An Overview on Post-Quantum Cryptography with an Emphasis on Code based Systems

Joachim Rosenthal
University of Zürich

Finite Geometries
Fifth Irsee Conference, September 10–16, 2017.

University of Zurich

Outline

University of Zurich

Where are Public Key Systems used:

Public Key Crypto Systems appear in a wide variety of applications such as

Where are Public Key Systems used:

Public Key Crypto Systems appear in a wide variety of applications such as

- Exchange of a secret key over an insecure channel.

Where are Public Key Systems used:

Public Key Crypto Systems appear in a wide variety of applications such as

- Exchange of a secret key over an insecure channel.
- Digital Signatures

University of Zurich

Where are Public Key Systems used:

Public Key Crypto Systems appear in a wide variety of applications such as

- Exchange of a secret key over an insecure channel.
- Digital Signatures
- Authentication protocols

Where are Public Key Systems used:

Public Key Crypto Systems appear in a wide variety of applications such as

- Exchange of a secret key over an insecure channel.
- Digital Signatures
- Authentication protocols
- Digital Cash systems such as BitCoins.

What mathematical techniques are currently in use?

University of Zurich

What mathematical techniques are currently in use?

- RSA system: Nowadays almost all key exchanges over the Internet make use of RSA. A bitsize of 1024 bits is considered a minimum requirement. The system is based on the hardness of factoring.

What mathematical techniques are currently in use?

- RSA system: Nowadays almost all key exchanges over the Internet make use of RSA. A bitsize of 1024 bits is considered a minimum requirement. The system is based on the hardness of factoring.
- Many web-servers give the user the option to use a protocol based on the hardness of the discrete logarithm problem over an elliptic curve. Unfortunately the available choices of curves are very few.

What mathematical techniques are currently in use?

- RSA system: Nowadays almost all key exchanges over the Internet make use of RSA. A bitsize of 1024 bits is considered a minimum requirement. The system is based on the hardness of factoring.
- Many web-servers give the user the option to use a protocol based on the hardness of the discrete logarithm problem over an elliptic curve. Unfortunately the available choices of curves are very few.
- Digital signatures and authentication protocols involve often a discrete logarithm problem over a finite field.

Complexity of factoring and DLP

University of Zurich

Complexity of factoring and DLP

- Both factoring integers and the DLP over a finite field have known sub-exponential time algorithms. As a result a key size of 1000 bits is the absolute minimum.

Complexity of factoring and DLP

- Both factoring integers and the DLP over a finite field have known sub-exponential time algorithms. As a result a key size of 1000 bits is the absolute minimum.
- There has been recently immense progress in the DLP problem over a finite field.

Complexity of factoring and DLP

- Both factoring integers and the DLP over a finite field have known sub-exponential time algorithms. As a result a key size of 1000 bits is the absolute minimum.
- There has been recently immense progress in the DLP problem over a finite field.
- The best known algorithm for the DLP problem over an elliptic curve is exponential time.

Complexity of factoring and DLP

- Both factoring integers and the DLP over a finite field have known sub-exponential time algorithms. As a result a key size of 1000 bits is the absolute minimum.
- There has been recently immense progress in the DLP problem over a finite field.
- The best known algorithm for the DLP problem over an elliptic curve is exponential time.
- On a quantum computer both the factoring problem and the DLP problem have polynomial running time. [Sho97].

NSA and NIST

NSA: ([nis15]) (From Wikipedia) In August, 2015, NSA announced that it is planning to transition "in the not too distant future" to a new cipher suite that is resistant to quantum attacks. "Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy." NSA advised: "For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

NSA and NIST

NIST: ([nis16]) In February 2016 NIST released a "Report on Post-Quantum Cryptography". Quote: "It is unclear when scalable quantum computers will be available, however in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking RSA - 2048 in a matter of hours could be built by 2030 for a budget of about a billion dollars. This is a serious long - term threat to the cryptosystems currently standardized by NIST"

Main contenders for Post-Quantum Crypto Systems

Research in post-quantum cryptography has currently three major directions:

Main contenders for Post-Quantum Crypto Systems

Research in post-quantum cryptography has currently three major directions:

- Code based Cryptography

Main contenders for Post-Quantum Crypto Systems

Research in post-quantum cryptography has currently three major directions:

- Code based Cryptography
- Latttice Based Cryptography

Main contenders for Post-Quantum Crypto Systems

Research in post-quantum cryptography has currently three major directions:

- Code based Cryptography
- Latttice Based Cryptography
- Multivariate Cryptography

University of Zurich

Lattice Based Cryptography

Lattice based cryptography has its origin on the following facts:

Lattice Based Cryptography

Lattice based cryptography has its origin on the following facts:

- It is an NP hard problem to find the shortest nonzero vector in a lattice (SVP problem) and the closest vector to some given vector (CVP problem).

Lattice Based Cryptography

Lattice based cryptography has its origin on the following facts:

- It is an NP hard problem to find the shortest nonzero vector in a lattice (SVP problem) and the closest vector to some given vector (CVP problem).
- It is not difficult to construct lattices where the designer knows a very short vector or the shortest vector.

Lattice Based Cryptography

Lattice based cryptography has its origin on the following facts:

- It is an NP hard problem to find the shortest nonzero vector in a lattice (SVP problem) and the closest vector to some given vector (CVP problem).
- It is not difficult to construct lattices where the designer knows a very short vector or the shortest vector.
- As public key serves a lattice basis which does not contain the short vector.

Multivariate Cryptography

Multivariate cryptography has its origin on the following facts:

Multivariate Cryptography

Multivariate cryptography has its origin on the following facts:

- Solving systems of polynomial equations over a finite field can be a hard problem.

Multivariate Cryptography

Multivariate cryptography has its origin on the following facts:

- Solving systems of polynomial equations over a finite field can be a hard problem.
- There are many systems in some reduced form which can be readily solved.

Multivariate Cryptography

Multivariate cryptography has its origin on the following facts:

- Solving systems of polynomial equations over a finite field can be a hard problem.
- There are many systems in some reduced form which can be readily solved.
- It is possible to transform an 'easy system' into a 'hard system' without a huge increase in the equation size.

Traditional McEliece Crypto System

In 1978 Robert McEliece [McE78] proposed an asymmetric encryption scheme based on the hardness of decoding a generic linear code. The original paper proposed

Traditional McEliece Crypto System

In 1978 Robert McEliece [McE78] proposed an asymmetric encryption scheme based on the hardness of decoding a generic linear code. The original paper proposed

- an $[n, k] = [1024, 512]$ classical binary Goppa code having designed distance $d = 50$ and generator matrix G.

Traditional McEliece Crypto System

In 1978 Robert McEliece [McE78] proposed an asymmetric encryption scheme based on the hardness of decoding a generic linear code. The original paper proposed

- an $[n, k] = [1024, 512]$ classical binary Goppa code having designed distance $d = 50$ and generator matrix G.
- Public will be $\tilde{G} := SGP$ where S is a random invertible matrix and P a permutation matrix. - The matrices S, G, P are kept private.

Traditional McEliece Crypto System

In 1978 Robert McEliece [McE78] proposed an asymmetric encryption scheme based on the hardness of decoding a generic linear code. The original paper proposed

- an $[n, k] = [1024, 512]$ classical binary Goppa code having designed distance $d = 50$ and generator matrix G.
- Public will be $\tilde{G} := SGP$ where S is a random invertible matrix and P a permutation matrix. - The matrices S, G, P are kept private.
- **Encryption:** $m \mapsto m\tilde{G} + e$, where e is an error vector with weight half the minimum distance. The designer has available the Berlekamp-Massey algorithm for decoding in polynomial time.

Advantages/Disadvantages of McEliece System

Advantages/Disadvantages of McEliece System

- **Positive:** Both encryption and decryption have quadratic complexity in block length. (Compares very well to the RSA system).

University of Zurich

Advantages/Disadvantages of McEliece System

- **Positive:** Both encryption and decryption have quadratic complexity in block length. (Compares very well to the RSA system).
- **Positive:** No polynomial time quantum algorithm is known to decode a general linear block code. Even better, it is known that decoding a general linear code is a NP-hard problem [BMvT78].

Advantages/Disadvantages of McEliece System

- **Positive:** Both encryption and decryption have quadratic complexity in block length. (Compares very well to the RSA system).
- **Positive:** No polynomial time quantum algorithm is known to decode a general linear block code. Even better, it is known that decoding a general linear code is a NP-hard problem [BMvT78].
- **Negative:** The public key is fairly large. - About 0.5 Megabites compared to 0.1 Megabites for RSA and 0.02 Megabites for elliptic curves.

University of Zurich

Using Generalized Reed-Solomon Codes:

The use of GRS codes together with general monomial transformations to disguise the code structure was proposed in the mid 80'th.

Using Generalized Reed-Solomon Codes:

The use of GRS codes together with general monomial transformations to disguise the code structure was proposed in the mid 80'th.

- **Positive:** An $[n, k]$ GRS code over a field $\mathbb{F}_q$ with $q > n$ has distance equal to the Singleton bound. It is therefore possible to work with much smaller public keys.

University of Zurich

Using Generalized Reed-Solomon Codes:

The use of GRS codes together with general monomial transformations to disguise the code structure was proposed in the mid 80'th.

- **Positive:** An $[n, k]$ GRS code over a field $\mathbb{F}_q$ with $q > n$ has distance equal to the Singleton bound. It is therefore possible to work with much smaller public keys.
- **Negative:** Sidelnikov and Shestakov [SS92] were able to retrieve the underlying code structure in polynomial time.

Using Generalized Reed-Solomon Codes:

The use of GRS codes together with general monomial transformations to disguise the code structure was proposed in the mid 80'th.

- **Positive:** An $[n, k]$ GRS code over a field $\mathbb{F}_q$ with $q > n$ has distance equal to the Singleton bound. It is therefore possible to work with much smaller public keys.
- **Negative:** Sidelnikov and Shestakov [SS92] were able to retrieve the underlying code structure in polynomial time.
- **Puncturing and Subspace Constructions:** There were many variants proposed when the starting code is a Reed-Solomon code and the code structure is further disguised through puncturing and adding extra parity check equations. — There are powerful recent "distinguisher attacks" (Valérie Gauthier, Ayoub Otmani, Jean-Pierre Tillich and Alain Couvreur, Irene Marquez-Corbella, Ruud Pellikaan.)

Using Reed-Muller Codes:

Using Reed-Muller Codes:

- **Proposal:** In 1994 V.M.Sidelnikov proposed to use Reed-Muller codes in the McEliece public key system.

Using Reed-Muller Codes:

- **Proposal:** In 1994 V.M.Sidelnikov proposed to use Reed-Muller codes in the McEliece public key system.
- **Breaking:** In 2007 Minder and Shokrollahi came up with an adaptation of the Sidelnikov and Shestakov attack and this resulted in polynomial time algorithm to recover the underlying code structure.

Using Low Density Parity Check Codes:

In 2000 [MRS00], Monico, Shokrollahi and R. proposed the use of LDPC codes in the McEliece system.

Using Low Density Parity Check Codes:

In 2000 [MRS00], Monico, Shokrollahi and R. proposed the use of LDPC codes in the McEliece system.

- **Problem:** Size of code has to be very large in order to make sure that no low weight vectors in the dual code can be retrieved. If the density is very low (e.g. Gallager's (3,6) regular code) then a brute force search of all low weight code words of the dual code is possible.

Using Low Density Parity Check Codes:

In 2000 [MRS00], Monico, Shokrollahi and R. proposed the use of LDPC codes in the McEliece system.

- **Problem:** Size of code has to be very large in order to make sure that no low weight vectors in the dual code can be retrieved. If the density is very low (e.g. Gallager's (3,6) regular code) then a brute force search of all low weight code words of the dual code is possible.
- **MDPC Codes:** Medium Density Parity check codes are still a viable and one of the most promising proposals and research is ongoing.

University of Zurich

Further Variants of McEliece System

Further Variants of McEliece System

- **Niederreiter cryptosystem:** Harald Niederreiter proposed this variant in 1986 and it works with syndromes and disguised parity check matrices. The security is equivalent to the original McEliece system, the transmitted messages are shorter and encryption is faster. - In particular for signature schemes attractive.

Further Variants of McEliece System

- **Niederreiter cryptosystem:** Harald Niederreiter proposed this variant in 1986 and it works with syndromes and disguised parity check matrices. The security is equivalent to the original McEliece system, the transmitted messages are shorter and encryption is faster. - In particular for signature schemes attractive.
- **Specifying the errors:** Together with Baldi, Chiaraluce and Schipani [BBC+16] we showed that it is possible to do a transformation of the generator matrix (e.g. with low rank matrices) where encryption then requires that the error vectors have to lie in a specified variety.

Further Variants of McEliece System

- **Niederreiter cryptosystem:** Harald Niederreiter proposed this variant in 1986 and it works with syndromes and disguised parity check matrices. The security is equivalent to the original McEliece system, the transmitted messages are shorter and encryption is faster. - In particular for signature schemes attractive.
- **Specifying the errors:** Together with Baldi, Chiaraluce and Schipani [BBC+16] we showed that it is possible to do a transformation of the generator matrix (e.g. with low rank matrices) where encryption then requires that the error vectors have to lie in a specified variety.
- **Low weight transformations:** Instead of using monomial transformations it is possible to use transformations where low weight vectors are mapped onto low weight vectors.

Crucial for the cryptanalysis of many variants of Reed-Solomon based systems are the following concept:

Crucial for the cryptanalysis of many variants of Reed-Solomon based systems are the following concept:

Definition

Let $\mathcal{C} \subset \mathbb{F}^n$ be a $[n, k]$ block code. Then the square $\mathcal{C}^2$ of $\mathcal{C}$ is defined as the span of all vectors of the form

$$\{a \star b \mid a, b \in \mathcal{C}\}$$

where $a \star b$ denotes the (component-wise) Hadamard product.

Crucial for the cryptanalysis of many variants of Reed-Solomon based systems are the following concept:

Definition

Let $\mathcal{C} \subset \mathbb{F}^n$ be a $[n, k]$ block code. Then the square $\mathcal{C}^2$ of $\mathcal{C}$ is defined as the span of all vectors of the form

$$\{a \star b \mid a, b \in \mathcal{C}\}$$

where $a \star b$ denotes the (component-wise) Hadamard product.

Remark

Nota Bene: *The dimension of $\mathcal{C}^2$ is invariant under an isometry transformation.*

Couvreur, Gauthier, Otmani, Tillich Marquez-Corbella and Pellikaan showed:

Theorem

When $\mathcal{C} \subset \mathbb{F}^n$ be a $[n, k]$ block code then

$$\dim(\mathcal{C}^2) \leq \frac{1}{2}k(k+1).$$

For an $[n, k]$ Reed Solomon code one has:

$$\dim(\mathcal{C}^2) \leq 2k - 1.$$

Couvreur, Gauthier, Otmani, Tillich Marquez-Corbella and Pellikaan showed:

Theorem

When $\mathcal{C} \subset \mathbb{F}^n$ be a $[n, k]$ block code then

$$\dim(\mathcal{C}^2) \leq \frac{1}{2}k(k+1).$$

For an $[n, k]$ Reed Solomon code one has:

$$\dim(\mathcal{C}^2) \leq 2k - 1.$$

The small dimension of a disguised square code is often the basis to recover the hidden Reed-Solomon type structure. The square code also serves as **distinguisher** for algebraic geometric codes.

Instead of using monomial transformations one can use transformations represented by some matrix having 'low row weight' everywhere. This idea has its origin in [BBC+16].

Instead of using monomial transformations one can use transformations represented by some matrix having 'low row weight' everywhere. This idea has its origin in [BBC+16].

- When the average row weight of the transforming matrix is strictly less than 2 Couvreur e.al. extended their distinguisher attack [COTGU15].

Instead of using monomial transformations one can use transformations represented by some matrix having 'low row weight' everywhere. This idea has its origin in [BBC+16].

- When the average row weight of the transforming matrix is strictly less than 2 Couvreur e.al. extended their distinguisher attack [COTGU15].
- In joint work Jessalyn Bolkema, Heide Gluesing-Luerssen, Christine A. Kelley, Kristin Lauter and Beth Malmskog we could show that constant row weight 2 results often in a code whose square $\mathcal{C}^2$ has maximal dimension.

Instead of using monomial transformations one can use transformations represented by some matrix having 'low row weight' everywhere. This idea has its origin in [BBC$^+$16].

- When the average row weight of the transforming matrix is strictly less than 2 Couvreur e.al. extended their distinguisher attack [COTGU15].
- In joint work Jessalyn Bolkema, Heide Gluesing-Luerssen, Christine A. Kelley, Kristin Lauter and Beth Malmskog we could show that constant row weight 2 results often in a code whose square $\mathcal{C}^2$ has maximal dimension.
- Violetta Weger derived further conditions which guarantee maximal dimension of the square code. In this situation the distingusiher is 'hidden'.

McEliece for Rank Metric Codes

In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

McEliece for Rank Metric Codes

In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

Definition

On the set $\mathbb{F}^{m \times n}$ *consisting of all* $m \times n$ *matrices over* $\mathbb{F}$ *define the* rank distance*:*

$$d_R(X, Y) := rank(X - Y)$$

McEliece for Rank Metric Codes

In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

Definition

On the set $\mathbb{F}^{m \times n}$ *consisting of all* $m \times n$ *matrices over* $\mathbb{F}$ *define the* rank distance*:*

$$d_R(X, Y) := rank(X - Y)$$

Remark

$d_R(X, Y)$ *is a metric.*

University of Zurich

McEliece for Rank Metric Codes

In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

Definition

On the set $\mathbb{F}^{m\times n}$ *consisting of all* $m \times n$ *matrices over* $\mathbb{F}$ *define the* rank distance*:*

$$d_R(X, Y) := rank(X - Y)$$

Remark

$d_R(X, Y)$ *is a metric.*

Remark

Gabidulin provided several constructions and decoding algorithms of linear rank metric codes with good distances.

Gabidulin Codes

Definition

Let $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n) \in \mathbb{F}_{q^m}^n$ be such that α_i are independent over $\mathbb{F}_q$. The Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ is given by

$$\mathrm{Gab}_{n,k}(\boldsymbol{\alpha}) = \{(f(\alpha_1), f(\alpha_2), ..., f(\alpha_n)) \mid f \in \mathcal{L}_{q,m,k}\}.$$

Gabidulin Codes

Definition

Let $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n) \in \mathbb{F}_{q^m}^n$ be such that α_i are independent over $\mathbb{F}_q$. The Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ is given by

$$\mathrm{Gab}_{n,k}(\boldsymbol{\alpha}) = \{(f(\alpha_1), f(\alpha_2), ..., f(\alpha_n)) \mid f \in \mathcal{L}_{q,m,k}\}.$$

- The maximum possible rank distance d of any $[n, k, d]$ rank metric code $\mathcal{C} \subset \mathbb{F}^{m \times n}$ is $d = n - k + 1$.

University of Zurich

Gabidulin Codes

Definition

Let $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n) \in \mathbb{F}_{q^m}^n$ be such that α_i are independent over $\mathbb{F}_q$. The Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ is given by

$$\mathrm{Gab}_{n,k}(\boldsymbol{\alpha}) = \{(f(\alpha_1), f(\alpha_2), ..., f(\alpha_n)) \mid f \in \mathcal{L}_{q,m,k}\}.$$

- The maximum possible rank distance d of any $[n, k, d]$ rank metric code $\mathcal{C} \subset \mathbb{F}^{m \times n}$ is $d = n - k + 1$.
- Gabidulin codes are maximum rank-distance (MRD) codes attaining the Singleton bound, $d = n - k + 1$.

McEliece for Rank Metric Codes

- Gabidulin, Paramonov and Tretjakov ([GPT91]) introduced in 1991 a McEliece type crypto system based on disguised Gabidulin codes referred to as **GPT system**. The disguising is based on the isometry group of rank metric codes.

McEliece for Rank Metric Codes

- Gabidulin, Paramonov and Tretjakov ([GPT91]) introduced in 1991 a McEliece type crypto system based on disguised Gabidulin codes referred to as **GPT system**. The disguising is based on the isometry group of rank metric codes.
- Gibson [Gib95] came up with a first attack and Overbeck [Ove08] derived a general structural attack which also broke this system in 2008.

McEliece for Rank Metric Codes

- Gabidulin, Paramonov and Tretjakov ([GPT91]) introduced in 1991 a McEliece type crypto system based on disguised Gabidulin codes referred to as **GPT system**. The disguising is based on the isometry group of rank metric codes.
- Gibson [Gib95] came up with a first attack and Overbeck [Ove08] derived a general structural attack which also broke this system in 2008.
- Berger and Loidreau [BL05, Loi10] proposed a McEliece type system based on disguised Gabidulin rank metric codes.

University of Zurich

McEliece for Rank Metric Codes

- Gabidulin, Paramonov and Tretjakov ([GPT91]) introduced in 1991 a McEliece type crypto system based on disguised Gabidulin codes referred to as **GPT system**. The disguising is based on the isometry group of rank metric codes.
- Gibson [Gib95] came up with a first attack and Overbeck [Ove08] derived a general structural attack which also broke this system in 2008.
- Berger and Loidreau [BL05, Loi10] proposed a McEliece type system based on disguised Gabidulin rank metric codes.
- The general version also involves an enlargement of the matrix space.

University of Zurich

Original GPT McEliece system[GPT91]

Consider the generator matrix of an $[n, k, t]$ Gabidulin code:

$$G := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \dots & \alpha_n^{[1]} \\ & & \vdots & \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \dots & \alpha_n^{[k-1]} \end{pmatrix}$$

Original GPT McEliece system[GPT91]

Consider the generator matrix of an $[n, k, t]$ Gabidulin code:

$$G := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \dots & \alpha_n^{[1]} \\ & & \vdots & \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \dots & \alpha_n^{[k-1]} \end{pmatrix}$$

Let $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$, and $X \in \mathbb{F}_{q^m}^{k \times n}$ a matrix of column rank $t < t'$ over $\mathbb{F}_q$. The public key for the GPT system is given by:

$$\kappa_{\text{pub}} = (SG + X, t' - t).$$

Original GPT McEliece system[GPT91]

To encrypt a message $\boldsymbol{m}$, one chooses an error vector $\boldsymbol{e}$ of rank weight at most $t' - t$ and sends

$$\boldsymbol{m}(SG + X) + \boldsymbol{e} = \boldsymbol{m}SG + \boldsymbol{m}X + \boldsymbol{e}.$$

Original GPT McEliece system[GPT91]

To encrypt a message $\boldsymbol{m}$, one chooses an error vector $\boldsymbol{e}$ of rank weight at most $t' - t$ and sends

$$\boldsymbol{m}(SG + X) + \boldsymbol{e} = \boldsymbol{m}SG + \boldsymbol{m}X + \boldsymbol{e}.$$

Since

$$\mathrm{wt}_{\mathrm{R}}(\boldsymbol{m}X + \boldsymbol{e}) \leq t + (t' - t) = t,$$

we can decode this to $\boldsymbol{m}S$ and recover $\boldsymbol{m}$.

University of Zurich

Cryptanalysis by Overbeck[Ove08]

Let $\varphi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ be the Frobenius automorphism. Let $\mathcal{C} \subset \mathbb{F}_q^{m \times n} = (\mathbb{F}_{q^m})^n$ be an $[n, k, t]$ rank metric code and let $\varphi(\mathcal{C})$ denote the rank metric code when applying the Frobenius component-wise on the vectors in $(\mathbb{F}_{q^m})^n$. Overbeck observed that when $\mathcal{C}$ is a Gabidulin code having generator matrix

$$G := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \dots & \alpha_n^{[1]} \\ & & \vdots & \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \dots & \alpha_n^{[k-1]} \end{pmatrix}$$

then

$$\varphi(\mathcal{C}) \cap \mathcal{C}$$

represents a Gabidulin code of dimension $k-1$. This was the basis of a polynomial time algorithm to retrieve the hidden Gabidulin

Variants of rank metric McEliece Systems

Variants of rank metric McEliece Systems

- **Berger and Loidreau** [BL05] have proposed to use subcodes of Gabidulin codes as the basis of a GPT cryptosystem, as their structure is more complicated and would resist Gibson's attack.

Variants of rank metric McEliece Systems

- **Berger and Loidreau** [BL05] have proposed to use subcodes of Gabidulin codes as the basis of a GPT cryptosystem, as their structure is more complicated and would resist Gibson's attack.
- **Loidreau** [Loi10] constructs a specific variant where G_{ext} of Overbeck's attack has a large dimensional kernel: The public generator matrix has the form:

$$S(G \mid Z)T, \tag{1}$$

for G a generator matrix of a $\text{Gab}_{n,k}(\alpha)$ code, $S \in \text{GL}_n(\mathbb{F}_{q^m})$, Z a random $k \times t$ matrix with entries in $\mathbb{F}_{q^m}$ and $T \in \text{GL}_{n+t}(\mathbb{F}_q)$ an isometry of the rank metric.

Variants of rank metric McEliece Systems

- **Berger and Loidreau** [BL05] have proposed to use subcodes of Gabidulin codes as the basis of a GPT cryptosystem, as their structure is more complicated and would resist Gibson's attack.
- **Loidreau** [Loi10] constructs a specific variant where G_{ext} of Overbeck's attack has a large dimensional kernel: The public generator matrix has the form:

$$S(G \mid Z)T, \tag{1}$$

  for G a generator matrix of a $\text{Gab}_{n,k}(\alpha)$ code, $S \in \text{GL}_n(\mathbb{F}_{q^m})$, Z a random $k \times t$ matrix with entries in $\mathbb{F}_{q^m}$ and $T \in \text{GL}_{n+t}(\mathbb{F}_q)$ an isometry of the rank metric.
- **Gabidulin, Rashwan and Honary** [GRH09] proposed a column scrambler variant which is supposed to resist Overbeck's attack.

Distinguisher for rank metric McEliece Systems

The following result allows one to build distinguishers for Gabidulin variants of rank metric McEliece Systems.

Theorem (Marshall-Trautmann 2015)

(Marshall-Trautmann 2015) *An $[n, k, d]$ (linear) rank metric code is isometrically equivalent to a Gabidulin code if and only if*

$$\varphi(\mathcal{C}) \cap \mathcal{C}$$

has dimension equal to $k - 1$.

Distinguisher for rank metric McEliece Systems

Lemma

The set of $[n, k, d]$ rank metric codes for which

$$\varphi(\mathcal{C}) \cap \mathcal{C} = \{0\}$$

forms a generic set in the Grassmann variety.

Distinguisher for rank metric McEliece Systems

Lemma

The set of $[n, k, d]$ rank metric codes for which

$$\varphi(\mathcal{C}) \cap \mathcal{C} = \{0\}$$

forms a generic set in the Grassmann variety.

Remark

As we can see, using above distinguisher, many if not all published variants based on Gabidulin codes are insecure.

Research Questions:

- **Complexity of Decoding:** Berlekamp, McEliece and van Tilborg showed [BMvT78] that decoding a generic linear code is a NP-complete problem. Can something similar been shown for rank metric codes or more generally for subspace codes.

University of Zurich

Research Questions:

- **Complexity of Decoding:** Berlekamp, McEliece and van Tilborg showed [BMvT78] that decoding a generic linear code is a NP-complete problem. Can something similar been shown for rank metric codes or more generally for subspace codes.
- **Classes of rank metric and subspace Codes:** Find classes of rank metric and subspace codes, in particular orbit codes which come with decoding algorithm of polynomial time. Is it possible to come up with McEliece type systems.

Research Questions:

- **Complexity of Decoding:** Berlekamp, McEliece and van Tilborg showed [BMvT78] that decoding a generic linear code is a NP-complete problem. Can something similar been shown for rank metric codes or more generally for subspace codes.
- **Classes of rank metric and subspace Codes:** Find classes of rank metric and subspace codes, in particular orbit codes which come with decoding algorithm of polynomial time. Is it possible to come up with McEliece type systems.
- **Variants of McEliece:** Can one specify transformations which are "almost isometries" or which can correct certain error patterns.

A McEliece variant based on Subspace Codes

Consider an orbit code

$$\mathcal{C} = \{\mathcal{U} \cdot A \mid A \in \mathfrak{G}\},$$

where $\mathcal{U} \in \mathcal{G}(k, n)$ and $\mathfrak{G} < GL_n(\mathbb{F}_q)$ and where we know that a polynomial time decoding algorithm exists.

A McEliece variant based on Subspace Codes

Consider an orbit code

$$\mathcal{C} = \{\mathcal{U} \cdot A \mid A \in \mathfrak{G}\},$$

where $\mathcal{U} \in \mathcal{G}(k, n)$ and $\mathfrak{G} < GL_n(\mathbb{F}_q)$ and where we know that a polynomial time decoding algorithm exists.

- **Public key:** Let T be a random invertible matrix. Public are then the "base point" $\mathcal{U}T$ and the acting group $T^{-1}\mathfrak{G}T$.

A McEliece variant based on Subspace Codes

Consider an orbit code

$$\mathcal{C} = \{\mathcal{U} \cdot A \mid A \in \mathfrak{G}\},$$

where $\mathcal{U} \in \mathcal{G}(k, n)$ and $\mathfrak{G} < GL_n(\mathbb{F}_q)$ and where we know that a polynomial time decoding algorithm exists.

- **Public key:** Let T be a random invertible matrix. Public are then the "base point" $\mathcal{U}T$ and the acting group $T^{-1}\mathfrak{G}T$.
- **Private Key:** The invertible matrix T.

University of Zurich

A McEliece variant based on Subspace Codes

Consider an orbit code

$$\mathcal{C} = \{\mathcal{U} \cdot A \mid A \in \mathfrak{G}\},$$

where $\mathcal{U} \in \mathcal{G}(k, n)$ and $\mathfrak{G} < GL_n(\mathbb{F}_q)$ and where we know that a polynomial time decoding algorithm exists.

- **Public key:** Let T be a random invertible matrix. Public are then the "base point" $\mathcal{U}T$ and the acting group $T^{-1}\mathfrak{G}T$.
- **Private Key:** The invertible matrix T.
- **Security:** Is based on the hardness of decoding a general orbit code.

University of Zurich

Interesting Variants which might survive a quantum computer:

- **Medium Density Parity Check Codes:** Baldi, Bambozzi and Chiaraluce [BBC11] proposed a concatination of disguised quasi cyclic codes. These codes have moderate public key size and are of the type 'medium density parity check code'.

University of Zurich

Interesting Variants which might survive a quantum computer:

- **Medium Density Parity Check Codes:** Baldi, Bambozzi and Chiaraluce [BBC11] proposed a concatination of disguised quasi cyclic codes. These codes have moderate public key size and are of the type 'medium density parity check code'.
- **Near Isometries:** As a Public key choose $\tilde{G} := SGP$ where S is a random invertible matrix and P is a low weight transformation, i.e. 'near isometry'. Such variants were proposed in [BBC$^+$16].

Thank you for your attention.

Special thanks to:

Marco Baldi, Franco Chiaraluce, Josep Climent, Felix Fontein, Heide Gluesing Luerssen, Elisa Gorla, Juan Antonio Lopez Ramos, Gerard Maze, Giacomo Micheli, Chris Monico, Davide Schipani, Reto Schnyder, Urs Wagner, Violetta Weger, Jens Zumbrägel.

University of Zurich

M. Baldi, F. Bambozzi, and F. Chiaraluce.
On a family of circulant matrices for quasi-cyclic low-density generator matrix codes.
IEEE Trans. Inform. Theory, 57(9):6052–6067, 2011.

M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani.
Enhanced public key security for the McEliece cryptosystem.
Journal of Cryptology, pages 1–27, 2016.

T. P. Berger and P. Loidreau.
How to mask the structure of codes for a cryptographic use.
Des. Codes Cryptogr., 35(1):63–79, 2005.

E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg.
On the inherent intractability of certain coding problems.
IEEE Trans. Information Theory, IT-24(3):384–386, 1978.

Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich, and Valérie Gauthier-Umaña.

A polynomial-time attack on the BBCRS scheme.

In *Public-key cryptography—PKC 2015*, volume 9020 of *Lecture Notes in Comput. Sci.*, pages 175–193. Springer, Heidelberg, 2015.

J. K. Gibson.

Severely denting the Gabidulin version of the McEliece public key cryptosystem.

Des. Codes Cryptogr., 6(1):37–45, 1995.

E.M. Gabidulin, A.V. Paramonov, and O.V. Tretjakov.
Ideals over a non-commutative ring and their application in cryptology.
In DonaldW. Davies, editor, *Advances in Cryptology, EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pages 482–489. Springer Berlin Heidelberg, 1991.

E.M. Gabidulin, H. Rashwan, and B. Honary.
On improving security of gpt cryptosystems.
In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 1110–1114, June 2009.

P. Loidreau.
Designing a rank metric based McEliece cryptosystem.
In *Post-quantum cryptography*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 142–152. Springer, Berlin, 2010.

R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.

Technical report, DSN Progress report # 42-44, Jet Propulsion Laboratory, Pasadena, Californila, 1978.

C. Monico, J. Rosenthal, and A. Shokrollahi.

Using low density parity check codes in the McEliece cryptosystem.

In *Proceedings of the 2000 IEEE International Symposium on Information Theory*, page 215, Sorrento, Italy, 2000.

Use of Public Standards for the Secure sharing of Information Among National Security Systems.

Technical report, Committee on National Security Systems, July 2015.

CNSS Advisory Memorandum.

Report on Post-Quantum Cryptography.
Technical report, National Institute of Standards and Technology, February 2016.
NISTIR 8105.

R. Overbeck.
Structural attacks for public key cryptosystems based on Gabidulin codes.
J. Cryptology, 21(2):280–301, 2008.

P. W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5):1484–1509, 1997.

V. M. Sidelnikov and S. O. Shestakov.

On an encoding system constructed on the basis of generalized Reed-Solomon codes.

Diskret. Mat., 4(3):57–63, 1992.