Post-Quantum Cryptography

P. Felke

26th of October
2023

How it all started

An:

E. Becker
Ralph Berr
Peter Caspers
Patrick Felke
Hagen Hannemann
Boris Hemkemeier
Helma Lettau
Carsten Moeller
Michael Niermann
Axel Pawellek
Frank Vallentin

Liebe Kryptographie-Seminar Interessenten,

Herr Becker und ich haben einen ersten Vorschlag fuer den Ablauf des Blockseminars "Kryptographie und Algebra" fertiggestellt.

TERMIN:
Preferenz:
Fr, 13. Nov/Sa, 14. Nov.

Ausweichtermin:
Fr, 6. Nov./Sa, November
Wir bitten um Stellungnahmen zu diesem Terminvorschlag.

VORBESPRECHUNG:
Der Termin fuer Seminarvorbesprechung ist nach wie vor:
Mittwoch, 21.10.98. 10.15 Uhr im Seminarraum M/SR 911.

LEKTUERE:
Dem Seminar liegen im Wesentlichen 2 Quellen zu Grunde:
1) Neal Koblitz: Algebraic Aspects of Cryptography, Springer Verlag

2) Beutelsbacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie, Vieweg Verlag

Als Lektuere fuer alle vor dem Seminar setzen wir die Kapitel 1 und 2 aus dem Buch von Koblitz voraus (sind sehr gut zu lesen). Diese werden als Fotokopien bei Frau Jahn Anfang Oktober erhaeltlich sein. Das Buch von Koblitz ist leider teuer. Wir sehen zu es bald am Lehrstuhl zur Verfuegung zu haben.

Symmetric Cryptography

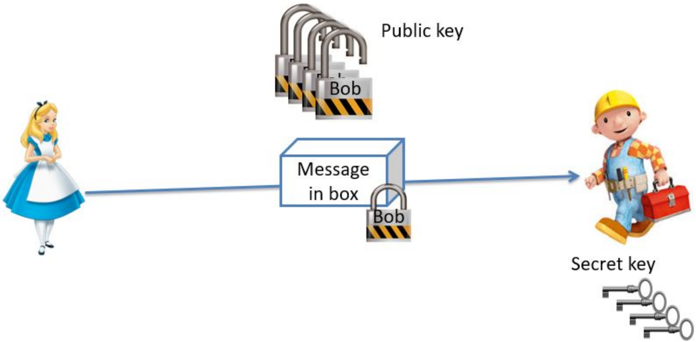
- Symmetric cryptography is a tool developed to ensure the confidentiality of a message.
- Alice encrypts a secret message with an encryption algorithm E and key k_{AB}. Bob decrypts the ciphertext by using a decryption algorithm D together with the same k_{AB}.
- An attacker with access to the channel should not be able to understand the communication.
- The key must be transmitted via a secure channel (out-of-band) between Alice and Bob.

Public-Key Cryptography

Public-key cryptography gives positive answers to the following questions:

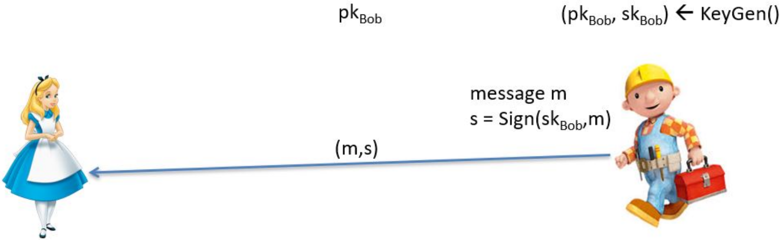
- Can two people who have never met have a private conversation?
- Is it possible to digitally sign documents?

Public-Key Encryption



- This is achieved by introducing cryptosystems using a pair of keys.
- Alice encrypts a message for Bob with Bob's public key pk_{Bob}.
- Bob decrypts the message with his secret key sk_{Bob}.
- pk_{Bob} can be transmitted over an insecure channel.
sk_{Bob} has to be stored securely.

Digital Signatures



- Bob signs a message for Alice with his secret key sk_{Bob}.
- Alice verifies the received signature with Bob's pk_{Bob}.

☞The famous RSA public-key cryptosystem can be easily turned into a signature algorithm. This also explains why it is so widespread nowadays.

☞The result of these positive answers is that

Cryptography is Ubiquitious

Cryptography is Ubiquitous

Signal

It is deployed in

Cryptography is Ubiquitious

It is deployed in

- messenger services,
- electronic commerce,
- automotive industry,
- cloud computing,
- ⋮

Security Principles of Public-Key Cryptography

Security Principles of Public-Key Cryptography

All widely used public-key systems rely on hard problems from algebraic number theory.

Security Principles of Public-Key Cryptography

All widely used public-key systems rely on hard problems from algebraic number theory.

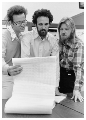
- RSA is based on the hardness of integer factorization, $n = pq$.

Security Principles of Public-Key Cryptography

All widely used public-key systems rely on hard problems from algebraic number theory.

- RSA is based on the hardness of integer factorization, $n = pq$.

- Diffie-Hellman(-Merkle) key exchange is based on the hardness of computing the discrete logarithm, $y = g^a, \log_g(y) = a$ (dlog).

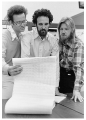


Security Principles of Public-Key Cryptography

All widely used public-key systems rely on hard problems from algebraic number theory.

- RSA is based on the hardness of integer factorization, $n = pq$.

- Diffie-Hellman(-Merkle) key exchange is based on the hardness of computing the discrete logarithm, $y = g^a, \log_g(y) = a$ (dlog).



- Elliptic curve cryptography (ECC) is based on the special case of the elliptic curve discrete logarithm, $Q = sP, \log_P(Q) = s$.

These problems allow systems of small key sizes.

Practical Key Sizes

RSA bit size of modulus n		Dlog bit size of prime field $\mathbb{F}_p$		ECC bit size of field $\mathbb{F}_n$
2800	$\sim$	2800	$\sim$	240
3000	$\sim$	3000	$\sim$	250

Practical Key Sizes

RSA bit size of modulus n		Dlog bit size of prime field $\mathbb{F}_p$		ECC bit size of field $\mathbb{F}_n$
2800	$\sim$	2800	$\sim$	240
3000	$\sim$	3000	$\sim$	250

Technical guideline TR-02102-1, Version 2023-1 from the Federal Office for Information Security (FOIS).

With these key sizes the underlying problems are supposed to be hard and the systems considered practical secure.

Practical Key Sizes

RSA		Dlog		ECC
bit size of modulus n		bit size of prime field $\mathbb{F}_p$		bit size of field $\mathbb{F}_n$
2800	$\sim$	2800	$\sim$	240
3000	$\sim$	3000	$\sim$	250

Technical guideline TR-02102-1, Version 2023-1 from the Federal Office for Information Security (FOIS).
With these key sizes the underlying problems are supposed to be hard and the systems considered practical secure.

Practical Security (informal)

A cryptosystem is practical secure if the best known algorithm for breaking it requires (almost for sure) an unreasonable amount of time or memory using available computing power.

For the systems above the best known algorithms require to solve the underlying hard problem.

What are hard Problems?

James L. Massey:“A hard problem is a problem nobody works on.”

What if Somebody Works on it...

What if Somebody Works on it...

If large enough quantum computers can be built

What if Somebody Works on it...

If large enough quantum computers can be built

- all schemes based on RSA, Dlog, ECC are insecure (Shor'94).

Is this not just thinking about the far future?

What if Somebody Works on it...

If large enough quantum computers can be built

- all schemes based on RSA, Dlog, ECC are insecure (Shor'94).

Is this not just thinking about the far future?
News in Jan. 2014 (Washington Post, Snowden Files)

- NSA has spent 85M$ on research to build a quantum computer.
- After the disclosure the National Institute for Standards and Technology (NIST, US pendant to FOIS) initiated the PQC competition.

What if Somebody Works on it...

If large enough quantum computers can be built

- all schemes based on RSA, Dlog, ECC are insecure (Shor'94).

Is this not just thinking about the far future?
News in Jan. 2014 (Washington Post, Snowden Files)

- NSA has spent 85M$ on research to build a quantum computer.
- After the disclosure the National Institute for Standards and Technology (NIST, US pendant to FOIS) initiated the PQC competition.

☞Symmetric cryptography remains secure when employed with larger but still moderate sized keys. These schemes remain practical.

The NIST Post-Quantum Cryptography Competition

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

- Start: 2016
- End: 2022, Draft standards until 2024.
- 2022: Round 4 submissions for backup candidates.

☞Post-quantum cryptography deals with designing cryptographic algorithms which are still secure even if large enough quantum computers can be built.

The NIST Post-Quantum Cryptography Competition

`https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`

- Start: 2016
- End: 2022, Draft standards until 2024.
- 2022: Round 4 submissions for backup candidates.

☞Post-quantum cryptography deals with designing cryptographic algorithms which are still secure even if large enough quantum computers can be built.
Secure means again practical secure.

The new Candidates

The submitted candidates are based on the following hard problems with respect to post-quantum cryptography.

- Lattice-based crypto (e.g. hardness of finding short vectors).
- Code-based crypto (hardness of decoding a random code).
- Multivariate crypto (hardness of solving a random system of quadratic equations).

- Most designs discussed in this competition are not new. Due to their large key sizes they were rarely employed in practice before this competition.
  Up to 1 Mb for a security level of e.g. 2048 bit ≈ 200 byte RSA.

The new Candidates

The submitted candidates are based on the following hard problems with respect to post-quantum cryptography.

- Lattice-based crypto (e.g. hardness of finding short vectors).
- Code-based crypto (hardness of decoding a random code).
- Multivariate crypto (hardness of solving a random system of quadratic equations).

- Most designs discussed in this competition are not new. Due to their large key sizes they were rarely employed in practice before this competition.
  Up to 1 Mb for a security level of e.g. 2048 bit ≈ 200 byte RSA.
- E.g. multivariate cryptosystems have been studied by E. Becker and others long before this competition (diploma theses by M. Daum and P.Felke).

The new Candidates

The submitted candidates are based on the following hard problems with respect to post-quantum cryptography.

- Lattice-based crypto (e.g. hardness of finding short vectors).
- Code-based crypto (hardness of decoding a random code).
- Multivariate crypto (hardness of solving a random system of quadratic equations).

- Most designs discussed in this competition are not new. Due to their large key sizes they were rarely employed in practice before this competition.
  Up to 1 Mb for a security level of e.g. 2048 bit ≈ 200 byte RSA.
- E.g. multivariate cryptosystems have been studied by E. Becker and others long before this competition (diploma theses by M. Daum and P.Felke).
  A good reason to have a look at these cryptosystems.

Introduction

The PQC Competition

Multivariate Cryptography

Finalists of PQC Competition

Going Back to the 80s

The Imai-Matsumoto Cryptosystem C^* (1988)

Going Back to the 80s

The Imai-Matsumoto Cryptosystem C^* (1988)

- Presented at Eurocrypt 1988.
- Particularly useful for lightweight cryptography, e.g. lowcost smartcards, IoT devices, ...

Going Back to the 80s

The Imai-Matsumoto Cryptosystem C^* (1988)

- Presented at Eurocrypt 1988.
- Particularly useful for lightweight cryptography, e.g. lowcost smartcards, IoT devices, ...
- It resists known attacks based on quantum computers.

Going Back to the 80s

The Imai-Matsumoto Cryptosystem C^* (1988)

- Presented at Eurocrypt 1988.
- Particularly useful for lightweight cryptography, e.g. lowcost smartcards, IoT devices, . . .
- It resists known attacks based on quantum computers.
- Drawback is its public key size - 127 kbyte for a security level of 2048 bit RSA.
  The secret key size is 4 kbyte.

Going Back to the 80s

The Imai-Matsumoto Cryptosystem C^* (1988)

- Presented at Eurocrypt 1988.
- Particularly useful for lightweight cryptography, e.g. lowcost smartcards, IoT devices, ...
- It resists known attacks based on quantum computers.
- Drawback is its public key size - 127 kbyte for a security level of 2048 bit RSA.
  The secret key size is 4 kbyte.
- FOIS planned in the 90th to implement a variant in devices employed for national security.

The Imai-Matsumoto Cryptosystem C^*

The Imai-Matsumoto Cryptosystem C^*

General parameters:

The Imai-Matsumoto Cryptosystem C^*

General parameters:

1. A finite Field $\mathbb{F}_q$, $q := 2^m$, a field extension of $\mathbb{F}_{q^n}$ of degree n, an $\mathbb{F}_q$-basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$.

The Imai-Matsumoto Cryptosystem C^*

General parameters:

1. A finite Field $\mathbb{F}_q$, $q := 2^m$, a field extension of $\mathbb{F}_{q^n}$ of degree n, an $\mathbb{F}_q$-basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$.
2. A $0 \leq \theta \leq n-1$, s.t. the power function $\pi(X) := X^{q^\theta+1}$ is bijective, i.e. $\gcd(q^\theta+1, q^n-1) = 1$.
3. The inverse mapping, which is the power mapping $\pi^{-1}(X) = X^h$ with $h(q^\theta+1) = 1 \bmod q^n - 1$.

The Imai-Matsumoto Cryptosystem C^*

General parameters:

1. A finite Field $\mathbb{F}_q$, $q := 2^m$, a field extension of $\mathbb{F}_{q^n}$ of degree n, an $\mathbb{F}_q$-basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$.
2. A $0 \leq \theta \leq n-1$, s.t. the power function $\pi(X) := X^{q^\theta + 1}$ is bijective, i.e. $\gcd(q^\theta + 1, q^n - 1) = 1$.
3. The inverse mapping, which is the power mapping $\pi^{-1}(X) = X^h$ with $h(q^\theta + 1) = 1 \bmod q^n - 1$.

Secret key:

The Imai-Matsumoto Cryptosystem C^*

General parameters:

1. A finite Field $\mathbb{F}_q$, $q := 2^m$, a field extension of $\mathbb{F}_{q^n}$ of degree n, an $\mathbb{F}_q$-basis $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$ of $\mathbb{F}_{q^n}$.
2. A $0 \leq \theta \leq n-1$, s.t. the power function $\pi(X) := X^{q^\theta+1}$ is bijective, i.e. $\gcd(q^\theta + 1, q^n - 1) = 1$.
3. The inverse mapping, which is the power mapping $\pi^{-1}(X) = X^h$ with $h(q^\theta + 1) = 1 \bmod q^n - 1$.

Secret key:

1. Affine Transformations $S = Ax + d$, $T = Bx + e$, $A, B \in GL(n, \mathbb{F}_q)$, und $d, e \in \mathbb{F}_q^n$.

☞Condition 2 requires q^n to be even. It is easy to find proper n such that condition 2 can be fulfilled.

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^{n} p_{il}^{(\theta)} \beta_l$ and $\beta_i \beta_j = \sum_{l=1}^{n} m_{ijl} \beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^{n} p_{il}^{(\theta)} \beta_l$ and $\beta_i \beta_j = \sum_{l=1}^{n} m_{ijl} \beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^{n} u_i \beta_i, u_i \in \mathbb{F}_q$ then

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)} \beta_l$ and $\beta_i \beta_j = \sum_{l=1}^n m_{ijl} \beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i \beta_i, u_i \in \mathbb{F}_q$ then

$\mathbf{v} = \sum_{l=1}^n v_l \beta_l =$

$\left(\sum_{i=1}^n u_i \beta_i^{q^\theta}\right) \left(\sum_{j=1}^n u_j \beta_j\right) =$

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)} \beta_l$ and $\beta_i\beta_j = \sum_{l=1}^n m_{ijl}\beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i\beta_i, u_i \in \mathbb{F}_q$ then

$\mathbf{v} = \sum_{l=1}^n v_l\beta_l =$

$\left(\sum_{i=1}^n u_i\beta_i^{q^\theta}\right)\left(\sum_{j=1}^n u_j\beta_j\right) = \left(\sum_{1\le i,\le \boldsymbol{\mu} \le n} p_{i\boldsymbol{\mu}}^{(\theta)} u_i\beta_{\boldsymbol{\mu}}\right)\left(\sum_{j=1}^n u_j\beta_j\right) =$

$\sum_{l=1}^n \left(\sum_{1\le i,j,\boldsymbol{\mu}\le n} p_{i\boldsymbol{\mu}}^{(\theta)} m_{\boldsymbol{\mu}jl} u_i u_j\right)\beta_l =$

$\sum_{l=1}^n \left(\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j\right)\beta_l.$

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.
It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)}\beta_l$ and $\beta_i\beta_j = \sum_{l=1}^n m_{ijl}\beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.
Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i\beta_i, u_i \in \mathbb{F}_q$ then
$\mathbf{v} = \sum_{l=1}^n v_l\beta_l =$
$\left(\sum_{i=1}^n u_i\beta_i^{q^\theta}\right)\left(\sum_{j=1}^n u_j\beta_j\right) = \left(\sum_{1\le i,\le \mu\le n} p_{i\mu}^{(\theta)} u_i\beta_\mu\right)\left(\sum_{j=1}^n u_j\beta_j\right) =$
$\sum_{l=1}^n\left(\sum_{1\le i,j,\mu\le n} p_{i\mu}^{(\theta)} m_{\mu jl}u_iu_j\right)\beta_l =$
$\sum_{l=1}^n\left(\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_iu_j\right)\beta_l$. Comparing coeff. yields $v_l =$
$\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_iu_j =: f_l(u_1,\dots,u_n) \Rightarrow \pi(\mathbf{u}) = \sum_{l=1}^n f_i(u_1,\dots,u_n)\beta_l$.

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)} \beta_l$ and $\beta_i\beta_j = \sum_{l=1}^n m_{ijl}\beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i\beta_i, u_i \in \mathbb{F}_q$ then

$\mathbf{v} = \sum_{l=1}^n v_l\beta_l =$

$\left(\sum_{i=1}^n u_i\beta_i^{q^\theta}\right)\left(\sum_{j=1}^n u_j\beta_j\right) = \left(\sum_{1\le i,\le \mu\le n} p_{i\mu}^{(\theta)} u_i\beta_\mu\right)\left(\sum_{j=1}^n u_j\beta_j\right) =$

$\sum_{l=1}^n \left(\sum_{1\le i,j,\mu\le n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j\right)\beta_l =$

$\sum_{l=1}^n \left(\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j\right)\beta_l$. Comparing coeff. yields $v_l =$

$\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j =: f_l(u_1,\ldots,u_n) \Rightarrow \pi(\mathbf{u}) = \sum_{l=1}^n f_i(u_1,\ldots,u_n)\beta_l$.

The mult. representation of $\pi(X)$ is $f_1,\ldots,f_n$ and hidden by

$$T \circ \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \circ S =$$

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)}\beta_l$ and $\beta_i\beta_j = \sum_{l=1}^n m_{ijl}\beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i\beta_i, u_i \in \mathbb{F}_q$ then

$\mathbf{v} = \sum_{l=1}^n v_l\beta_l =$

$\left(\sum_{i=1}^n u_i\beta_i^{q^\theta}\right)\left(\sum_{j=1}^n u_j\beta_j\right) = \left(\sum_{1\le i,\le \mu\le n} p_{i\mu}^{(\theta)} u_i\beta_\mu\right)\left(\sum_{j=1}^n u_j\beta_j\right) =$

$\sum_{l=1}^n \left(\sum_{1\le i,j,\mu\le n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j\right)\beta_l =$

$\sum_{l=1}^n \left(\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j\right)\beta_l$. Comparing coeff. yields $v_l =$

$\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j =: f_l(u_1,\dots,u_n) \Rightarrow \pi(\mathbf{u}) = \sum_{l=1}^n f_i(u_1,\dots,u_n)\beta_l$.

The mult. representation of $\pi(X)$ is $f_1,\dots,f_n$ and hidden by

$$T \circ \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \circ S = B \begin{pmatrix} f_1((Ax+d)_1,\dots,(Ax+d)_n) \\ \vdots \\ f_n((Ax+d)_1,\dots,(Ax+d)_n) \end{pmatrix} + e = \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix}$$

Construction of the Public-Key

Compute the multivariate representation of $\pi(X) = X^{q^\theta+1}$ with respect to $\mathcal{B}$.

It is $\beta_i^{q^\theta} = \sum_{l=1}^n p_{il}^{(\theta)} \beta_l$ and $\beta_i\beta_j = \sum_{l=1}^n m_{ijl}\beta_l, p_{il}^{(\theta)}, m_{ijl} \in \mathbb{F}_q$.

Set $\mathbf{v} := \pi(\mathbf{u}) = \mathbf{u}^{q^\theta+1}, \mathbf{u} := \sum_{i=1}^n u_i\beta_i, u_i \in \mathbb{F}_q$ then

$\mathbf{v} = \sum_{l=1}^n v_l\beta_l =$

$\left(\sum_{i=1}^n u_i\beta_i^{q^\theta}\right)\left(\sum_{j=1}^n u_j\beta_j\right) = \left(\sum_{1\le i,\le\mu\le n} p_{i\mu}^{(\theta)} u_i\beta_\mu\right)\left(\sum_{j=1}^n u_j\beta_j\right) =$

$\sum_{l=1}^n \left(\sum_{1\le i,j,\mu\le n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j\right)\beta_l =$

$\sum_{l=1}^n \left(\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j\right)\beta_l$. Comparing coeff. yields $v_l =$

$\sum_{1\le i\le j\le n} a_{ij}^{(l)} u_i u_j =: f_l(u_1,\dots,u_n) \Rightarrow \pi(\mathbf{u}) = \sum_{l=1}^n f_i(u_1,\dots,u_n)\beta_l$.

The mult. representation of $\pi(X)$ is $f_1,\dots,f_n$ and hidden by

$$T \circ \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \circ S = B \begin{pmatrix} f_1((Ax+d)_1,\dots,(Ax+d)_n) \\ \vdots \\ f_n((Ax+d)_1,\dots,(Ax+d)_n) \end{pmatrix} + e = \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix}$$

The quadratic polynomials $p_1,\dots,p_n$ constitute the public key.

The computations are mod $x_1^q + x_1,\dots,x_n^q + x_n$.

Encryption/Decryption with C^*

Encryption (public):

$$m \in \mathbb{F}_q^n \xrightarrow{c=(p_1(m),\ldots,p_n(m))^t=T\circ\boldsymbol{\pi}\circ S(m)} c \in \mathbb{F}_q^n$$

Encryption/Decryption with C^*

Encryption (public):

$$m \in \mathbb{F}_q^n \xrightarrow{\quad c=(p_1(m),\dots,p_n(m))^t = T\circ\pi\circ S(m) \quad} c \in \mathbb{F}_q^n$$

Decryption (secret):

$$\begin{array}{ccccccc}
m & \xleftarrow{S^{-1}} & \mathbb{F}_q^n & & \mathbb{F}_q^n & \xleftarrow{T^{-1}} & c \\
 & & \uparrow \Phi_{\mathcal{B}}^{-1} & & \downarrow \Phi_{\mathcal{B}} & & \\
 & & \mathbb{F}_{q^n} & \xleftarrow{\pi(X)^{-1}=X^h} & \mathbb{F}_{q^n} & &
\end{array}$$

$$\Phi_{\mathcal{B}}(v) := \sum_{i=1}^n v_i\beta_i$$

Encryption/Decryption

- Alice encrypts a message $m = (m_1, \ldots, m_n)$ by computing

$$
\begin{aligned}
c_1 &= p_1(m_1, \ldots, m_n) \\
&\vdots \\
c_n &= p_n(m_1, \ldots, m_n)
\end{aligned}
$$

- Bob decrypts the ciphertext $c = (c_1, \ldots, c_n)$ by computing
  1. $v = T^{-1}(c)$
  2. $\pi^{-1}(\sum v_i \beta_i) = (\mathbf{v})^h = \mathbf{u} = \sum u_i \beta_i \Rightarrow u = (u_1, \ldots, u_n)$
  3. $m = S^{-1}(u)$

Security

Security

Malicious Eve (attacker) faces the problem to solve the following system of quadratic equations

$$
\begin{aligned}
c_1 &= p_1(x_1, \ldots, x_n) \\
&\vdots \\
c_n &= p_n(x_1, \ldots, x_n),
\end{aligned}
$$

which has the unique solution $(m_1, \ldots, m_n)^t$ in $\mathbb{F}_q^n$.

Security

Malicious Eve (attacker) faces the problem to solve the following system of quadratic equations

$$\begin{aligned} c_1 &= p_1(x_1, \ldots, x_n) \\ &\vdots \\ c_n &= p_n(x_1, \ldots, x_n), \end{aligned}$$

which has the unique solution $(m_1, \ldots, m_n)^t$ in $\mathbb{F}_q^n$.

Gröbner Bases are commonly used to solve such systems.

Security

Malicious Eve (attacker) faces the problem to solve the following system of quadratic equations

$$\begin{aligned} c_1 &= p_1(x_1, \ldots, x_n) \\ &\vdots \\ c_n &= p_n(x_1, \ldots, x_n), \end{aligned}$$

which has the unique solution $(m_1, \ldots, m_n)^t$ in $\mathbb{F}_q^n$.
Gröbner Bases are commonly used to solve such systems.

Systems of quadratic equations

Solving a system of m quadratic equations in n variables is NP-hard with respect to worst case complexity.

Security

Malicious Eve (attacker) faces the problem to solve the following system of quadratic equations

$$\begin{aligned} c_1 &= p_1(x_1, \ldots, x_n) \\ &\vdots \\ c_n &= p_n(x_1, \ldots, x_n), \end{aligned}$$

which has the unique solution $(m_1, \ldots, m_n)^t$ in $\mathbb{F}_q^n$.
Gröbner Bases are commonly used to solve such systems.

Systems of quadratic equations

Solving a system of m quadratic equations in n variables is NP-hard with respect to worst case complexity.

The decomposition problem, i.e. recovering the secret key S, T is supposed to be even harder.
Interpolating the inverse mapping is also infeasible.

The Big Surprise (especially for FOIS)

The Big Surprise (especially for FOIS)

- C^* was broken by J. Patarin in 1995. Independently by Dobbertin in 1993 while being employed at FOIS and thus his work was classified at this time.

The Big Surprise (especially for FOIS)

- C^* was broken by J. Patarin in 1995. Independently by Dobbertin in 1993 while being employed at FOIS and thus his work was classified at this time.
- The attack makes use of the unforeseen relation for $Y = X^{q^\theta+1}$:
  $YX^{q^{2\theta}} + Y^{q^\theta}X = 0$ for all $Y = X^{q^\theta+1}, X \in \mathbb{F}_{q^n}$.

The Big Surprise (especially for FOIS)

- C^* was broken by J. Patarin in 1995. Independently by Dobbertin in 1993 while being employed at FOIS and thus his work was classified at this time.
- The attack makes use of the unforeseen relation for $Y = X^{q^\theta+1}$:
  $YX^{q^{2\theta}} + Y^{q^\theta}X = 0$ for all $Y = X^{q^\theta+1}, X \in \mathbb{F}_{q^n}$.
- This yields at least $k \geq n$ multivariate relations
  $r_l(x,y) = \sum_{i,j}^n \gamma_{ij}^{(l)} x_i y_j + \sum_{i=1}^n \alpha_i^{(l)} x_i + \sum_{i=1}^n \beta_i^{(l)} y_i + \delta^{(l)}$
  fulfilled for all plaintext-ciphertext pairs (m, c).
  These can be easily computed from the public key.

The Big Surprise (especially for FOIS)

- C^* was broken by J. Patarin in 1995. Independently by Dobbertin in 1993 while being employed at FOIS and thus his work was classified at this time.
- The attack makes use of the unforeseen relation for $Y = X^{q^\theta+1}$:
  $YX^{q^{2\theta}} + Y^{q^\theta}X = 0$ for all $Y = X^{q^\theta+1}, X \in \mathbb{F}_{q^n}$.
- This yields at least $k \geq n$ multivariate relations $r_l(x,y) = \sum_{i,j}^n \gamma_{ij}^{(l)} x_i y_j + \sum_{i=1}^n \alpha_i^{(l)} x_i + \sum_{i=1}^n \beta_i^{(l)} y_i + \delta^{(l)}$ fulfilled for all plaintext-ciphertext pairs (m,c).
  These can be easily computed from the public key.
- Both proved that plugging in an intercepted ciphertext c yields a system of linear equations $r_l(x,c) = 0, 1 \leq l \leq k$ with a solution space of dimension $\leq \frac{n}{3}$.
  ☠ The plaintext can be recovered efficiently for all practical key sizes.
- The attack does not recover the secret key.

The Dawn of new Ideas and Cryptanalytic Techniques

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i+q^j}, a_{ij} \in \mathbb{F}_{q^n}$.

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i + q^j}$, $a_{ij} \in \mathbb{F}_{q^n}$.
☞The birth of the HFE-Cryptosystem (HFE=Hidden Field Equations).

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i+q^j}$, $a_{ij} \in \mathbb{F}_{q^n}$.
☞The birth of the HFE-Cryptosystem (HFE=Hidden Field Equations).
Drawback of HFE:

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i+q^j}$, $a_{ij} \in \mathbb{F}_{q^n}$.
☞The birth of the HFE-Cryptosystem (HFE=Hidden Field Equations).
Drawback of HFE:

1. Decryption is more complex.

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i + q^j}, a_{ij} \in \mathbb{F}_{q^n}$.
☞The birth of the HFE-Cryptosystem (HFE=Hidden Field Equations).
Drawback of HFE:

1. Decryption is more complex.
2. Secret key is larger.

The Dawn of new Ideas and Cryptanalytic Techniques

Patarin suggested to substitute $\pi(X)$ by
$P(X) := \sum a_{ij} X^{q^i + q^j}$, $a_{ij} \in \mathbb{F}_{q^n}$.
☞The birth of the HFE-Cryptosystem (HFE=Hidden Field Equations).
Drawback of HFE:

1. Decryption is more complex.
2. Secret key is larger.
3. Security evaluations are more complicated.

The Dawn of New Ideas and Cryptanalytic Techniques

The Dawn of New Ideas and Cryptanalytic Techniques

C^* and HFE can be modified to supposedly efficient signature schemes by removing equations (public polynomials) or adding "dummy" variables.

The Dawn of New Ideas and Cryptanalytic Techniques

C^* and HFE can be modified to supposedly efficient signature schemes by removing equations (public polynomials) or adding "dummy" variables.

- SFLASH and Quartz are systems based on these approach.
- Both had been submitted to the NESSIE Project (New European Schemes for Signature, Integrity and Encryption,2002-2003, project to support standardization) and accepted.

The Dawn of New Ideas and Cryptanalytic Techniques

C^* and HFE can be modified to supposedly efficient signature schemes by removing equations (public polynomials) or adding "dummy" variables.

- SFLASH and Quartz are systems based on these approach.
- Both had been submitted to the NESSIE Project (New European Schemes for Signature, Integrity and Encryption,2002-2003, project to support standardization) and accepted.
- First discussions about these schemes in Dortmund.
- Later a security analysis by N. Courtois, M. Daum and P. Felke rendered Quartz impractical.

The Dawn of New Ideas and Cryptanalytic Techniques

C^* and HFE can be modified to supposedly efficient signature schemes by removing equations (public polynomials) or adding "dummy" variables.

- SFLASH and Quartz are systems based on these approach.
- Both had been submitted to the NESSIE Project (New European Schemes for Signature, Integrity and Encryption,2002-2003, project to support standardization) and accepted.
- First discussions about these schemes in Dortmund.
- Later a security analysis by N. Courtois, M. Daum and P. Felke rendered Quartz impractical.
- Later SFLASH and certain HFE-type cryptosystems were broken with methods from the theory of nonassociative algebras and quadratic forms. In some cases even the secret key could be fully recovered (D. Coppersmith, P. Felke, P.A. Fouque, J. Stern et al.).

The Dawn of New Ideas and Cryptanalytic Techniques

C^* and HFE can be modified to supposedly efficient signature schemes by removing equations (public polynomials) or adding "dummy" variables.

- SFLASH and Quartz are systems based on these approach.
- Both had been submitted to the NESSIE Project (New European Schemes for Signature, Integrity and Encryption,2002-2003, project to support standardization) and accepted.
- First discussions about these schemes in Dortmund.
- Later a security analysis by N. Courtois, M. Daum and P. Felke rendered Quartz impractical.
- Later SFLASH and certain HFE-type cryptosystems were broken with methods from the theory of nonassociative algebras and quadratic forms. In some cases even the secret key could be fully recovered (D. Coppersmith, P. Felke, P.A. Fouque, J. Stern et al.).

☞ Many new approaches followed.

Current Status (excerpt)

- C^* (Imai-Matsumoto, Eurocrypt'88):
  broken (Dobbertin '93 (classified), Patarin, Crypto'95).
- Quartz (Patarin et al., Cryptographers Track RSA 2001):
  broken (Courtois, Daum, Felke , PKC 2003).
- SFLASH (Patatrin et al., 2001):
  broken (V. Dubois, P.A. Fouque, Crypto 2007)
- HFE and variants with branches (Patarin, Eurocrypt 1996):
  broken (L. Bettale et al., DCC 2013, P. Felke, WCC 2006).
- EFLASH (Cartor at al., SAC'18):
  broken (Øygarden, Felke et al., Cryptographers Track RSA 2020).
- Dob (Patarin et al., IACR Cryptol. ePrint Arch., 2018):
  broken (Øygarden, Felke et al., PKC 2021/J. of Crypt. (wip)).
- GeMSS (Faugere et al, submission to NIST PQC comp.):
  broken (Chengdong et al, Crypto 2021).
- Rainbow (Ding et al., NIST PQC candidate):
  broken (W. Beullens, Crypto, 2022).

Introduction

The PQC Competition

Multivariate Cryptography

Finalists of PQC Competition

Finalists and 4th Round Candidates

- None of the multivariate candidates survived in the NIST PQC competition. Research for new strong candidates is still ongoing.

Finalists and 4th Round Candidates

☠ None of the multivariate candidates survived in the NIST PQC competition. Research for new strong candidates is still ongoing.

On the 7th of July 2022 NIST announced after 3 rounds the algorithms to be standardized:

- public-key encryption: CRYSTALS-Kyber (lattice-based),
- digital signatures : CRYSTALS-Dilithium, FALCON, SPHINCS+ (all lattice-based).

4th round candidates (to have non-lattice-based alternatives):

- public-key encryption: Classic McEliece, Bike and HQC (code-based).

☠ The promising 4th round candidate SIKE (isogeny-based) was broken shortly after announcement (W. Castryck et al., Eurocrypt 2023).

Finalists and 4th Round Candidates

☠ None of the multivariate candidates survived in the NIST PQC competition. Research for new strong candidates is still ongoing.

On the 7th of July 2022 NIST announced after 3 rounds the algorithms to be standardized:

- public-key encryption: CRYSTALS-Kyber (lattice-based),
- digital signatures : CRYSTALS-Dilithium, FALCON, SPHINCS+ (all lattice-based).

4th round candidates (to have non-lattice-based alternatives):

- public-key encryption: Classic McEliece, Bike and HQC (code-based).

☠ The promising 4th round candidate SIKE (isogeny-based) was broken shortly after announcement (W. Castryck et al., Eurocrypt 2023).

This raises the question . . .

. . . should one start to implement the candidates?

- Companies like Google, Microsoft etc. started to employ and promote usage of PQC.
  Thus customers will ask for it in other branches.
- FOIS gives the following advice (technical guidelines 2021-1): Employ Classic McElice (as cryptanalysed since 1978) or another candidate in combination with a classic standard like ECC to e.g. derive two separate symmetric keys and from those a single key.
  The details are given in the guideline.
- Sooner or later PQC will be compulsory to fulfil certain guidelines.
- The keys are much bigger. Up to 1 Mb in comparison to 3000 bit nowadays.

☞ Industry has to react now as changes later might be impossible, e.g. in a hardware solutions or devices with too less memory.

A big challenge . . .

Security Issues

- History has shown that most of the cyberattacks against security solutions do not break the underlying crypto. It is exploited how the crypto is implemented or employed.
- The transition to PQC requires considerable changes in software and hardware.
- It is expected that these will open the door for new cyberattacks.

Thank you.
Any Questions?