From error-correction coding to cryptography for resisting quantum computers

Marco Baldi

Università Politecnica delle Marche
Ancona, Italy
m.baldi@univpm.it

Korea Cryptography Forum Annual Symposium

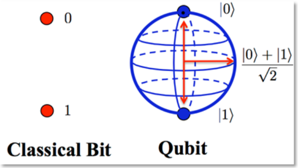
Seoul, Korea
November 14, 2019

Quantum computing

- Computer using quantum mechanics phenomena, such as quantum superposition and quantum correlation for performing calculations.
- Theorized by Richard Feynman and Yuri Manin in the early 1980s.
- Shor's algorithm (1994):
  - factorizes integers on a quantum computer,
  - given an integer N, it factors it in a time polynomial in $\log(N)$,
  - on a classic computer the time is exponential in N.
- Grover's algorithm (1996):
  - performs a search in an unordered list on a quantum computer,
  - it finds an entry in a list of N in a time proportional to $\sqrt{N}$,
  - on a classic computer the time is proportional to N.

Quantum computing

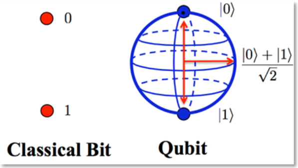
- Computer using quantum mechanics phenomena, such as quantum superposition and quantum correlation for performing calculations.
- Theorized by Richard Feynman and Yuri Manin in the early 1980s.



- Shor's algorithm (1994):
  - factorizes integers on a quantum computer,
  - given an integer N, it factors it in a time polynomial in $\log(N)$,
  - on a classic computer the time is exponential in N.
- Grover's algorithm (1996):
  - performs a search in an unordered list on a quantum computer,
  - it finds an entry in a list of N in a time proportional to $\sqrt{N}$,
  - on a classic computer the time is proportional to N.

Quantum computing

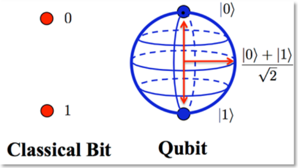
- Computer using quantum mechanics phenomena, such as quantum superposition and quantum correlation for performing calculations.
- Theorized by Richard Feynman and Yuri Manin in the early 1980s.



- Shor's algorithm (1994):
  - factorizes integers on a quantum computer,
  - given an integer N, it factors it in a time polynomial in $\log(N)$,
  - on a classic computer the time is exponential in N.
- Grover's algorithm (1996):
  - performs a search in an unordered list on a quantum computer,
  - it finds an entry in a list of N in a time proportional to $\sqrt{N}$,
  - on a classic computer the time is proportional to N.

Quantum computing

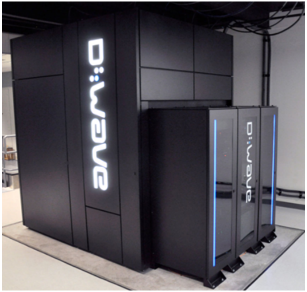
- Computer using quantum mechanics phenomena, such as quantum superposition and quantum correlation for performing calculations.
- Theorized by Richard Feynman and Yuri Manin in the early 1980s.



- Shor's algorithm (1994):
  - factorizes integers on a quantum computer,
  - given an integer N, it factors it in a time polynomial in $\log(N)$,
  - on a classic computer the time is exponential in N.
- Grover's algorithm (1996):
  - performs a search in an unordered list on a quantum computer,
  - it finds an entry in a list of N in a time proportional to $\sqrt{N}$,
  - on a classic computer the time is proportional to N.

Towards practical quantum computers

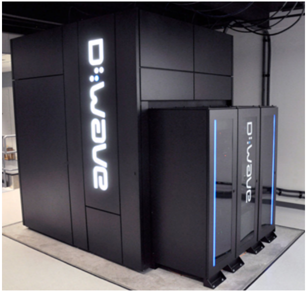
- **October 2011**: First academic center of quantum computing (USC, Lockheed Martin and D-Wave Systems).
- **January 2012**: D-Wave announces a quantum computer with 84 qubits.
- **Spring 2013**: Quantum D-Wave Two™ computer installed at the NASA Advanced Supercomputing (NAS) center of the Ames Research Center.



- ...
- **January 2017**: D-Wave 2000Q with 2000 qubits announced.
- Systems based on quantum annealing, less versatile than those based on quantum superposition.

Towards practical quantum computers

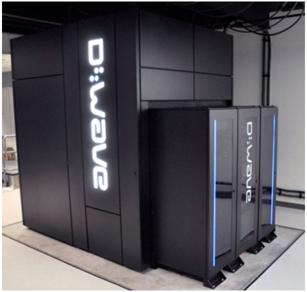
- **October 2011**: First academic center of quantum computing (USC, Lockheed Martin and D-Wave Systems).
- **January 2012**: D-Wave announces a quantum computer with 84 qubits.
- **Spring 2013**: Quantum D-Wave Two™ computer installed at the NASA Advanced Supercomputing (NAS) center of the Ames Research Center.



- ...
- **January 2017**: D-Wave 2000Q with 2000 qubits announced.
- Systems based on quantum annealing, less versatile than those based on quantum superposition.

Towards practical quantum computers

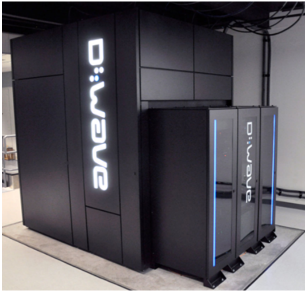
- **October 2011**: First academic center of quantum computing (USC, Lockheed Martin and D-Wave Systems).
- **January 2012**: D-Wave announces a quantum computer with 84 qubits.
- **Spring 2013**: Quantum D-Wave Two™ computer installed at the NASA Advanced Supercomputing (NAS) center of the Ames Research Center.



- ...
- **January 2017**: D-Wave 2000Q with 2000 qubits announced.
- Systems based on quantum annealing, less versatile than those based on quantum superposition.

Towards practical quantum computers

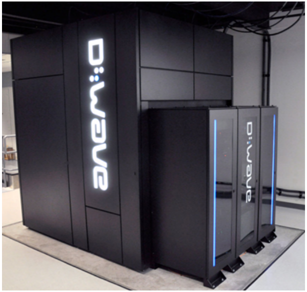
- **October 2011**: First academic center of quantum computing (USC, Lockheed Martin and D-Wave Systems).
- **January 2012**: D-Wave announces a quantum computer with 84 qubits.
- **Spring 2013**: Quantum D-Wave Two™ computer installed at the NASA Advanced Supercomputing (NAS) center of the Ames Research Center.



- ...
- **January 2017**: D-Wave 2000Q with 2000 qubits announced.
- Systems based on quantum annealing, less versatile than those based on quantum superposition.

Towards practical quantum computers

- **October 2011**: First academic center of quantum computing (USC, Lockheed Martin and D-Wave Systems).
- **January 2012**: D-Wave announces a quantum computer with 84 qubits.
- **Spring 2013**: Quantum D-Wave Two™ computer installed at the NASA Advanced Supercomputing (NAS) center of the Ames Research Center.

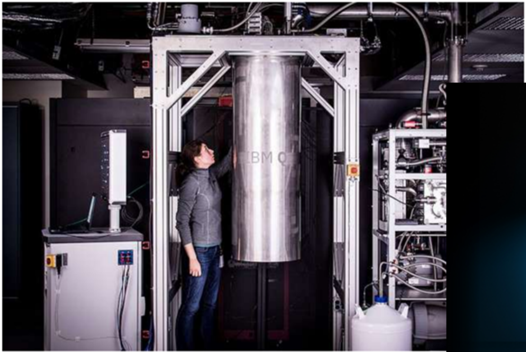


- ...
- **January 2017**: D-Wave 2000Q with 2000 qubits announced.
- Systems based on quantum annealing, less versatile than those based on quantum superposition.

Towards practical quantum computers (2)

IBM builds its most powerful universal quantum computing processors

May 17, 2017



IBM Research Staff Member Katie Pooley, a Physics PhD from Harvard who recently joined IBM, pictured
Center, working on a new prototype of a commercial quantum processor, which will be the core for the firs

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).
- It exploits quantum superposition.
- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).

- It exploits quantum superposition.
- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).
- It exploits quantum superposition.

- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).
- It exploits quantum superposition.
- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).
- It exploits quantum superposition.

- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Towards practical quantum computers (3)

- On January 2019 IBM announced Q System One, the first commercial quantum computer.
- It has 20 qubits (50 qubits are deemed necessary to compete with classic computers).
- It exploits quantum superposition.
- It must be kept at a very low temperature and isolated from any form of electromagnetic noise.
- Quantum equivalent of the first computers of the 1950s and 1960s.
- Simulators and software models available for programming.

Quantum supremacy

- Google and IBM are competing towards achieving quantum supremacy.
- The 72-qubit system that Google was developing in 2017 proved too difficult to control.
- Google then started the development of a 53-qubit system called Sycamore.
- In October 2019, Google claimed that the Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years.
- IBM disclaimed this, stating that Google's system is specialized to solve a single problem, differently from IBM's general-purpose quantum computer.

▶ F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.

Quantum supremacy

- Google and IBM are competing towards achieving quantum supremacy.
- The 72-qubit system that Google was developing in 2017 proved too difficult to control.
- Google then started the development of a 53-qubit system called Sycamore.
- In October 2019, Google claimed that the Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years.
- IBM disclaimed this, stating that Google's system is specialized to solve a single problem, differently from IBM's general-purpose quantum computer.

▶ F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.

Quantum supremacy

- Google and IBM are competing towards achieving quantum supremacy.
- The 72-qubit system that Google was developing in 2017 proved too difficult to control.
- Google then started the development of a 53-qubit system called Sycamore.
- In October 2019, Google claimed that the Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years.
- IBM disclaimed this, stating that Google's system is specialized to solve a single problem, differently from IBM's general-purpose quantum computer.

- F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.

Quantum supremacy

- Google and IBM are competing towards achieving quantum supremacy.
- The 72-qubit system that Google was developing in 2017 proved too difficult to control.
- Google then started the development of a 53-qubit system called Sycamore.
- In October 2019, Google claimed that the Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years.
- IBM disclaimed this, stating that Google's system is specialized to solve a single problem, differently from IBM's general-purpose quantum computer.

▶ F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.

Quantum supremacy

- Google and IBM are competing towards achieving quantum supremacy.
- The 72-qubit system that Google was developing in 2017 proved too difficult to control.
- Google then started the development of a 53-qubit system called Sycamore.
- In October 2019, Google claimed that the Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world's most powerful supercomputer 10,000 years.
- IBM disclaimed this, stating that Google's system is specialized to solve a single problem, differently from IBM's general-purpose quantum computer.

▶ F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.

Quantum-vulnerable cryptography

The most widespread cryptographic systems today are based on mathematical problems that can be solved with Shor's algorithm:

- **RSA**: public key cryptosystem based on integer factorization (used in SSL/TLS, online banking, ATM, ...).
- **ElGamal**: public key cryptosystem based on discrete logarithm (used in SSL/TLS, ...).
- **DSA**: digital signature algorithm based on discrete logarithm (used in SSL/TLS, ...).
- **Diffie-Hellman**: key exchange protocol based on discrete logarithm (used in SSL/TLS, NFC, contactless payments, ...).
- **ECDH**: Elliptic-curve Diffie–Hellman, used for end-to-end encryption (Signal, WhatsApp, Facebook Messenger, Skype, ...).
- **ECDSA**: Elliptic-curve digital signature algorithm (used in Bitcoin (secp256k1), Ethereum, ...).

Post-quantum cryptography

Asymmetric schemes:

- Based on lattices
- Based on codes
- Based on multivariate polynomials
- Based on hash functions
- Others (isogenies ...)

Symmetric schemes:

- Symmetric encryption schemes (AES ...)
- Hash functions (SHA ...)
- Can still be used as long as Grover's algorithm is taken into account

NIST PQcrypto Project

- **NIST** has initiated a process for the development and standardization of one or more public-key cryptographic algorithms to enrich:

  - Recommendation FIPS 186-4 (Digital Signature Standard - DSS)
  - Special publication SP 800-56A Rev 2 (key establishment systems based on discrete logarithm)
  - Special publication SP 800-56B (key establishment systems based on integer factorization)

NIST PQcrypto call timeline

- **2-3 April 2015**: NIST Workshop on Cybersecurity in a Post-Quantum World
- **24-26 February 2016**: Announcement and description of the NIST call
- **28 April 2016**: NISTIR 8105 report on post-quantum cryptography released
- **20 December 2016**: Official publication of the call
- **30 November 2017**: Deadline for submission of candidates

NIST PQcrypto requirements

Public-key encryption

Shall include algorithms for key generation, encryption, and decryption. At a minimum, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits.

Key encapsulation mechanism (KEM)

Shall include algorithms for key generation, encapsulation, and decapsulation. At a minimum, the KEM functionality shall support the establishment of shared keys of length at least 256 bits.

Digital signature

Shall include algorithms for key generation, signature generation and signature verification. The scheme shall be capable of supporting a message size up to 2^{63} bits.

NIST PQcrypto requirements

Public-key encryption

Shall include algorithms for key generation, encryption, and decryption. At a minimum, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits.

Key encapsulation mechanism (KEM)

Shall include algorithms for key generation, encapsulation, and decapsulation. At a minimum, the KEM functionality shall support the establishment of shared keys of length at least 256 bits.

Digital signature

Shall include algorithms for key generation, signature generation and signature verification. The scheme shall be capable of supporting a message size up to 2^{63} bits.

NIST PQcrypto requirements

Public-key encryption

Shall include algorithms for key generation, encryption, and decryption. At a minimum, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits.

Key encapsulation mechanism (KEM)

Shall include algorithms for key generation, encapsulation, and decapsulation. At a minimum, the KEM functionality shall support the establishment of shared keys of length at least 256 bits.

Digital signature

Shall include algorithms for key generation, signature generation and signature verification. The scheme shall be capable of supporting a message size up to 2^{63} bits.

NIST PQcrypto security categories

Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for:

1. Key search on a block cipher with a **128-bit key** (e.g. AES128)
2. Collision search on a **256-bit hash** function (e.g. SHA256/ SHA3-256)
3. Key search on a block cipher with a **192-bit key** (e.g. AES192)
4. Collision search on a **384-bit hash** function (e.g. SHA384/ SHA3-384)
5. Key search on a block cipher with a **256-bit key** (e.g. AES 256)

NIST PQcrypto 1st round candidates

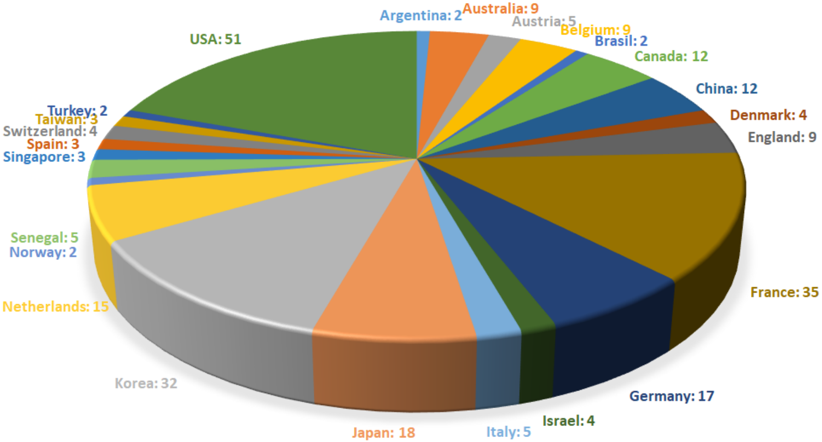
FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

NIST PQcrypto 1st round - Countries involved

263 researchers from **24** Countries



NIST PQcrypto selection steps

- **21 December 2017**: Round 1 algorithms announced (69 submissions accepted as "complete and proper")
- Candidates analyzed for over a year by NIST and international community
- Security has been the main criterion for the first round
- **11-13 April 2018**: First PQC Standardization Conference
- **30 January 2019**: Second round candidates announced (26 algorithms)
- **22-24 August 2019**: Second PQC Standardization Conference
- **2020/2021**: Round 3 begins
- **2022/2024**: Draft standards available

NIST PQcrypto 2nd round KEM/PKC candidates

Code-based

- BIKE
- Classic McEliece
- HQC
- LEDAcrypt
- NTS-KEM
- ROLLO
- RQC

Isogeny-based

- SIKE

Lattice-based

- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU
- NTRU Prime
- Round5
- SABER
- Three Bears

NIST PQcrypto 2nd round digital signature candidates

Lattice-based

- CRYSTALS-DILITHIUM
- FALCON
- qTESLA

Hash-based+

- Picnic
- SPHINCS+

Multivariate

- GeMSS
- LUOV
- MQDSS
- Rainbow

Lattice-based cryptography

- **1996**: Miklós Ajtai introduces the first asymmetric lattice-based scheme and shows that the average case of certain lattice-related problems is as difficult to solve as the worst case.
- **1998**: Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman introduce the lattice-based public-key scheme known as NTRU.
- **2005**: Oded Regev introduces the first lattice-based cryptosystem compliant with the average-to-worst case reduction.
- Regev has shown that the problem of **learning with errors** (LWE) is as difficult to solve as several lattice problems in their worst case.
- **2009**: Craig Gentry introduces the first fully homomorphic lattice-based cryptosystem.

- M. Ajtai, "Generating Hard Instances of Lattice Problems," Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.
- J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, vol. 1423 of Lecture Notes in Computer Science. pp. 267–288, 1998.
- O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proc. Thirty-seventh Annual ACM Symposium on Theory of Computing, pp. 84–93, 2005.
- C. Gentry, "A Fully Homomorphic Encryption Scheme," Thesis, Stanford University, 2009.

Lattice-based cryptography

- **1996**: Miklós Ajtai introduces the first asymmetric lattice-based scheme and shows that the average case of certain lattice-related problems is as difficult to solve as the worst case.
- **1998**: Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman introduce the lattice-based public-key scheme known as NTRU.
- **2005**: Oded Regev introduces the first lattice-based cryptosystem compliant with the average-to-worst case reduction.
- Regev has shown that the problem of **learning with errors** (LWE) is as difficult to solve as several lattice problems in their worst case.
- **2009**: Craig Gentry introduces the first fully homomorphic lattice-based cryptosystem.

▶ M. Ajtai, "Generating Hard Instances of Lattice Problems," Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.

▶ J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, vol. 1423 of Lecture Notes in Computer Science. pp. 267–288, 1998.

▶ O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proc. Thirty-seventh Annual ACM Symposium on Theory of Computing, pp. 84–93, 2005.

▶ C. Gentry, "A Fully Homomorphic Encryption Scheme," Thesis, Stanford University, 2009.

Lattice-based cryptography

- **1996**: Miklós Ajtai introduces the first asymmetric lattice-based scheme and shows that the average case of certain lattice-related problems is as difficult to solve as the worst case.
- **1998**: Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman introduce the lattice-based public-key scheme known as NTRU.
- **2005**: Oded Regev introduces the first lattice-based cryptosystem compliant with the average-to-worst case reduction.
- Regev has shown that the problem of **learning with errors** (LWE) is as difficult to solve as several lattice problems in their worst case.
- **2009**: Craig Gentry introduces the first fully homomorphic lattice-based cryptosystem.

- M. Ajtai, "Generating Hard Instances of Lattice Problems," Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.
- J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, vol. 1423 of Lecture Notes in Computer Science. pp. 267–288, 1998.
- O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proc. Thirty-seventh Annual ACM Symposium on Theory of Computing, pp. 84–93, 2005.
- C. Gentry, "A Fully Homomorphic Encryption Scheme," Thesis, Stanford University, 2009.

Lattice-based cryptography

- **1996**: Miklós Ajtai introduces the first asymmetric lattice-based scheme and shows that the average case of certain lattice-related problems is as difficult to solve as the worst case.
- **1998**: Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman introduce the lattice-based public-key scheme known as NTRU.
- **2005**: Oded Regev introduces the first lattice-based cryptosystem compliant with the average-to-worst case reduction.
- Regev has shown that the problem of **learning with errors** (LWE) is as difficult to solve as several lattice problems in their worst case.
- **2009**: Craig Gentry introduces the first fully homomorphic lattice-based cryptosystem.

- M. Ajtai, "Generating Hard Instances of Lattice Problems," Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.
- J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, vol. 1423 of Lecture Notes in Computer Science. pp. 267–288, 1998.
- O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proc. Thirty-seventh Annual ACM Symposium on Theory of Computing, pp. 84–93, 2005.
- C. Gentry, "A Fully Homomorphic Encryption Scheme," Thesis, Stanford University, 2009.

Lattice-based cryptography

- **1996**: Miklós Ajtai introduces the first asymmetric lattice-based scheme and shows that the average case of certain lattice-related problems is as difficult to solve as the worst case.
- **1998**: Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman introduce the lattice-based public-key scheme known as NTRU.
- **2005**: Oded Regev introduces the first lattice-based cryptosystem compliant with the average-to-worst case reduction.
- Regev has shown that the problem of **learning with errors** (LWE) is as difficult to solve as several lattice problems in their worst case.
- **2009**: Craig Gentry introduces the first fully homomorphic lattice-based cryptosystem.

- M. Ajtai, "Generating Hard Instances of Lattice Problems," Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.
- J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, vol. 1423 of Lecture Notes in Computer Science. pp. 267–288, 1998.
- O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proc. Thirty-seventh Annual ACM Symposium on Theory of Computing, pp. 84–93, 2005.
- C. Gentry, "A Fully Homomorphic Encryption Scheme," Thesis, Stanford University, 2009.

Lattice-based cryptography (2)

- A lattice $\mathbf{L} \subset \mathbb{R}^n$ is the set of all integer combinations of vectors of a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^n$ such that $\mathbf{L} = \{\sum a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$.
- The most important computational problem defined on lattices is the Shortest Vector Problem (SVP).
- It consists in finding the non-zero vector with the minimum (Euclidean) length inside a lattice.
- This problem is considered difficult to solve, even with the availability of a quantum computer.

Lattice-based cryptography (2)

- A lattice $\mathbf{L} \subset \mathbb{R}^n$ is the set of all integer combinations of vectors of a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^n$ such that $\mathbf{L} = \{\sum a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$.
- The most important computational problem defined on lattices is the Shortest Vector Problem (SVP).
- It consists in finding the non-zero vector with the minimum (Euclidean) length inside a lattice.
- This problem is considered difficult to solve, even with the availability of a quantum computer.

Lattice-based cryptography (2)

- A lattice $\mathbf{L} \subset \mathbb{R}^n$ is the set of all integer combinations of vectors of a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^n$ such that $\mathbf{L} = \{\sum a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$.
- The most important computational problem defined on lattices is the Shortest Vector Problem (SVP).
- It consists in finding the non-zero vector with the minimum (Euclidean) length inside a lattice.
- This problem is considered difficult to solve, even with the availability of a quantum computer.

Lattice-based cryptography (2)

- A lattice $\mathbf{L} \subset \mathbb{R}^n$ is the set of all integer combinations of vectors of a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\} \in \mathbb{R}^n$ such that $\mathbf{L} = \{\sum a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$.
- The most important computational problem defined on lattices is the Shortest Vector Problem (SVP).
- It consists in finding the non-zero vector with the minimum (Euclidean) length inside a lattice.
- This problem is considered difficult to solve, even with the availability of a quantum computer.

Multivariate cryptography

- Solving multivariate polynomial equation systems is a computationally intensive problem.
- **1988**: Matsumoto and Imai presented the C* scheme, which was broken in 1995.
- **1996**: Jacques Patarin introduced the Hidden Field Equations (HFE) scheme.
- The original scheme is now considered weak, but some of its variants are considered secure.
- These schemes are particularly efficient for the construction of digital signature primitives.

▶ T. Matsumoto, H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Advances in Cryptology – EUROCRYPT '88, vol. 330 of Lecture Notes in Computer Science, 1988.

▶ J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology – EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 1996.

Multivariate cryptography

- Solving multivariate polynomial equation systems is a computationally intensive problem.
- **1988**: Matsumoto and Imai presented the C* scheme, which was broken in 1995.
- **1996**: Jacques Patarin introduced the Hidden Field Equations (HFE) scheme.
- The original scheme is now considered weak, but some of its variants are considered secure.
- These schemes are particularly efficient for the construction of digital signature primitives.

► T. Matsumoto, H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Advances in Cryptology – EUROCRYPT '88, vol. 330 of Lecture Notes in Computer Science, 1988.

► J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology – EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 1996.

Multivariate cryptography

- Solving multivariate polynomial equation systems is a computationally intensive problem.
- **1988**: Matsumoto and Imai presented the C* scheme, which was broken in 1995.
- **1996**: Jacques Patarin introduced the Hidden Field Equations (HFE) scheme.
- The original scheme is now considered weak, but some of its variants are considered secure.
- These schemes are particularly efficient for the construction of digital signature primitives.

- T. Matsumoto, H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Advances in Cryptology – EUROCRYPT '88, vol. 330 of Lecture Notes in Computer Science, 1988.
- J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology – EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 1996.

Multivariate cryptography

- Solving multivariate polynomial equation systems is a computationally intensive problem.
- **1988**: Matsumoto and Imai presented the C* scheme, which was broken in 1995.
- **1996**: Jacques Patarin introduced the Hidden Field Equations (HFE) scheme.
- The original scheme is now considered weak, but some of its variants are considered secure.
- These schemes are particularly efficient for the construction of digital signature primitives.

- T. Matsumoto, H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Advances in Cryptology – EUROCRYPT '88, vol. 330 of Lecture Notes in Computer Science, 1988.
- J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology – EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 1996.

Multivariate cryptography

- Solving multivariate polynomial equation systems is a computationally intensive problem.
- **1988**: Matsumoto and Imai presented the C* scheme, which was broken in 1995.
- **1996**: Jacques Patarin introduced the Hidden Field Equations (HFE) scheme.
- The original scheme is now considered weak, but some of its variants are considered secure.
- These schemes are particularly efficient for the construction of digital signature primitives.

- T. Matsumoto, H. Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Advances in Cryptology – EUROCRYPT '88, vol. 330 of Lecture Notes in Computer Science, 1988.
- J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology – EUROCRYPT '96, vol. 1070 of Lecture Notes in Computer Science, 1996.

Isogeny-based cryptography

- Derives from Elliptic Curve Cryptography (ECC), started in the **1980s** by Miller and Koblitz.
- Schoof's algorithm made it possible to easily find elliptic curves of large prime order, enabling the diffusion of ECC.
- A surjective group morphism, not necessarily invertible, between two elliptic curves is called an isogeny.
- Isogeny-based cryptography, initiated in mid **2000s**, resists quantum computers, differently from ECC.
- Supersingular isogeny key exchange introduced in **2011**.

- V. S. Miller, "Use of elliptic curves in cryptography," In Advances in cryptology - CRYPTO 85, vol. 2018 of Lecture notes in computer sciences, pp. 417–426, 1986.
- N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
- René Schoof, "Counting points on elliptic curves over finite fields," Journal de Théorie des Nombres de Bordeaux, vol. 7, pp. 219–254, 1995.
- D. Jao, L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," PQCrypto 2011, vol. 7071 of Lecture Notes in Computer Science, pp 19–34, 2011.

Isogeny-based cryptography

- Derives from Elliptic Curve Cryptography (ECC), started in the **1980s** by Miller and Koblitz.
- Schoof's algorithm made it possible to easily find elliptic curves of large prime order, enabling the diffusion of ECC.
- A surjective group morphism, not necessarily invertible, between two elliptic curves is called an isogeny.
- Isogeny-based cryptography, initiated in mid **2000s**, resists quantum computers, differently from ECC.
- Supersingular isogeny key exchange introduced in **2011**.

- V. S. Miller, "Use of elliptic curves in cryptography," In Advances in cryptology - CRYPTO 85, vol. 2018 of Lecture notes in computer sciences, pp. 417–426, 1986.
- N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
- René Schoof, "Counting points on elliptic curves over finite fields," Journal de Théorie des Nombres de Bordeaux, vol. 7, pp. 219–254, 1995.
- D. Jao, L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," PQCrypto 2011, vol. 7071 of Lecture Notes in Computer Science, pp 19–34, 2011.

Isogeny-based cryptography

- Derives from Elliptic Curve Cryptography (ECC), started in the **1980s** by Miller and Koblitz.
- Schoof's algorithm made it possible to easily find elliptic curves of large prime order, enabling the diffusion of ECC.
- A surjective group morphism, not necessarily invertible, between two elliptic curves is called an isogeny.
- Isogeny-based cryptography, initiated in mid **2000s**, resists quantum computers, differently from ECC.
- Supersingular isogeny key exchange introduced in **2011**.

- V. S. Miller, "Use of elliptic curves in cryptography," In Advances in cryptology - CRYPTO 85, vol. 2018 of Lecture notes in computer sciences, pp. 417–426, 1986.
- N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
- René Schoof, "Counting points on elliptic curves over finite fields," Journal de Théorie des Nombres de Bordeaux, vol. 7, pp. 219–254, 1995.
- D. Jao, L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," PQCrypto 2011, vol. 7071 of Lecture Notes in Computer Science, pp 19–34, 2011.

Isogeny-based cryptography

- Derives from Elliptic Curve Cryptography (ECC), started in the **1980s** by Miller and Koblitz.
- Schoof's algorithm made it possible to easily find elliptic curves of large prime order, enabling the diffusion of ECC.
- A surjective group morphism, not necessarily invertible, between two elliptic curves is called an isogeny.
- Isogeny-based cryptography, initiated in mid **2000s**, resists quantum computers, differently from ECC.
- Supersingular isogeny key exchange introduced in **2011**.

- V. S. Miller, "Use of elliptic curves in cryptography," In Advances in cryptology - CRYPTO 85, vol. 2018 of Lecture notes in computer sciences, pp. 417–426, 1986.
- N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
- René Schoof, "Counting points on elliptic curves over finite fields," Journal de Théorie des Nombres de Bordeaux, vol. 7, pp. 219–254, 1995.
- D. Jao, L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," PQCrypto 2011, vol. 7071 of Lecture Notes in Computer Science, pp 19–34, 2011.

Isogeny-based cryptography

- Derives from Elliptic Curve Cryptography (ECC), started in the **1980s** by Miller and Koblitz.
- Schoof's algorithm made it possible to easily find elliptic curves of large prime order, enabling the diffusion of ECC.
- A surjective group morphism, not necessarily invertible, between two elliptic curves is called an isogeny.
- Isogeny-based cryptography, initiated in mid **2000s**, resists quantum computers, differently from ECC.
- Supersingular isogeny key exchange introduced in **2011**.

- V. S. Miller, "Use of elliptic curves in cryptography," In Advances in cryptology - CRYPTO 85, vol. 2018 of Lecture notes in computer sciences, pp. 417–426, 1986.
- N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203–209, 1987.
- René Schoof, "Counting points on elliptic curves over finite fields," Journal de Théorie des Nombres de Bordeaux, vol. 7, pp. 219–254, 1995.
- D. Jao, L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," PQCrypto 2011, vol. 7071 of Lecture Notes in Computer Science, pp 19–34, 2011.

Code-based cryptography

- Introduced by Robert McEliece in **1978** for asymmetric encryption
- Security reduced to the problem of decoding a random(-looking) linear code
- Resisted 40+ years of cryptanalysis
- No considerable quantum speedup of attacks
- In the 2nd round of NIST's post-quantum crypto competition:
  - **8** out of 17 KEM/PKC proposals are code-based
  - **0** out of 9 digital signature proposals are code-based

- R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.
- 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.
- National Institute of Standards and Technology. (2016, Dec.) Post-quantum crypto project. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Code-based cryptography

- Introduced by Robert McEliece in **1978** for asymmetric encryption
- Security reduced to the problem of decoding a random(-looking) linear code
- Resisted 40+ years of cryptanalysis
- No considerable quantum speedup of attacks
- In the 2nd round of NIST's post-quantum crypto competition:
  - **8** out of 17 KEM/PKC proposals are code-based
  - **0** out of 9 digital signature proposals are code-based

▶ R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.

▶ 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.

▶ National Institute of Standards and Technology. (2016, Dec.) Post-quantum crypto project. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Code-based cryptography

- Introduced by Robert McEliece in **1978** for asymmetric encryption
- Security reduced to the problem of decoding a random(-looking) linear code
- Resisted 40+ years of cryptanalysis
- No considerable quantum speedup of attacks
- In the 2nd round of NIST's post-quantum crypto competition:
  - **8** out of 17 KEM/PKC proposals are code-based
  - **0** out of 9 digital signature proposals are code-based

- R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.
- 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.
- National Institute of Standards and Technology. (2016, Dec.) Post-quantum crypto project. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Code-based cryptography

- Introduced by Robert McEliece in **1978** for asymmetric encryption
- Security reduced to the problem of decoding a random(-looking) linear code
- Resisted 40+ years of cryptanalysis
- No considerable quantum speedup of attacks
- In the 2nd round of NIST's post-quantum crypto competition:
  - **8** out of 17 KEM/PKC proposals are code-based
  - **0** out of 9 digital signature proposals are code-based

- R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.
- 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.
- National Institute of Standards and Technology. (2016, Dec.) Post-quantum crypto project. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Code-based cryptography

- Introduced by Robert McEliece in **1978** for asymmetric encryption
- Security reduced to the problem of decoding a random(-looking) linear code
- Resisted 40+ years of cryptanalysis
- No considerable quantum speedup of attacks
- In the 2nd round of NIST's post-quantum crypto competition:
  - **8** out of 17 KEM/PKC proposals are code-based
  - **0** out of 9 digital signature proposals are code-based

- R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory." *DSN Progress Report*, pp. 114–116, 1978.
- 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.
- National Institute of Standards and Technology. (2016, Dec.) Post-quantum crypto project. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Trapdoors from decoding

First ingredient for a trapdoor

The problem of decoding a random linear code cannot be solved in polynomial time.

Second ingredient for a trapdoor

Many families of non-random (Goppa, GRS, convolutional) and quasi-random (LDPC, MDPC) linear codes admit polynomial-time decoding algorithms.

- 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.
- A. May, A. Meurer, E. Thomae, "Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$," Advances in Cryptology – ASIACRYPT 2011, Dec. 2011.

Trapdoors from decoding

First ingredient for a trapdoor

The problem of decoding a random linear code cannot be solved in polynomial time.

Second ingredient for a trapdoor

Many families of non-random (Goppa, GRS, convolutional) and quasi-random (LDPC, MDPC) linear codes admit polynomial-time decoding algorithms.

- 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.
- A. May, A. Meurer, E. Thomae, "Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$," Advances in Cryptology – ASIACRYPT 2011, Dec. 2011.

McEliece cryptosystem

- Proposed by Robert McEliece in **1978**.
- Irreducible Goppa codes were used in the original proposal.
- Secret irreducible Goppa code:
  - based on an 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.

Rationale

1. The probability that a random polynomial is irreducible is $\approx 1/t$, and a fast algorithm exists for testing irreducibility.
2. The number of irreducible polynomials of degree t over $GF(n)$ is $\approx n^t/t$.

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

McEliece cryptosystem

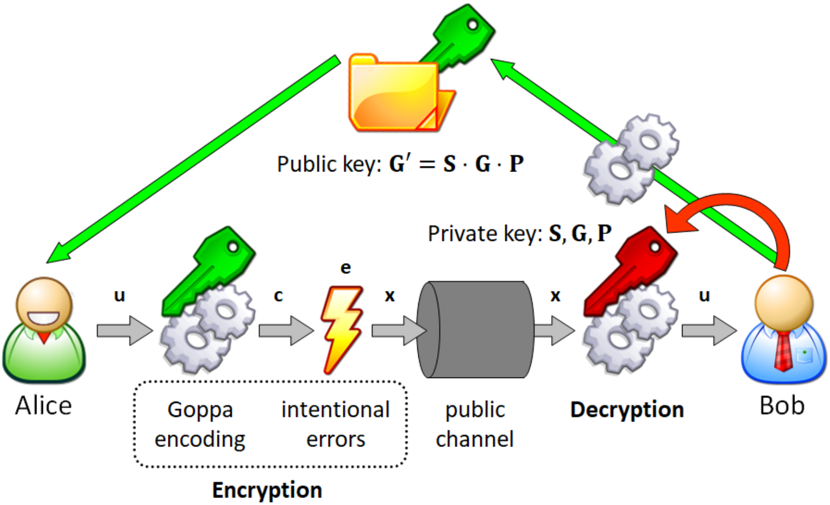
- Proposed by Robert McEliece in **1978**.
- Irreducible Goppa codes were used in the original proposal.
- Secret irreducible Goppa code:
  - based on an irreducible polynomial of degree t over $GF(2^m)$,
  - length (maximum): $n = 2^m$,
  - dimension: $k \geq n - t \cdot m$,
  - correction capability: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

Rationale

1. The probability that a random polynomial is irreducible is $\approx 1/t$, and a fast algorithm exists for testing irreducibility.
2. The number of irreducible polynomials of degree t over $GF(n)$ is $\approx n^t/t$.

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

McEliece cryptosystem (2)



McEliece cryptosystem - key generation

Private key

- $k \times n$ generator matrix $\mathbf{G}$ of a secret Goppa code,
- random dense $k \times k$ non-singular "scrambling" matrix $\mathbf{S}$,
- random $n \times n$ permutation matrix $\mathbf{P}$.

Public key

$$\mathbf{G}' = \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}$$

- The public code is permutation equivalent to the secret code.
- Is the secret Goppa code matrix $\mathbf{G}$ well disguised enough to make $\mathbf{G}'$ look like the generator matrix of a random linear code?

McEliece cryptosystem - key generation

Private key

- $k \times n$ generator matrix $\mathbf{G}$ of a secret Goppa code,
- random dense $k \times k$ non-singular "scrambling" matrix $\mathbf{S}$,
- random $n \times n$ permutation matrix $\mathbf{P}$.

Public key

$$\mathbf{G}' = \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}$$

- The public code is permutation equivalent to the secret code.
- Is the secret Goppa code matrix $\mathbf{G}$ well disguised enough to make $\mathbf{G}'$ look like the generator matrix of a random linear code?

McEliece cryptosystem - key generation

Private key

- $k \times n$ generator matrix $\mathbf{G}$ of a secret Goppa code,
- random dense $k \times k$ non-singular "scrambling" matrix $\mathbf{S}$,
- random $n \times n$ permutation matrix $\mathbf{P}$.

Public key

$$\mathbf{G}' = \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}$$

- The public code is permutation equivalent to the secret code.
- Is the secret Goppa code matrix $\mathbf{G}$ well disguised enough to make $\mathbf{G}'$ look like the generator matrix of a random linear code?

McEliece cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{G}'$.
2. She generates a random error vector of length n and weight t.
3. She encrypts any k-bit block $\mathbf{u}$ as

$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e} = \mathbf{c} + \mathbf{e}$$

Alert

This only provides semantic security!

McEliece cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{G}'$.
2. She generates a random error vector of length n and weight t.
3. She encrypts any k-bit block $\mathbf{u}$ as

$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e} = \mathbf{c} + \mathbf{e}$$

Alert

This only provides semantic security!

McEliece cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{G}'$.
2. She generates a random error vector of length n and weight t.
3. She encrypts any k-bit block $\mathbf{u}$ as

$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e} = \mathbf{c} + \mathbf{e}$$

Alert

This only provides semantic security!

McEliece cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{G}'$.
2. She generates a random error vector of length n and weight t.
3. She encrypts any k-bit block $\mathbf{u}$ as

$$\mathbf{x} = \mathbf{u} \cdot \mathbf{G}' + \mathbf{e} = \mathbf{c} + \mathbf{e}$$

Alert

This only provides semantic security!

McEliece cryptosystem - decryption

1. Bob computes

$$
\begin{aligned}
\mathbf{x}' = \mathbf{x} \cdot \mathbf{P}^{-1} = \\
= (\mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P} + \mathbf{e}) \cdot \mathbf{P}^{-1} = \\
= \mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} + \mathbf{e} \cdot \mathbf{P}^{-1}
\end{aligned}
$$

2. Bob decodes the secret code and obtains

$$\mathbf{u}' = \mathbf{u} \cdot \mathbf{S}$$

3. Bob computes $\mathbf{u} = \mathbf{u}' \cdot \mathbf{S}^{-1}$.

McEliece cryptosystem - decryption

1. Bob computes

$$\begin{aligned}\mathbf{x}' = \mathbf{x} \cdot \mathbf{P}^{-1} = \\ = (\mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P} + \mathbf{e}) \cdot \mathbf{P}^{-1} = \\ = \mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} + \mathbf{e} \cdot \mathbf{P}^{-1}\end{aligned}$$

2. Bob decodes the secret code and obtains

$$\mathbf{u}' = \mathbf{u} \cdot \mathbf{S}$$

3. Bob computes $\mathbf{u} = \mathbf{u}' \cdot \mathbf{S}^{-1}$.

McEliece cryptosystem - decryption

1. Bob computes

$$\begin{aligned}\mathbf{x}' &= \mathbf{x} \cdot \mathbf{P}^{-1} = \\ &= (\mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P} + \mathbf{e}) \cdot \mathbf{P}^{-1} = \\ &= \mathbf{u} \cdot \mathbf{S} \cdot \mathbf{G} + \mathbf{e} \cdot \mathbf{P}^{-1}\end{aligned}$$

2. Bob decodes the secret code and obtains

$$\mathbf{u}' = \mathbf{u} \cdot \mathbf{S}$$

3. Bob computes $\mathbf{u} = \mathbf{u}' \cdot \mathbf{S}^{-1}$.

Niederreiter cryptosystem - key generation

Private key

- $r \times n$ parity-check matrix $\mathbf{H}$ of a secret code,
- random dense $r \times r$ non-singular “scrambling” matrix $\mathbf{S}$.

Public key

$$\mathbf{H}' = \mathbf{S} \cdot \mathbf{H}$$

Niederreiter cryptosystem - key generation

Private key

- $r \times n$ parity-check matrix $\mathbf{H}$ of a secret code,
- random dense $r \times r$ non-singular "scrambling" matrix $\mathbf{S}$.

Public key

$$\mathbf{H}' = \mathbf{S} \cdot \mathbf{H}$$

Niederreiter cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{H}'$.
2. She maps each block of the secret message into an error pattern $\mathbf{e}$ with length n and weight t.
3. She encrypts $\mathbf{e}$ as

$$\mathbf{x} = \mathbf{H}' \cdot \mathbf{e}^{\mathrm{T}} = \mathbf{S} \cdot \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$

Alert

We still only have semantic security!

Niederreiter cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{H}'$.
2. She maps each block of the secret message into an error pattern $\mathbf{e}$ with length n and weight t.
3. She encrypts $\mathbf{e}$ as

$$\mathbf{x} = \mathbf{H}' \cdot \mathbf{e}^{\mathrm{T}} = \mathbf{S} \cdot \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$

Alert

We still only have semantic security!

Niederreiter cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{H}'$.
2. She maps each block of the secret message into an error pattern $\mathbf{e}$ with length n and weight t.
3. She encrypts $\mathbf{e}$ as

$$\mathbf{x} = \mathbf{H}' \cdot \mathbf{e}^{\mathrm{T}} = \mathbf{S} \cdot \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$

Alert

We still only have semantic security!

Niederreiter cryptosystem - encryption

1. Alice gets Bob's public key $\mathbf{H}'$.
2. She maps each block of the secret message into an error pattern $\mathbf{e}$ with length n and weight t.
3. She encrypts $\mathbf{e}$ as

$$\mathbf{x} = \mathbf{H}' \cdot \mathbf{e}^{\mathrm{T}} = \mathbf{S} \cdot \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$

Alert

We still only have semantic security!

Niederreiter cryptosystem - decryption

1. Bob computes
$$\mathbf{x}' = \mathbf{S}^{-1} \cdot \mathbf{x} = \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$
2. Bob performs syndrome decoding of the secret code and obtains $\mathbf{e}$ from $\mathbf{x}'$.
3. He demaps $\mathbf{e}$ into the corresponding secret message block.

Niederreiter cryptosystem - decryption

1. Bob computes
$$\mathbf{x}' = \mathbf{S}^{-1} \cdot \mathbf{x} = \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$
2. Bob performs syndrome decoding of the secret code and obtains $\mathbf{e}$ from $\mathbf{x}'$.
3. He demaps $\mathbf{e}$ into the corresponding secret message block.

Niederreiter cryptosystem - decryption

1. Bob computes
$$\mathbf{x}' = \mathbf{S}^{-1} \cdot \mathbf{x} = \mathbf{H} \cdot \mathbf{e}^{\mathrm{T}}$$
2. Bob performs syndrome decoding of the secret code and obtains $\mathbf{e}$ from $\mathbf{x}'$.
3. He demaps $\mathbf{e}$ into the corresponding secret message block.

Attacks against McEliece/Niederreiter

General attacks

General attacks against McEliece/Niederreiter are those aimed at decoding the random-like public code.

Code-specific attacks

Specific attacks are those tailored to each code family (Goppa, GRS, convolutional, LDPC, MDPC, ...).

Attacks against McEliece/Niederreiter

Decryption attacks

Aimed at decrypting one or more ciphertexts without knowing the private key.

Key recovery attacks

Aimed at recovering the private key from the public key.

Decoding attacks

- The most dangerous decoding attacks (DAs) exploit information set decoding (ISD).
- The ISD principle was introduced by Prange in 1962.
- Improved variants were introduced by Lee-Brickell and Leon-Stern in 1988/89.
- A great research effort has been devoted to improving these techniques in recent years.

- E. Prange, "The use of information sets in decoding cyclic codes," Information Theory," IRE Transactions on, vol. 8, no. 5, pp. 5–9, 1962.
- P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.
- J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes," IEEE Trans. Inform. Theory, vol. 34, no. 5, pp. 1354–1359, 1988.
- J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications, vol. 388 of Springer LNCS, pp. 106-–113, 1989.

Decoding attacks

- The most dangerous DAs exploit ISD.
- The ISD principle was introduced by Prange in 1962.
- Improved variants were introduced by Lee-Brickell and Leon-Stern in 1988/89.
- A great research effort has been devoted to improving these techniques in recent years.

- E. Prange, "The use of information sets in decoding cyclic codes," Information Theory," IRE Transactions on, vol. 8, no. 5, pp. 5–9, 1962.
- P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.
- J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes," IEEE Trans. Inform. Theory, vol. 34, no. 5, pp. 1354–1359, 1988.
- J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications, vol. 388 of Springer LNCS, pp. 106-–113, 1989.

Decoding attacks

- The most dangerous DAs exploit ISD.
- The ISD principle was introduced by Prange in 1962.
- Improved variants were introduced by Lee-Brickell and Leon-Stern in 1988/89.
- A great research effort has been devoted to improving these techniques in recent years.

- E. Prange, "The use of information sets in decoding cyclic codes," Information Theory," IRE Transactions on, vol. 8, no. 5, pp. 5–9, 1962.
- P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.
- J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes," IEEE Trans. Inform. Theory, vol. 34, no. 5, pp. 1354–1359, 1988.
- J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications, vol. 388 of Springer LNCS, pp. 106-–113, 1989.

Decoding attacks

- The most dangerous DAs exploit ISD.
- The ISD principle was introduced by Prange in 1962.
- Improved variants were introduced by Lee-Brickell and Leon-Stern in 1988/89.
- A great research effort has been devoted to improving these techniques in recent years.

- E. Prange, "The use of information sets in decoding cyclic codes," Information Theory," IRE Transactions on, vol. 8, no. 5, pp. 5–9, 1962.
- P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.
- J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes," IEEE Trans. Inform. Theory, vol. 34, no. 5, pp. 1354–1359, 1988.
- J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications, vol. 388 of Springer LNCS, pp. 106-–113, 1989.

Classical information set decoding

Rationale

For some ciphertext, random errors may not affect a (randomly chosen) information set of the code.

$$\mathbf{x}_{\mathcal{K}} = \mathbf{u} \cdot \mathbf{G}'_{\mathcal{K}} + \mathbf{e}_{\mathcal{K}}$$

- If $\mathcal{K}$ represents an information set, then $\mathbf{G}'_{\mathcal{K}}$ is invertible.
- if $\mathbf{e}_{\mathcal{K}} = \mathbf{0}$, then

$$\mathbf{u} = \mathbf{x}_{\mathcal{K}} \cdot \mathbf{G}'^{-1}_{\mathcal{K}}$$

- If there are a few errors in the information set, Eve can try to guess $\mathbf{e}_{\mathcal{K}}$ at random.

▶ P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.

Classical information set decoding

Rationale

For some ciphertext, random errors may not affect a (randomly chosen) information set of the code.

$$\mathbf{x}_{\mathcal{K}} = \mathbf{u} \cdot \mathbf{G}'_{\mathcal{K}} + \mathbf{e}_{\mathcal{K}}$$

- If $\mathcal{K}$ represents an information set, then $\mathbf{G}'_{\mathcal{K}}$ is invertible.
- if $\mathbf{e}_{\mathcal{K}} = \mathbf{0}$, then

$$\mathbf{u} = \mathbf{x}_{\mathcal{K}} \cdot \mathbf{G}'^{-1}_{\mathcal{K}}$$

- If there are a few errors in the information set, Eve can try to guess $\mathbf{e}_{\mathcal{K}}$ at random.

▶ P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.

Classical information set decoding

Rationale

For some ciphertext, random errors may not affect a (randomly chosen) information set of the code.

$$\mathbf{x}_{\mathcal{K}} = \mathbf{u} \cdot \mathbf{G}'_{\mathcal{K}} + \mathbf{e}_{\mathcal{K}}$$

- If $\mathcal{K}$ represents an information set, then $\mathbf{G}'_{\mathcal{K}}$ is invertible.
- if $\mathbf{e}_{\mathcal{K}} = \mathbf{0}$, then
$$\mathbf{u} = \mathbf{x}_{\mathcal{K}} \cdot \mathbf{G}'^{-1}_{\mathcal{K}}$$
- If there are a few errors in the information set, Eve can try to guess $\mathbf{e}_{\mathcal{K}}$ at random.

► P. Lee, E. Brickell, "An observation on the security of McEliece's public-key cryptosystem," Advances in Cryptology - EUROCRYPT 88, pp 275–280, 1988.

Modern information set decoding

- The general decoding problem can be reduced to that of searching low weight codewords.
- Modern approaches exploit the birthday paradox to search for low weight codewords.
- Lower bounds on complexity have been found by Niebuhr et al.

- C. Peters, "Information-set decoding for linear codes over F_q," Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 81–94, 2010.
- D. J. Bernstein, T. Lange, C. Peters, "Smaller decoding exponents: ball-collision decoding," CRYPTO 2011, vol. 6841 of Springer LNCS, pp 743–760, 2011.
- A. May, A. Meurer, E. Thomae, "Decoding random linear codes in $O(2^{0.054n})$," ASIACRYPT 2011, vol. 7073 of Springer LNCS, pp. 107–124, 2011.
- A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding," Advances in Cryptology - EUROCRYPT 2012, vol. 7237 of Springer LNCS, pp. 520–536, 2012.
- R. Niebuhr, E. Persichetti, P.-L. Cayrel, S. Bulygin, J. Buchmann, "On lower bounds for information set decoding over F_q and on the effect of partial knowledge," Int. J. Inf. Coding Theory, vol. 4, no. 1, pp. 47–78, 2017.

Modern information set decoding

- The general decoding problem can be reduced to that of searching low weight codewords.
- Modern approaches exploit the birthday paradox to search for low weight codewords.
- Lower bounds on complexity have been found by Niebuhr et al.

- C. Peters, "Information-set decoding for linear codes over F_q," Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 81–94, 2010.
- D. J. Bernstein, T. Lange, C. Peters, "Smaller decoding exponents: ball-collision decoding," CRYPTO 2011, vol. 6841 of Springer LNCS, pp 743–760, 2011.
- A. May, A. Meurer, E. Thomae, "Decoding random linear codes in $O(2^{0.054n})$," ASIACRYPT 2011, vol. 7073 of Springer LNCS, pp. 107–124, 2011.
- A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding," Advances in Cryptology - EUROCRYPT 2012, vol. 7237 of Springer LNCS, pp. 520–536, 2012.
- R. Niebuhr, E. Persichetti, P.-L. Cayrel, S. Bulygin, J. Buchmann, "On lower bounds for information set decoding over F_q and on the effect of partial knowledge," Int. J. Inf. Coding Theory, vol. 4, no. 1, pp. 47–78, 2017.

Modern information set decoding

- The general decoding problem can be reduced to that of searching low weight codewords.
- Modern approaches exploit the birthday paradox to search for low weight codewords.
- Lower bounds on complexity have been found by Niebuhr et al.

- C. Peters, "Information-set decoding for linear codes over F_q," Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 81–94, 2010.
- D. J. Bernstein, T. Lange, C. Peters, "Smaller decoding exponents: ball-collision decoding," CRYPTO 2011, vol. 6841 of Springer LNCS, pp 743–760, 2011.
- A. May, A. Meurer, E. Thomae, "Decoding random linear codes in $O(2^{0.054n})$," ASIACRYPT 2011, vol. 7073 of Springer LNCS, pp. 107–124, 2011.
- A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding," Advances in Cryptology - EUROCRYPT 2012, vol. 7237 of Springer LNCS, pp. 520–536, 2012.
- R. Niebuhr, E. Persichetti, P.-L. Cayrel, S. Bulygin, J. Buchmann, "On lower bounds for information set decoding over F_q and on the effect of partial knowledge," Int. J. Inf. Coding Theory, vol. 4, no. 1, pp. 47–78, 2017.

Decoding attacks - Goppa codes with rate $\approx 1/2$

n	k	m	t	Lee-Brickell	Stern	Peters	Becker et al.
512	260	9	28	45.39	41.57	40.44	33.10
1024	524	10	50	70.56	63.54	62.34	53.05
2048	1036	11	92	114.97	104.83	103.61	94.10
4096	2056	12	170	195.79	182.46	180.63	171.36
8192	4110	13	314	345.37	328.31	325.94	316.74
16384	8208	14	584	623.24	601.40	596.69	590.36

Work factor ($\log_2$) of decoding attacks against McEliece/Niederreiter cryptosystems using Goppa codes with rate about $1/2$.

Decoding attacks - Goppa codes with rate $\approx 2/3$

n	k	m	t	Lee-Brickell	Stern	Peters	Becker et al.
512	350	9	18	46.94	41.24	39.66	33.13
1024	684	10	34	73.11	64.37	62.80	54.16
2048	1366	11	62	119.79	107.88	106.29	97.47
4096	2752	12	112	204.65	189.46	187.56	178.37
8192	5462	13	210	362.10	342.84	339.86	331.63
16384	10924	14	390	654.48	630.37	623.88	619.72

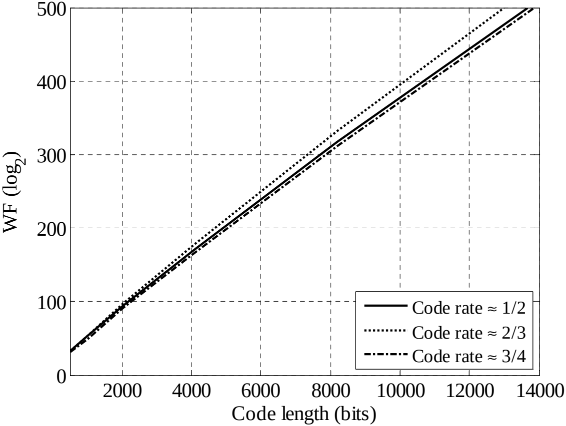
Work factor ($\log_2$) of decoding attacks against McEliece/Niederreiter cryptosystems using Goppa codes with rate about 2/3.

Decoding attacks - Goppa codes with rate $\approx 3/4$

n	k	m	t	Lee-Brickell	Stern	Peters	Becker et al.
512	386	9	14	45.40	39.18	37.50	31.30
1024	784	10	24	69.15	59.61	57.92	49.58
2048	1542	11	46	113.93	101.30	99.62	91.03
4096	3088	12	84	193.91	178.04	176.05	166.91
8192	6164	13	156	342.25	322.02	318.63	311.00
16384	12296	14	292	619.00	593.92	586.76	583.47

Work factor ($\log_2$) of decoding attacks against McEliece/Niederreiter cryptosystems using Goppa codes with rate about 3/4.

Complexity of BJMM against Goppa codes



- Y. Hamdaoui, N. Sendrier, "A non asymptotic analysis of information set decoding," IACR Cryptology ePrint Archive, Report 2013/162.

Pre-quantum VS post-quantum

- Grover's algorithm is a quantum algorithm introduced for performing efficient database searches.
- For searching one entry of an unsorted list of n entries,
  - Grover's algorithm requires $\pi/4\sqrt{n}$ steps using $\log_2(n)$ qubits.
  - The best classical algorithm requires $n/2$ steps on average.
- Grover' algorithm reduces the number of iterations but does not reduce the cost per iteration.
- However, it somehow impacts the work factor of ISD.

- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.
- S.H.S. de Vries, "Achieving 128-bit Security against Quantum Attacks in OpenVPN," Master Thesis, University of Twente, 2016.

Pre-quantum VS post-quantum

- Grover's algorithm is a quantum algorithm introduced for performing efficient database searches.
- For searching one entry of an unsorted list of n entries,
  - Grover's algorithm requires $\pi/4\sqrt{n}$ steps using $\log_2(n)$ qubits.
  - The best classical algorithm requires $n/2$ steps on average.
- Grover' algorithm reduces the number of iterations but does not reduce the cost per iteration.
- However, it somehow impacts the work factor of ISD.

▶ D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

▶ S.H.S. de Vries, "Achieving 128-bit Security against Quantum Attacks in OpenVPN," Master Thesis, University of Twente, 2016.

Pre-quantum VS post-quantum

- Grover's algorithm is a quantum algorithm introduced for performing efficient database searches.
- For searching one entry of an unsorted list of n entries,
  - Grover's algorithm requires $\pi/4\sqrt{n}$ steps using $\log_2(n)$ qubits.
  - The best classical algorithm requires $n/2$ steps on average.
- Grover' algorithm reduces the number of iterations but does not reduce the cost per iteration.
- However, it somehow impacts the work factor of ISD.

- D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.
- S.H.S. de Vries, "Achieving 128-bit Security against Quantum Attacks in OpenVPN," Master Thesis, University of Twente, 2016.

Pre-quantum VS post-quantum

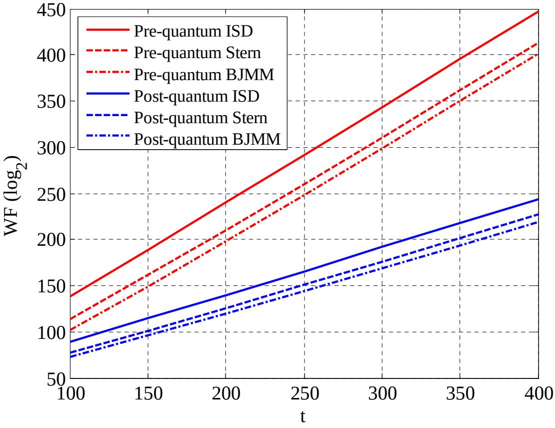
- Grover's algorithm is a quantum algorithm introduced for performing efficient database searches.
- For searching one entry of an unsorted list of n entries,
  - Grover's algorithm requires $\pi/4\sqrt{n}$ steps using $\log_2(n)$ qubits.
  - The best classical algorithm requires $n/2$ steps on average.
- Grover' algorithm reduces the number of iterations but does not reduce the cost per iteration.
- However, it somehow impacts the work factor of ISD.

▶ D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, vol. 6061 of Springer LNCS, pp. 73–80, 2010.

▶ S.H.S. de Vries, "Achieving 128-bit Security against Quantum Attacks in OpenVPN," Master Thesis, University of Twente, 2016.

Pre-quantum VS post-quantum

Pre- and post-quantum WF of some ISD algorithms versus t, for codes with $n = 12000$, $k = 6000$.



CCA2 secure conversions

- McEliece/Niederreteir cannot be used naively:
  - Ciphertexts are malleable.
  - Message resend and related messages attacks are possible.
- Some conversions of these systems exist that achieve CCA2 security.
- Main ingredients:
  - Using a substitute message based on OTP-like encryption.
  - Embedding a hash digest of the message into the ciphertext.
  - Using constant weight encoding to compute the error vector from the message.

▶ K. Kobara, H. Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," PKC 2001, vol. 1992 of Springer LNCS, pp. 19–35, 2001.

CCA2 secure conversions

- McEliece/Niederreteir cannot be used naively:
  - Ciphertexts are malleable.
  - Message resend and related messages attacks are possible.
- Some conversions of these systems exist that achieve CCA2 security.
- Main ingredients:
  - Using a substitute message based on OTP-like encryption.
  - Embedding a hash digest of the message into the ciphertext.
  - Using constant weight encoding to compute the error vector from the message.

► K. Kobara, H. Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," PKC 2001, vol. 1992 of Springer LNCS, pp. 19–35, 2001.

CCA2 secure conversions

- McEliece/Niederreteir cannot be used naively:
    - Ciphertexts are malleable.
    - Message resend and related messages attacks are possible.
- Some conversions of these systems exist that achieve CCA2 security.
- Main ingredients:
    - Using a substitute message based on OTP-like encryption.
    - Embedding a hash digest of the message into the ciphertext.
    - Using constant weight encoding to compute the error vector from the message.

► K. Kobara, H. Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," PKC 2001, vol. 1992 of Springer LNCS, pp. 19–35, 2001.

Goppa code-based McEliece/Niederreiter

- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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.

Goppa code-based McEliece/Niederreiter

- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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.

Goppa code-based McEliece/Niederreiter

- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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.

Goppa code-based McEliece/Niederreiter

- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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.

Goppa code-based McEliece/Niederreiter

- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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.

Goppa code-based McEliece/Niederreiter

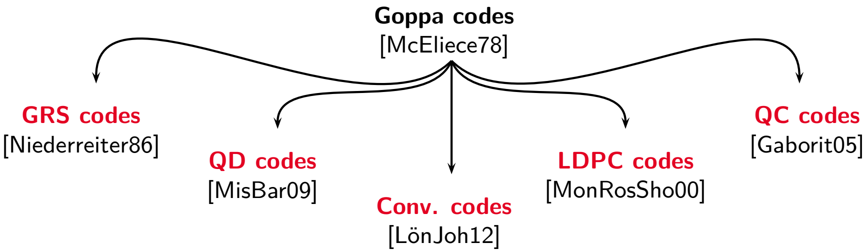
- GRS codes originally used in Niederreiter were attacked.
- But Goppa codes resisted cryptanalysis for about 40 years.
- These systems are faster than competing solutions...
- ...but they require large public keys:
  - 188 KiB for 128-bit security in [Bernstein2008]
  - 255 KiB for 128-bit security in Classic McEliece
- Recent attacks based on distinguishers pose some threats on high rate Goppa codes.
- They also invalidate all existing McEliece cryptosystem security proofs for high rate Goppa codes.

- D. J. Bernstein, T. Lange, and C. Peters, “Attacking and defending the McEliece cryptosystem,” in *Post-Quantum Cryptography*, vol. 5299 of Springer LNCS, pp. 31–46, 2008.
- Classic McEliece, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Classic-McEliece-Round2.zip
- 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)

Goppa codes
[McEliece78]

Alternatives to Goppa codes (Hamming metric)



Alternatives to Goppa codes (Hamming metric)

Goppa codes
[McEliece78]

GRS codes
[Niederreiter86]

QD codes
[MisBar09]

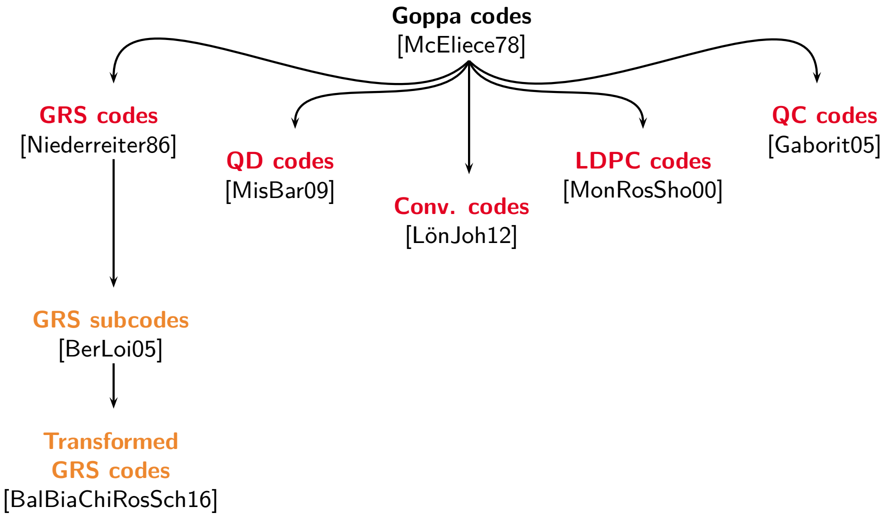
Conv. codes
[LönJoh12]

LDPC codes
[MonRosSho00]

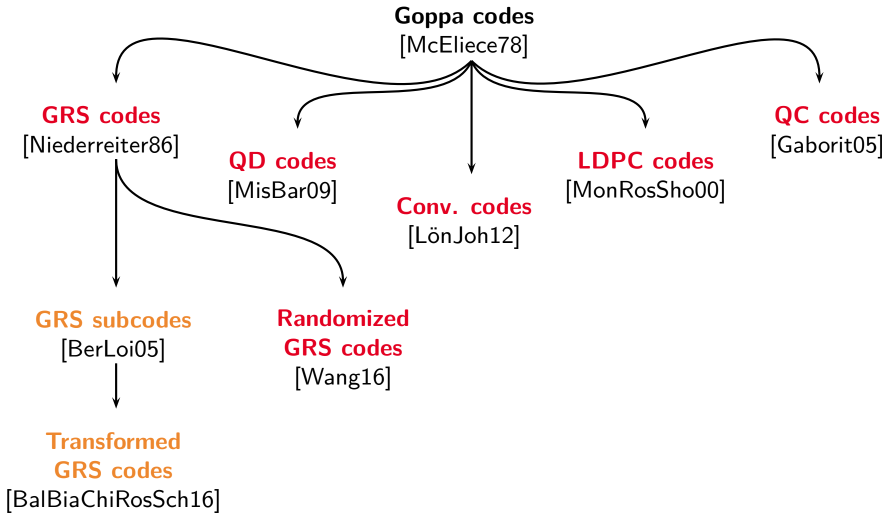
QC codes
[Gaborit05]

GRS subcodes
[BerLoi05]

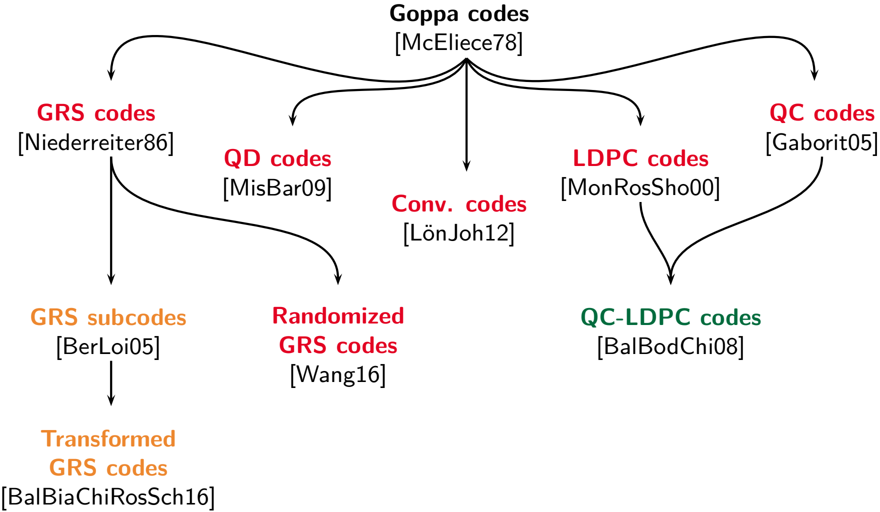
Alternatives to Goppa codes (Hamming metric)



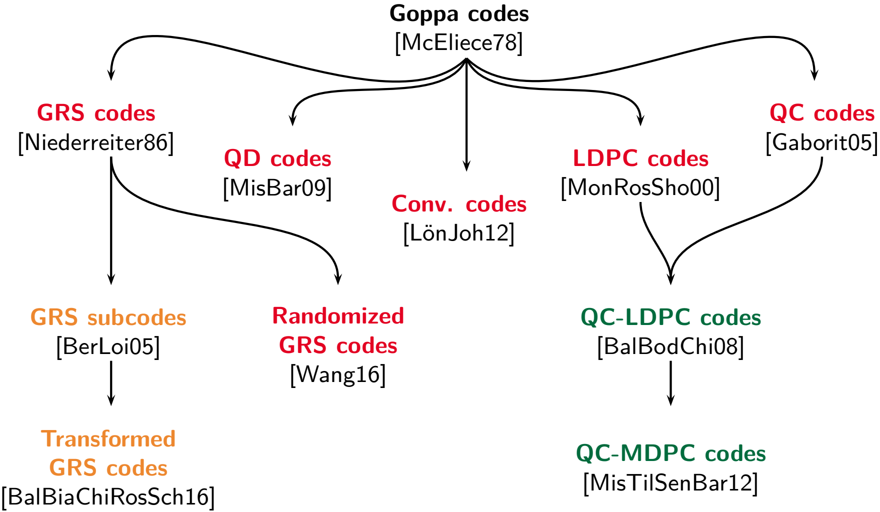
Alternatives to Goppa codes (Hamming metric)



Alternatives to Goppa codes (Hamming metric)



Alternatives to Goppa codes (Hamming metric)



Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

Variants in other metrics (rank)

- Gabidulin codes are optimal codes in the rank metric (like GRS codes in the Hamming metric).
- The Gabidulin-Paramonov-Tretjakov (GPT) cryptosystem exploits them to build a code-based trapdoor in the rank metric domain.
- Using codes in the rank metric prevents the use of information set decoding approaches.
- But other dangerous attacks have been found.
- Secure instances still exist, with reasonably small keys.
- Complexity of decoding in the rank domain may be an issue.

- R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," Journal of Cryptology, vol. 21, no. 2, pp. 280–301, 2008.
- H. Rashwan, E.M. Gabidulin, B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," Security and Communication Networks. vol. 4, no. 8, pp. 937–946, 2011.

QC-LDPC code-based cryptography

- Quasi-cyclic low-density parity-check (QC-LDPC) codes have important advantages over Goppa codes:
  - The sparsity of their matrices enables very efficient decoding
  - Quasi-cyclicity enables very compact keys
- QC-LDPC code-based systems introduced in 2007.
- quasi-cyclic moderate-density parity-check (QC-MDPC) code-based systems introduced in 2013.

- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes," Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591–2595, Nice, France, 2007.
- 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.
- R. Misoczki, J.-P. Tillich, N. Sendrier, P.S.L.M. Barreto, "MDPC-McEliece: new McEliece variants from moderate density parity-check codes", Proc. IEEE ISIT 2013, pp. 2069–2073, July 2013.

QC-LDPC code-based cryptography

- QC-LDPC codes have important advantages over Goppa codes:
  - The sparsity of their matrices enables very efficient decoding
  - Quasi-cyclicity enables very compact keys
- QC-LDPC code-based systems introduced in 2007.
- QC-MDPC code-based systems introduced in 2013.

- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes," Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591–2595, Nice, France, 2007.
- 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.
- R. Misoczki, J.-P. Tillich, N. Sendrier, P.S.L.M. Barreto, "MDPC-McEliece: new McEliece variants from moderate density parity-check codes", Proc. IEEE ISIT 2013, pp. 2069–2073, July 2013.

QC-LDPC code-based cryptography

- QC-LDPC codes have important advantages over Goppa codes:
  - The sparsity of their matrices enables very efficient decoding
  - Quasi-cyclicity enables very compact keys
- QC-LDPC code-based systems introduced in 2007.
- QC-MDPC code-based systems introduced in 2013.

- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes," Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591–2595, Nice, France, 2007.
- 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.
- R. Misoczki, J.-P. Tillich, N. Sendrier, P.S.L.M. Barreto, "MDPC-McEliece: new McEliece variants from moderate density parity-check codes", Proc. IEEE ISIT 2013, pp. 2069–2073, July 2013.

QC-LDPC code-based cryptography

- QC-LDPC codes have important advantages over Goppa codes:
  - The sparsity of their matrices enables very efficient decoding
  - Quasi-cyclicity enables very compact keys
- QC-LDPC code-based systems introduced in 2007.
- QC-MDPC code-based systems introduced in 2013.

- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes," Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591–2595, Nice, France, 2007.
- 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.
- R. Misoczki, J.-P. Tillich, N. Sendrier, P.S.L.M. Barreto, "MDPC-McEliece: new McEliece variants from moderate density parity-check codes", Proc. IEEE ISIT 2013, pp. 2069–2073, July 2013.

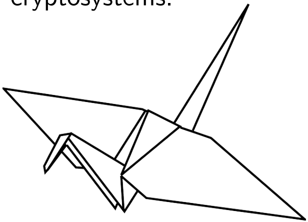
QC-LDPC code-based cryptography

- QC-LDPC codes have important advantages over Goppa codes:
  - The sparsity of their matrices enables very efficient decoding
  - Quasi-cyclicity enables very compact keys
- QC-LDPC code-based systems introduced in 2007.
- QC-MDPC code-based systems introduced in 2013.

- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes," Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591–2595, Nice, France, 2007.
- 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.
- R. Misoczki, J.-P. Tillich, N. Sendrier, P.S.L.M. Barreto, "MDPC-McEliece: new McEliece variants from moderate density parity-check codes", Proc. IEEE ISIT 2013, pp. 2069–2073, July 2013.

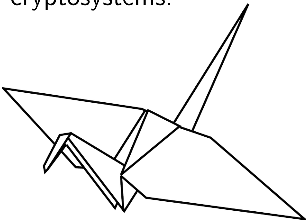
LEDAcrypt

- Suite of Low-Density Parity-Check code-based cryptosystems.
- Among the 26 second round candidates of the NIST pqcrypto competition.
- Proposing team:
  - Marco Baldi (Univpm, Italy)
  - Alessandro Barenghi (Polimi, Italy)
  - Franco Chiaraluce (Univpm, Italy)
  - Gerardo Pelosi (Polimi, Italy)
  - Paolo Santini (Univpm, Italy)
- Official website (https://www.ledacrypt.org/):
  - First and second round specifications.
  - Full ANSI-C99 codebase.
  - Upcoming updates.
- Upcoming hardware implementation.



LEDAcrypt

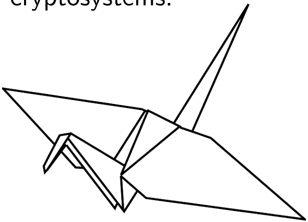
- Suite of Low-Density Parity-Check code-based cryptosystems.
- Among the 26 second round candidates of the NIST pqcrypto competition.
- Proposing team:
  - Marco Baldi (Univpm, Italy)
  - Alessandro Barenghi (Polimi, Italy)
  - Franco Chiaraluce (Univpm, Italy)
  - Gerardo Pelosi (Polimi, Italy)
  - Paolo Santini (Univpm, Italy)



- Official website (https://www.ledacrypt.org/):
  - First and second round specifications.
  - Full ANSI-C99 codebase.
  - Upcoming updates.
- Upcoming hardware implementation.

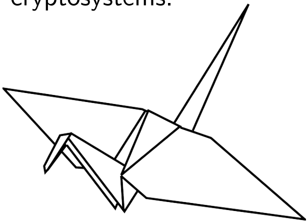
LEDAcrypt

- Suite of Low-Density Parity-Check code-based cryptosystems.
- Among the 26 second round candidates of the NIST pqcrypto competition.
- Proposing team:
  - Marco Baldi (Univpm, Italy)
  - Alessandro Barenghi (Polimi, Italy)
  - Franco Chiaraluce (Univpm, Italy)
  - Gerardo Pelosi (Polimi, Italy)
  - Paolo Santini (Univpm, Italy)
- Official website (`https://www.ledacrypt.org/`):
  - First and second round specifications.
  - Full ANSI-C99 codebase.
  - Upcoming updates.
- Upcoming hardware implementation.



LEDAcrypt

- Suite of Low-Density Parity-Check code-based cryptosystems.
- Among the 26 second round candidates of the NIST pqcrypto competition.
- Proposing team:
  - Marco Baldi (Univpm, Italy)
  - Alessandro Barenghi (Polimi, Italy)
  - Franco Chiaraluce (Univpm, Italy)
  - Gerardo Pelosi (Polimi, Italy)
  - Paolo Santini (Univpm, Italy)
- Official website (`https://www.ledacrypt.org/`):
  - First and second round specifications.
  - Full ANSI-C99 codebase.
  - Upcoming updates.
- Upcoming hardware implementation.



LEDAcrypt features

1. Both KEM and PKC modes.
2. Closed-form upper bound on the decoding failure rate (DFR).
3. Algorithmic approach to the design of parameter sets.
4. Instances with:
   - Ephemeral keys and a DFR in the order of 10^{-9}, or
   - Long-term keys and a DFR of 2^{-64} or smaller than $2^{-\lambda}$, with $\lambda = 128, 192, 256$.

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate," Proc. Code-Based Cryptography Workshop (CBC) 2019, pages 11–43, vol. 11666 of Springer LNCS, 2019.

LEDAcrypt features

1. Both KEM and PKC modes.
2. Closed-form upper bound on the DFR.
3. Algorithmic approach to the design of parameter sets.
4. Instances with:
   - Ephemeral keys and a DFR in the order of 10^{-9}, or
   - Long-term keys and a DFR of 2^{-64} or smaller than $2^{-\lambda}$, with $\lambda = 128, 192, 256$.

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate," Proc. Code-Based Cryptography Workshop (CBC) 2019, pages 11–43, vol. 11666 of Springer LNCS, 2019.

LEDAcrypt features

1. Both KEM and PKC modes.
2. Closed-form upper bound on the DFR.
3. Algorithmic approach to the design of parameter sets.
4. Instances with:
   - Ephemeral keys and a DFR in the order of 10^{-9}, or
   - Long-term keys and a DFR of 2^{-64} or smaller than $2^{-\lambda}$, with $\lambda = 128, 192, 256$.

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate," Proc. Code-Based Cryptography Workshop (CBC) 2019, pages 11–43, vol. 11666 of Springer LNCS, 2019.

LEDAcrypt features

1. Both KEM and PKC modes.
2. Closed-form upper bound on the DFR.
3. Algorithmic approach to the design of parameter sets.
4. Instances with:
   - Ephemeral keys and a DFR in the order of 10^{-9}, or
   - Long-term keys and a DFR of 2^{-64} or smaller than $2^{-\lambda}$, with $\lambda = 128, 192, 256$.

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini, "LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate," Proc. Code-Based Cryptography Workshop (CBC) 2019, pages 11–43, vol. 11666 of Springer LNCS, 2019.

Performance of LEDAcrypt KEM (ephemeral)

Software running on an Intel i5-6500, 3.2 GHz

NIST Category	n_0	KeyGen (ms)	Encap. (ms)	Decap. (ms)	Total exec. time (ms)	Ctx+kpub Size (kiB)
1	2	1.32	0.06	0.24	1.62	3.65
	3	0.50	0.03	0.23	0.77	3.04
	4	0.47	0.02	0.26	0.76	3.68
3	2	3.63	0.12	0.61	4.37	6.28
	3	1.72	0.07	0.54	2.33	5.91
	4	1.50	0.07	0.69	2.27	7.03
5	2	7.18	0.20	0.95	8.35	9.01
	3	4.64	0.16	1.05	5.86	10.05
	4	3.83	0.13	1.05	5.02	11.09

Code-based digital 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 and B. Smeets, "A digital signature scheme based on random error correcting codes," Proc. 6th IMA Int. Conf. on Cryptography and Coding, pp. 161–167, London, UK, 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.

Code-based digital 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 and B. Smeets, "A digital signature scheme based on random error correcting codes," Proc. 6th IMA Int. Conf. on Cryptography and Coding, pp. 161–167, London, UK, 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.

Code-based digital 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 and B. Smeets, "A digital signature scheme based on random error correcting codes," Proc. 6th IMA Int. Conf. on Cryptography and Coding, pp. 161–167, London, UK, 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.

Code-based digital 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 and B. Smeets, "A digital signature scheme based on random error correcting codes," Proc. 6th IMA Int. Conf. on Cryptography and Coding, pp. 161–167, London, UK, 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.

Code-based digital 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 and B. Smeets, "A digital signature scheme based on random error correcting codes," Proc. 6th IMA Int. Conf. on Cryptography and Coding, pp. 161–167, London, UK, 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.

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 low-density generator matrix (LDGM) codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage, only one-time or few-times signatures
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - based on generalized $(U; U+V)$ codes
  - degraded version cryptanalyzed on hundreds of signatures
  - full version under analysis

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 codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage, only one-time or few-times signatures
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - based on generalized $(U; U + V)$ codes
  - degraded version cryptanalyzed on hundreds of signatures
  - full version under analysis

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 codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage, only one-time or few-times signatures
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - based on generalized $(U; U+V)$ codes
  - degraded version cryptanalyzed on hundreds of signatures
  - full version under analysis

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 codes
  - very small keys, no decoding required
  - statistical attacks exploiting key leakage, only one-time or few-times signatures
- **2018**: Debris-Alazard-Sendrier-Tillich: Wave scheme
  - based on generalized $(U; U + V)$ codes
  - degraded version cryptanalyzed on hundreds of signatures
  - full version under analysis

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, "An efficient attack on all concrete KKS proposals," Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., "One-time signature scheme from syndrome decoding over generic error-correcting codes," Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, “An efficient attack on all concrete KKS proposals,” Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., “One-time signature scheme from syndrome decoding over generic error-correcting codes,” Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, "An efficient attack on all concrete KKS proposals," Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., "One-time signature scheme from syndrome decoding over generic error-correcting codes," Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, "An efficient attack on all concrete KKS proposals," Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., "One-time signature scheme from syndrome decoding over generic error-correcting codes," Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, "An efficient attack on all concrete KKS proposals," Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., "One-time signature scheme from syndrome decoding over generic error-correcting codes," Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

Classic code-based digital signature schemes

- In KKS, two codes with different size are used to create the trapdoor, one selecting the subset support of the other.
- An important weakness of this system has been pointed out.
- There are still some parameter choices which make it secure.
- In any case, KKS can only be used as a one-time or few-times signature scheme.
- The CFS scheme instead implements a hash-and-sign scheme exploiting only one secret Goppa code.
- The most dangerous attacks against CFS are generalized birthday attacks and Goppa-code distinguishers.

- A. Otmani and J. P. Tillich, "An efficient attack on all concrete KKS proposals," Proc. PQCrypto 2011, Nov. 29–Dec. 2, Taipei, Taiwan.
- P. S.L.M. Barreto, R. Misoczki, M. A. Simplicio Jr., "One-time signature scheme from syndrome decoding over generic error-correcting codes," Journal of Systems and Software, vol. 84, no. 2, pp. 198–204, Feb. 2011.

CFS scheme

- $\mathcal{H}$: public hash algorithm with r-bit digest.
- $\mathcal{F}$: function able to transform (in a reasonable time) any hash value computed through $\mathcal{H}$ into a correctable syndrome through C.

Private key

$$\{\boldsymbol{S}, \boldsymbol{H}\}$$

- $\boldsymbol{H}$: parity-check matrix of a secret t-error correcting Goppa code $C(n, k)$.
- $\boldsymbol{S}$: $n \times n$ non-singular random matrix.

Public key

$$\boldsymbol{H}' = \boldsymbol{S} \cdot \boldsymbol{H}$$

CFS scheme

- $\mathcal{H}$: public hash algorithm with r-bit digest.
- $\mathcal{F}$: function able to transform (in a reasonable time) any hash value computed through $\mathcal{H}$ into a correctable syndrome through C.

Private key

$$\{\boldsymbol{S}, \boldsymbol{H}\}$$

- $\boldsymbol{H}$: parity-check matrix of a secret t-error correcting Goppa code $C(n, k)$.
- $\boldsymbol{S}$: $n \times n$ non-singular random matrix.

Public key

$$\boldsymbol{H}' = \boldsymbol{S} \cdot \boldsymbol{H}$$

CFS scheme

- $\mathcal{H}$: public hash algorithm with r-bit digest.
- $\mathcal{F}$: function able to transform (in a reasonable time) any hash value computed through $\mathcal{H}$ into a correctable syndrome through C.

Private key

$$\{\boldsymbol{S}, \boldsymbol{H}\}$$

- $\boldsymbol{H}$: parity-check matrix of a secret t-error correcting Goppa code $C(n, k)$.
- $\boldsymbol{S}$: $n \times n$ non-singular random matrix.

Public key

$$\boldsymbol{H}' = \boldsymbol{S} \cdot \boldsymbol{H}$$

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (2)

Signature generation for a file D:

1. The signer computes $\boldsymbol{h} = \mathcal{H}(D)$.
2. The signer computes $\boldsymbol{s} = \mathcal{F}(\boldsymbol{h})$ such that $\boldsymbol{s}' = \boldsymbol{S}^{-1} \cdot \boldsymbol{s}$ is a correctable syndrome (the parameters to be used in $\mathcal{F}$ are made public).
3. Through syndrome decoding, the signer finds $\boldsymbol{e}$ with weight $\leq t$ such that $\boldsymbol{s}' = \boldsymbol{H} \cdot \boldsymbol{e}$.
4. The signature of D is $\boldsymbol{e}$.

Verification of the signature of D:

1. The verifier receives the signed $\widehat{D}$ and computes $\boldsymbol{H}' \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{e} = \boldsymbol{S} \cdot \boldsymbol{s}' = \boldsymbol{s}$.
2. He also computes $\widehat{\boldsymbol{h}} = \mathcal{H}(\widehat{D})$ and $\widehat{\boldsymbol{s}} = \mathcal{F}(\widehat{\boldsymbol{h}})$.
3. If $\widehat{\boldsymbol{s}} = \boldsymbol{s}$, $\widehat{D}$ is accepted, otherwise discarded.

CFS scheme (3)

Main limitation of the CFS scheme

It is very hard to find a function $\mathcal{F}$ that quickly transforms an arbitrary hash vector into a correctable syndrome.

- Two possible solutions:
  1. appending a counter to the message,
  2. performing complete decoding.

Drawbacks

- Codes with very high rate and very small error correction capability are needed.
- This has exposed the cryptosystem to attacks based on the generalized birthday algorithm and Goppa codes distinguishers.

J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. Tillich, "A Distinguisher for High-Rate McEliece Cryptosystems," in IEEE Transactions on Information Theory, vol. 59, no. 10, pp. 6830-6844, Oct. 2013.

CFS scheme (3)

Main limitation of the CFS scheme

It is very hard to find a function $\mathcal{F}$ that quickly transforms an arbitrary hash vector into a correctable syndrome.

- Two possible solutions:
  1. appending a counter to the message,
  2. performing complete decoding.

Drawbacks

- Codes with very high rate and very small error correction capability are needed.
- This has exposed the cryptosystem to attacks based on the generalized birthday algorithm and Goppa codes distinguishers.

▶ J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. Tillich, "A Distinguisher for High-Rate McEliece Cryptosystems," in IEEE Transactions on Information Theory, vol. 59, no. 10, pp. 6830-6844, Oct. 2013.

CFS scheme (3)

Main limitation of the CFS scheme

It is very hard to find a function $\mathcal{F}$ that quickly transforms an arbitrary hash vector into a correctable syndrome.

- Two possible solutions:
  1. appending a counter to the message,
  2. performing complete decoding.

Drawbacks

- Codes with very high rate and very small error correction capability are needed.
- This has exposed the cryptosystem to attacks based on the generalized birthday algorithm and Goppa codes distinguishers.

▶ J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. Tillich, "A Distinguisher for High-Rate McEliece Cryptosystems," in IEEE Transactions on Information Theory, vol. 59, no. 10, pp. 6830-6844, Oct. 2013.

CFS scheme (4)

- Moreover, the key size and decoding complexity can be very large.
- For 80-bit security, the original CFS system needs a Goppa code with $n = 2^{21}$ and $r = 210$, which gives a key size of 52.5 MiB.
- By using the parallel CFS, the same security level is obtained with key sizes between 1.25 MiB and 20 MiB.

▶ M. Finiasz, "Parallel-CFS strengthening the CFS McEliece-based signature scheme," Proc. PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, pp. 61–72.

CFS scheme (4)

- Moreover, the key size and decoding complexity can be very large.
- For 80-bit security, the original CFS system needs a Goppa code with $n = 2^{21}$ and $r = 210$, which gives a key size of 52.5 MiB.
- By using the parallel CFS, the same security level is obtained with key sizes between 1.25 MiB and 20 MiB.

▶ M. Finiasz, "Parallel-CFS strengthening the CFS McEliece-based signature scheme," Proc. PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, pp. 61–72.

CFS scheme (4)

- Moreover, the key size and decoding complexity can be very large.
- For 80-bit security, the original CFS system needs a Goppa code with $n = 2^{21}$ and $r = 210$, which gives a key size of 52.5 MiB.
- By using the parallel CFS, the same security level is obtained with key sizes between 1.25 MiB and 20 MiB.

▶ M. Finiasz, "Parallel-CFS strengthening the CFS McEliece-based signature scheme," Proc. PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, pp. 61–72.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Sparse code-based signatures

Main differences with CFS

1. Only a subset of sparse syndromes is considered.
2. Goppa codes are replaced with low-density generator-matrix (LDGM) codes.
3. Decoding is simplified.

Main advantages over CFS

1. Significant reductions in the public key size.
2. Attacks against Goppa codes and CFS inapplicable.
3. Decoding complexity considerably reduced.

- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures,* Proc. PQCrypto 2013, Limoges, France, June 2013.
- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100′000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100'000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100'000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100′000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100'000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

Attacks against sparse code-based signatures

- A statistical attack against this scheme has been devised.
- It is based on the observation of a large number of signatures.
- It exploits some residual correlation among signature bits to recover an equivalent secret key.
- For parameter sets with 80-bit security, it was successful after the observation of 100′000 signatures originating from the same secret key.
- The scheme can still be used as a few times signature scheme.
- Moving to metrics other than Hamming may help countering this attack.

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

System examples - key size

Category	ID	Private Key Size At rest (B)	Private Key Size In memory (kiB)	Public Key size (kiB)	Signature size (kiB)
1	a_3	56	53.66	315.67	3.55
	a_6	56	21.89	540.80	6.52
	α_3	56	32.54	828.81	9.32
2–3	b_3	64	76.29	1364.28	9.16
	b_6	80	40.30	3160.47	27.98
	β_3	64	55.77	3619.48	35.15
4–5	c_3	88	86.03	2818.20	18.92
	c_6	88	69.79	11661.05	89.02
	γ_3	88	159.01	15590.80	112.17

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

System examples - speed

Category	ID	KeyGen (ms)	Sign (ms)	Sign+Decomp. (ms)	Verify (ms)
1	a_3	35.51	0.29	1.96	28.71
	a_6	27.23	0.14	1.06	31.18
	α_3	43.45	0.28	1.52	51.10
2–3	b_3	154.49	0.27	2.29	97.83
	b_6	227.14	0.55	2.30	179.89
	β_3	249.69	1.11	2.62	212.19
4–5	c_3	290.95	0.71	5.97	186.30
	c_6	840.74	2.59	3.81	650.78
	γ_3	1714.01	4.27	9.16	926.35

- M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, J. Rosenthal, P. Santini, D. Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes," arXiv eprint 1807.06127, 2018.

End of presentation

Thank you!

`www.univpm.it/marco.baldi`

`m.baldi@univpm.it`

CBCrypto 2020 ← submit your papers!
(`cbcrypto.dii.univpm.it`)