Towards post-quantum cryptographic standards

focus on code-based cryptography

Jean-Christophe Deneuville

<jean-christophe.deneuville@enac.fr>

June 2021, the 4th

10 CTCRYPT 2021 | The 10th Workshop on «Current Trends in Cryptology» CTCrypt 2021

Outline

Outline

NIST PQC standardization process

NIST **N**ational **I**nstitute of **S**tandards and **T**echnology

NIST PQC standardization process

NIST National Institute of Standards and Technology

- 3rd call for standardization
- Asks for post-quantum cryptographic algorithms
- 3 categories :
  - Encryption
  - Key exchange
  - Signature

NIST PQC standardization process

NIST **N**ational **I**nstitute of **S**tandards and **T**echnology

- 3rd call for standardization
- Asks for post-quantum cryptographic algorithms
- 3 categories :
  - Encryption
  - Key exchange
  - Signature

- Many candidates:
  - Error correcting codes,
  - Lattices,
  - Multivariate,
  - Hash functions,
  - Elliptic curves isogenies,
  - ...

NIST PQC standardization process

NIST National Institute of Standards and Technology

- 3rd call for standardization
- Asks for post-quantum cryptographic algorithms
- 3 categories :
  - Encryption
  - Key exchange
  - Signature

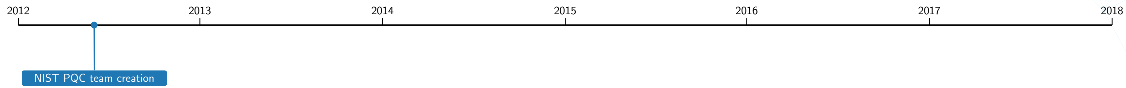
- Many candidates:
  - Error correcting codes,
  - Lattices,
  - Multivariate,
  - Hash functions,
  - Elliptic curves isogenies,
  - ...

security level I	At least as hard to break as AES128 (exhaustive key search)
security level II	At least as hard to break as SHA256 (collision search)
security level III	At least as hard to break as AES192 (exhaustive key search)
security level IV	At least as hard to break as SHA384 (collision search)
security level V	At least as hard to break as AES256 (exhaustive key search)

Timeline NIST

2012 — 2013 — 2014 — 2015 — 2016 — 2017 — 2018

Timeline NIST

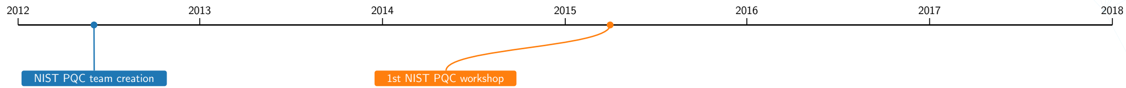


Timeline NIST

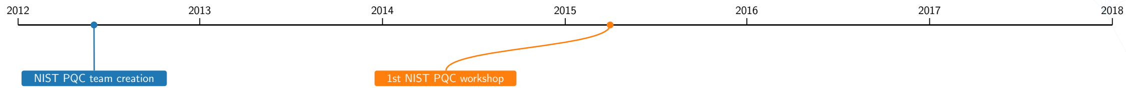
2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018

NIST PQC team creation

Timeline NIST



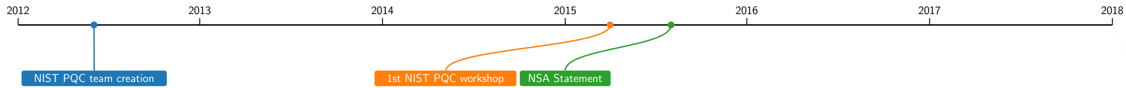
Timeline NIST



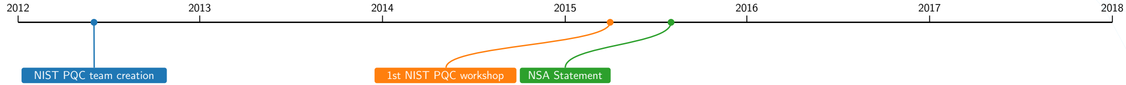
Workshop on Cybersecurity in a Post-Quantum World

The advent of practical quantum computing will break all commonly used public key cryptographic algorithms. In response, NIST is researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. NIST is holding this workshop to engage academic, industry, and government stakeholders. The Post Quantum Workshop will be held on April 2-3, 2015, immediately following the *2015 International Conference on Practice and Theory of Public-Key Cryptography* . NIST seeks to discuss issues related to post-quantum cryptography and its potential future standardization.

Timeline NIST



Timeline NIST



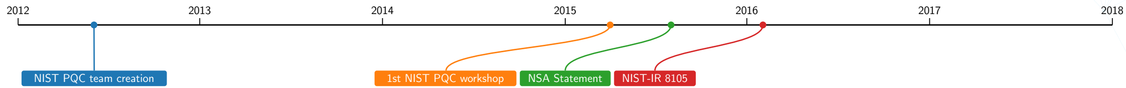
Commercial National Security Algorithm Suite

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

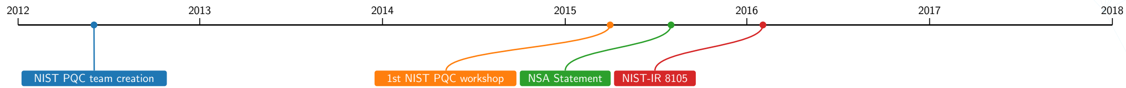
Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

Timeline NIST



Timeline NIST



NISTIR 8105

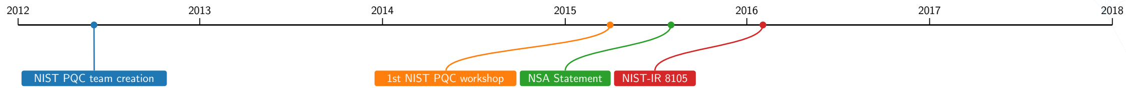
Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

Abstract

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares the National Institute of Standards and Technology (NIST)'s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

Timeline NIST



NISTIR 8105

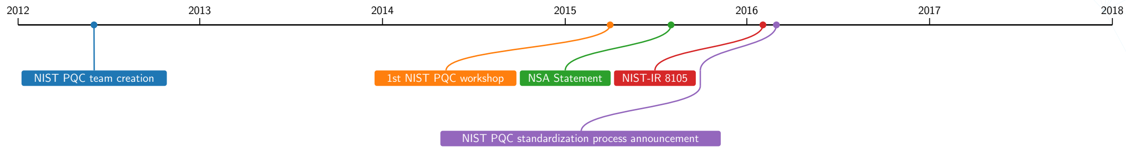
Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

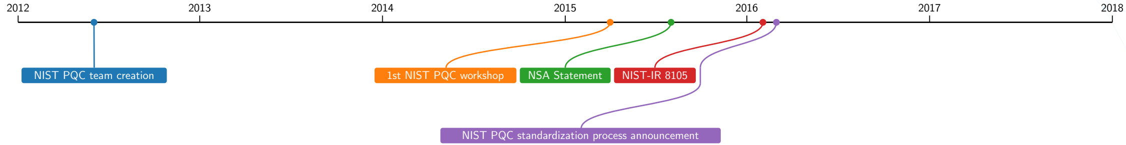
Abstract

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares the National Institute of Standards and Technology (NIST)'s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

Timeline NIST



Timeline NIST



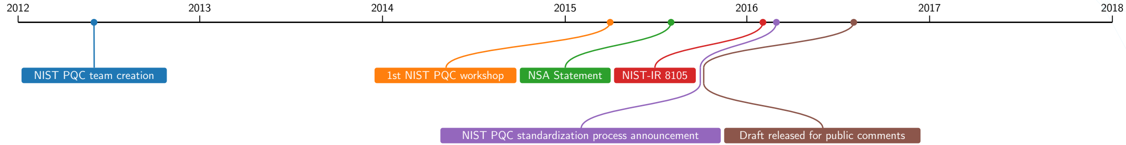
NEWS

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

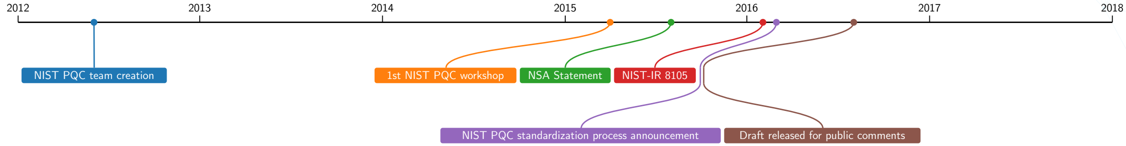
April 28, 2016

"We're looking to replace three NIST cryptographic standards and guidelines that would be the most vulnerable to quantum computers," Moody said, referring to FIPS 186-4, NIST SP 800-56A and NIST SP 800-56B. "They deal with encryption, key establishment and digital signatures, all of which use forms of public key cryptography."

Timeline NIST



Timeline NIST



Moody, Dustin (Fed) Aug. 2019, 1st, 14:47:39

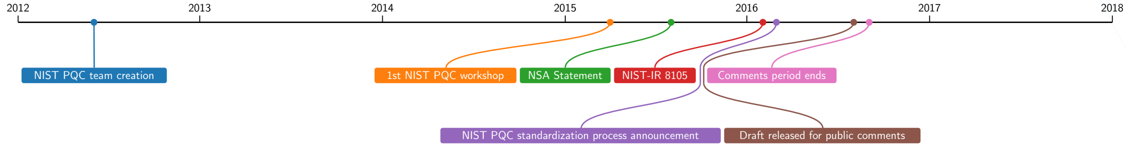
à pqc-...@list.nist.gov

The National Institute of Standards and Technology (NIST) is requesting comments on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, Digital Signature Standard, as well as special publications SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and SP 800-56B Revision 1, Recommendation for Pair-Wises Key-Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105 Report on Post Quantum Cryptography<http://dx.doi.org/10.6028/NIST.IR.8105>).
As a first step in this process, NIST is publishing draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms to solicit public comment. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.
The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center website: http://www.nist.gov/pqcrypto. The public comment period closes on September 16, 2016. Send comments to pqc-comments at nist.gov<mailto:pqc-comments at nist.gov>, with subject line "Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria."

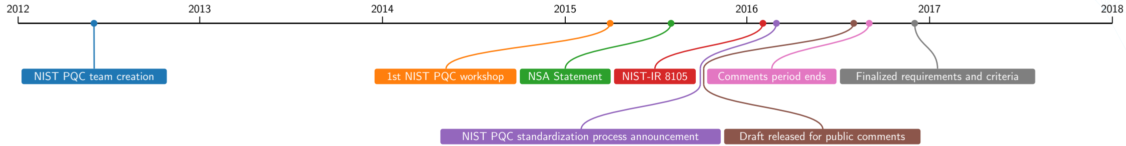
Dustin Moody
NIST

As a reminder, you can use this forum to discuss issues related to NIST's post-quantum standardization efforts.

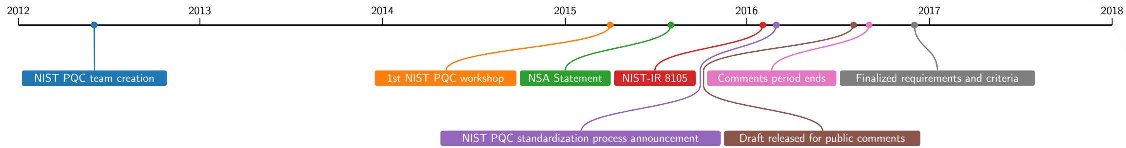
Timeline NIST



Timeline NIST



Timeline NIST



Moody, Dustin (Fed) Dec. 2016, 15th, 20:26:26

à pqc-...@list.nist.gov

The final submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found at http://www.nist.gov/pqcrypto<http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html>. Nominations for post-quantum candidate algorithms may now be submitted, up until the final deadline of November 30, 2017. Complete instructions on how to submit a candidate package are posted at http://www.nist.gov/pqcrypto<http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html>.

Dustin Moody

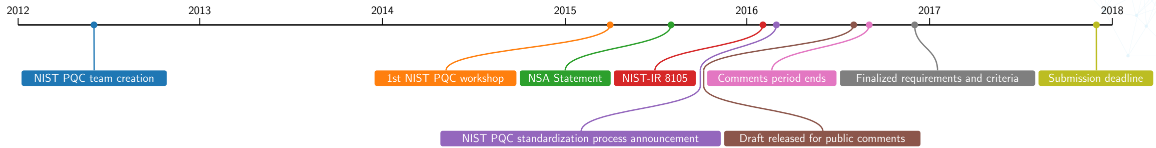
NIST

---

https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

Timeline NIST



Moody, Dustin (Fed) — Dec. 2016, 15th, 20:26:26

à pqc-...@list.nist.gov

The final submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found at http://www.nist.gov/pqcrypto<http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html>. Nominations for post-quantum candidate algorithms may now be submitted, up until the final deadline of November 30, 2017. Complete instructions on how to submit a candidate package are posted at http://www.nist.gov/pqcrypto<http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html>.

Dustin Moody

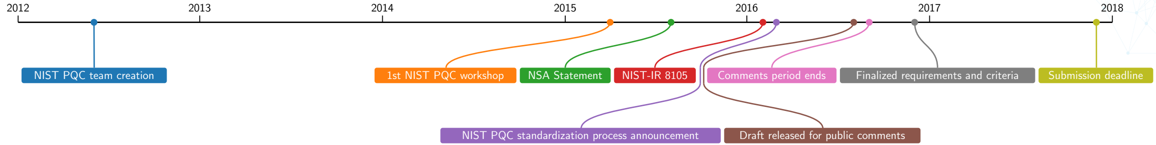
NIST

---

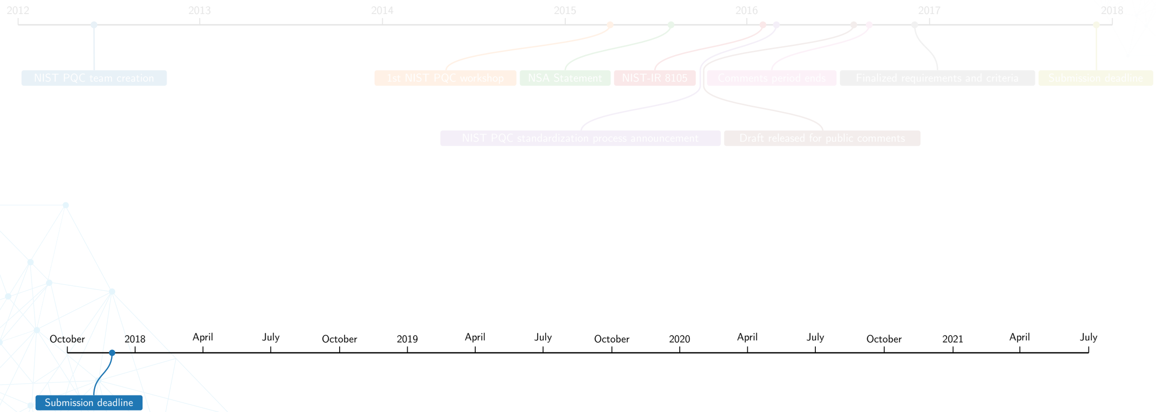
https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

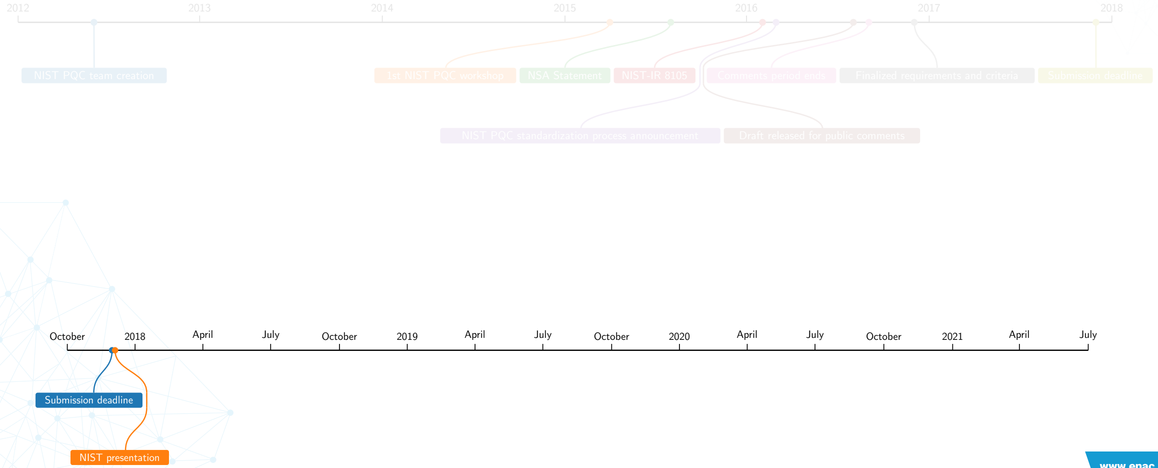
Timeline NIST



Timeline NIST

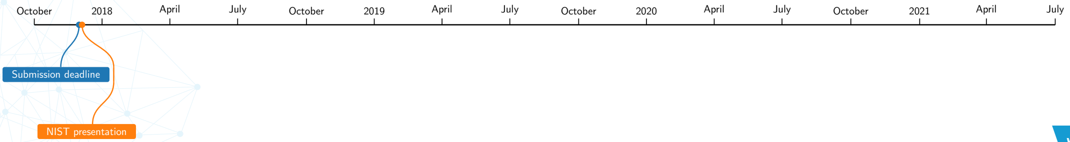


Timeline NIST

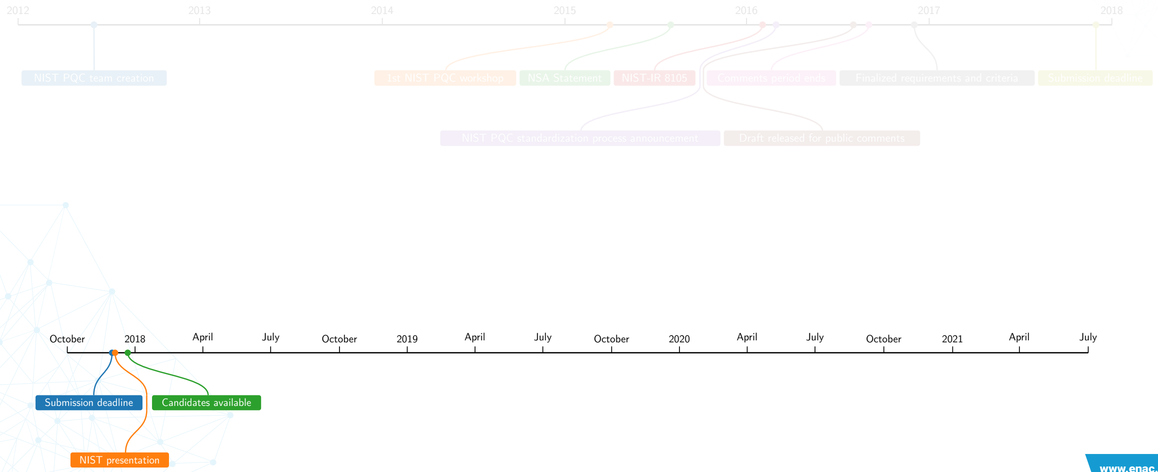


Timeline NIST

AsiaCrypt'17



Timeline NIST



Timeline NIST

Moody, Dustin (Fed) — Dec. 2017, 21st 19:50:51

à pqc-...@list.nist.gov

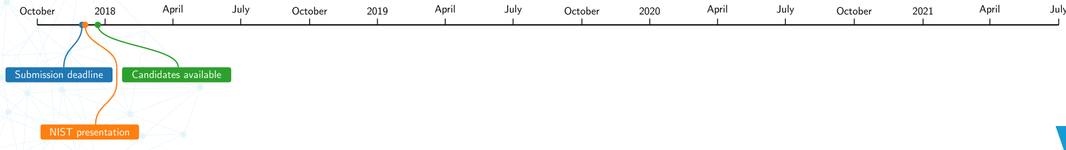
Everyone,

Sorry for the delay - it took a little longer to put up on our website than we originally though. The complete list of accepted submissions is available at:

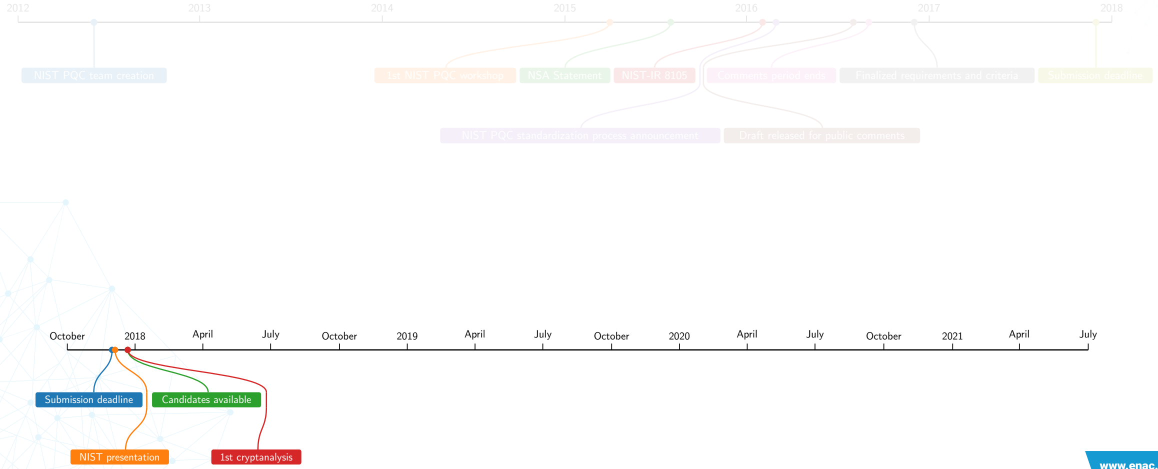
https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

Thanks!

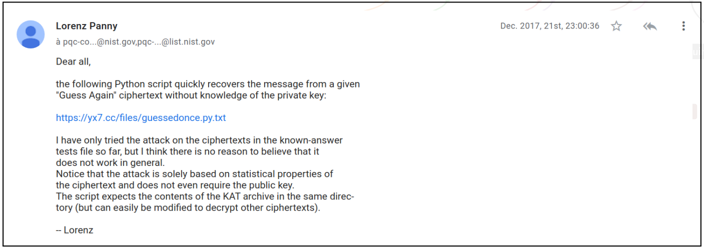
Dustin Moody



Timeline NIST



Timeline NIST


Lorenz Panny
à pqc-co...@nist.gov,pqc-...@list.nist.gov
Dec. 2017, 21st, 23:00:36

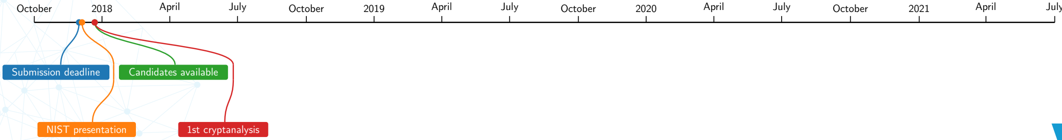
Dear all,

the following Python script quickly recovers the message from a given "Guess Again" ciphertext without knowledge of the private key:

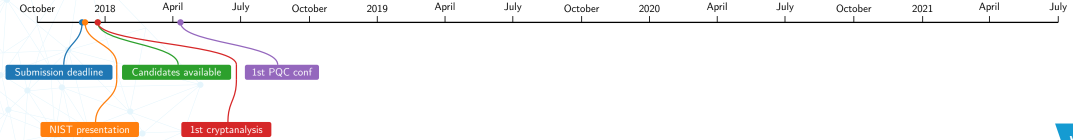
https://yx7.cc/files/guessedonce.py.txt

I have only tried the attack on the ciphertexts in the known-answer tests file so far, but I think there is no reason to believe that it does not work in general.
Notice that the attack is solely based on statistical properties of the ciphertext and does not even require the public key.
The script expects the contents of the KAT archive in the same directory (but can easily be modified to decrypt other ciphertexts).

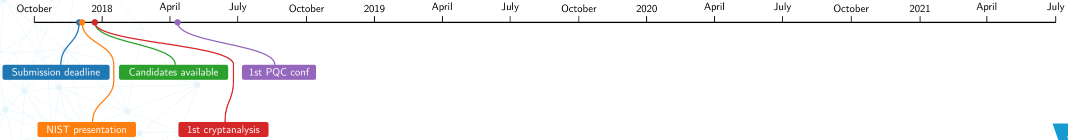
-- Lorenz



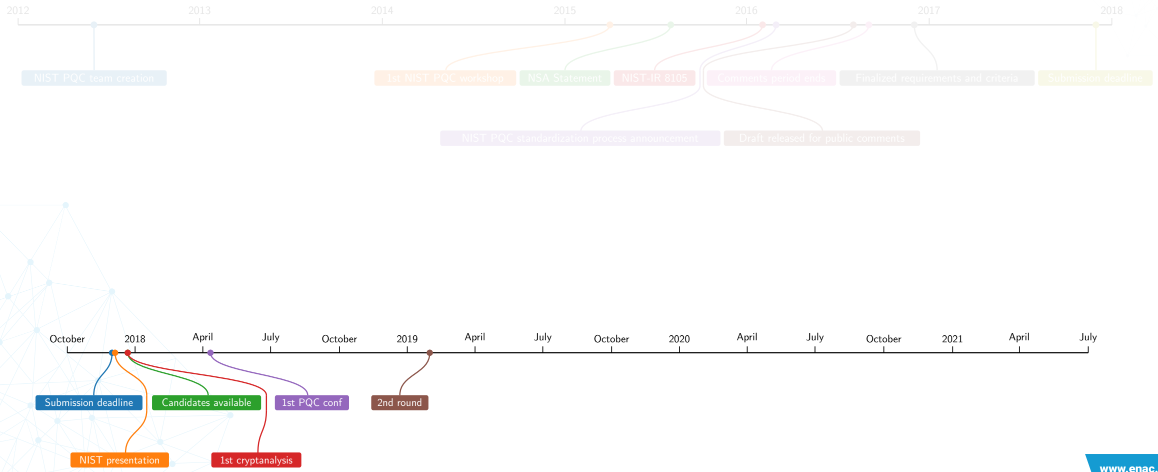
Timeline NIST



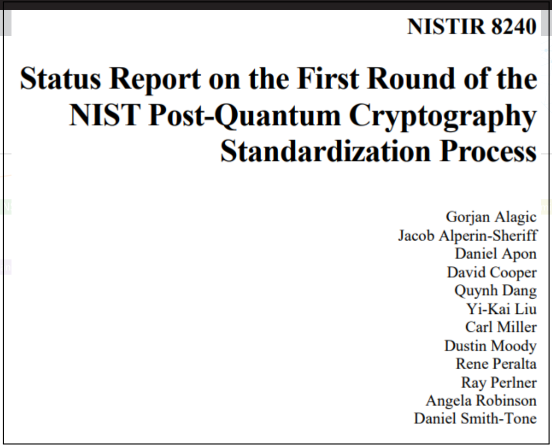
Timeline NIST



Timeline NIST



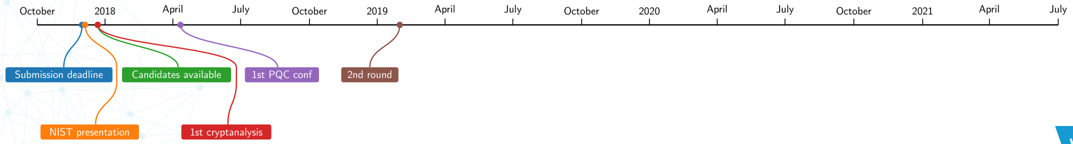
Timeline NIST



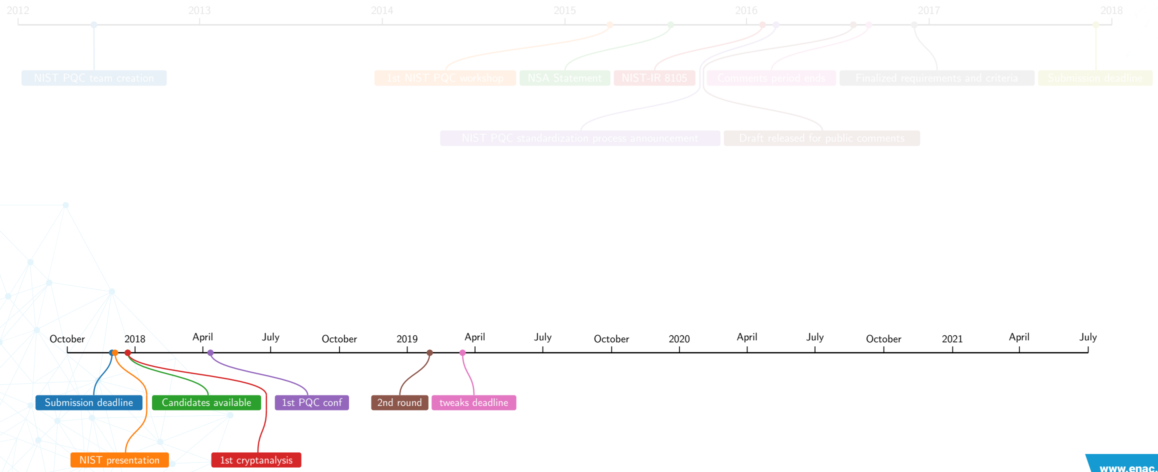
NISTIR 8240

Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process

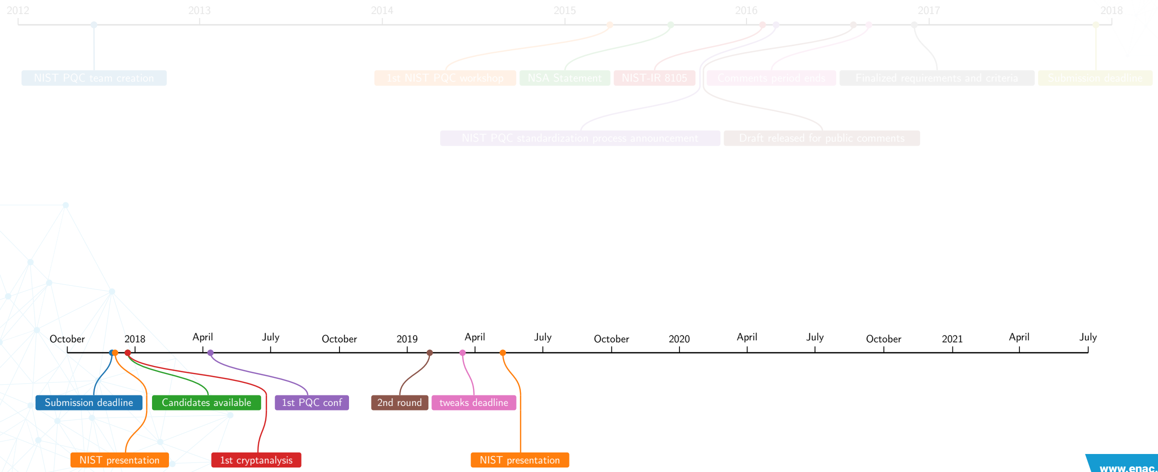
Gorjan Alagic
Jacob Alperin-Sheriff
Daniel Apon
David Cooper
Quynh Dang
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone



Timeline NIST

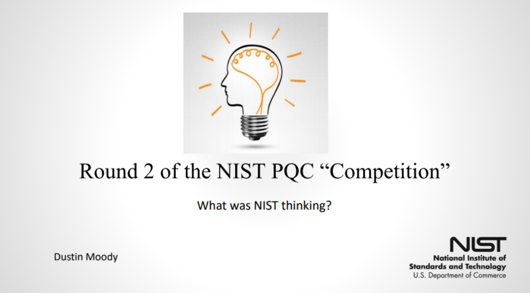


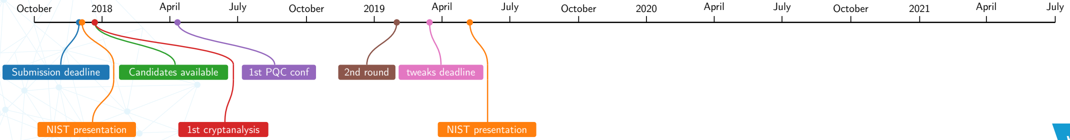
Timeline NIST



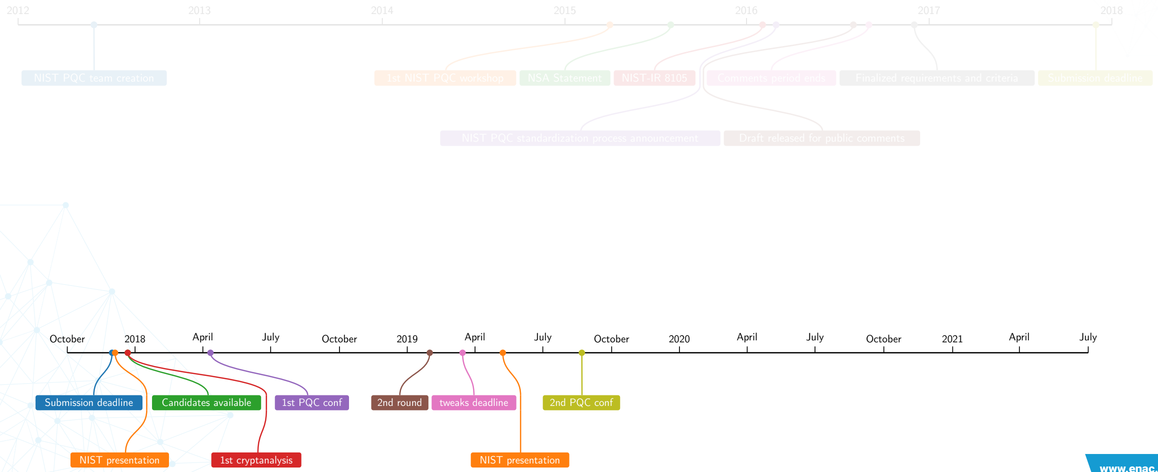
Timeline NIST

PQCrypto'19

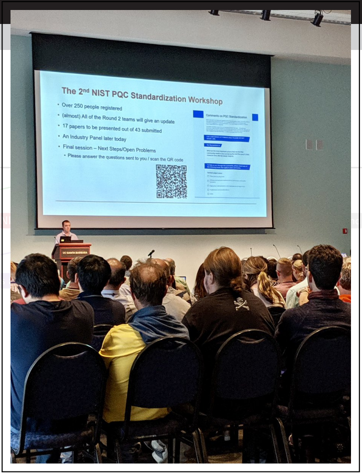


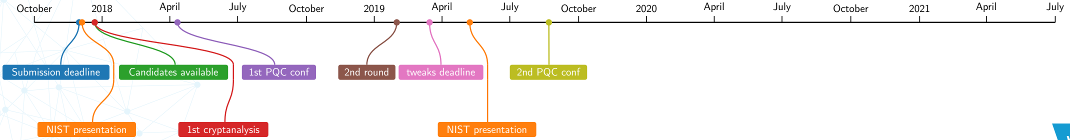


Timeline NIST

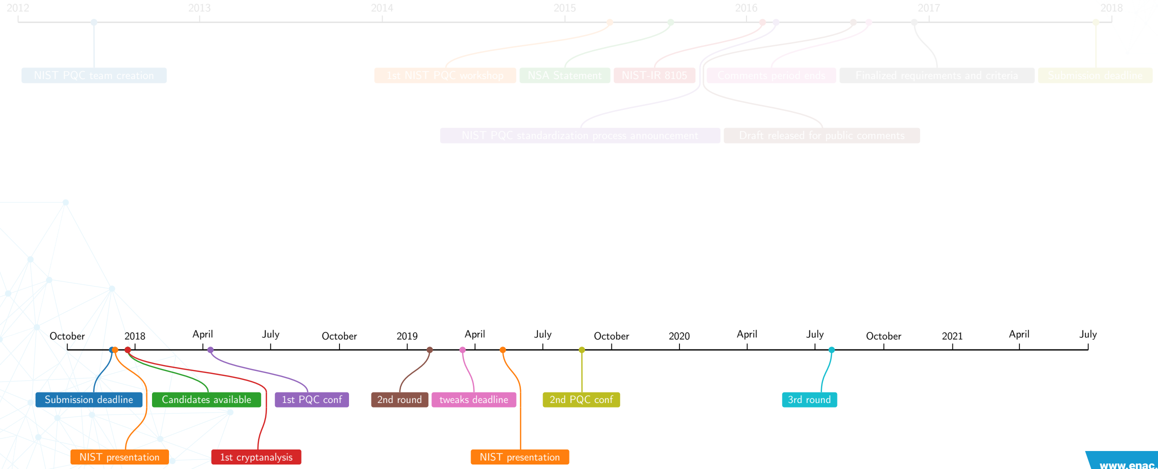


Timeline NIST





Timeline NIST



Timeline NIST

Moody, Dustin (Fed)
à pqc-forum
Jul. 2020, 22nd, 22:51:32

Announcement

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round. The seven third-round Finalists are:

Third Round Finalists

Public-Key Encryption/KEMs
Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

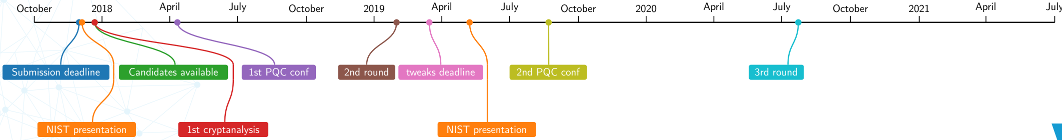
Digital Signatures
CRYSTALS-DILITHIUM
FALCON
Rainbow

In addition, the following eight candidate algorithms will advance to the third round:

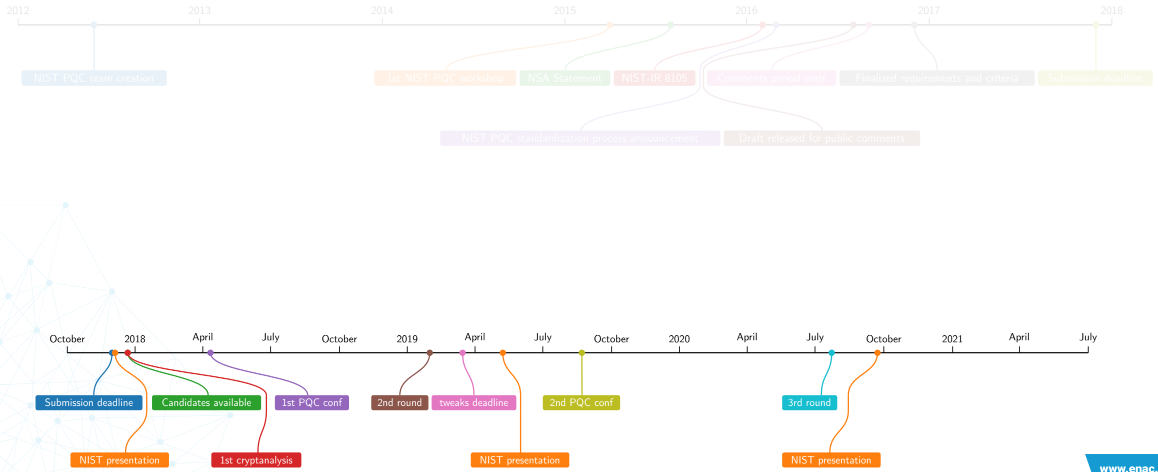
Alternate Candidates

Public-Key Encryption/KEMs
BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

Digital Signatures
GeMSS
Picnic
SPHINCS+

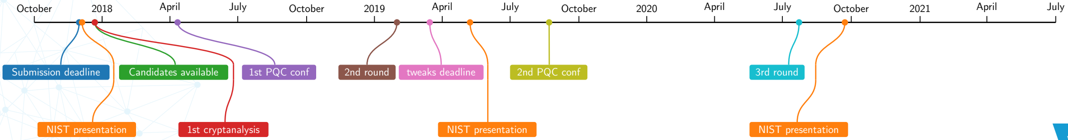


Timeline NIST

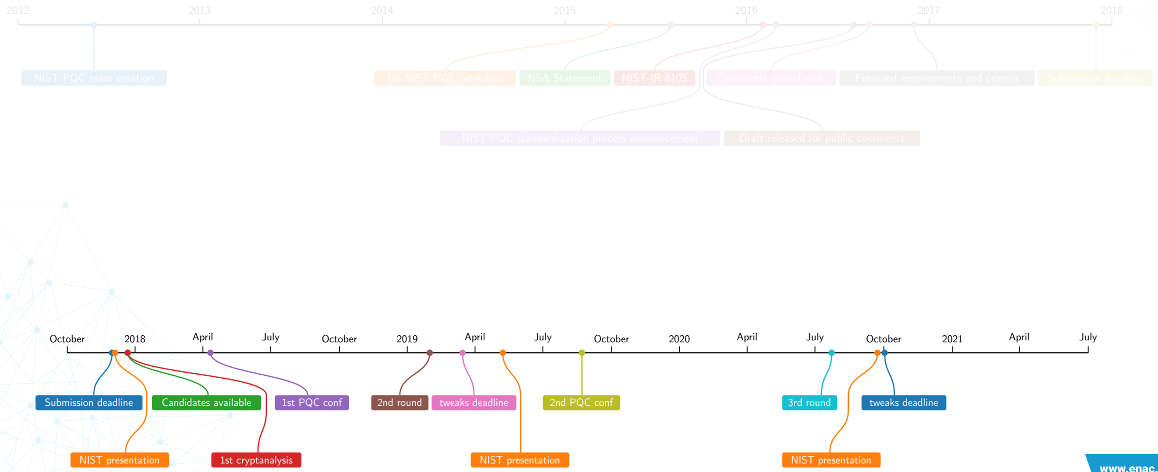


Timeline NIST

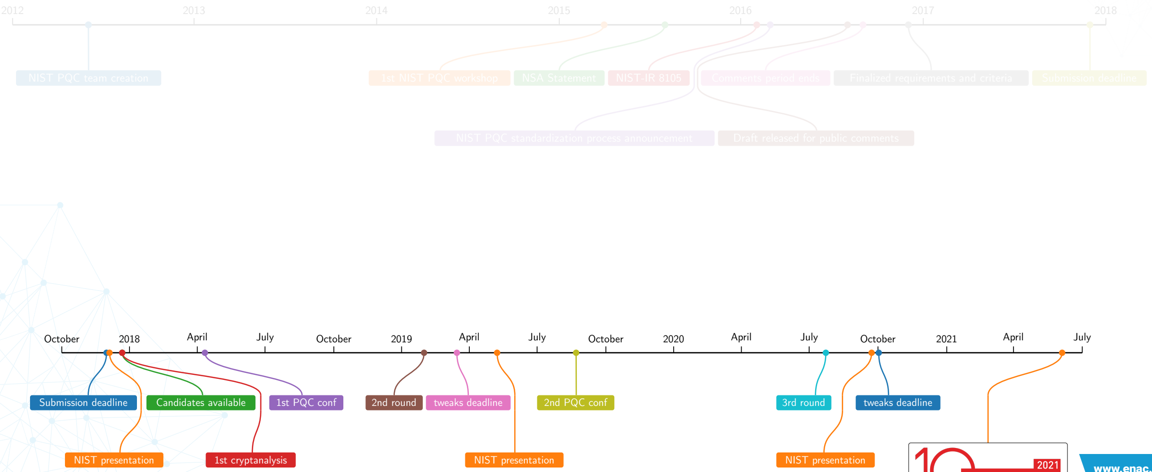
PQCrypto'20



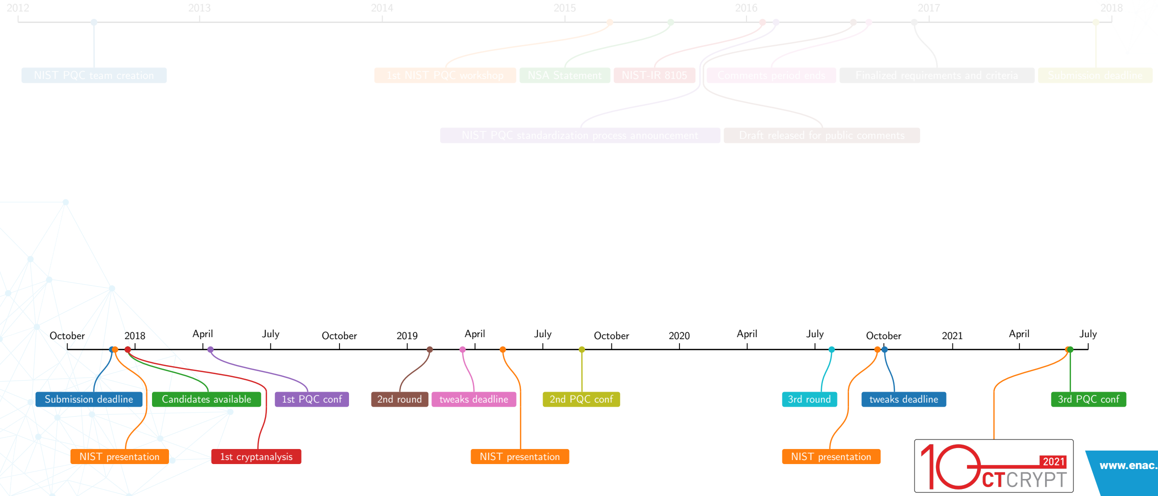
Timeline NIST



Timeline NIST



Timeline NIST



Third PQC Standardization Conference

REGISTRATION

The NIST Post-Quantum Cryptography Standardization Process has entered the third phase, in which 7 third round finalists and eight alternate candidates are being considered for standardization. NIST plans to hold a third NIST PQC Standardization Conference in June 2021 to discuss various aspects of these candidates, and to obtain valuable feedback for the final selection(s). NIST will invite each submission team of the 15 finalists and alternates to give a short update on their algorithm.

The conference will take place virtually.

Call for Papers

- ~~Submission deadline: **April 23, 2021**~~
- ~~Notification date: **May 7, 2021**~~
- Conference Dates: **June 7-9, 2021**

Conference Inquiries: pqc2021@nist.gov

DRAFT AGENDA

+ expand all

Accepted Papers

Registration Info

Registration Fee: $25.00 USD

REGISTER

The link to attend the meeting will be sent to registered attendees on **June 3, 2021.**

Registration Questions? Please contact **Crissy Robinson**.

EVENT DETAILS

Starts: June 07, 2021 - 10:00 AM EST
Ends: June 09, 2021 - 04:00 PM EST

Format: Virtual **Type:** Conference

Agenda

Attendance Type: Open to public
Audience Type: Industry,Government,Academia,Other

PARENT PROJECT

See: Post-Quantum Cryptography

RELATED EVENTS

Previous:
<< Second PQC Standardization Conference

RELATED TOPICS

Security and Privacy: post-quantum cryptography

RELATED PAGES

Event: PQC Conference 2018
News Item: PQC Third Round Candidate Announcement

Third PQC Standardization Conference

REGISTRATION

The NIST Post-Quantum Cryptography Standardization Process has entered the third phase, in which 7 third round finalists and eight alternate candidates are being considered for standardization. NIST plans to hold a third NIST PQC Standardization Conference in June 2021 to discuss various aspects of these candidates, and to obtain valuable feedback for the final selection(s). NIST will invite each submission team of the 15 finalists and alternates to give a short update on their algorithm.

The conference will take place virtually.

Call for Papers

- ~~Submission deadline: **April 23, 2021**~~
- ~~Notification date: **May 7, 2021**~~
- Conference Dates: **June 7-9, 2021**

Conference Inquiries: pqc2021@nist.gov

DRAFT AGENDA

+ expand all

Accepted Papers

Registration Info

Registration Fee: $25.00 USD

REGISTER

The link to attend the meeting will be sent to registered attendees on **June 3, 2021.**

Registration Questions? Please contact **Crissy Robinson**.

https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference

EVENT DETAILS

Starts: June 07, 2021 - 10:00 AM EST
Ends: June 09, 2021 - 04:00 PM EST

Format: Virtual **Type:** Conference

Agenda

Attendance Type: Open to public
Audience Type: Industry,Government,Academia,Other

PARENT PROJECT

See: Post-Quantum Cryptography

RELATED EVENTS

Previous:
<< Second PQC Standardization Conference

RELATED TOPICS

Security and Privacy: post-quantum cryptography

RELATED PAGES

Event: PQC Conference 2018
News Item: PQC Third Round Candidate Announcement

Overview of the candidates

category \ primitive	PKE / KEM	Signature	Total
Lattice-based			
Code-based			
Hash-based			
Multivariate-based			
Isogeny-based			
Other			
Total			

Overview of the candidates

primitive / category	PKE / KEM	Signature	Total
Lattice-based	22	5	27
Code-based	19	3	22
Hash-based	0	3	3
Multivariate-based	2	7	9
Isogeny-based	1	0	1
Other	5	2	7
Total	49	20	69

Overview of the candidates

category \ primitive	PKE / KEM	Signature	Total
Lattice-based	$22 \rightarrow 9$	$5 \rightarrow 3$	$27 \rightarrow 12$
Code-based	$19 \rightarrow 7$	$3 \rightarrow 0$	$22 \rightarrow 7$
Hash-based	$0 \rightarrow 0$	$3 \rightarrow 2$	$3 \rightarrow 2$
Multivariate-based	$2 \rightarrow 0$	$7 \rightarrow 4$	$9 \rightarrow 4$
Isogeny-based	$1 \rightarrow 1$	$0 \rightarrow 0$	$1 \rightarrow 1$
Other	$5 \rightarrow 0$	$2 \rightarrow 0$	$7 \rightarrow 0$
Total	$49 \rightarrow 17$	$20 \rightarrow 9$	$69 \rightarrow 26$

Overview of the candidates

category \ primitive	PKE / KEM	Signature	Total
Lattice-based	$22 \to 9 \to 3+2$	$5 \to 3 \to 2+0$	$27 \to 12 \to 5+2$
Code-based	$19 \to 7 \to 1+2$	$3 \to 0 \to 0+0$	$22 \to 7 \to 1+2$
Hash-based	$0 \to 0 \to 0+0$	$3 \to 2 \to 0+2$	$3 \to 2 \to 0+2$
Multivariate-based	$2 \to 0 \to 0+0$	$7 \to 4 \to 1+1$	$9 \to 4 \to 1+1$
Isogeny-based	$1 \to 1 \to 0+1$	$0 \to 0 \to 0+0$	$1 \to 1 \to 0+1$
Other	$5 \to 0 \to 0+0$	$2 \to 0 \to 0+0$	$7 \to 0 \to 0+0$
Total	$49 \to 17 \to 4+5$	$20 \to 9 \to 3+3$	$69 \to 26 \to 7+8$

3rd round candidates

	Finalists	Alternates
PKE/KEM	Classic McEliece	BIKE
	CRYSTALS-KYBER	FrodoKEM
	NTRU	HQC
	SABER	NTRU Prime
		SIKE
Signature	CRYSTALS-DILITHIUM	GeMSS
	FALCON	Picnic
	Rainbow	SPHINCS+

3rd round candidates

	Finalists	Alternates
PKE/KEM	Classic McEliece	BIKE
	CRYSTALS-KYBER	FrodoKEM
	NTRU	HQC
	SABER	NTRU Prime
		SIKE
Signature	CRYSTALS-DILITHIUM	GeMSS
	FALCON	Picnic
	Rainbow	SPHINCS+

Lattice - Code - Hash - Multivariate - Isogeny

3rd round candidates

	Finalists	Alternates
PKE/KEM	Classic McEliece	BIKE
		HQC
Signature		

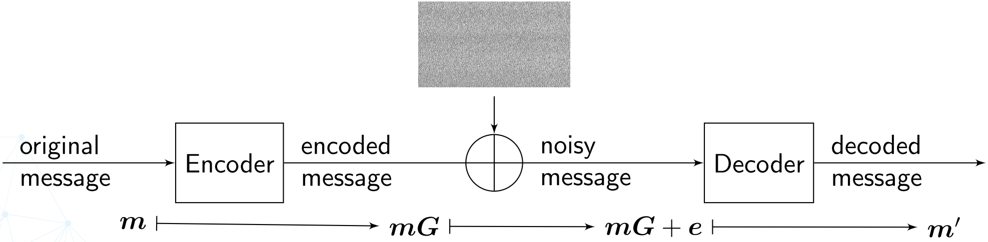
Lattice - Code - Hash - Multivariate - Isogeny

this talk

Outline

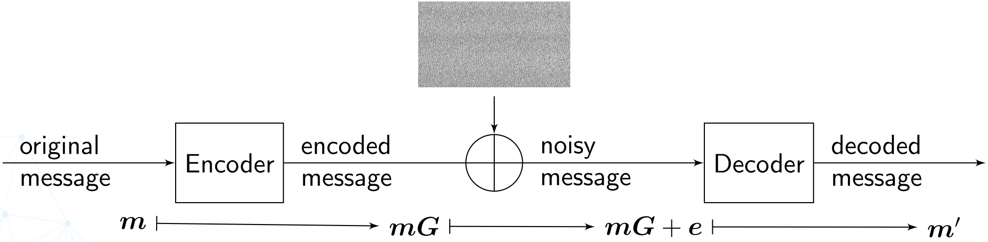
Coding theory

Coding theory is the science of (efficiently) adding redundancy to information in order to detect/correct errors that could occur during transmission.



Coding theory

Coding theory is the science of (efficiently) adding redundancy to information in order to detect/correct errors that could occur during transmission.

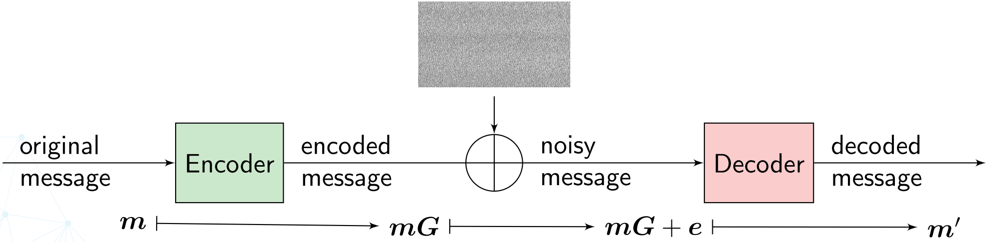


Preliminary remarks:

- Hopefully, we have $m' = m$

Coding theory

Coding theory is the science of (efficiently) adding redundancy to information in order to detect/correct errors that could occur during transmission.



Preliminary remarks:

- Hopefully, we have $m' = m$
- For code-based PKC, most of the time, public encoder / private decoder.

Definitions

Linear code

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

A linear code $\mathcal{C}[n, k]$ is fully determined by one of the following matrices:

Definitions

Linear code

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

A linear code $\mathcal{C}[n, k]$ is fully determined by one of the following matrices:

Generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$

$\mathcal{C} = \left\{ \mathbf{x}\mathbf{G}, \text{ for } \mathbf{x} \in \mathbb{F}_q^k \right\}$

Definitions

Linear code

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

A linear code $\mathcal{C}[n, k]$ is fully determined by one of the following matrices:

Generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$

$\mathcal{C} = \left\{ \mathbf{xG}, \text{ for } \mathbf{x} \in \mathbb{F}_q^k \right\}$

Parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k) \times n}$

$\mathcal{C} = \left\{ \boldsymbol{s} \in \mathbb{F}_q^n \text{ such that } \boldsymbol{H}\boldsymbol{s}^\top = \mathbf{0} \right\}$

Definitions

Linear code

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

A linear code $\mathcal{C}[n,k]$ is fully determined by one of the following matrices:

Generator matrix $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$

$\mathcal{C} = \left\{ \mathbf{xG}, \text{ for } \mathbf{x} \in \mathbb{F}_q^k \right\}$

Parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k) \times n}$

$\mathcal{C} = \left\{ \boldsymbol{s} \in \mathbb{F}_q^n \text{ such that } \boldsymbol{H}\boldsymbol{s}^\top = \mathbf{0} \right\}$

The Hamming weight of a word $\boldsymbol{u}$ is the number of its non-zero coordinates:

$$|\boldsymbol{u}| = \# \{ i \in \{0, \ldots, n-1\} \text{ such that } \boldsymbol{u}_i \neq 0 \}$$

$$\text{example : } \; |(0,1,0,0,1,0,1,0)| = 3$$

Hard problems for cryptography

Syndrome Decoding (SD) problem

Given $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$, find $\boldsymbol{x} \in \mathbb{F}_q^{n}$ of Hamming weight $|\boldsymbol{x}| \leq w$ such that:

$$\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{s}^\top.$$

Hard problems for cryptography

Syndrome Decoding (SD) problem

Given $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ of Hamming weight $|\boldsymbol{x}| \leq w$ such that:

$$\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{s}^\top.$$

Hard problems for cryptography

Syndrome Decoding (SD) problem

Given $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ and $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ of Hamming weight $|\boldsymbol{x}| \leq w$ such that:

$$\boldsymbol{H}\boldsymbol{x}^\top = \boldsymbol{s}^\top.$$

- The SD problem has been proved NP-complete [BMvT78]
- Hardest instances are obtained with w close to the Gilbert-Varshamov bound (essentially $w \approx n/9$ for $k = n/2$)
- Best-known algorithms: Information Set Decoding (ISD), see later

Outline

McEliece cryptosystem [McE78]

McEliece cryptosystem [McE78]

Let $\boldsymbol{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of a (binary Goppa) code $\mathcal{C}$ capable of correcting up to t errors (using decoding algorithm $\mathcal{D}_{\mathcal{C}}$).

McEliece cryptosystem [McE78]

Let $\boldsymbol{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of a (binary Goppa) code $\mathcal{C}$ capable of correcting up to t errors (using decoding algorithm $\mathcal{D}_{\mathcal{C}}$).

Legend: public-private-randomness

McEliece cryptosystem [McE78]

Let $\boldsymbol{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of a (binary Goppa) code $\mathcal{C}$ capable of correcting up to t errors (using decoding algorithm $\mathcal{D}_{\mathcal{C}}$).

Legend: public-private-randomness

Alice:

invertible matrix $\boldsymbol{S} \xleftarrow{\$} \mathbb{F}_2^{k \times k}$

permutation matrix $\boldsymbol{P} \xleftarrow{\$} \mathbb{F}_2^{n \times n}$

Alice → Bob: pk$=\left(\tilde{\boldsymbol{G}}=\boldsymbol{SGP}, t\right)$

Bob:

message $\mathbf{m} \in \mathbb{F}_2^k$

$\boldsymbol{e} \in \mathbb{F}_2^n$ such that $|\boldsymbol{e}| \leq t$

$\boldsymbol{c} = \boldsymbol{m}\tilde{\boldsymbol{G}} + \boldsymbol{e} \in \mathbb{F}_2^n$

Bob → Alice: $\boldsymbol{c}$

Alice:

$$\tilde{\boldsymbol{c}} = \mathcal{D}_{\mathcal{C}}\left(\boldsymbol{c}\boldsymbol{P}^{-1}\right) = \mathcal{D}_{\mathcal{C}}\left(\boldsymbol{m}\boldsymbol{S}\boldsymbol{G} + \boldsymbol{e}\boldsymbol{P}^{-1}\right)$$
$$\boldsymbol{m} = \tilde{\boldsymbol{c}}\boldsymbol{S}^{-1}$$

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal (1978)

Parameters	Key size	Security level
$[1024, 524, 101]_2$	≈ 67 KB	2^{62}
$[2048, 1608, 48]_2$	≈ 412 KB	2^{96}

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal (1978)

Parameters	Key size	Security level
$[1024, 524, 101]_2$	≈ 67 KB	2^{62}
$[2048, 1608, 48]_2$	≈ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k(\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal (1978)

Parameters	Key size	Security level
$[1024, 524, 101]_2$	≈ 67 KB	2^{62}
$[2048, 1608, 48]_2$	≈ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k(\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

Niederreiter's approach:

if $k > n - k$ then we can rewrite McEliece using the parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal (1978)

Parameters	Key size	Security level
$[1024, 524, 101]_2$	$\approx$ 67 KB	2^{62}
$[2048, 1608, 48]_2$	$\approx$ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k (\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

Niederreiter's approach:

if $k > n - k$ then we can rewrite McEliece using the parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$

pk size reduction:

Using structured codes, pk can have a more compact description.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal (1978)

Parameters	Key size	Security level
$[1024, 524, 101]_2$	≈ 67 KB	2^{62}
$[2048, 1608, 48]_2$	≈ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k(\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

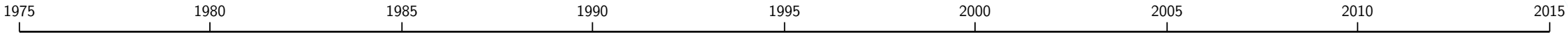
Niederreiter's approach:

if $k > n - k$ then we can rewrite McEliece using the parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$

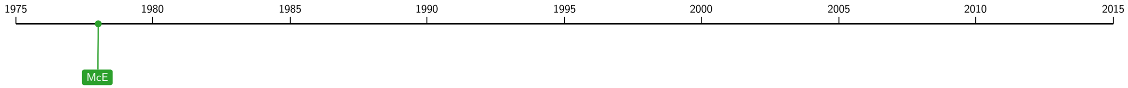
pk size reduction:

Using structured codes, pk can have a more compact description.

Instantiations and cryptanalyses

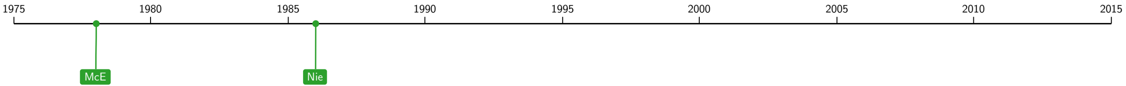


Instantiations and cryptanalyses



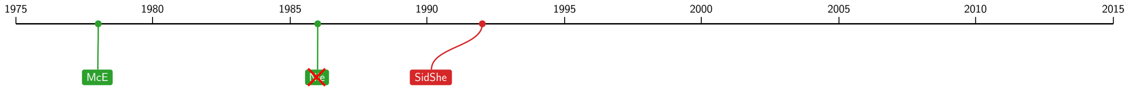
McEliece original proposal with binary Goppa codes [McE78]

Instantiations and cryptanalyses



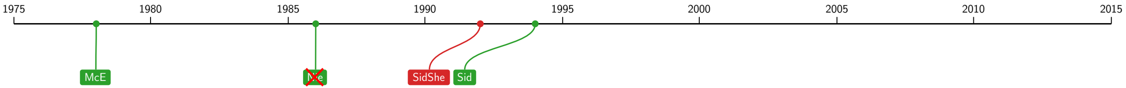
Niederreiter's (dual) approach, with GRS codes [Nie86]

Instantiations and cryptanalyses



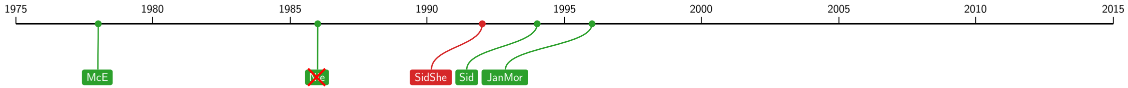
Sidelnikov Shestakov, cryptanalysis of Niederreiter's proposal [SS92]

Instantiations and cryptanalyses



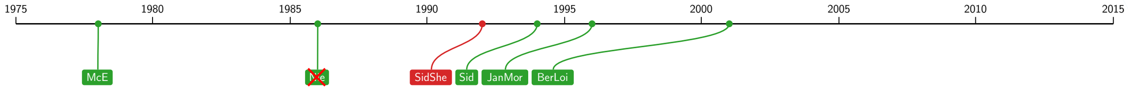
Sidelnikov proposes Reed-Muller codes [Sid94]

Instantiations and cryptanalyses



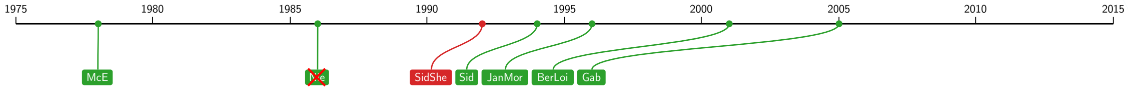
Janwa Moreno propose Alg. Geo. codes and their subfield subcodes [JM96]

Instantiations and cryptanalyses



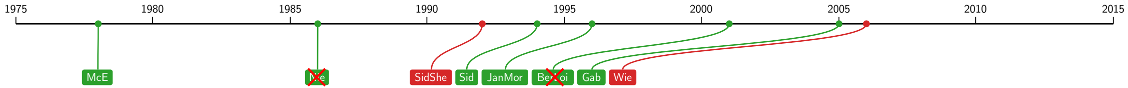
Berger Loidreau, propose subcodes of GRS codes [BL04]

Instantiations and cryptanalyses



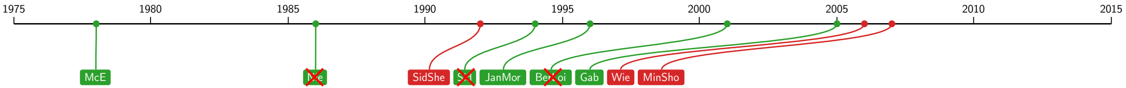
Gaborit proposes QC-BCH codes [Gab05]

Instantiations and cryptanalyses



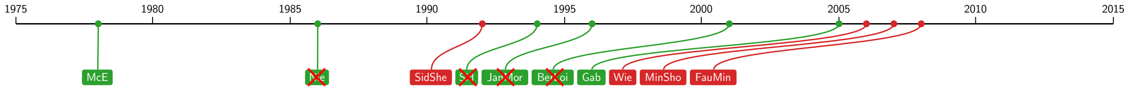
Wieschebrink's square attack: $\mathcal{C} \star \mathcal{C}$ [Wie06]

Instantiations and cryptanalyses



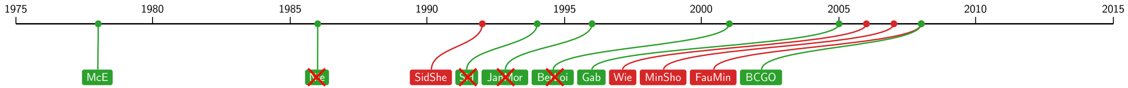
Minder Shokrollahi, subexponential time attack on RM codes [MS07]

Instantiations and cryptanalyses



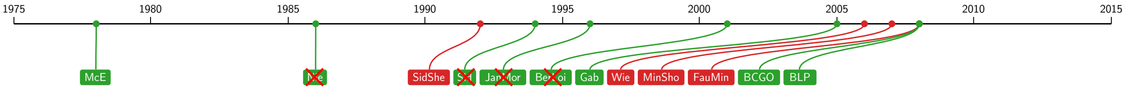
Faure Minder, attack on AG codes for genus ≤ 2 [FM08]

Instantiations and cryptanalyses



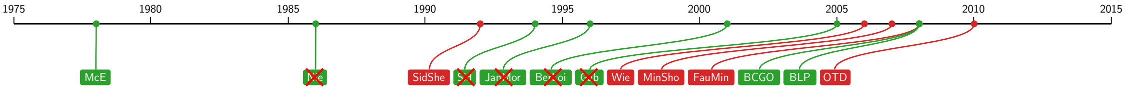
Berger Cayrel Gaborit Otmani, propose QC alternant codes [BCGO09]

Instantiations and cryptanalyses



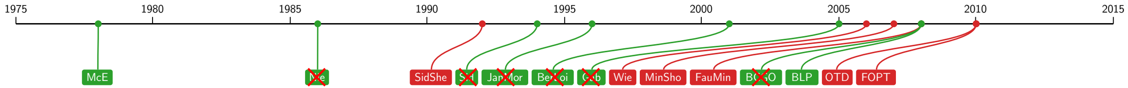
Bernstein Lange Peters, propose q-ary "wild" Goppa codes [BLP10]

Instantiations and cryptanalyses



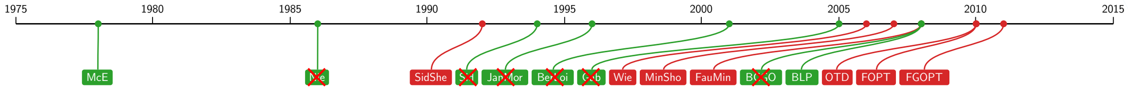
Otmani Tillich Dallot, Attacks on QC codes [OTD10]

Instantiations and cryptanalyses



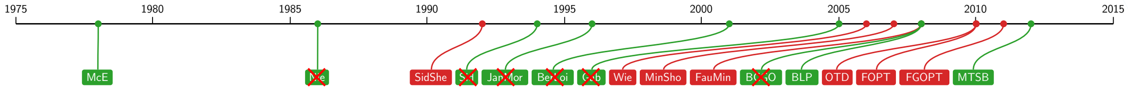
Faugère Otmani Perret Tillich, more attacks on QC codes [FOPT10]

Instantiations and cryptanalyses



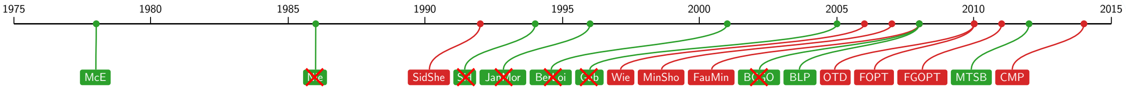
Faugère Otmani Gautier Perret Tillich, distinguisher high rate goppa codes [FGUO^{+}13]

Instantiations and cryptanalyses



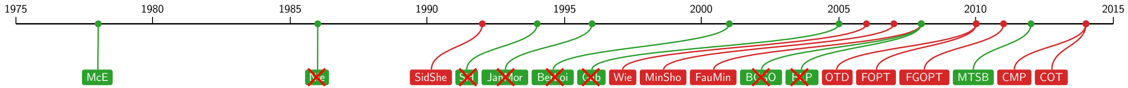
Misoczki Tillich Sendrier Barreto, propose (QC-)MDPC codes [MTSB13]

Instantiations and cryptanalyses



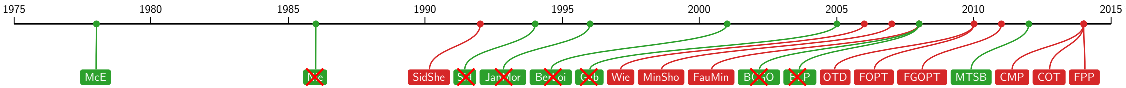
Couvreur Márquez Pellikaan, attack on AG codes [CMCP14]

Instantiations and cryptanalyses



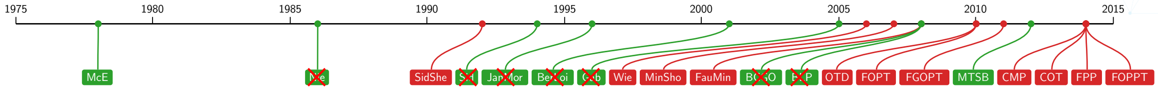
Couvreur Otmani Tillich, Goppa codes with $m = 2$ [COT14]

Instantiations and cryptanalyses



Faugère Perret Portzamparc, some Goppa codes with $m = 2, 3$ [FPdP14]

Instantiations and cryptanalyses



Faugère Otmani Perret Portzamparc Tillich, Further attack on QC and QD codes [FOP+16]

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal

Parameters	Key size	Security level
$[1024, 524, 101]_2$	$\approx$ 67 KB	2^{62}
$[2048, 1608, 48]_2$	$\approx$ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k(\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

Niederreiter's approach:

if $k > n - k$ then we can rewrite McEliece using the parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$

pk size reduction:

Using structured codes, pk can have a more compact description.

Key sizes and Niederreiter's approach

McEliece' security is clearly based on the hardness of "decoding efficiently" a "seemingly" random code.

Efficiently decode (polynomial-time) sufficiently many errors to recover the plaintext.

The public generator (or parity-check) matrix should not reveal the code structure.

McEliece original proposal

Parameters	Key size	Security level
$[1024, 524, 101]_2$	≈ 67 KB	2^{62}
$[2048, 1608, 48]_2$	≈ 412 KB	2^{96}

pk $= \boldsymbol{G}$ of size: $n \times k(\times \log_2(q))$.
Unpractical in 1978, doable in 2020.

Niederreiter's approach:

if $k > n - k$ then we can rewrite McEliece using the parity-check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$

pk size reduction:

Using structured codes, pk can have a more compact description.

Outline

SD problem and Information Set Decoding

Best approach to solve the SD problem: Information Set Decoding (ISD).

Definition: information set

Let $\mathcal{C}[n,k]$ be a linear code generated by $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$. An information set $\mathcal{I}$ of $\mathcal{C}$ is a subset of $\{1,\ldots,n\}$ that completely describes the code $\mathcal{C}$ (hence $\#\mathcal{I} = k$).

SD problem and Information Set Decoding

Best approach to solve the SD problem: Information Set Decoding (ISD).

Definition: information set

Let $\mathcal{C}[n,k]$ be a linear code generated by $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$. An information set $\mathcal{I}$ of $\mathcal{C}$ is a subset of $\{1,\dots,n\}$ that completely describes the code $\mathcal{C}$ (hence $\#\mathcal{I} = k$).

Prange ISD [Pra62] algorithm main steps

1. Sample an information set $\mathcal{I}$ of $\mathcal{C}$
2. Assume $\mathcal{I}$ is error-free, then $\boldsymbol{c}_i = \boldsymbol{m}_i$ for $i \in \mathcal{I}$
3. Retreive message $\boldsymbol{m}$ from ciphertext $\boldsymbol{c}$ using linear algebra
4. If $|\boldsymbol{e}| = t$ output $\boldsymbol{m}$, else restart ($\mathcal{I}$ was not error-free)

SD problem and Information Set Decoding

Best approach to solve the SD problem: Information Set Decoding (ISD).

Definition: information set

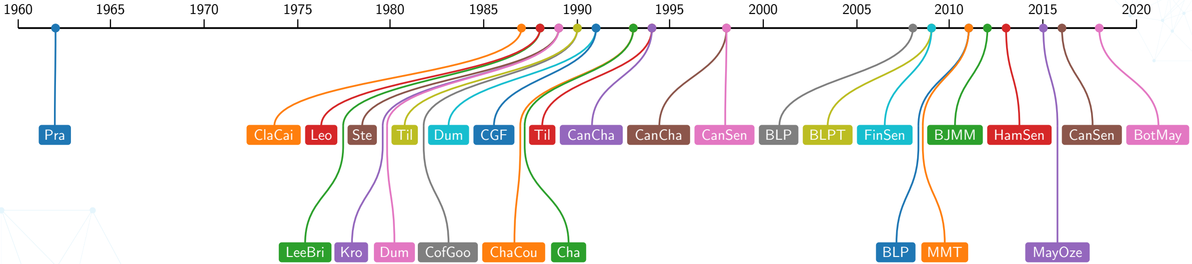
Let $\mathcal{C}[n,k]$ be a linear code generated by $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$. An information set $\mathcal{I}$ of $\mathcal{C}$ is a subset of $\{1,\ldots,n\}$ that completely describes the code $\mathcal{C}$ (hence $\#\mathcal{I} = k$).

Prange ISD [Pra62] algorithm main steps

1. Sample an information set $\mathcal{I}$ of $\mathcal{C}$
2. Assume $\mathcal{I}$ is error-free, then $\boldsymbol{c}_i = \boldsymbol{m}_i$ for $i \in \mathcal{I}$
3. Retreive message $\boldsymbol{m}$ from ciphertext $\boldsymbol{c}$ using linear algebra
4. If $|\boldsymbol{e}| = t$ output $\boldsymbol{m}$, else restart ($\mathcal{I}$ was not error-free)

Complexity: $\left(\frac{1}{1-\frac{k}{n}} + o(1)\right)^t$ with $t = \Theta\left(\frac{n}{\log n}\right) \longrightarrow$ pk size: $(c+o(1))\,\lambda^2 \log_2(\lambda)^2$ bits

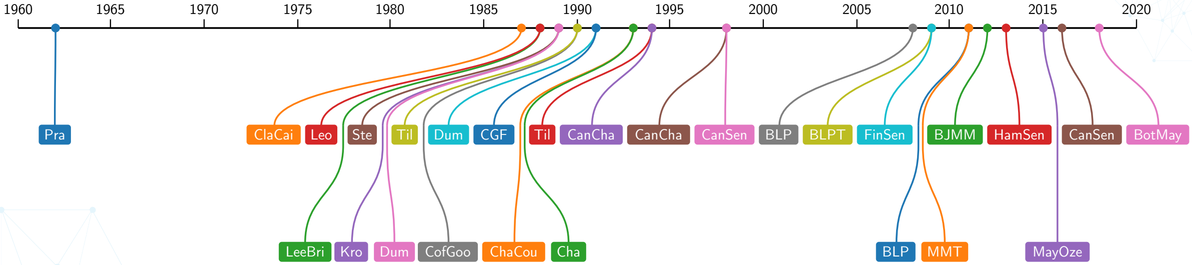
Information Set Decoding improvements



References:

- [Pra62]
- [CC81]
- [LB88]
- [Leo88]
- [Kro89]
- [Ste88]
- [CG90]
- [vT90]
- [Dum91]
- [CGF91]
- [Cha92]
- [CC93]
- [vT94]
- [CC94]
- [CC98]
- [CS98]
- [BLP08]
- [BLPvT09]
- [FS09]
- [BLP11]
- [MMT11]
- [BJMM12]
- [HS13]
- [MO15]
- [CS16]
- [BM18]

Information Set Decoding improvements



≈ 60 years of research: same complexity, same constant in exponent, slightly improved $o(1)$

References:
- [Pra62]
- [CC81]
- [LB88]
- [Leo88]
- [Kro89]
- [Ste88]
- [CG90]
- [vT90]
- [Dum91]
- [CGF91]
- [Cha92]
- [CC93]
- [vT94]
- [CC94]
- [CC98]
- [CS98]
- [BLP08]
- [BLPvT09]
- [FS09]
- [BLP11]
- [MMT11]
- [BJMM12]
- [HS13]
- [MO15]
- [CS16]
- [BM18]

Outline

BIKE – bit flipping key encapsulation [AAB+19]

BIKE – bit flipping key encapsulation [AAB+19]

$h_0, h_1 \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$ with h_0 invertible

$h \leftarrow h_1 h_0^{-1}$

message $m \in \mathbb{F}_2^k$

pk=(h, t) $\longrightarrow$

$e_0, e_1 \leftarrow \mathcal{H}(m) \in \mathcal{S}_t{}^n(\mathbb{F}_2)$

$c = e_0 + e_1 h \in \mathbb{F}_2^n$

$\xleftarrow{\quad c \quad}$

$e_0, e_1 \leftarrow$ Bit-Flipping(c, h_0, h_1)

BIKE – bit flipping key encapsulation [AAB+19]

Alice:

$\mathbf{h}_0, \mathbf{h}_1 \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$ with $\mathbf{h}_0$ invertible

$\mathbf{h} \leftarrow \mathbf{h}_1 \mathbf{h}_0^{-1}$

$\xrightarrow{\text{pk}=(\mathbf{h},t)}$

Bob:

message $\mathbf{m} \in \mathbb{F}_2^k$

$\mathbf{e}_0, \mathbf{e}_1 \leftarrow \mathcal{H}(\mathbf{m}) \in \mathcal{S}_t{}^n(\mathbb{F}_2)$

$\mathbf{c} = \mathbf{e}_0 + \mathbf{e}_1 \mathbf{h} \in \mathbb{F}_2^n$

$\xleftarrow{\mathbf{c}}$

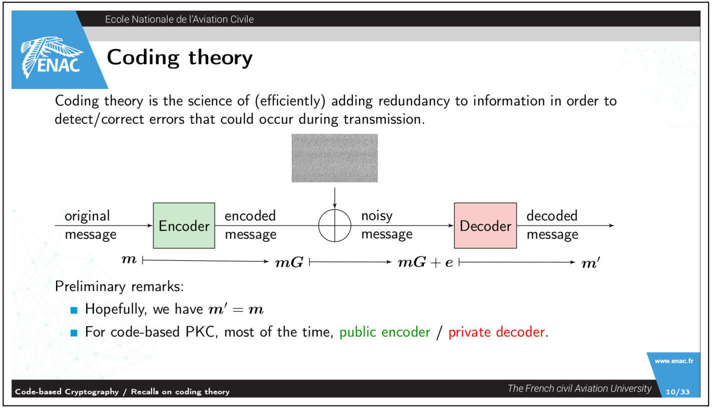
Alice:

$\mathbf{e}_0, \mathbf{e}_1 \leftarrow$ Bit-Flipping$(\mathbf{c}, \mathbf{h}_0, \mathbf{h}_1)$

Shared key derived from $\mathbf{e}_0, \mathbf{e}_1$

HQC [ABD+18]

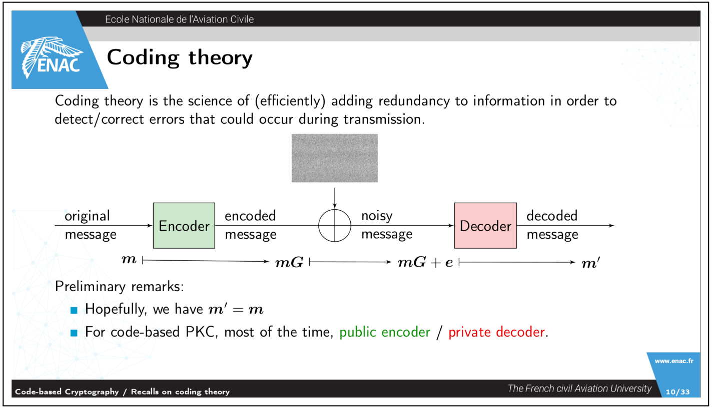
HQC [ABD+18]


Ecole Nationale de l'Aviation Civile
Coding theory
Coding theory is the science of (efficiently) adding redundancy to information in order to detect/correct errors that could occur during transmission.
original message
Encoder
encoded message
noisy message
Decoder
decoded message
$m \longmapsto mG \longmapsto mG + e \longmapsto m'$
Preliminary remarks:
Hopefully, we have $m' = m$
For code-based PKC, most of the time, public encoder / private decoder.
www.enac.fr
Code-based Cryptography / Recalls on coding theory
The French civil Aviation University
10/33

HQC [ABD+18]

HQC uses a **public** decoder!

The secret key allows to remove more errors.

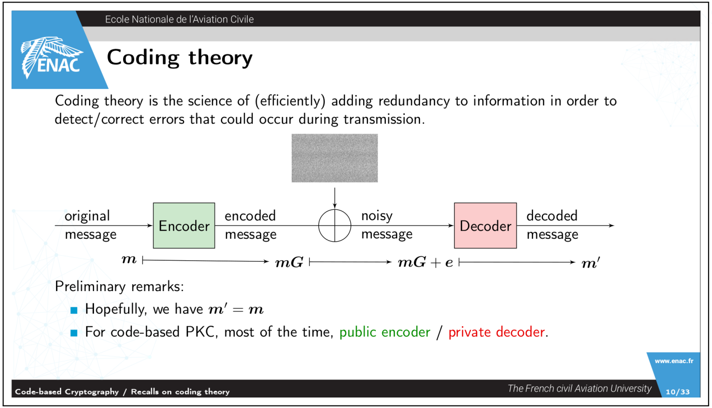


HQC [ABD+18]

HQC uses a **public** decoder!

The secret key allows to remove more errors.

The public key won't leak the (public) decoding algorithm!

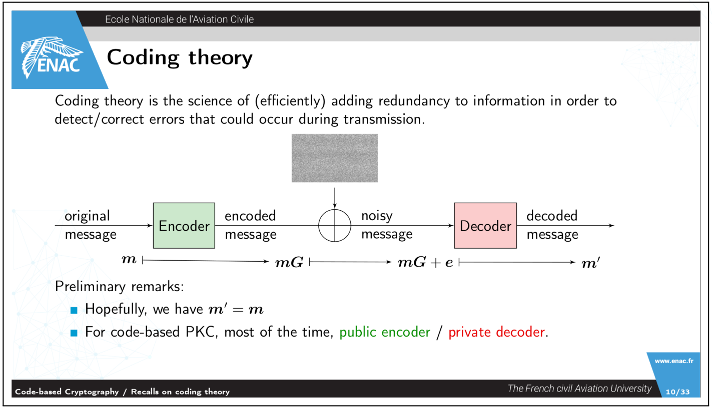


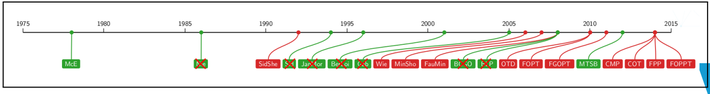
HQC [ABD+18]

HQC uses a **public** decoder!

The secret key allows to remove more errors.

The public key won't leak the (public) decoding algorithm!





HQC [ABD+18]

Let $G \in \mathbb{F}_2^{k \times n}$ be a generator matrix of a **any** code $\mathcal{C}$ capable of correcting up to t errors (using **public** decoding algorithm $\mathcal{D}_{\mathcal{C}}$).

HQC [ABD+18]

Let $G \in \mathbb{F}_2^{k\times n}$ be a generator matrix of a **any** code $\mathcal{C}$ capable of correcting up to t errors (using **public** decoding algorithm $\mathcal{D}_{\mathcal{C}}$).

Alice:

$$\boldsymbol{x},\boldsymbol{y} \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$$

$$\boldsymbol{h} \xleftarrow{\$} \mathbb{F}_2^n,\ \boldsymbol{s} \leftarrow \boldsymbol{x} + \boldsymbol{y}\boldsymbol{h}$$

$$\xrightarrow{\text{pk}=(\boldsymbol{h},\boldsymbol{s},t)}$$

Bob:

message $\boldsymbol{m} \in \mathbb{F}_2^k$

$$\boldsymbol{e}_0,\boldsymbol{e}_1,\boldsymbol{e} \xleftarrow{\$} {\mathcal{S}_t}^n(\mathbb{F}_2)$$

$$\boldsymbol{c}_0 = \boldsymbol{e}_0 + \boldsymbol{e}_1\boldsymbol{h} \in \mathbb{F}_2^n$$

$$\boldsymbol{c}_1 = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\boldsymbol{e}_1 + \boldsymbol{e} \in \mathbb{F}_2^n$$

$$\xleftarrow{\boldsymbol{c}_0,\boldsymbol{c}_1}$$

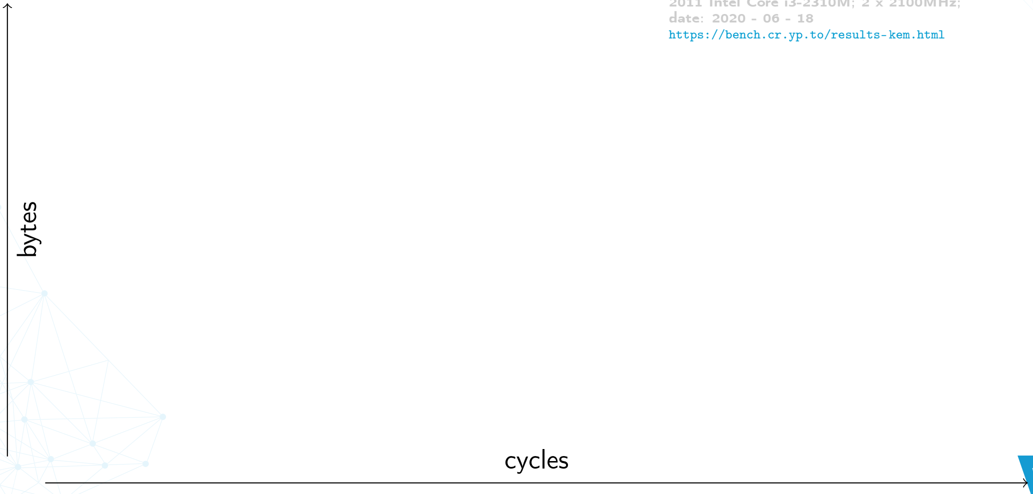
Alice:

$$\boldsymbol{m} \leftarrow \mathcal{D}_{\mathcal{C}}(\boldsymbol{c}_0 - \boldsymbol{c}_1\boldsymbol{y})$$

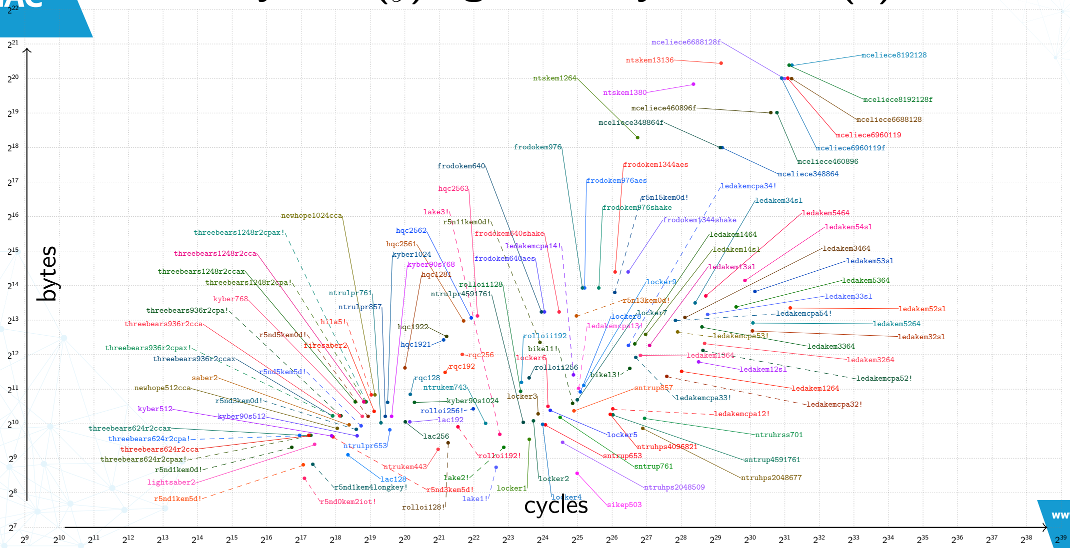
Outline

Public key size (y) against KeyGen time (x)

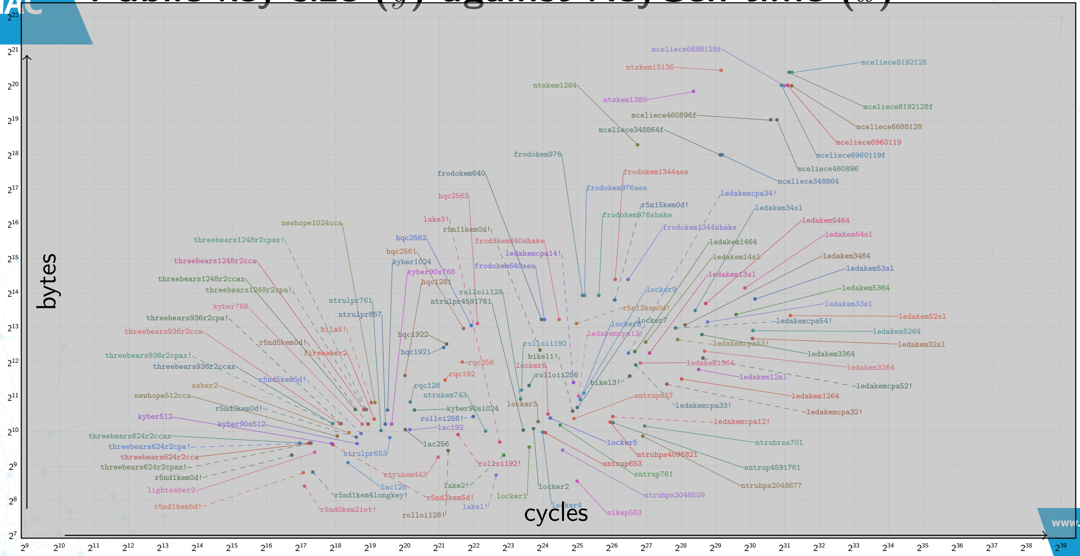
Source: supercop
amd64; Sandy Bridge (206a7);
2011 Intel Core i3-2310M; 2 x 2100MHz;
date: 2020 - 06 - 18
https://bench.cr.yp.to/results-kem.html



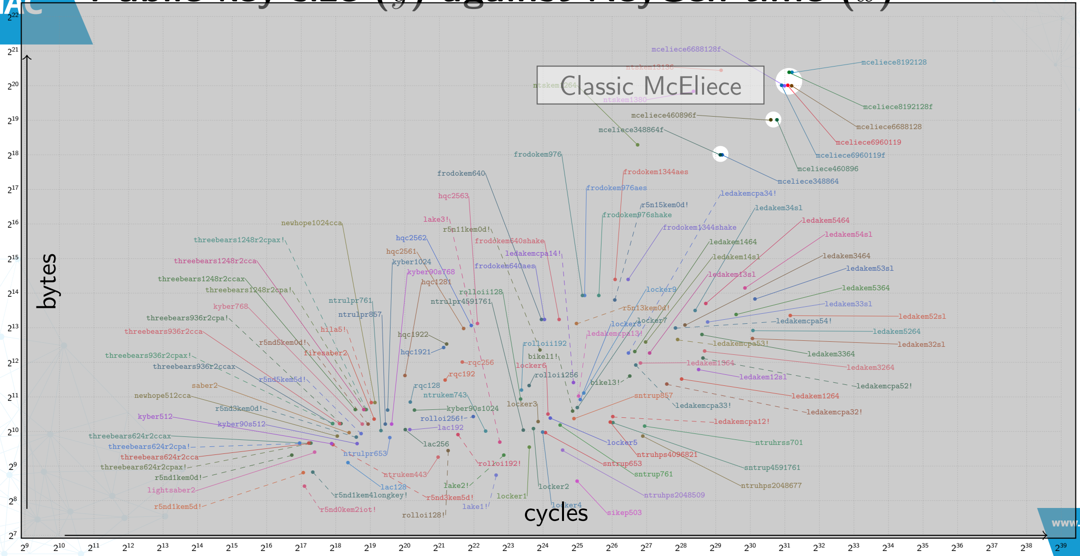
Public key size (y) against KeyGen time (x)



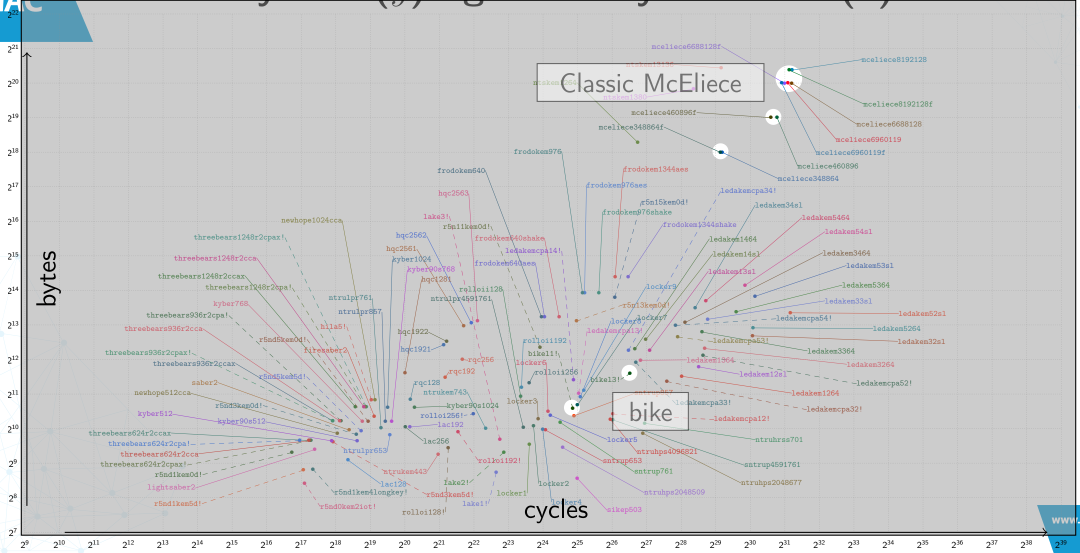
Public key size (y) against KeyGen time (x)



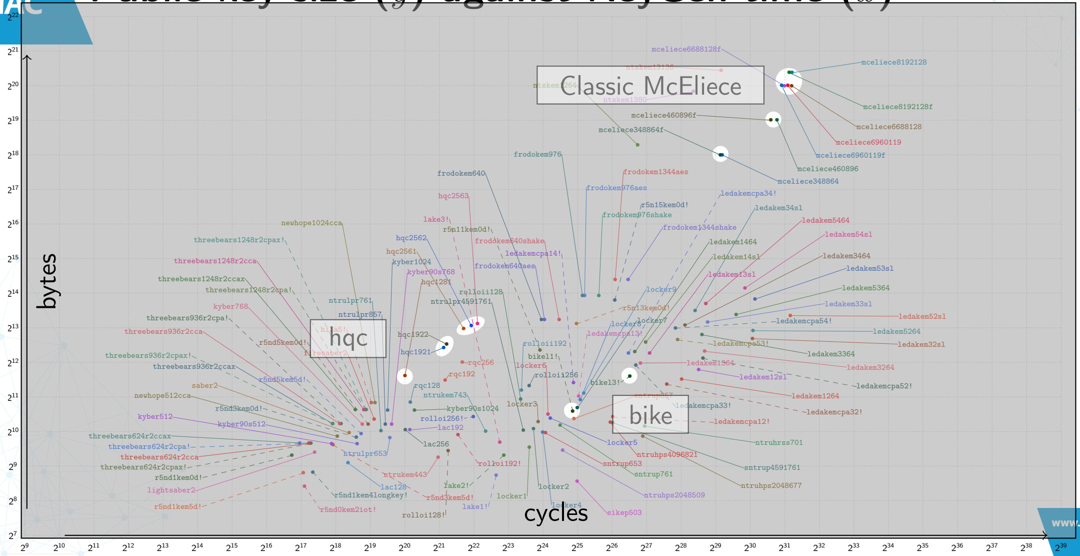
Public key size (y) against KeyGen time (x)



Public key size (y) against KeyGen time (x)

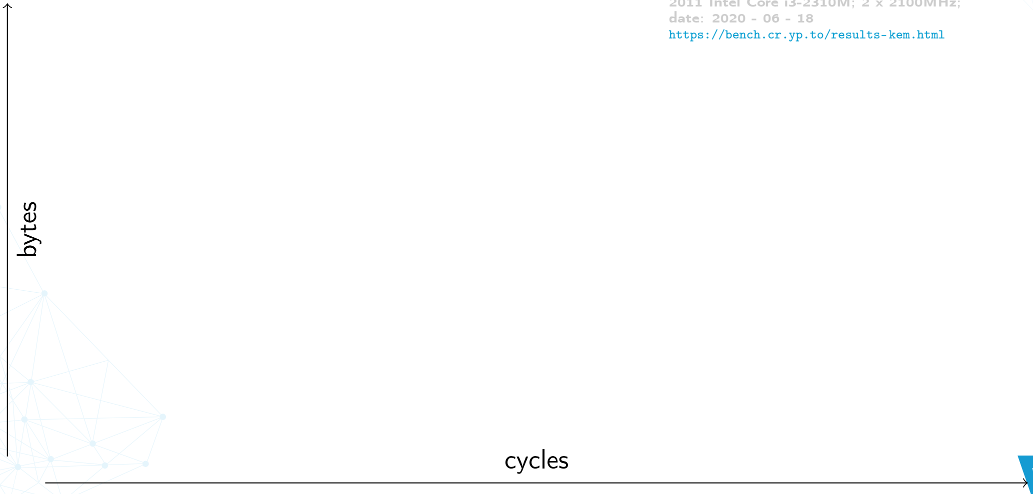


Public key size (y) against KeyGen time (x)

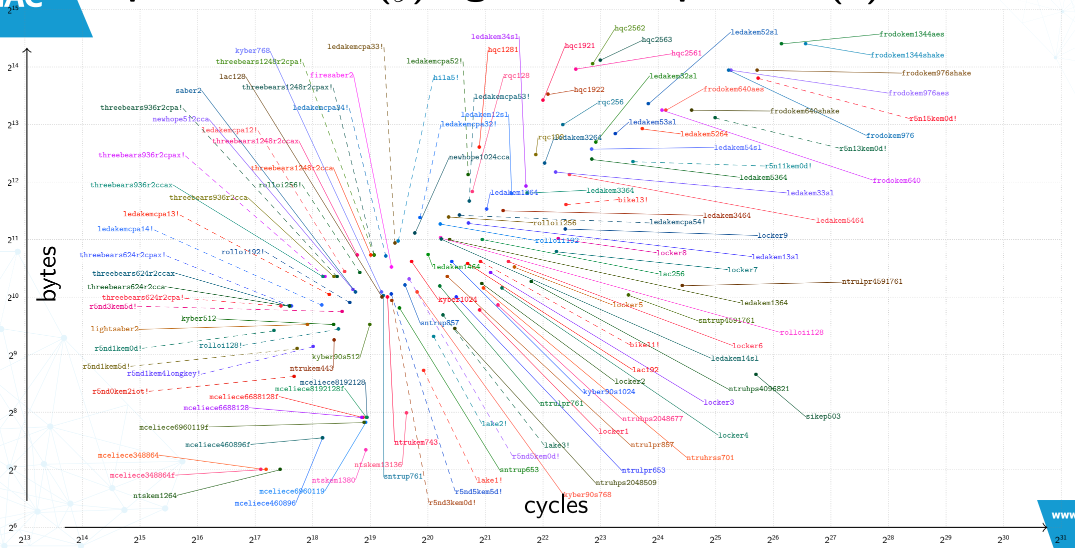


Ciphertext size (y) against Encaps time (x)

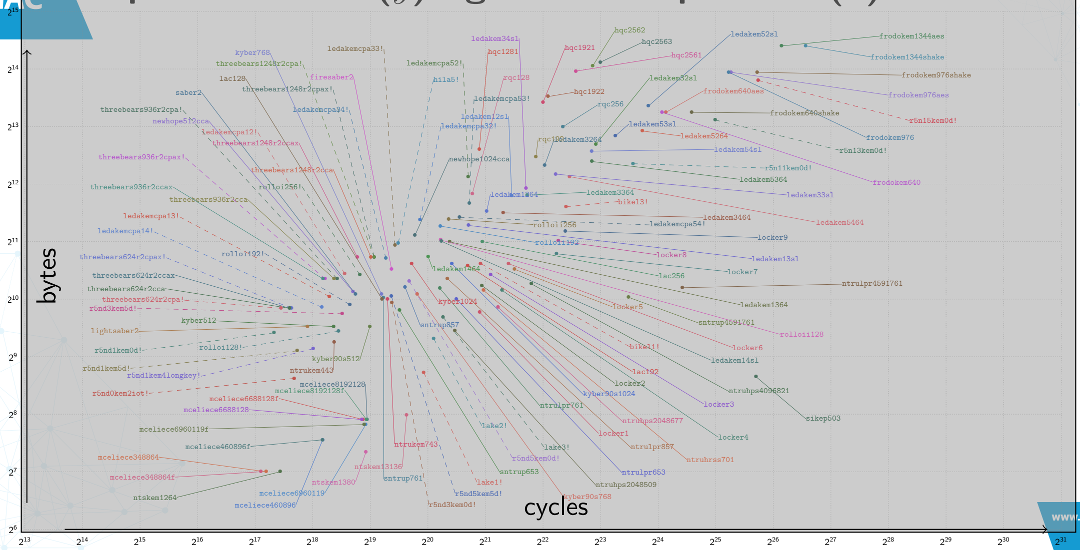
Source: supercop
amd64; Sandy Bridge (206a7);
2011 Intel Core i3-2310M; 2 x 2100MHz;
date: 2020 - 06 - 18
https://bench.cr.yp.to/results-kem.html



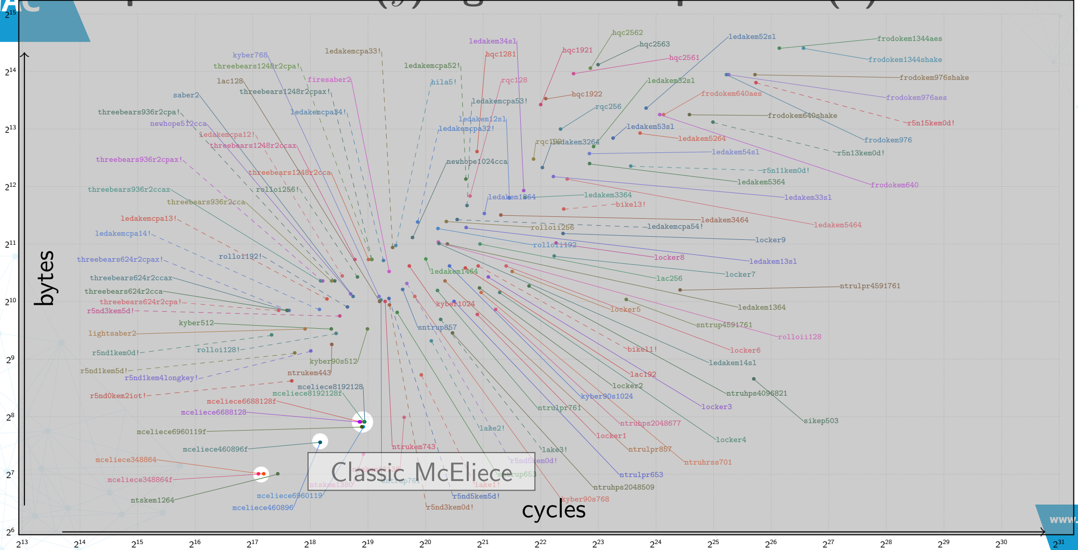
Ciphertext size (y) against Encaps time (x)



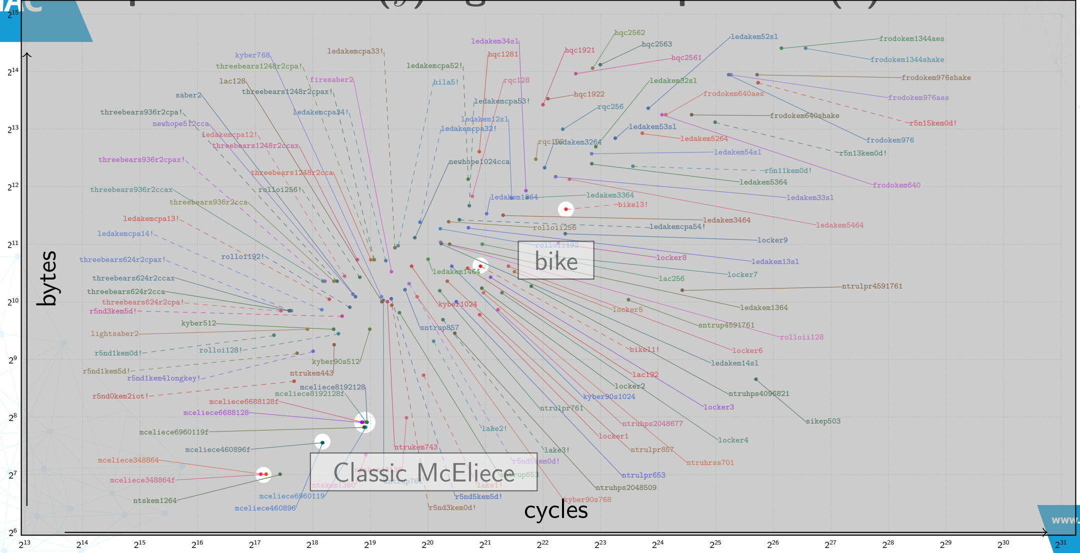
Ciphertext size (y) against Encaps time (x)



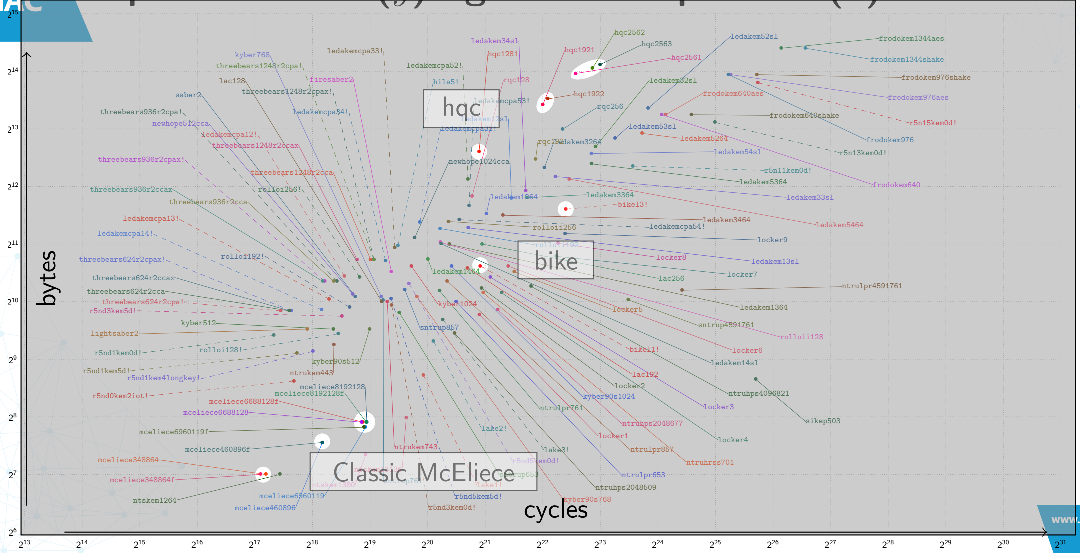
Ciphertext size (y) against Encaps time (x)



Ciphertext size (y) against Encaps time (x)

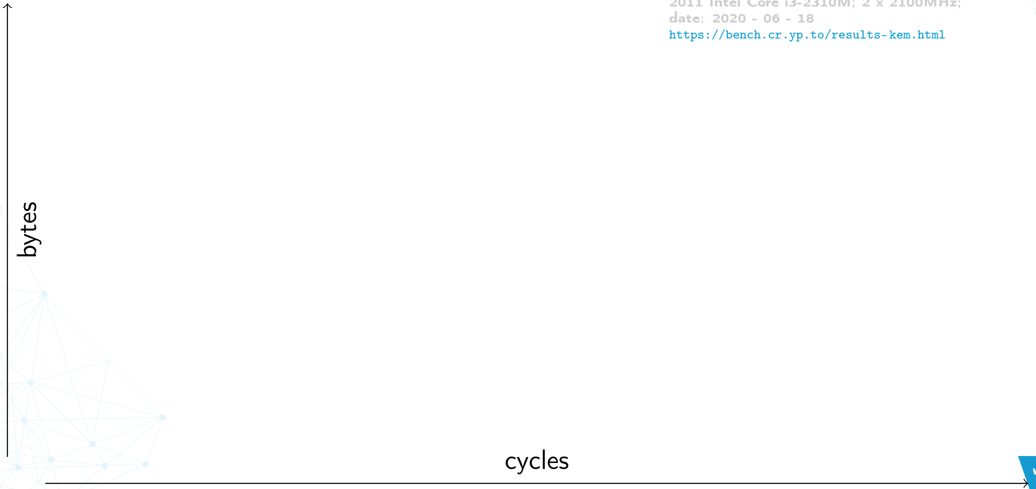


Ciphertext size (y) against Encaps time (x)

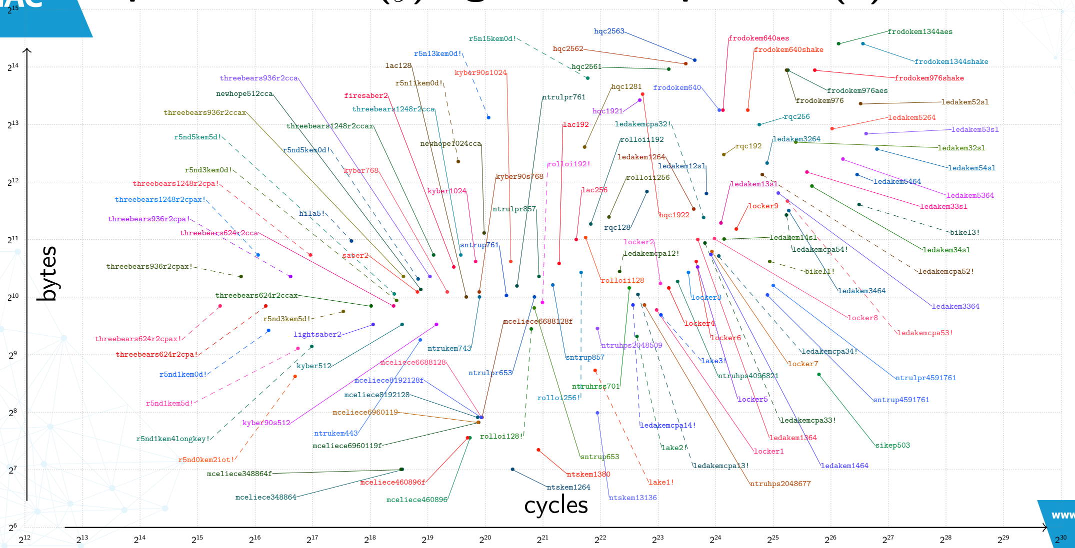


Ciphertext size (y) against Decaps time (x)

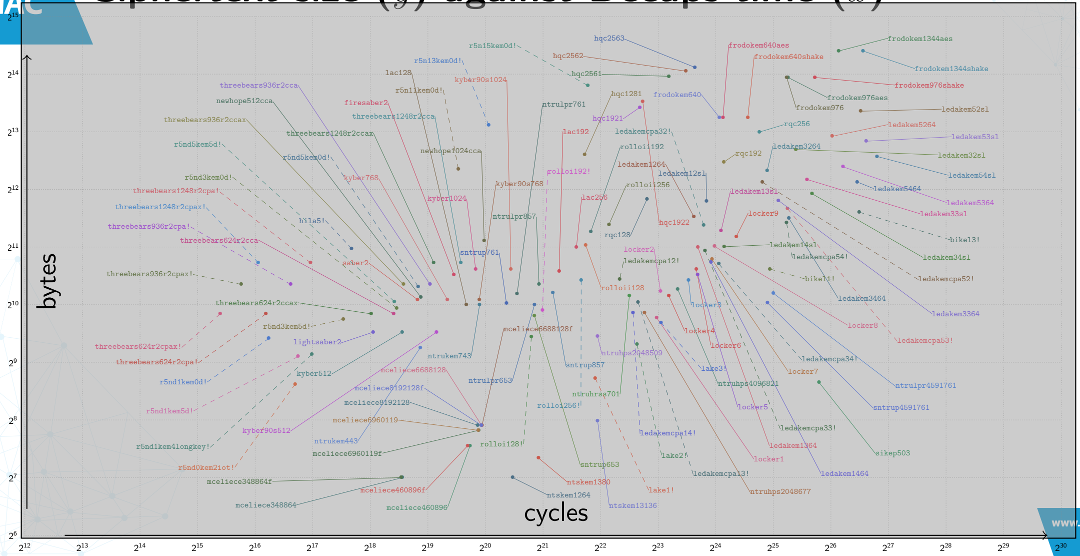
Source: supercop
amd64; Sandy Bridge (206a7);
2011 Intel Core i3-2310M; 2 x 2100MHz;
date: 2020 - 06 - 18
https://bench.cr.yp.to/results-kem.html



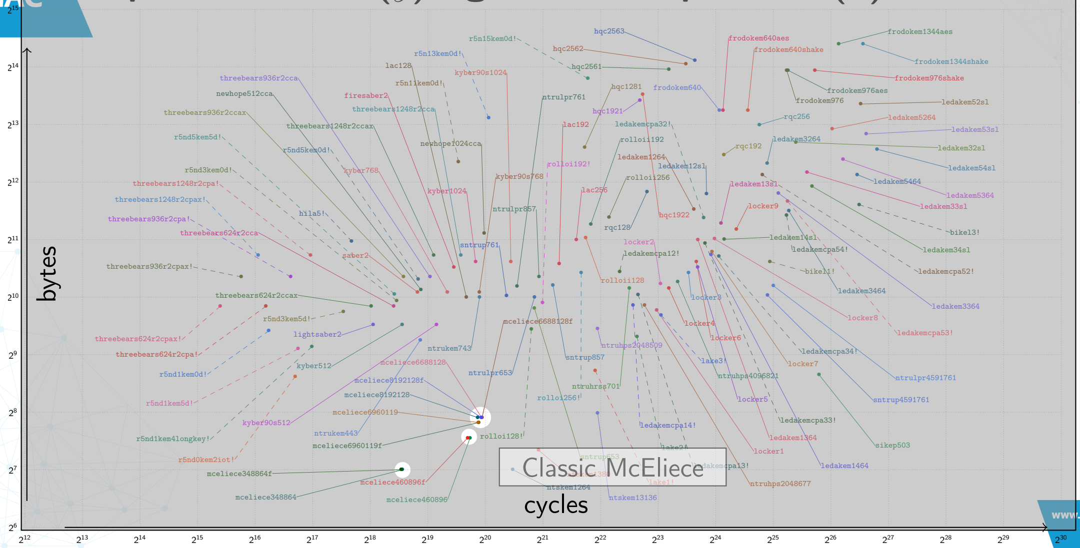
Ciphertext size (y) against Decaps time (x)



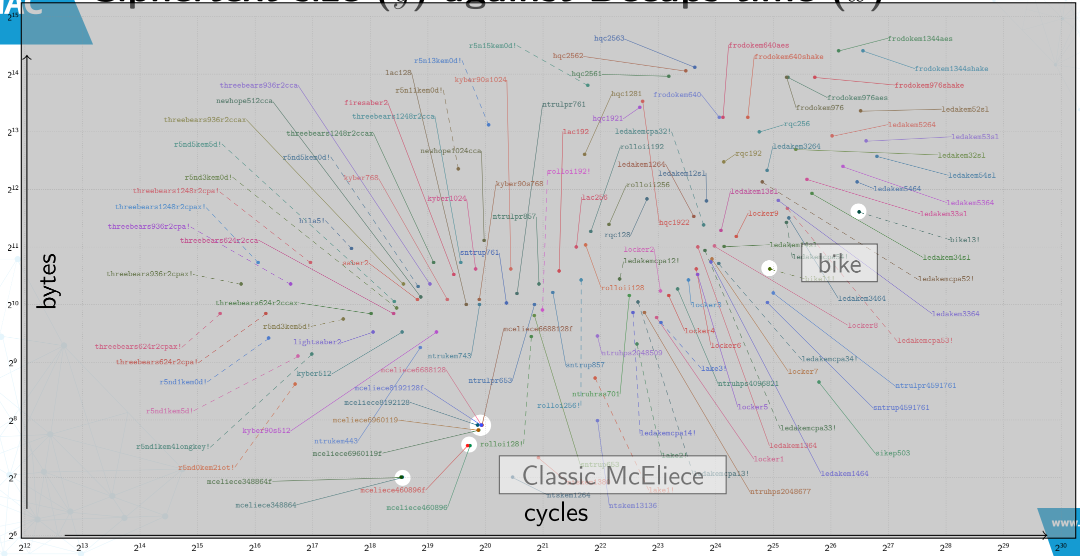
Ciphertext size (y) against Decaps time (x)



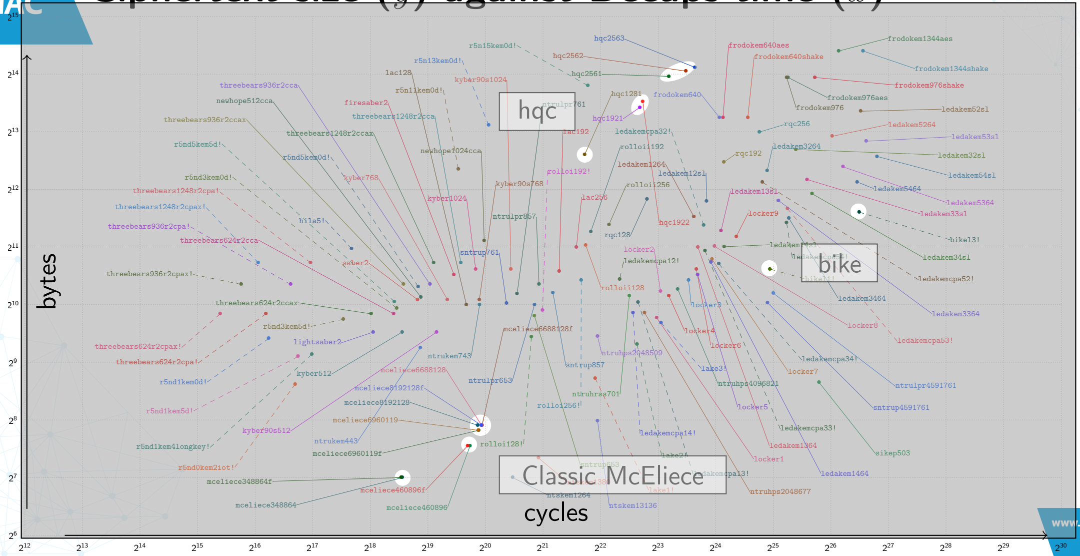
Ciphertext size (y) against Decaps time (x)



Ciphertext size (y) against Decaps time (x)



Ciphertext size (y) against Decaps time (x)



Energy-consumption (mJ)

		KeyGen	Encaps	Decaps
Classic McEliece	128	6384.90	1.84	588.10
	192	11632.40	3.09	1497.50
	256	38234.60	4.81	2625.30
BIKE	128	11.85	2.70	46.30
	192	38.29	8.75	119.60
	256	85.95	21.54	270.70
HQC	128	8.76	18.42	27.03
	192	25.68	41.81	70.26
	256	49.80	87.53	145.55

Ongoing work: hardware implementation for HQC

For security level 1, targeting 128 bits of security

		LUT	FF	Slices	BRAM	Freq	kcycles	μs
Classic McEliece	KeyGen	25 327	49 383	—	168	108	1 600	14 800
	Encaps	25 327	49 383	—	168	108	2.7	25.2
	Decaps	25 327	49 383	—	168	108	18.3	169.8
BIKE	KeyGen	29 448	5 498	8 419	28	96	259	2 691
	Encaps	29 448	5 498	8 419	28	96	12	127
	Decaps	29 448	5 498	8 419	28	96	13 120	136 443
HQC*	KeyGen	1 589	1 369	580	15	150	80	528
	Encaps	2 817	2 720	1 165	22	150	162	1 067
	Decaps	5 726	4 612	2 066	46	150	225	1 487

* preliminary results, simulation only...

Brief summary of the last CBC candidates' features

Classic McEliece	BIKE	HQC
Algebraic codes in H. metric	Non-algebraic codes in Hamming metric	
binary Goppa codes	Quasi-Cyclic Moderate Density Parity-Check Codes	
■ longevity ■ super fast encrypt ■ ridiculously small ct ■ fast decrypt ■ biggest pk ■ slowest KeyGen ■ energy-consuming	■ originally proposed in 2012 ■ small pk ■ reasonable ct ■ energy-efficient ■ slow decrypt ■ slow KeyGen	■ reasonable pk ■ fast KeyGen ■ reasonable encrypt ■ energy-efficient ■ security assumption ■ decryption failure analysis ■ hardware compact ■ somehow young (2016) ■ pk/ct larger than BIKE

Outline

Conclusions

- Code-based public key cryptography stands as a strong PQC candidate:
  - long standing / strong original proposal by McEliece
  - best-known classical attacks well understood *and* stable for ~ 60 years
  - pretty clear quantum impact (Grover) over key sizes

Conclusions

- Code-based public key cryptography stands as a strong PQC candidate:
  - long standing / strong original proposal by McEliece
  - best-known classical attacks well understood *and* stable for ~ 60 years
  - pretty clear quantum impact (Grover) over key sizes
- Several ways to circumvent key sizes issues:
  - Niederreiter’s approach
  - Structured matrices/codes

Conclusions

- Code-based public key cryptography stands as a strong PQC candidate:
  - long standing / strong original proposal by McEliece
  - best-known classical attacks well understood *and* stable for ~ 60 years
  - pretty clear quantum impact (Grover) over key sizes
- Several ways to circumvent key sizes issues:
  - Niederreiter's approach
  - Structured matrices/codes
- Existing approaches to securely use structured codes:
  - multiple proposals were broken by distinguishing the disguised code
  - issue thwarted using Alekhnovich's approach (*e.g.* HQC/RQC)

Conclusions

- Code-based public key cryptography stands as a strong PQC candidate:
  - long standing / strong original proposal by McEliece
  - best-known classical attacks well understood *and* stable for ~ 60 years
  - pretty clear quantum impact (Grover) over key sizes
- Several ways to circumvent key sizes issues:
  - Niederreiter's approach
  - Structured matrices/codes
- Existing approaches to securely use structured codes:
  - multiple proposals were broken by distinguishing the disguised code
  - issue thwarted using Alekhnovich's approach (*e.g.* HQC/RQC)
- KEM constructions allow for versatile, efficient, and secure encryption

Conclusions

- Code-based public key cryptography stands as a strong PQC candidate:
  - long standing / strong original proposal by McEliece
  - best-known classical attacks well understood *and* stable for ~ 60 years
  - pretty clear quantum impact (Grover) over key sizes
- Several ways to circumvent key sizes issues:
  - Niederreiter's approach
  - Structured matrices/codes
- Existing approaches to securely use structured codes:
  - multiple proposals were broken by distinguishing the disguised code
  - issue thwarted using Alekhnovich's approach (*e.g.* HQC/RQC)
- KEM constructions allow for versatile, efficient, and secure encryption

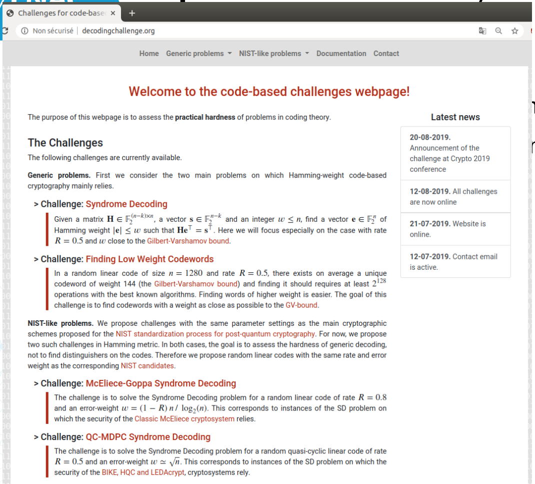
Code-based crypto is ready, mature enough for standardization!

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment

Aspects that could/should be improved



Challenges for code-base

Non sécurisé | decodingchallenge.org

Home Generic problems NIST-like problems Documentation Contact

Welcome to the code-based challenges webpage!

The purpose of this webpage is to assess the **practical hardness** of problems in coding theory.

The Challenges

The following challenges are currently available.

Generic problems. First we consider the two main problems on which Hamming-weight code-based cryptography mainly relies.

> Challenge: Syndrome Decoding

Given a matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, a vector $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and an integer $w \leq n$, find a vector $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight $|\mathbf{e}| \leq w$ such that $\mathbf{He}^\top = \mathbf{s}^\top$. Here we will focus especially on the case with rate $R = 0.5$ and w close to the Gilbert-Varshamov bound.

> Challenge: Finding Low Weight Codewords

In a random linear code of size $n = 1280$ and rate $R = 0.5$, there exists on average a unique codeword of weight 144 (the Gilbert-Varshamov bound) and finding it should requires at least 2^{128} operations with the best known algorithms. Finding words of higher weight is easier. The goal of this challenge is to find codewords with a weight as close as possible to the GV-bound.

NIST-like problems. We propose challenges with the same parameter settings as the main cryptographic schemes proposed for the NIST standardization process for post-quantum cryptography. For now, we propose two such challenges in Hamming metric. In both cases, the goal is to assess the hardness of generic decoding, not to find distinguishers on the codes. Therefore we propose random linear codes with the same rate and error weight as the corresponding NIST candidates.

> Challenge: McEliece-Goppa Syndrome Decoding

The challenge is to solve the Syndrome Decoding problem for a random linear code of rate $R = 0.8$ and an error-weight $w = (1-R)\,n/\log_2(n)$. This corresponds to instances of the SD problem on which the security of the Classic McEliece cryptosystem relies.

> Challenge: QC-MDPC Syndrome Decoding

The challenge is to solve the Syndrome Decoding problem for a random quasi-cyclic linear code of rate $R = 0.5$ and an error-weight $w \simeq \sqrt{n}$. This corresponds to instances of the SD problem on which the security of the BIKE, HQC and LEDAcrypt, cryptosystems rely.

Latest news

20-08-2019. Announcement of the challenge at Crypto 2019 conference

12-08-2019. All challenges are now online

21-07-2019. Website is online.

12-07-2019. Contact email is active.

n:

ment: see decodingchallenge.org

www.enac.fr

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see decodingchallenge.org
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see decodingchallenge.org
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])
- proof that disguised Goppa codes are (or aren't) indistinguishable from random codes

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see decodingchallenge.org
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])
- proof that disguised Goppa codes are (or aren't) indistinguishable from random codes
- a search-to-decision reduction for the SD problem with ideal codes

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see decodingchallenge.org
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])
- proof that disguised Goppa codes are (or aren't) indistinguishable from random codes
- a search-to-decision reduction for the SD problem with ideal codes
- more scrutiny for rank metric codes and Gröbner bases attacks (see [BBB+20, BBC+20])

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see decodingchallenge.org
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])
- proof that disguised Goppa codes are (or aren't) indistinguishable from random codes
- a search-to-decision reduction for the SD problem with ideal codes
- more scrutiny for rank metric codes and Gröbner bases attacks (see [BBB+20, BBC+20])
- signature schemes with strong security arguments (see [DST19, ABG+19])

Aspects that could/should be improved

Despite its maturity, CBC could benefit from:

- additional practical cryptanalysis assessment: see `decodingchallenge.org`
- efficient and constant-time decoders with negl. decryption failure rate (see [CS16, SV19])
- proof that disguised Goppa codes are (or aren't) indistinguishable from random codes
- a search-to-decision reduction for the SD problem with ideal codes
- more scrutiny for rank metric codes and Gröbner bases attacks (see [BBB+20, BBC+20])
- signature schemes with strong security arguments (see [DST19, ABG+19])

THANKS!

References I

Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, and Gilles Zémor.
BIKE.
Second round submission to the NIST post-quantum cryptography call, April 2019.

Carlos Aguilar Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor.
Efficient encryption from random quasi-cyclic codes.
IEEE Trans. Information Theory, 64(5):3927–3943, 2018.

Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor.
Durandal: a rank metric based signature scheme.
In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *LNCS*, pages 728–758. Springer, 2019.

Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich.
An algebraic attack on rank metric code-based cryptosystems.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 64–93. Springer, 2020.

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel.
Improvements of algebraic attacks for solving the rank decoding and minrank problems.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 507–536. Springer, 2020.

Thierry P Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani.
Reducing key length of the mceliece cryptosystem.
In *International Conference on Cryptology in Africa*, pages 77–97. Springer, 2009.

References II

Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer.
Decoding random binary linear codes in $2^{n/20}$: How $1+1=0$ improves information set decoding.
In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

Thierry P. Berger and Pierre Loidreau.
Designing an efficient and secure public-key cryptosystem based on reducible rank codes.
In *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 218–229, 2004.

Daniel J Bernstein, Tanja Lange, and Christiane Peters.
Attacking and defending the mceliece cryptosystem.
In *Post-Quantum Cryptography*, pages 31–46. Springer, 2008.

Daniel J. Bernstein, Tanja Lange, and Christiane Peters.
Wild McEliece.
In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *LNCS*, pages 143–158, 2010.

Daniel J. Bernstein, Tanja Lange, and Christiane Peters.
Smaller decoding exponents: ball-collision decoding.
In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760, 2011.

D. J. Bernstein, T. Lange, C. Peters, and H. van Tilborg.
Explicit bounds for generic decoding algorithms for code-based cryptography.
In *Pre-proceedings of WCC 2009*, pages 168–180, 2009.

Leif Both and Alexander May.
Decoding linear codes with high error rate and its impact for LPN security.
In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography 2018*, volume 10786 of *LNCS*, pages 25–46, Fort Lauderdale, FL, USA, April 2018. Springer.

References III

Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg.
On the inherent intractability of certain coding problems.
IEEE Trans. Inform. Theory, 24(3):384–386, May 1978.

GC Jr Clark and JB Cain.
Error-correction coding for digital communications.
New York, Plenum Press, 1981. 434 p., 1981.

Hervé Chabanne and Bernard Courteau.
Application de la méthode de décodage itérative d'Omura a la cryptanalyse du système de McEliece.
Technical Report 122, University of Sherbrooke, 1993.

Anne Canteaut and Hervé Chabanne.
A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem.
In *EUROCODE 94*, pages 169–173. INRIA, 1994.

Anne Canteaut and Florent Chabaud.
A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511.
IEEE Trans. Inform. Theory, 44(1):367–378, 1998.

John T Coffey and Rodney M Goodman.
The complexity of information set decoding.
IEEE Transactions on Information Theory, 36(5):1031–1037, 1990.

John T Coffey, Rodney M Goodman, and Patrick G Farrell.
New approaches to reduced-complexity decoding.
Discrete Applied Mathematics, 33(1-3):43–60, 1991.

References IV

Florent Chabaud.
Asymptotic analysis of probabilistic algorithms for finding short codewords.
In Sami Harari Paul Camion, Pascale Charpin, editor, *Eurocode '92. Proceedings of the International Symposium on Coding Theory and Applications*, pages 175–183, Udine, Italy, October 1992. Springer.

Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan.
A polynomial time attack against algebraic geometry code based public key cryptosystems.
In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2014*, pages 1446–1450, June 2014.

Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich.
New identities relating wild Goppa codes.
Finite Fields Appl., 29:178–197, 2014.

Anne Canteaut and Nicolas Sendrier.
Cryptanalysis of the original McEliece cryptosystem.
In *Advances in Cryptology - ASIACRYPT 1998*, volume 1514 of *LNCS*, pages 187–199. Springer, 1998.

Julia Chaulet and Nicolas Sendrier.
Worst case qc-mdpc decoder for mceliece cryptosystem.
In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 1366–1370. IEEE, 2016.

Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich.
Wave: A new family of trapdoor one-way preimage sampleable functions based on codes.
In *Advances in Cryptology - ASIACRYPT 2019*, LNCS, Kobe, Japan, December 2019.

Ilya Dumer.
On minimum distance decoding of linear codes.
In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pages 50–52, Moscow, 1991.

References V

Jean-Charles Faugere, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich.
A distinguisher for high-rate mceliece cryptosystems.
IEEE Transactions on Information Theory, 59(10):6830–6844, 2013.

Cédric Faure and Lorenz Minder.
Cryptanalysis of the McEliece cryptosystem over hyperelliptic curves.
In *Proceedings of the eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, pages 99–107, Pamporovo, Bulgaria, June 2008.

Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Frédéric de Portzamparc, and Jean-Pierre Tillich.
Folding alternant and Goppa Codes with non-trivial automorphism groups.
IEEE Trans. Inform. Theory, 62(1):184–198, 2016.

Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich.
Algebraic cryptanalysis of McEliece variants with compact keys.
In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298, 2010.

Jean-Charles Faugère, Ludovic Perret, and Frédéric de Portzamparc.
Algebraic attack against variants of McEliece with Goppa polynomial of a special form.
In *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 21–41, Kaoshiung, Taiwan, R.O.C., December 2014. Springer.

Matthieu Finiasz and Nicolas Sendrier.
Security bounds for the design of code-based cryptosystems.
In M. Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.

Philippe Gaborit.
Shorter keys for code based cryptography.
In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–91, Bergen, Norway, March 2005.

References VI

Yann Hamdaoui and Nicolas Sendrier.
A non asymptotic analysis of information set decoding.
IACR Cryptology ePrint Archive, Report2013/162, 2013.
http://eprint.iacr.org/2013/162.

Heeralal Janwa and Oscar Moreno.
McEliece public key cryptosystems using algebraic-geometric codes.
Des. Codes Cryptogr., 8(3):293–307, 1996.

Evgenii Avramovich Krouk.
Decoding complexity bound for linear block codes.
Problemy Peredachi Informatsii, 25(3):103–107, 1989.

Pil J. Lee and Ernest F. Brickell.
An observation on the security of McEliece's public-key cryptosystem.
In *Advances in Cryptology - EUROCRYPT'88*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

Jeffrey Leon.
A probabilistic algorithm for computing minimum weights of large error-correcting codes.
IEEE Trans. Inform. Theory, 34(5):1354–1359, 1988.

Robert J. McEliece.
A Public-Key System Based on Algebraic Coding Theory, pages 114–116.
Jet Propulsion Lab, 1978.
DSN Progress Report 44.

References VII

Alexander May, Alexander Meurer, and Enrico Thomae.
Decoding random linear codes in $O(2^{0.054n})$.
In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

Alexander May and Ilya Ozerov.
On computing nearest neighbors with applications to decoding of binary linear codes.
In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

Lorenz Minder and Amin Shokrollahi.
Cryptanalysis of the Sidelnikov cryptosystem.
In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 347–360, Barcelona, Spain, 2007.

Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto.
Mdpc-mceliece: New mceliece variants from moderate density parity-check codes.
In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE, 2013.

Harald Niederreiter.
Knapsack-type cryptosystems and algebraic coding theory.
Problems of Control and Information Theory, 15(2):159–166, 1986.

Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot.
Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes.
Special Issues of Mathematics in Computer Science, 3(2):129–140, January 2010.

Eugene Prange.
The use of information sets in decoding cyclic codes.
IRE Transactions on Information Theory, 8(5):5–9, 1962.

References VIII

Vladimir Michilovich Sidelnikov.
A public-key cryptosytem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191–207, 1994.

Vladimir Michilovich Sidelnikov and S.O. Shestakov.
On the insecurity of cryptosystems based on generalized Reed-Solomon codes.
Discrete Math. Appl., 1(4):439–444, 1992.

Jacques Stern.
A method for finding codewords of small weight.
In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.

Nicolas Sendrier and Valentin Vasseur.
On the decoding failure rate of QC-MDPC bit-flipping decoders.
In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography 2019*, volume 11505 of *LNCS*, pages 404–416, Chongquing, China, May 2019. Springer.

Johan van Tilburg.
On the McEliece public-key cryptosystem.
In *Advances in Cryptology - CRYPTO'88*, volume 403 of *LNCS*, pages 119–131, London, UK, 1990. Springer.

Johan van Tilburg.
Security-analysis of a class of cryptosystems based on linear error-correcting codes.
PhD thesis, Technische Universiteit Eindhoven, 1994.

Christian Wieschebrink.
Two NP-complete problems in coding theory with an application in code based cryptography.
In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 1733–1737, 2006.