Coding theory in post-quantum cryptography

Vlad F. Dragoi

vlad.dragoi@uav.ro

"Aurel Vlaicu" University of Arad, Romania

Funded by Romanian Governement:
PN-III-P1-1.1-PD-2019-0285 CodebasedCrypto

Modern cryptography [DH78]

Modern Cryptography

A pair $(\mathbf{sk}, \mathbf{pk})$ s.t.

sk	$\rightsquigarrow$	**pk**	easy	
sk	$\hookleftarrow$	**pk**	difficult	RSA ('78), El Gamal ('85)

Modern Cryptography

A pair $(\mathbf{sk}, \mathbf{pk})$ s.t.

$$\begin{array}{lcll} \mathbf{sk} & \rightsquigarrow & \mathbf{pk} & \text{easy} \\ \mathbf{sk} & \hookleftarrow & \mathbf{pk} & \text{difficult} \quad \text{RSA ('78), El Gamal ('85)} \end{array}$$

The difficulty of the mathematical problems [1] [2]

1. 2014. R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. "A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic."
   2018. R. Granger, T. Kleinjung, and J. Zumbragel. "On the discrete logarithm problem in finite fields of fixed characteristic".
2. 1997. Peter W. Shor. "Polynomial-time algorithms for prime factorization and

Modern Cryptography

A pair $(\mathbf{sk}, \mathbf{pk})$ s.t.

$$\begin{array}{llll} \mathbf{sk} & \rightsquigarrow & \mathbf{pk} & \text{easy} \\ \mathbf{sk} & \hookleftarrow & \mathbf{pk} & \text{difficult} \quad \text{RSA ('78), El Gamal ('85)} \end{array}$$

The difficulty of the mathematical problems

NIST – post-quantum cryptography project [1]

- Hash based cryptography
- Lattice based cryptography
- Code based cryptography
- Multivariate cryptography

1. http ://csrc.nist.gov/groups/ST/post-quantum-crypto/

Error correcting codes

Definition 1
A q-ary linear code $\mathscr{C}$ defined over $\mathbb{F}_q$, of length n is a k dimension sub-vector space of $\mathbb{F}_q^n$.

Error correcting codes

Definition 1

A q-ary linear code $\mathscr{C}$ defined over $\mathbb{F}_q$, of length n is a k dimension sub-vector space of $\mathbb{F}_q^n$.

Definition 2 (Hamming weight and distance)

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

$$\|\boldsymbol{x}\|_H \stackrel{def}{=} |\{i \mid x_i \neq 0\}| \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} |\{i \mid x_i \neq y_i\}|$$

Error correcting codes

Definition 1

A q-ary linear code $\mathscr{C}$ defined over $\mathbb{F}_q$, of length n is a k dimension sub-vector space of $\mathbb{F}_q^n$.

Definition 2 (Hamming weight and distance)

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

$$\|\boldsymbol{x}\|_H \stackrel{def}{=} |\{i \mid x_i \neq 0\}| \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} |\{i \mid x_i \neq y_i\}|$$

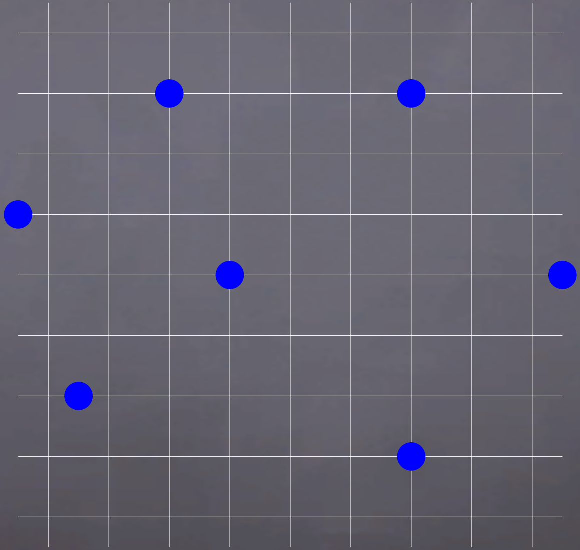
Example

Let $q = 2$ and $\boldsymbol{x} = (1, 0, 0, 1, 0)$, $\boldsymbol{y} = (1, 0, 0, 1, 1)$.
Then

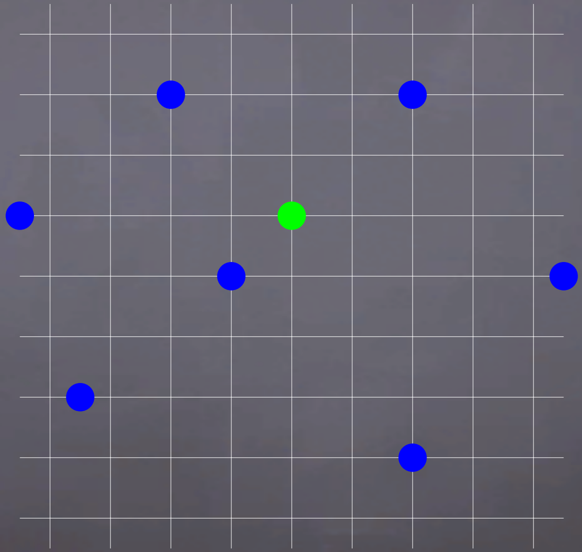
$$\|\boldsymbol{x}\|_H = 2 \quad \text{and} \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) = 1$$

Complete decoding

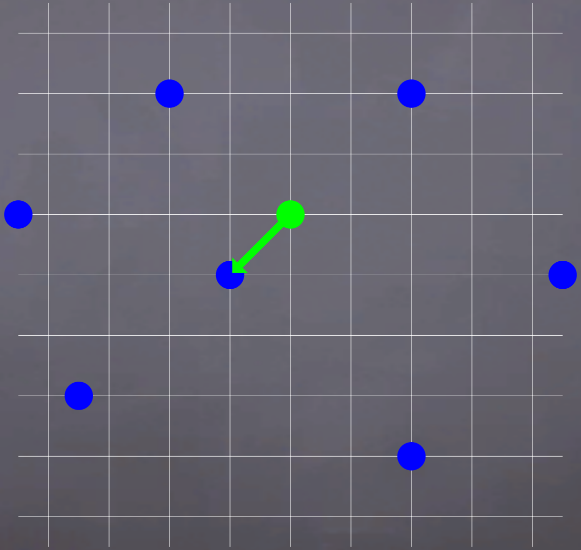
Complete decoding



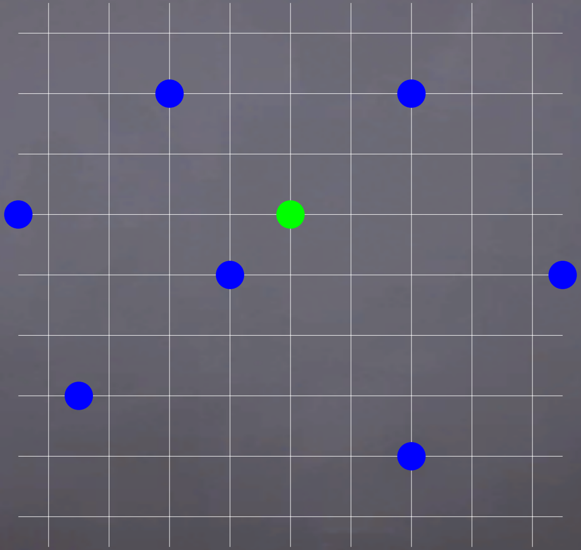
Complete decoding



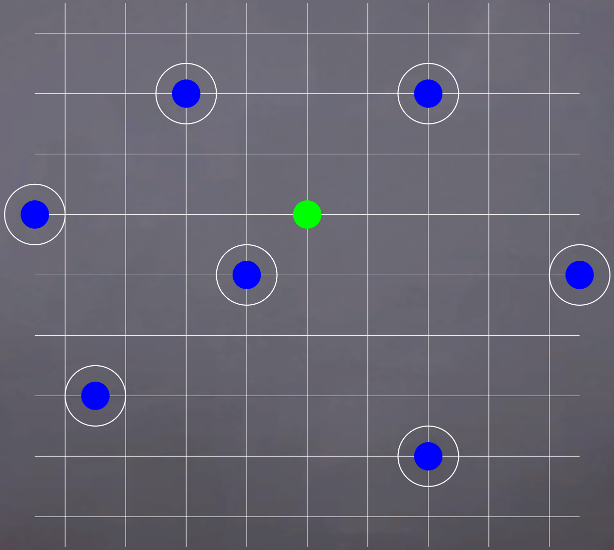
Complete decoding



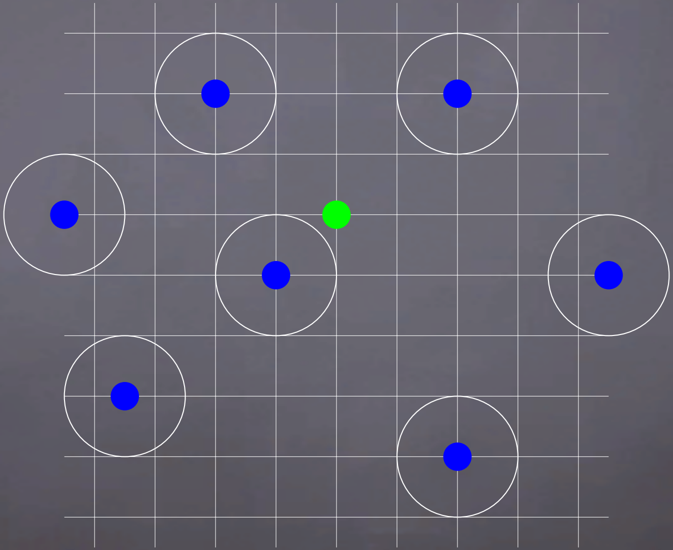
Bounded decoding



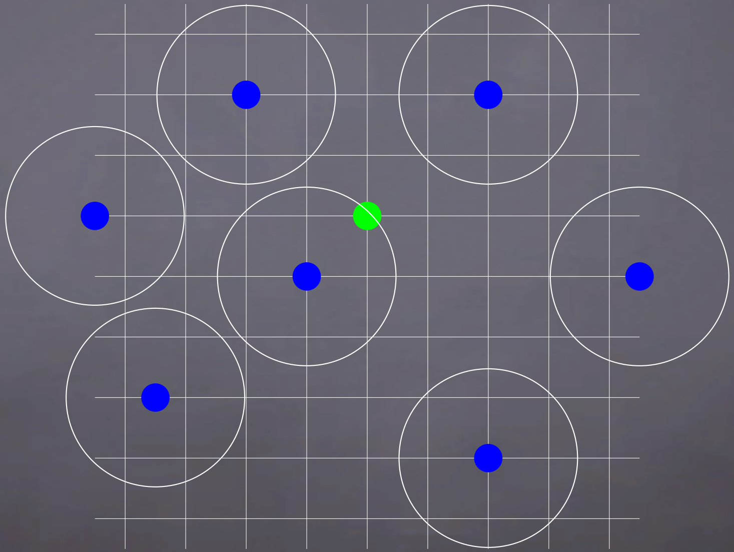
Bounded decoding



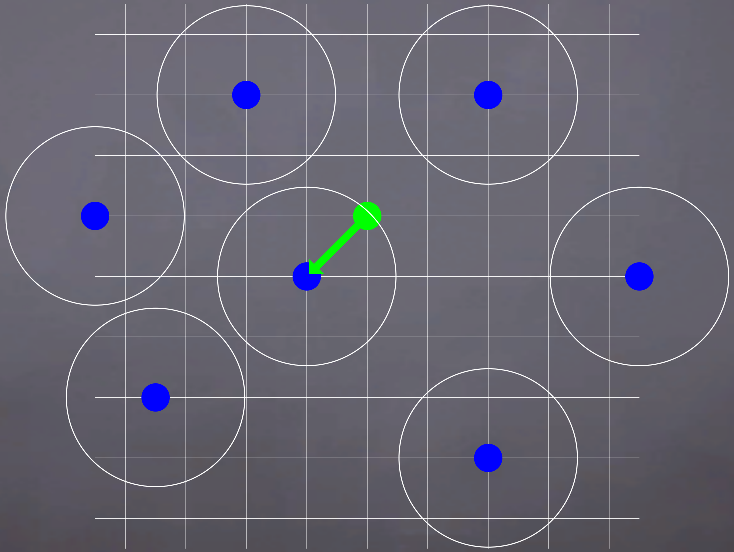
Bounded decoding



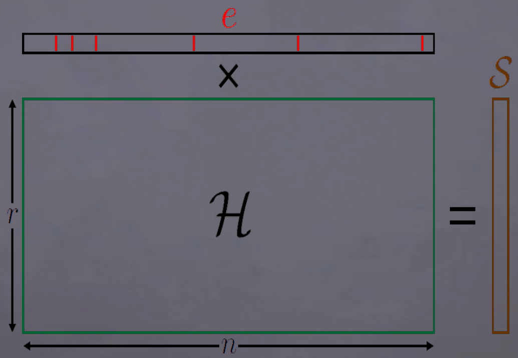
Bounded decoding



Bounded decoding

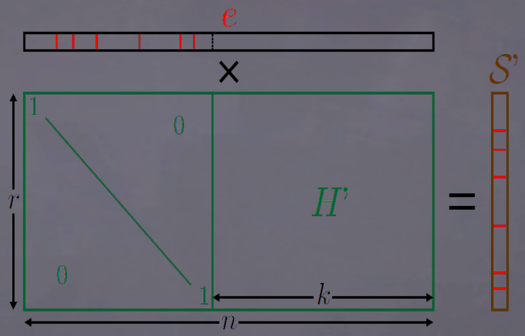


Syndrome decoding [2]



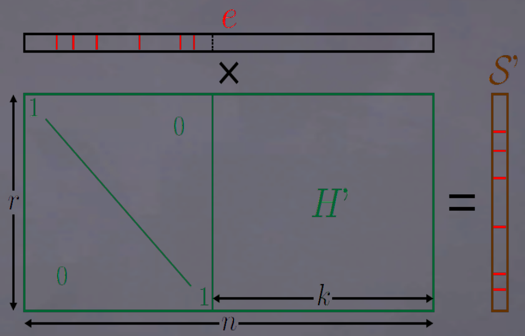
2. 1978. Berlekamp E., McEliece R.J., Van Tilborg "On the inherent intractability of certain coding problems."

Information Set Decoding (ISD) [3]



3. Prange(1957), Stern(1988), Dumer (1991), Canteaut and Chabaud (1998), May, Meurer and Thomae (2011), Becker, Joux, May and Meurer (2012), May and Ozerov (2015)

Information Set Decoding (ISD) [4]



Complexity of ISD [3] for $\|e\| = o(n)$ is roughly

$$2^{c\|e\|(1+o(1))}.$$

3. 2016. Canto-Torres and Sendrier - "Analysis of Information Set Decoding for a Sub-linear Error Weight".
4. Prange(1957), Stern(1988), Dumer (1991), Canteaut and Chabaud (1998), May, Meurer and Thomae (2011), Becker, Joux, May and Meurer (2012), May and Ozerov (2015)

McEliece cryptosystem ('78)

1. Main idea
   - The private key = a code $\mathscr{C}$ with an efficient decoding algorithm
   - The public key = a random basis for $\mathscr{C}$
2. McEliece propose to use binary Goppa codes.

McEliece cryptosystem

- *Key Gen :*

McEliece cryptosystem

- *Key Gen :*

  1. Chose a generator matrix $\boldsymbol{G} \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ for a code $\mathscr{C}$ (corrects t errors with an efficient algorithm).

McEliece cryptosystem

- *Key Gen :*

  1. Chose a generator matrix $\boldsymbol{G} \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ for a code $\mathscr{C}$ (corrects t errors with an efficient algorithm).

  2. Choose $\boldsymbol{P}$ a random $n \times n$ permutation matrix and $\boldsymbol{S}$ a $k \times k$ non-singular matrix.

McEliece cryptosystem

- *Key Gen :*

    1. Chose a generator matrix $\boldsymbol{G} \in \mathcal{M}_{k,n}(\mathbb{F}_q)$ for a code $\mathscr{C}$ (corrects t errors with an efficient algorithm).

    2. Choose $\boldsymbol{P}$ a random $n \times n$ permutation matrix and $\boldsymbol{S}$ a $k \times k$ non-singular matrix.

    3. The private key sk $= (\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$ and the public key pk $= (\boldsymbol{G}_{pub}, t)$ with

$$\boldsymbol{G}_{pub} = \boldsymbol{SGP}$$

McEliece cryptosystem

Encryption

Let $\boldsymbol{m} \in \mathbb{F}_q^k$,

1. Generate a random error vector $\boldsymbol{e} \in \mathbb{F}_q^n$ of Hamming weight t
2. Encrypt $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{pub} + \boldsymbol{e}$

McEliece cryptosystem

Encryption

Let $\boldsymbol{m} \in \mathbb{F}_q^k$,

1. Generate a random error vector $\boldsymbol{e} \in \mathbb{F}_q^n$ of Hamming weight t
2. Encrypt $\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{pub} + \boldsymbol{e}$

Decryption

1. Compute $\boldsymbol{z} = \boldsymbol{c}\boldsymbol{P}^{-1}$ $\qquad \boldsymbol{z} = \boldsymbol{m}\boldsymbol{S}\boldsymbol{G} + \boldsymbol{e}\boldsymbol{P}^{-1}$
2. Compute $\boldsymbol{y} = Decode_{\boldsymbol{G}}(\boldsymbol{z})$ $\qquad \boldsymbol{y} = \boldsymbol{m}\boldsymbol{S}$
3. Return $\boldsymbol{m}' = \boldsymbol{y}\boldsymbol{S}^{-1}$ $\qquad \boldsymbol{m}' = \boldsymbol{m}$

Security

- No structural (Key recovery) attacks against the binary Goppa codes.

Security

- No structural (Key recovery) attacks against the binary Goppa codes.
- No Message recovery attacks exploiting the structure of the underlying code.

Security

- No structural (Key recovery) attacks against the binary Goppa codes.
- No Message recovery attacks exploiting the structure of the underlying code.
- Weak keys. [5]

5. 2001, Loidreau and Sendrier, "Weak keys in the McEliece public-key cryptosystem".

Security

- No structural (Key recovery) attacks against the binary Goppa codes.
- No Message recovery attacks exploiting the structure of the underlying code.
- Weak keys. [5]
- Distinguisher [6] between a random linear code and the public code in the McEliece PKC. [7]

5. 2001, Loidreau and Sendrier, "Weak keys in the McEliece public-key cryptosystem".
6. 2001. Courtois, Finiasz and Sendrier - " How to Achieve a McEliece-based Digital Signature Scheme"
7. 2013. Faugère, Gauthier, Otmani, Perret and Tillich. - "A distinguisher for high rate McEliece cryptosystems"

Security

- No structural (Key recovery) attacks against the binary Goppa codes.
- No Message recovery attacks exploiting the structure of the underlying code.
- Weak keys.[5]
- Distinguisher[6] between a random linear code and the public code in the McEliece PKC.[7]
- Cryptanalysis of wild Goppa codes.[8]

5. 2001, Loidreau and Sendrier, "Weak keys in the McEliece public-key cryptosystem".
6. 2001. Courtois, Finiasz and Sendrier - " How to Achieve a McEliece-based Digital Signature Scheme"
7. 2013. Faugère, Gauthier, Otmani, Perret and Tillich. - "A distinguisher for high rate McEliece cryptosystems"
8. 2014. Couvreur, Otmani et Tillich - "Polynomial Time Attack on Wild McEliece Over Quadratic Extensions"

Advantages and disadvantages

- Advantages :
  - Encryption and decryption are very fast

Advantages and disadvantages

- Advantages :
  - Encryption and decryption are very fast
  - Its security : resistant to quantum attacks (for now), solving the syndrome pb. is NP hard.

Advantages and disadvantages

- Advantages :
  - Encryption and decryption are very fast
  - Its security : resistant to quantum attacks (for now), solving the syndrome pb. is NP hard.

- Disadvantages : key size

128 bits of security - 1.5 Megabits (McEliece - Goppa), 3072 bits (RSA), 256 bits (ECC)

Advantages and disadvantages

- Advantages :
  - Encryption and decryption are very fast
  - Its security : resistant to quantum attacks (for now), solving the syndrome pb. is NP hard.
- Disadvantages : key size

128 bits of security - 1.5 Megabits (McEliece - Goppa), 3072 bits (RSA), 256 bits (ECC)

1. **Increase the minimum distance**
2. **Add extra structure (quasi-cyclic, quasi-dyadic)**
3. Change the metric (Rank)

Classic variants	*Proposal*
Binary Goppa	1978 [McE78]
GRS	1986 [Nie86]
Reed-Muller	1994 [Sid94]
Concatenated	1994 [Sen94]
Algebraic geometric	1996 [JM96]
Wild Goppa	2010 [BLP10]
Convolutional	2012 [LJ12]
Polar	2014 [SK14]

QC, QD Variants	
QC-BCH	2005 [Gab05]
QC-LDPC	2008 [BBC08]
QC-Alternant	2009 [BCGO09]
QD-Goppa	2009 [MB09]
QD-Srivastava	2012 [Per12]
QC-MDPC	2012 [MTSB13]

Classic variants	*Proposal*	*Attacks*
Binary Goppa	1978 [McE78]	
GRS	1986 [Nie86]	1992 [SS92]
Reed-Muller	1994 [Sid94]	2007 [MS07]
Concatenated	1994 [Sen94]	1998 [Sen98]
Algebraic geometric	1996 [JM96]	2014 [CMCP14]
Wild Goppa	2010 [BLP10]	2014 [COT14, FPdP14]
Convolutional	2012 [LJ12]	2013 [LT13]
Polar	2014 [SK14]	

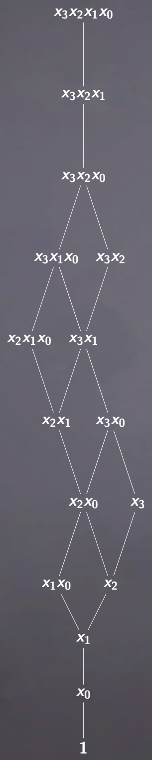
QC, QD Variants		
QC-BCH	2005 [Gab05]	2008 [OTD08]
QC-LDPC	2008 [BBC08]	
QC-Alternant	2009 [BCGO09]	2014 [FOP+16]
QD-Goppa	2009 [MB09]	2014 [FOP+16]
QD-Srivastava	2012 [Per12]	2014 [FOP+16]
QC-MDPC	2012 [MTSB13]	

Classic variants	*Proposal*	*Attacks*
Binary Goppa	1978 [McE78]	
GRS	1986 [Nie86]	1992 [SS92]
Reed-Muller	1994 [Sid94]	2007 [MS07]
Concatenated	1994 [Sen94]	1998 [Sen98]
Algebraic geometric	1996 [JM96]	2014 [CMCP14]
Wild Goppa	2010 [BLP10]	2014 [COT14, FPdP14]
Convolutional	2012 [LJ12]	2013 [LT13]
Polar	*2014 [SK14]*	

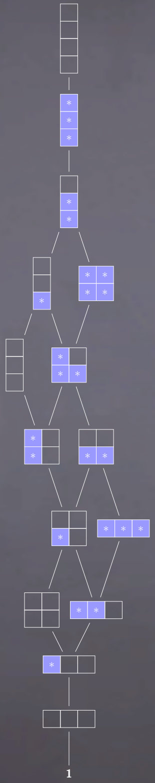
QC, QD Variants		
QC-BCH	2005 [Gab05]	2008 [OTD08]
QC-LDPC	2008 [BBC08]	
QC-Alternant	2009 [BCGO09]	2014 [FOP+16]
QD-Goppa	2009 [MB09]	2014 [FOP+16]
QD-Srivastava	2012 [Per12]	2014 [FOP+16]
QC-MDPC	*2012 [MTSB13]*	

Classic variants	*Proposal*	*Attacks*
Binary Goppa	1978 [McE78]	
GRS	1986 [Nie86]	1992 [SS92]
Reed-Muller	1994 [Sid94]	2007 [MS07]
Concatenated	1994 [Sen94]	1998 [Sen98]
Algebraic geometric	1996 [JM96]	2014 [CMCP14]
Wild Goppa	2010 [BLP10]	2014 [COT14, FPdP14]
Convolutional	2012 [LJ12]	2013 [LT13]
Polar	*2014 [SK14]*	*2016 [BCD+16]*

QC, QD Variants		
QC-BCH	2005 [Gab05]	2008 [OTD08]
QC-LDPC	2008 [BBC08]	
QC-Alternant	2009 [BCGO09]	2014 [FOP+16]
QD-Goppa	2009 [MB09]	2014 [FOP+16]
QD-Srivastava	2012 [Per12]	2014 [FOP+16]
QC-MDPC	*2012 [MTSB13]*	*2016 [BDLO16]*



$x_3x_2x_1x_0$
$x_3x_2x_1$
$x_3x_2x_0$
$x_3x_1x_0$
x_3x_2
$x_2x_1x_0$
x_3x_1
x_2x_1
x_3x_0
x_2x_0
x_3
x_1x_0
x_2
x_1
x_0
1



1

Questions ?

Bibliography I

Marco Baldi, Marco Bodrato, and Franco Chiaraluce.
A new analysis of the TMcEliece cryptosystem based on QC-LDPC codes.
In *Proceedings of the 6th international conference on Security and Cryptography for Networks*, SCN '08, pages 246–262, Berlin, Heidelberg, 2008. Springer-Verlag.

Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich.
Cryptanalysis of the McEliece public key cryptosystem based on polar codes.
In *Post-Quantum Cryptography2016*, Lecture Notes in Comput. Sci., Fukuoka, Japan, February 2016.

Bibliography II

Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani.
Reducing key length of the McEliece cryptosystem.
In Bart Preneel, editor, *Progress in Cryptology - AFRICACRYPT 2009*, volume 5580 of *Lecture Notes in Comput. Sci.*, pages 77–97, Gammarth, Tunisia, June 21-25 2009.

Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani.
Weak keys for the quasi-cyclic MDPC public key encryption scheme.
In *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, pages 346–367, 2016.

Bibliography III

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

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.

Bibliography IV

- Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich.
  Polynomial time attack on wild McEliece over quadratic extensions.
  In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Comput. Sci.*, pages 17–39. Springer Berlin Heidelberg, 2014.

- 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.

Bibliography V

- 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 *Lecture Notes in Comput. Sci.*, pages 21–41, Kaoshiung, Taiwan, R.O.C., December 2014. Springer.

- 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.

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

Bibliography VI

- Carl Löndahl and Thomas Johansson.
  A new version of McEliece PKC based on convolutional codes.
  In *Information and Communications Security, ICICS*, volume 7168 of *Lecture Notes in Comput. Sci.*, pages 461–470. Springer, 2012.

- Grégory Landais and Jean-Pierre Tillich.
  An efficient attack of a McEliece cryptosystem variant based on convolutional codes.
  In P. Gaborit, editor, *Post-Quantum Cryptography'13*, volume 7932 of *Lecture Notes in Comput. Sci.*, pages 102–117. Springer, June 2013.

- Rafael Misoczki and Paulo Barreto.
  Compact McEliece keys from Goppa codes.
  In *Selected Areas in Cryptography*, Calgary, Canada, August 13-14 2009.

Bibliography VII

Robert J. McEliece.
A Public-Key System Based on Algebraic Coding Theory, pages 114–116.

Jet Propulsion Lab, 1978.
DSN Progress Report 44.

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

Bibliography VIII

Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto.
MDPC-McEliece : New McEliece variants from moderate density parity-check codes.
In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2069–2073, 2013.

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

Bibliography IX

Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot.
Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes.
In *Proceedings of First International Conference on Symbolic Computation and Cryptography*, pages 69–81, Beijing, China, April 28-30 2008. LMIB Beihang University.

Edoardo Persichetti.
Compact McEliece keys based on quasi-dyadic Srivastava codes.
J. Math. Cryptol., 6(2) :149–169, 2012.

Nicolas Sendrier.
On the structure of a randomly permuted concatenated code.
In *EUROCODE'94*, pages 169–173, 1994.

Bibliography X

Nicolas Sendrier.
On the concatenated structure of a linear code.
Appl. Algebra Eng. Commun. Comput. (AAECC), 9(3) :221–242, 1998.

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

Sujan Raj Shrestha and Young-Sik Kim.
New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography.
In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pages 368–372. IEEE, 2014.

Bibliography XI

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.