# Fault Attacks on UOV and Rainbow

Juliane Krämer and Mirjam Loiero

Technische Universität Darmstadt
Germany

COSADE 2019

April 05, 2019

TECHNISCHE
UNIVERSITÄT
DARMSTADT

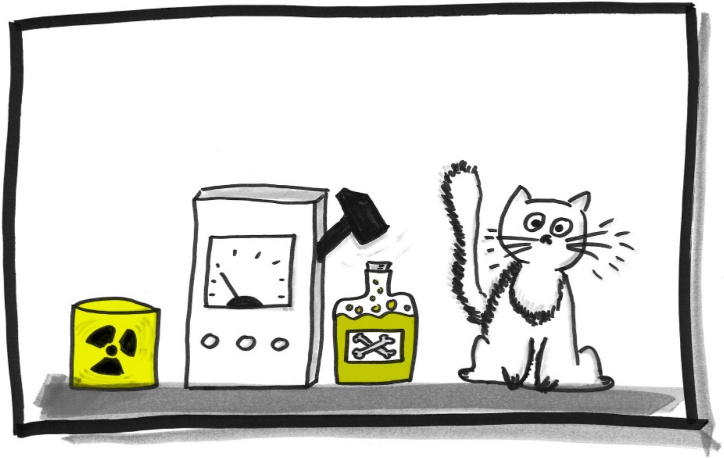
# Post-Quantum Cryptography

Post-Quantum Cryptography

$\longrightarrow$ Classical (Public-Key) Cryptography

threatened by Quantum Computers

# Superposition



# 1994

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor
Room 2D-149
AT&T Bell Labs
600 Mountain Avenue
Murray Hill, NJ 07974, USA
email: shor@research.att.com

**Abstract**

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time of at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, *e.g.,* the number of digits of the integer to be factored.

## Discrete Logarithm

Diffie-Hellman, DSA, El Gamal; ECC

## Factoring Problem

RSA

## Discrete Logarithm

~~Diffie-Hellman, DSA, El Gamal; ECC~~

## Factoring Problem

~~RSA~~


OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE?
$\psi^+$ or $\psi^-$ ?


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

# Candidates for Post-Quantum Cryptography

- … hash functions
- … isogenies
- … lattices
- … linear codes
- … multivariate equations

# Candidates for Post-Quantum Cryptography

- ... hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- ... isogenies
- ... lattices
- ... linear codes
- ... multivariate equations

# Candidates for Post-Quantum Cryptography

- ... hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- ... isogenies
  - ✓ can build on 25 years of research in ECC, simple parameter choice
  - ✗ very slow, not sufficiently scrutinized
- ... lattices
- ... linear codes
- ... multivariate equations

# Candidates for Post-Quantum Cryptography

- ... hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- ... isogenies
  - ✓ can build on 25 years of research in ECC, simple parameter choice
  - ✗ very slow, not sufficiently scrutinized
- ... lattices
  - ✓ versatile, security reductions
  - ✗ complicated parameter choice
- ... linear codes
- ... multivariate equations

# Candidates for Post-Quantum Cryptography

- ... hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- ... isogenies
  - ✓ can build on 25 years of research in ECC, simple parameter choice
  - ✗ very slow, not sufficiently scrutinized
- ... lattices
  - ✓ versatile, security reductions
  - ✗ complicated parameter choice
- ... linear codes
  - ✓ McEliece encryption, unbroken since 40 years
  - ✗ (too) large keys
- ... multivariate equations

# Candidates for Post-Quantum Cryptography

- ... hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- ... isogenies
  - ✓ can build on 25 years of research in ECC, simple parameter choice
  - ✗ very slow, not sufficiently scrutinized
- ... lattices
  - ✓ versatile, security reductions
  - ✗ complicated parameter choice
- ... linear codes
  - ✓ McEliece encryption, unbroken since 40 years
  - ✗ (too) large keys
- ... multivariate equations
  - ✓ MQ-Problem NP hard, very small signatures, very fast
  - ✗ all encryption schemes broken

# Candidates for Post-Quantum Cryptography

- … hash functions
  - ✓ minimal security assumptions, RFC for XMSS
  - ✗ only signature schemes possible
- … isogenies
  - ✓ can build on 25 years of research in ECC, simple parameter choice
  - ✗ very slow, not sufficiently scrutinized
- … lattices
  - ✓ versatile, security reductions
  - ✗ complicated parameter choice
- … linear codes
  - ✓ McEliece encryption, unbroken since 40 years
  - ✗ (too) large keys
- … **multivariate equations**
  - ✓ MQ-Problem NP hard, very small signatures, very fast
  - ✗ all encryption schemes broken

# Multivariate cryptography

$$p^{(1)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$\vdots$$

$$p^{(m)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

# Multivariate cryptography

$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

- central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ (easily invertible)
- two invertible affine maps $\mathcal{T} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{S} : \mathbb{F}^n \to \mathbb{F}^n$

- public key: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$
- private key: $\mathcal{T}$, $\mathcal{F}$, and $\mathcal{S}$

# Multivariate cryptography

- message $d$
- hash value $\mathbf{w} = \mathcal{H}(d)$
- signature $\mathbf{z}$

**Signature Generation**

$$\mathbf{w} \in \mathbb{F}^m \xrightarrow{\mathcal{T}^{-1}} \mathbf{x} \in \mathbb{F}^m \xrightarrow{\mathcal{F}^{-1}} \mathbf{y} \in \mathbb{F}^n \xrightarrow{\mathcal{S}^{-1}} \mathbf{z} \in \mathbb{F}^n$$

# Multivariate cryptography

- message $d$
- hash value $\mathbf{w} = \mathcal{H}(d)$
- signature $\mathbf{z}$

**Signature Generation**

$$\begin{tikzcd}
\mathbf{w} \in \mathbb{F}^m \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{x} \in \mathbb{F}^m \arrow[r, "\mathcal{F}^{-1}"] & \mathbf{y} \in \mathbb{F}^n \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{z} \in \mathbb{F}^n \arrow[lll, bend left, "\mathcal{P}"]
\end{tikzcd}$$

**Signature Verification**

# Fault Attacks on UOV and Rainbow

- targeting signature schemes UOV and Rainbow
- goal: reveal the affine maps $\mathcal{T}$ or $\mathcal{S}$
- decrease the complexity of a linear algebra attack by a fault attack

# Fault Attacks on UOV and Rainbow

- targeting signature schemes UOV and Rainbow
- goal: reveal the affine maps $\mathcal{T}$ or $\mathcal{S}$
- decrease the complexity of a linear algebra attack by a fault attack

- based on Hashimoto, Takagi, Sakurai: General fault attacks on multivariate public key cryptosystems, PQCrypto 2011

# Fault Attack on the Central Map 1/2

# Fault Attack on the Central Map 1/2

a permanent fault

# Fault Attack on the Central Map 1/2

a permanent fault changes a single coefficient

# Fault Attack on the Central Map 1/2

a permanent fault changes a single coefficient of the central map $\mathcal{F}$

# Fault Attack on the Central Map 1/2

a permanent fault changes a single coefficient
of the central map $\mathcal{F}$ during signature generation

# Fault Attack on the Central Map 1/2

a permanent fault changes a single coefficient
of the central map $\mathcal{F}$ during signature generation

- randomly chosen message $h$
- faulty signature of $h$: $z' := \mathcal{S}^{-1}(\mathcal{F}'^{-1}(\mathcal{T}^{-1}(h)))$

# Fault Attack on the Central Map 1/2

a permanent fault changes a single coefficient
of the central map $\mathcal{F}$ during signature generation

- randomly chosen message $h$
- faulty signature of $h$: $z' := \mathcal{S}^{-1}(\mathcal{F}'^{-1}(\mathcal{T}^{-1}(h)))$

$$\begin{aligned}\delta = h - h' &= \mathcal{P}'(z') - \mathcal{P}(z') \\ &= (\mathcal{T} \circ \mathcal{F}' \circ \mathcal{S})(z') - (\mathcal{T} \circ \mathcal{F} \circ \mathcal{S})(z') \\ &= (\mathcal{T} \circ \mathcal{F}' \circ \mathcal{S}(z')) - (\mathcal{T} \circ \mathcal{F} \circ \mathcal{S}(z')) \\ &= (T \circ (\mathcal{F}' - \mathcal{F}) \circ S)(z').\end{aligned}$$

# Fault Attack on the Central Map 2/2

- several rounds, at least $m - 1$
- deduce information about $T$, the linear part of $\mathcal{T}$
- apply the MinRank attack (with reduced complexity) to completely recover the affine map $\mathcal{T}$

# Fault Attack on the Central Map 2/2

- several rounds, at least $m-1$
- deduce information about $T$, the linear part of $\mathcal{T}$
- apply the MinRank attack (with reduced complexity) to completely recover the affine map $\mathcal{T}$

- 27 faults needed for current parameters

# Fault Attack on the Random Values 1/2

# Fault Attack on the Random Values 1/2

a permanent fault

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables
of the central map $\mathcal{F}$

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables of the central map $\mathcal{F}$ during signature generation

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables
of the central map $\mathcal{F}$ during signature generation

- variables $x_i$, $i \in \{1, \ldots, n\}$ divided into $o$ oil and $v$ vinegar variables with $n = o + v$ and $v > o$
- vinegar variables randomly assigned during signature generation

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables of the central map $\mathcal{F}$ during signature generation

- variables $x_i$, $i \in \{1, \ldots, n\}$ divided into $o$ oil and $v$ vinegar variables with $n = o + v$ and $v > o$
- vinegar variables randomly assigned during signature generation

$\Rightarrow$ fixed-randomness attack

# Fault Attack on the Random Values 1/2

a permanent fault fixes some of the random vinegar variables of the central map $\mathcal{F}$ during signature generation

- variables $x_i$, $i \in \{1, \ldots, n\}$ divided into $o$ oil and $v$ vinegar variables with $n = o + v$ and $v > o$
- vinegar variables randomly assigned during signature generation

$\Rightarrow$ fixed-randomness attack

- $u_2$ number of fixed vinegar variables
- randomly chosen message $h^{(i)}, i \in \{1, \ldots, n - u_2 + 1\}$
- (faulty) signatures $z^{(i)}, i \in \{1, \ldots, n - u_2 + 1\}$

# Fault Attack on the Random Values 2/2

- (faulty) signatures allow simpler representation of $S$, the linear part of $\mathcal{S}$
- apply the MinRank attack (with reduced complexity) to completely recover the affine map $\mathcal{S}$
- success probability of $\geq 0.933$ for fields $\mathbb{F}_{16}$, $\mathbb{F}_{31}$, $\mathbb{F}_{256}$

# Countermeasures

- smaller fields are better protected than larger fields
  (e.g., $\mathbb{F}_{16}$ instead of $\mathbb{F}_{256}$)

# Countermeasures

- smaller fields are better protected than larger fields (e.g., $\mathbb{F}_{16}$ instead of $\mathbb{F}_{256}$)

Attack on the Central Map

- checksums

# Countermeasures

- smaller fields are better protected than larger fields (e.g., $\mathbb{F}_{16}$ instead of $\mathbb{F}_{256}$)

Attack on the Central Map

- checksums

Attack on the Random Values

- save and compare values

# Future Work

- Further analysis of countermeasures (more in the paper)
- Practical experiments
- Analyzing further attack vectors (FA and SCA)

# Conclusion

promising attack vectors exist

# Conclusion

promising attack vectors exist

no known attack leads to complete key recovery

# Conclusion

promising attack vectors exist

no known attack leads to complete key recovery

$\Rightarrow$ multivariate signature schemes inherently offer a good protection against fault attacks

# References


- Schrödingers Katze — LEIFI Physik https://www.leifiphysik.de/atomphysik/quantenmech-atommodell/versuche/schroedingers-katze-ein-gedankenexperiment
- Alice and Bob communicate without transferring a single photon - Physics World https://physicsworld.com/a/alice-and-bob-communicate-without-transferring-a-single-photon/
- Dilbert Comic Strip on 2012-04-17 — Dilbert by Scott Adams https://dilbert.com/strip/2012-04-17


All links have been opened on February 6, 2019, at 12:15 pm, for the last time

Juliane Krämer
jkraemer@cdc.tu-darmstadt.de

(open PhD position ☺)