and $q_{i,j}(x)$ have degree $\leq p/4$, then $h_1(x)$ and $h_2(x)$ have degree $\leq p/2$.
- Probability to pick an ultra weak keys:

$$P_{LEDA} \approx \underbrace{\left(\left(\frac{p/4}{p}\right)^{\sqrt{v}}\right)^2}_{\text{Due to } \mathbf{H}'} \cdot \underbrace{\left(\left(\frac{p/4}{p}\right)^{\sqrt{v}}\right)^4}_{\text{Due to } \mathbf{Q}} = \left(\tfrac{1}{4}\right)^{6\sqrt{v}} = 2^{-12\sqrt{v}}$$



- D. Apon, R. Perlner, A. Robinson, and P. Santini, "Cryptanalysis of LEDAcrypt," Proc. CRYPTO 2020, Vol. 12172 of Springer LNCS, Santa Barbara, CA, Aug. 2020.

Reaction attacks

UNIVERSITÀ POLITECNICA DELLE MARCHE

Observations

1. Iterative decoding algorithms do not have a deterministic decoding radius, which entails a non-zero decoding failure rate (DFR).
2. Eve observes Bob's reactions and knows when decoding fails.
3. Events of decoding failure leak information about the secret key.

Countermeasures

- **IND-CPA** security: use ephemeral keys.
- **IND-CCA2** security: have a negligible DFR (i.e., $\leq 2^{-\lambda}$).

- Q. Guo, T. Johansson, and P. Stankovski, "A key recovery attack on MDPC with CCA security using decoding errors," Proc. ASIACRYPT 2016, Vol. 10031 of Springer LNCS, pages 789–815, Hanoi, Vietnam, Dec. 2016.
- T. Fabšič, V. Hromada, P. Stankovski, P. Zajac, Q. Guo, and T. Johansson, "A reaction attack on the QC-LDPC McEliece cryptosystem," Proc. PQCrypto 2017, pages 51–68, Vol. 10346 of Sprigner LNCS, Utrecht, the Netherlands, June 2017.
- P. Santini, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Analysis of Reaction and Timing Attacks Against Cryptosystems Based on Sparse Parity-Check Codes," Poc. CBC 2019, pages pp 115–136, Vol. 11666 of Springer LNCS, Darmstadt, Germany, May 2019.

UNIVERSITÀ POLITECNICA DELLE MARCHE

The DFR prediction issue

Issue 1

Iterative decoders are algorithmic $\Rightarrow$ no closed form formula for their error correction capability.

Issue 2

Useful mathematical models of iterative decoding algorithms work under some ideal assumptions (e.g., i.i.d. variables).

Issue 3

Performance curves may be simulated (Monte Carlo) down to DFR $\approx 10^{-9}$.

The difficulty of estimating the DFR

- Iterations are correlated: statistical independence is lost after the first iteration.
- Low DFR values are due to trapping sets: vectors with small weight such that the decoder is "trapped" into a bad configuration.
- Enumerating trapping sets is an NP-hard problem!
- Existing techniques become too complex when applied to MDPC codes (because of moderate density).

Solution (?)

We can still aim at finding efficient-to-compute upper bounds to the DFR.

- Y. Hashemi, A. H. Banihashemi, "On Characterization and Efficient Exhaustive Search of Elementary Trapping Sets of Variable-Regular LDPC Codes," in IEEE Communications Letters, vol. 19, no. 3, pp. 323-326, March 2015.
- A. McGregor, O. Milenkovic, "On the hardness of approximating stopping and trapping sets", in IEEE Transactions on Information Theory, 56(4), 1640-1650.

Analytical bounds for the DFR

UNIVERSITÀ POLITECNICA DELLE MARCHE

- We are able to study, without assumptions, only one decoder iteration:
  - **Tillich, 2018**: one iteration of BF can always correct (i.e., DFR $= 0$) up to αv errors, with $\alpha \in [0;1]$;
  - **Santini et al., 2019**: new theorem and optimization of the BF setting $\Rightarrow$ improve upon Tillich's α;
  - **Santini et al., 2020**: upper bound for the DFR of one BF iteration.

p	v	Keys achieving DFR $< 2^{-80}$	pk size (kB)	PK size reduction w.r.t. original McEliece
194'989	65	990 out of 1000	24 kB	58%
149'993	85	971 out of 1000	19 kB	67%
130'043	105	226 out of 1000	16 kB	72%

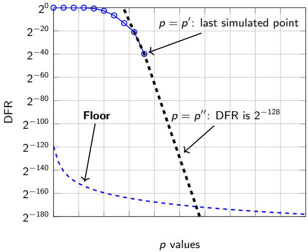
Limitations

BF can do way better with multiple iterations, but we do not have (at the moment) provable bounds!

- J. P. Tillich, "The decoding failure probability of MDPC codes", in 2018 IEEE International Symposium on Information Theory (ISIT) (pp. 941-945). IEEE.
- P. Santini, M. Battaglioni, M. Baldi, F. Chiaraluce, "Hard-decision iterative decoding of LDPC codes with bounded error rate", in ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
- P. Santini, M. Battaglioni, M. Baldi and F. Chiaraluce, "Analysis of the Error Correction Capability of LDPC and MDPC Codes Under Parallel Bit-Flipping Decoding and Application to Cryptography," in IEEE Transactions on Communications, vol. 68, no. 8, pp. 4648-4660, Aug. 2020.

DFR extrapolation

- In BIKE, the DFR curves of BF decoding are extrapolated assuming a monotone exponential decay.
- **Pros**: Considers any number of iterations.
- **Cons**: Requires intensive numerical simulations. Does not consider intersection with floor.



- **BIKE**: only 1.37 kB to reach 128 bits of IND-CCA2 security, with a BF decoder performing 5 iterations.

Conclusions

These numbers show the potential of QC-LDPC/QC-MDPC based schemes. Can we trust the DFR extrapolation? Open question...

- N. Sendrier and V. Vasseur, "About Low DFR for QC-MDPC Decoding", Post-Quantum Cryptography. Ed. by J. Ding and J.-P. Tillich. Cham: Springer International Publishing, 2020, pp. 20–34.
- M. Baldi, A. Barenghi, F. Chiaraluce, P. Santini, "Performance bounds for QC-MDPC codes decoders", CBCrypto 2021 (to be published).

Quantum vs signatures

- Quantum computers will also endanger many widespread signature schemes (like DSA and RSA signatures).
- Only a few replacements are available up to now (like hash-based signatures).
- Code-based digital signatures are post-quantum...
- But finding efficient code-based solutions is still a challenge!
- Two historical proposals: **Kabatianskii-Krouk-Smeets** (**KKS**) and **Courtois-Finiasz-Sendrier** (**CFS**) 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

The intrinsic difficulty of code-based signatures

- Natural approach to code-based signatures:
  - **Secret key**: error correcting code $\mathscr{C}$;
  - **Public key**: disguised parity-check matrix $\mathbf{H}$ of $\mathscr{C}$.
  - **Signature generation**: compute $\mathbf{s} = \text{Hash(m)}$ and decode $\mathbf{s}$ into low weight vector $\mathbf{e}$;
  - **Signature verification**: check that $\mathbf{e}$ 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 vectors = number of decodable syndromes = $N_e = \sum_{i=1}^{t} \binom{n}{i}(q-1)^i$.
  - The probability to pick a decodable syndrome is N_s/N_e: normally, $N_s \gg N_e$.
- Example with Goppa codes: $n = 2^m$, $r = mt \Rightarrow N_s = n^t$: t should be low. Number of attempts before picking a good syndrome $= \frac{N_s}{N_e} \approx \frac{N_s}{\binom{n}{t}} \approx \frac{1}{t!}$
- However, small t requires large k: public key size increases.

▶ 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 code-based digital signature schemes

- **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 (BBC$^+$) scheme
  - based on **LDGM!** (**LDGM!**) codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage, only one-time or few-times signatures

Lyubashevsky scheme

What if we grab the satisfactory lattice-based Lyubashevsky scheme and tweak it to use codes?

Lyubashevsky with codes and Hamming metric

- Attempts by Persichetti (2018), Song et al. (2020), Li et al. (2020).
- All of these solutions have been successfully cryptanalyzed!
- The problem lies within the signature generation:

$$\mathbf{z} = \underbrace{\mathbf{c}}_{\text{Public sparse vector}} \cdot \underbrace{\mathbf{E}}_{\text{Private sparse matrix}} + \underbrace{\mathbf{y}}_{\text{Private sparse vector}}$$

- Sparsity in the Hamming metric is too demanding: $\mathbf{c}$ and $\mathbf{E}$ have too many zeros and they leave a "mark" on $\mathbf{z}$.

- E. Persichetti, "Efficient one-time signatures from quasi-cyclic codes: A full treatment", Cryptography, 2(4), 30, 2018.
- Y. Song, X. Huang, Y. Mu, W. Wu, H. Wang, "A code-based signature scheme from the Lyubashevsky framework", Theoret. Comput. Sci. 835, 15–30, 2020.
- Z. Li, C. Xing and S. L. Yeo, "A new code based signature scheme without trapdoors", Proc. IACR, pp. 1250, 2020.
- J.-C. Deneuville, P. Gaborit, "Cryptanalysis of a code-based one-time signature", Designs, Codes and Cryptography, 88(9), 1857-1866, 2020.
- P. Santini, M. Baldi and F. Chiaraluce, "Cryptanalysis of a One-Time Code-Based Digital Signature Scheme," 2019 IEEE International Symposium on Information Theory (ISIT), 2019, pp. 2594-2598.
- N. Aragon, M. Baldi, J.C. Deneuville, K. Khathuria, E. Persichetti, P. Santini, "Cryptanalysis of a code-based full-time signature", Designs, Codes and Cryptography, 89(9), 2097-2112, 2021.
- M. Baldi, J. -C. Deneuville, E. Persichetti and P. Santini, "Cryptanalysis of a Code-Based Signature Scheme Based on the Schnorr-Lyubashevsky Framework," in IEEE Communications Letters, vol. 25, no. 9, pp. 2829-2833, 2021.

UNIVERSITÀ POLITECNICA DELLE MARCHE

Code-based signatures: difficult but not impossible!

- We have to say goodbye to the low Hamming weight... and/or use interactive schemes!
- Direct signature algorithms:
  - WAVE: hash and sign based on decoding in $\mathbb{F}_3$ with high Hamming weight;
  - Durandal: adaptation of Lyubashevsky to the rank metric.
- Identification (ID) scheme + Fiat-Shamir:
  - start from an interactive ID scheme;
  - apply Fiat-Shamir to remove interactivity.

Signatures from ID: pros and cons

- No trapdoor: the protocol uses a purely random instance of an hard-problem.
- Small public keys and small objects (e.g., small codes over small finite fields).
- Multiple repetitions to reach proper security levels: resulting signatures are large.

- T. Debris-Alazard, N. Sendrier, J. P. Tillich, "Wave: A new code-based signature scheme", 2018.
- N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, G. Zémor, "Durandal: a rank metric based signature scheme", in Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 728-758), Springer, Cham, 2019.
- A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO'86, Springer, 1986, pp. 186–194.

Identification schemes

- A **prover** (holding sk) wants to prove his 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.
- With **Fiat-Shamir**, an ID scheme can be turned into a fully-fledged signature scheme: the role of the verifier is replaced by hash functions.
- The signature size is given by the amount of exchanged bits.

Code-based ID schemes

- ID schemes can be built in a natural and intuitive way, starting from an instance of some hard problem.
- Based on binary SDP with low weight:
  - Stern, 1993;
  - Veron, 1997;
  - AGS, 2011.
- Based on non-binary SDP with low weight:
  - CVE, 2011.
- Based on SDP with low rank weight:
  - RVDC, 2019.
- Based on Code Equivalence Problem (decoding is not involved!):
  - LESS-FM, 2021.

Upcoming improvements

Several recent papers and drafts discuss tricks to optimize performances (e.g., trade signature length with public key size and/or computational complexity).

UNIVERSITÀ POLITECNICA DELLE MARCHE

A comparison between code-based signatures

Scheme	Security Level	Public Data	Public Key	Sig.	PK + Sig.	Security Assumption
Stern	80	18.43	0.048	113.57	113.62	Decoding with low Hamming
Veron	80	18.43	0.096	109.06	109.16	
CVE	80	5.18	0.072	66.44	66.54	
Wave	128	-	3205	1.04	3206.04	Decoding with high Hamming
cRVDC	125	0.050	0.15	22.48	22.63	Decoding with low rank
Durandal - I	128	307.31	15.24	4.06	19.3	
Durandal - II	128	419.78	18.60	5.01	23.61	
LESS-FM - I	128	9.78	9.78	15.2	24.97	Code Equivalence Problem
LESS-FM - II	128	13.71	205.74	5.25	210.99	
LESS-FM - III	128	11.57	11.57	10.39	21.96	

Table: A comparison of public keys and signature sizes with other code-based signature schemes. All sizes are in Kilobytes (kB).

A look at the NIST PQ competition

- **Dustin Moody**, NIST PQC team, June 2021:

  `NIST [...] recognizes that current and future research may lead to promising schemes which were not part of the NIST PQC Standardization Project. NIST may adopt a mechanism to accept such proposals at a later date. In particular, NIST would be interested in a general-purpose digital signature scheme which is not based on structured lattices.`[...] The more mature the scheme, the better.

- At the conclusion of the 3rd Round, NIST will issue a new Call for Proposals.

- NIST wants an alternative to lattice-based signatures.

Keep an eye on the competition

Probably, many candidates are about to appear: new solutions, new cryptanalysis, new implementations... but also lot of work!

- https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf

Conclusions

- Code-based cryptography is among the most studied and well understood areas of public key cryptography.
- For encryption schemes and KEMs, conservative solutions such as Classic McEliece are already viable and practical.
- Schemes based on QC-LDPC/QC-MDPC codes offer very small keys, but have problems with non null decryption failure rate.
- The panorama is less satisfying when it comes to signatures (due to intrinsic limitations).
- Yet, new solutions are appearing (and some new ones will appear in the near future).
- Pay attention, interesting things are about to happen!

UNIVERSITÀ POLITECNICA DELLE MARCHE

Greetings

Thank you very much for your attention

Questions?