Multivariate Quadratic Public-Key Cryptography Part 1: Basics

Bo-Yin Yang

Academia Sinica

PQCrypto Executive Summer School 2017
Eindhoven, the Netherlands
Friday, 23.06.2017

Multivariate Cryptography

MPKC: Multivariate (Quadratic) Public Key Cryptosystem
Public Key: System of nonlinear multivariate equations

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

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i \left(+p_0^{(2)}\right)$$

$$\vdots$$

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

Multivariate Cryptography

MPKC: Multivariate (Quadratic) Public Key Cryptosystem
Public Key: System of nonlinear multivariate equations

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i \left(+p_0^{(1)}\right)\\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i \left(+p_0^{(2)}\right)\\
&\vdots\\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)}\cdot x_i \left(+p_0^{(m)}\right)
\end{aligned}
$$

Public Key size $= m\binom{n+d}{d}$ at degree d, hence usually $d = 2$.

Security

The security of multivariate schemes is based on the

Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}), \ldots, p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

- NP hard
- believed to be hard on average even for quantum conputers:

Security

The security of multivariate schemes is based on the

Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}), \ldots, p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

- NP hard
- believed to be hard on average even for quantum conputers: suppose we have a probabilistic algorithm A and a subexponential function η, T terminates with an answer to a random instance from $MQ(n, m = an, \mathbb{F}_q)$ in time $\eta(n)$ with probability $\mathrm{negl}(n)$.
- higher order versions (MP for Multivariate Polynomials or PoSSo for Polynomial System Solving) clearly no less hard

However usually no direct reduction to MQ !!

Identification Scheme of Sakumoto *et al* and MQDSS

An example 5-pass ID scheme depending only on MQ

- $\mathcal{P}$ be a random MQ instance
- Its "polar" form $D\mathcal{P}(\mathbf{x}, \mathbf{y}) := \mathcal{P}(\mathbf{x} + \mathbf{y}) - \mathcal{P}(\mathbf{x}) - \mathcal{P}(\mathbf{y}) - \mathcal{P}(\mathbf{0})$
- $\mathcal{P}(\mathbf{s}) = \mathbf{p}$ is the public key, $\mathbf{s}$ is the secret.
- Peter picks and commits random $(\mathbf{r_0}, \mathbf{t_0}, \mathbf{e_0})$, sets $\mathbf{r_1} = \mathbf{s} - \mathbf{r_0}$ and commits $(\mathbf{r_1}, D\mathcal{P}(\mathbf{t_0}, \mathbf{r_1}) + \mathbf{e_0})$.
- Vera sends random α,
- Peter sets and sends $\mathbf{t_1} := \alpha\mathbf{r_0} - \mathbf{t_0}$, $\mathbf{e_1} := \alpha\mathcal{P}(\mathbf{r_0}) - \mathbf{e_0}$.
- Vera sends challenge Ch, Peter sends $\mathbf{r}_{Ch}$.
- Vera checks the commit of either $(\mathbf{r_0}, \alpha\mathbf{r_0} - \mathbf{t_1}, \alpha\mathcal{P}(\mathbf{r_0}) - \mathbf{e_1})$ or $(\mathbf{r_1}, \alpha(\mathbf{p} - \mathcal{P}(\mathbf{r_1})) - D\mathcal{P}(\mathbf{t_1}, \mathbf{r_1}) - \mathbf{e_1})$.

The Fiat-Shamir transform of this ID scheme is the MQDSS scheme.

Bipolar Construction

- Easily invertible quadratic map $\mathcal{Q} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible linear maps $\mathcal{T}(: \mathbb{F}^m \to \mathbb{F}^m)$ and $\mathcal{S}(: \mathbb{F}^n \to \mathbb{F}^n)$
- *Public key*: $\mathcal{P} = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S}$ supposed to look random
- *Private key*: $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{T}$ allows to invert the public key

Bipolar Construction

- Easily invertible quadratic map $\mathcal{Q} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible linear maps $\mathcal{T}(: \mathbb{F}^m \to \mathbb{F}^m)$ and $\mathcal{S}(: \mathbb{F}^n \to \mathbb{F}^n)$
- *Public key*: $\mathcal{P} = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S}$ supposed to look random
- *Private key*: $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{T}$ allows to invert the public key

Encryption Schemes ($m \geq n$)

- TTM-related schemes (all broken)
- PMI+, IPHFE+
- ZHFE ($\to$ broken cf. this conference)
- Simple Matrix ($\to$ cf. this conference)

Bipolar Construction

- Easily invertible quadratic map $\mathcal{Q} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible linear maps $\mathcal{T}(: \mathbb{F}^m \to \mathbb{F}^m)$ and $\mathcal{S}(: \mathbb{F}^n \to \mathbb{F}^n)$
- *Public key*: $\mathcal{P} = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S}$ supposed to look random
- *Private key*: $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{T}$ allows to invert the public key

Encryption Schemes ($m \geq n$)

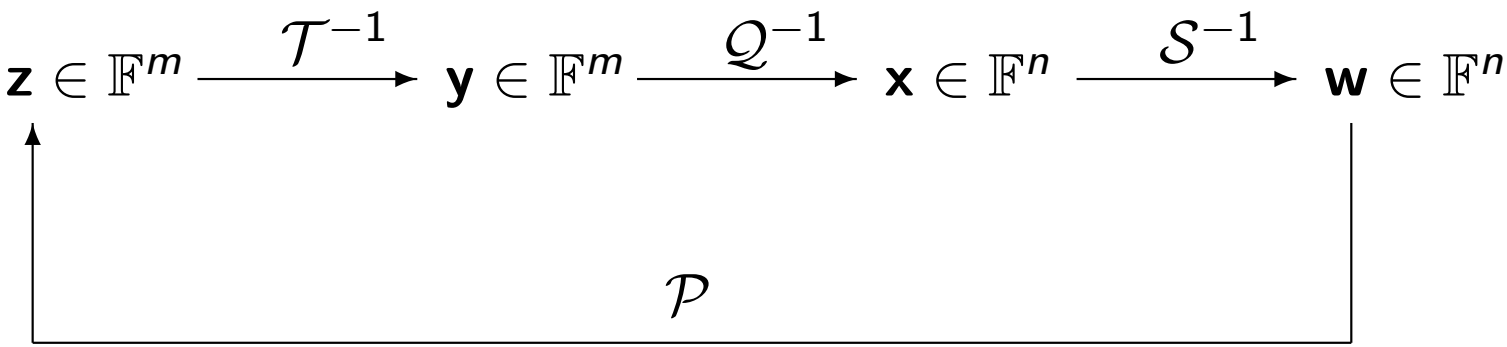
- TTM-related schemes (all broken)
- PMI+, IPHFE+
- ZHFE ($\to$ broken cf. this conference)
- Simple Matrix ($\to$ cf. this conference)

Signature Schemes ($m \leq n$)

- Unbalanced Oil and Vinegar (Rainbow, TTS)
- HFEv- (QUARTZ/Gui)
- pFLASH ($\to$ this conference)

Workflow

Decryption / Signature Generation



Encryption / Signature Verification

Isomorphism of Polynomials

Due to the bipolar construction, the security of MPKCs is also based on the

Problem EIP (Extended Isomorphism of Polynomials): Given the public key $\mathcal{P}$ of a multivariate public key cryptosystem, find affine maps $\bar{\mathcal{S}}$ and $\bar{\mathcal{T}}$ as well as quadratic map $\bar{\mathcal{Q}}$ in class $\mathcal{C}$ such that $\mathcal{P} = \bar{\mathcal{T}} \circ \bar{\mathcal{Q}} \circ \bar{\mathcal{S}}$.

$\Rightarrow$ Hardness of the problem depends heavily on the structure of the central map
$\Rightarrow$ In general, not much is known about the complexity
$\Rightarrow$ Security analysis of multivariate schemes is a hard task

Generic (Direct) Attacks

Try to solve the public equation $\mathcal{P}(\mathbf{w}) = \mathbf{z}$ as an instance of the MQ-Problem, all algorithms have exponential running time (for $m \approx n$)

Known Best Generic Algorithms

- For larger q, FXL ("Hybridized XL")
- For $q = 2$, smart enumerative methods

Generic (Direct) Attacks

Try to solve the public equation $\mathcal{P}(\mathbf{w}) = \mathbf{z}$ as an instance of the MQ-Problem, all algorithms have exponential running time (for $m \approx n$)

Known Best Generic Algorithms

- For larger q, FXL ("Hybridized XL")
- For $q = 2$, the Joux-Vitse Algorithm (an XL variant).

Complexity of Direct Attacks

How many equations are needed to meet given levels of security?

security level (bit)	number of equations			
	$\mathbb{F}_2$ *	$\mathbb{F}_{16}$	$\mathbb{F}_{31}$	$\mathbb{F}_{256}$
80	88	30	28	26
100	110	39	36	33
128	140	51	48	43
192	208	80	75	68
256	280	110	103	93

* depending on how we model the Joux-Vitse algorithm

XL Algorithm

Given: nonlinear polynomials $f_1, \ldots, f_m$ of degree d

1. **eXtend** multiply each polynomial $f_1, \ldots, f_m$ by every monomial of degree $\leq D - d$
2. **Linearize**: Apply (sparse) linear algebra to solve the extended system

$$\text{Complexity} = 3 \cdot \binom{n + d_{\text{XL}}}{d_{\text{XL}}}^2 \cdot \binom{n}{d} \qquad \text{(for larger } q\text{)}$$

or

2. or **Linearize and use an improved XL**: Many variants...

XL Variants

FXL – XL with k variables guessed or "hybridized"

if with k initial guesses / fixing / "hybridization":

$$\text{Complexity} = \min_k 3q^k \cdot \binom{n-k+d_{\text{XL}}}{d_{\text{XL}}}^2 \cdot \binom{n-k}{d}.$$

[generic method with the best asymptotic multiplicative complexity].

XL Variants

FXL – XL with k variables guessed or "hybridized"

XL'

1. **eXtend:** multiply each polynomial $f_1, \ldots, f_m$ by monomials, up to total degree $\leq D$
2. **Linearize**: Apply linear algebra to eliminate all monomials involving the first k variables (and get at least $n - k$ such equations).
3. **Enumerate over** remaining $n - k$ variables.

XL Variants

FXL – XL with k variables guessed or "hybridized"

XL'

1. **eXtend:** multiply each polynomial $f_1, \ldots, f_m$ by monomials, up to total degree $\leq D$
2. **Linearize**: Apply linear algebra to eliminate all monomials involving the first k variables (and get at least $n - k$ such equations).
3. **Enumerate over** remaining $n - k$ variables.

XL2 – simplified F_4

1. **eXtend:** multiply each polynomial $f_1, \ldots, f_m$ by monomials, up to total degree $\leq D$
2. **Linearize**: Apply linear algebra to eliminate top level monomials
3. Multiply degree $D - 1$ equations by variables, **Eliminate Again**.

XL Variants

FXL – XL with k variables guessed or "hybridized"

Joux-Vitse ("Hybridized XL-related method")

1. **eXtend:** multiply each polynomial $f_1, \ldots, f_m$ by monomials, up to total degree $\leq D$
2. **Linearize**: Apply linear algebra to eliminate all monomials of total degree ≥ 2 in the first k variables (and get at least k such equations).
3. **Fix** $n - k$ variables, solve for the initial k in linear equations.

XL2 – simplified F_4

1. **eXtend:** multiply each polynomial $f_1, \ldots, f_m$ by monomials, up to total degree $\leq D$
2. **Linearize**: Apply linear algebra to eliminate top level monomials
3. Multiply degree $D - 1$ equations by variables, **Eliminate Again**.

More Advanced Gröbner Bases Algorithms

- find a "nice" basis of the ideal $\langle f_1, \ldots, f_m \rangle$
- first studied by B. Buchberger
- later improved by Faugére et al. (F_4, F_5)
- With linear algebra constant $2 < \omega \leq 3$.

$$\text{Complexity}(q, m, n) = O\left(\binom{n + d_{\text{reg}} - 1}{d_{\text{reg}}}^{\omega}\right) \qquad \text{(for larger } q\text{)}$$

- "Hybridized":

$$\text{Complexity}(q, m, n) = \min_k \; q^k \cdot O\left(\binom{n - k + d_{\text{reg}} - 1}{d_{\text{reg}}}^{\omega}\right)$$

Do not blithely set $\omega = 2$ here

Even if $\omega \to 2$, there is a huge constant factor which cannot be neglected.

Remarks

Every cryptosystem can be represented as a set of nonlinear multivariate equations

- Direct attacks can be used in the cryptanalysis of other cryptographic schemes (in particular block and stream ciphers)
- The MQ (or PoSSo) Problem can be seen as one of the central problems in cryptography

Post-Quantum-ness of MQ

MQ is quantum-resistant: the best Grover-based quantum attack against n-bits of input takes $2^{\frac{n}{2}+1}n^3$ time.

Features of Multivariate Cryptosystems

Advantages

- resistant against attacks with quantum computers
- very fast (much faster than RSA)
- only simple arithmetic operations required
  $\Rightarrow$ can be implemented on low cost devices
  $\Rightarrow$ suitable for security solutions for the IoT
- many practical signature schemes (UOV, Rainbow, HFEv-, ...)
- short signatures (e.g. 120 bit signatures for 80 bit security)

Disadvantages

- large key sizes (public key size $\sim 10 - 100$ kB)
- no security proofs
- mainly restricted to digital signatures

BB08 D.J. Bernstein, J. Buchmann, E. Dahmen (eds.): Post Quantum Cryptography. Springer, 2009.

DG06 J. Ding, J. E. Gower, D. S. Schmidt: Multivariate Public Key Cryptosystems. Springer, 2006.

GJ79 M. R. Garey and D. S. Johnson: Computers and Intractability: A Guide to the Theory of NP-Completeness.

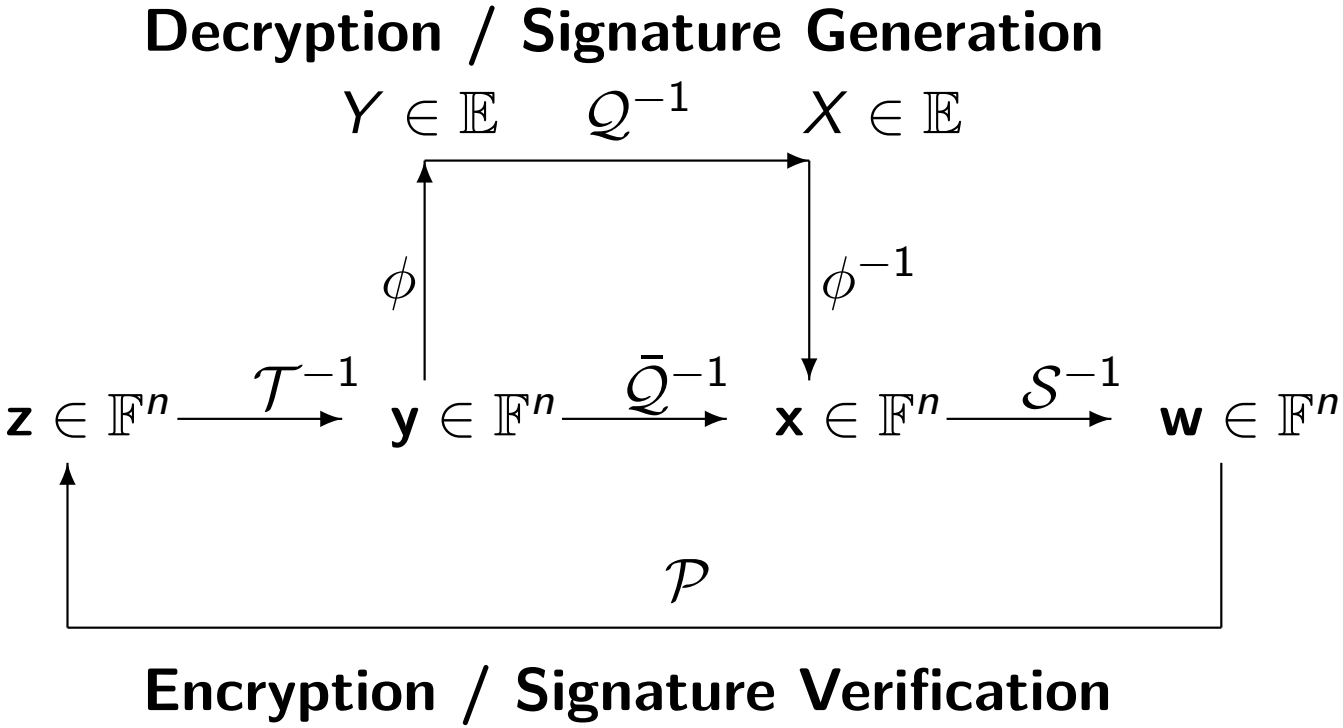
Multivariate Quadratic Public-Key Cryptography Part 2: Big Field Schemes

Bo-Yin Yang

Academia Sinica

PQCrypto Executive Summer School 2017
Eindhoven, the Netherlands
Friday, 23.06.2017

Big Field Schemes



Extension Fields

- $\mathbb{F}_q$: finite field with q elements
- $g(X)$ irreducible polynomial in $\mathbb{F}[X]$ of degree n
  $\Rightarrow \mathbb{F}_{q^n} \cong \mathbb{F}[X]/\langle g(X) \rangle$ finite field with q^n elements
- isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$, $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i \cdot X^{i-1}$
- Addition in $\mathbb{F}_{q^n}$: Addition in $\mathbb{F}_q[X]$
- Multiplication in $\mathbb{F}_{q^n}$: Multiplication in $\mathbb{F}_q[X]$ modulo $g(X)$

The Matsumoto-Imai Cryptosystem (1988) [MI88]

- $\mathbb{F}_q$: finite field of characteristic 2
- degree n extension field $\mathbb{E} = \mathbb{F}_{q^n}$
- isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{E}$
- MI parameter $\theta \in \mathbb{N}$ with

$$\gcd(q^\theta + 1, q^n - 1) = 1.$$

Key Generation

- *central map* $\mathcal{Q} : \mathbb{E} \to \mathbb{E}$, $X \mapsto X^{q^\theta+1} \Rightarrow \mathcal{Q}$ is bijective
- choose 2 invertible linear or affine maps $\mathcal{S}, \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{T} \circ \phi^{-1} \circ \mathcal{Q} \circ \phi \circ \mathcal{S} : \mathbb{F}^n \to \mathbb{F}^n$ quadratic multivariate map
- use the extended Euclidian algorithm to compute $h \in \mathbb{N}$ with

$$h \cdot \theta \equiv 1 \bmod q^n - 1$$

- *private key*: $\mathcal{S}, \mathcal{T}$

Both Encryption and Signature

Encryption or Verification

Given: plaintext or signature $\mathbf{w} \in \mathbb{F}^n$ or Compute $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{P}(\mathbf{w})$.
This is the ciphertext. Or the result to be matched against a hash digest.

Decryption or Signing

Given: ciphertext or hash digest $\mathbf{z} \in \mathbb{F}^n$

1. Compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{z})$.
2. Compute $Y = \phi(\mathbf{y}) \in \mathbb{E}$
3. Compute $X = \mathcal{Q}^{-1}(Y)$ by $X = Y^h$
4. Compute $\mathbf{x} = \phi^{-1}(X) \in \mathbb{F}^n$
5. Compute the plaintext or signature $\mathbf{w} \in \mathbb{F}^n$ by $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{x})$.

Linearization, a Message Recovery Attack [Pa95]

Given public key $\mathcal{P}$, $\mathbf{z}^\star \in \mathbb{F}^n$, find plaintext $\mathbf{w}^\star \in \mathbb{F}^n$, s.t. $\mathcal{P}(\mathbf{w}^\star) = \mathbf{z}^\star$

Proposed by J. Patarin in 1995

Taking the $q^\theta - 1$ st power of $Y = X^{q^\theta+1}$ and multiplying with XY yields

$$X \cdot Y^{q^\theta} = X^{q^{2\theta}} \cdot Y$$

$\Rightarrow$ bilinear equation in X and Y, hence, same in $\mathbf{w}$ and $\mathbf{z}$

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij} w_i z_j + \sum_{i=1}^{n} \beta_i w_i + \sum_{j=1}^{n} \gamma_j z_j + \delta = 0. \quad (\star)$$

1. Compute $N \geq \frac{(n+1)\cdot(n+2)}{2}$ pairs $(\mathbf{z}^{(k)}/\mathbf{w}^{(k)})$ and substitute into $(\star)$.
2. Solve the resulting linear system for the coefficients α_{ij}, β_i, γ_j and δ.
   $\Rightarrow$ n bilinear equations in $w_1, \ldots, w_n, z_1, \ldots, z_n$
3. Substitute $\mathbf{z}^\star$ into these bilinear equations and solve for $\mathbf{w}^\star$.

C^{*-} Schemes

C^{*-} schemes are C^* schemes with a truncated public key [PGC98]

Construction of a C^{*-} scheme

(n, θ, r) are the parameters of the scheme

1. Generate a C^* with parameters (n, θ): $\mathcal{Q}(x) = x^{1+q^\theta}$
2. Remove the last r polynomials from the public key

$$T \circ \mathcal{Q} \circ S = \begin{cases} p_1(x_1, \ldots, x_n) \\ \vdots \\ \vdots \\ p_n(x_1, \ldots, x_n) \end{cases} \xrightarrow{\Pi} \begin{cases} p_1(x_1, \ldots, x_n) \\ \vdots \\ p_{n-r}(x_1, .., x_n) \end{cases} = \Pi \circ \mathcal{P}$$

SFLASH$=C^{*-}$ ($\mathbb{F}_{128}$,37,26)

Signing

1. Append r random values μ to the message m to be signed
2. Find a preimage σ of (m, μ) by $T \circ \mathcal{Q} \circ S$ using S, T
3. Such a preimage always exists since a C^* monomial is bijective
4. σ is a valid signature since $\Pi \circ \mathcal{P}(\sigma) = m$

Parameters (n, θ) must define a bijective C^*

$$\mathcal{Q}(x) = x^{1+q^\theta}$$

- $\mathcal{Q}$ is bijective when $\gcd(q^\theta + 1, q^n - 1) = 1 \quad (q = 2^k)$
- This condition is equivalent to n/d odd where $d = \gcd(n, \theta)$

SFLASH=C^{*-} ($\mathbb{F}_{128}$,37,26)

Signing

1. Append r random values μ to the message m to be signed
2. Find a preimage σ of (m, μ) by $T \circ \mathcal{Q} \circ S$ using S, T
3. Such a preimage always exists since a C^* monomial is bijective
4. σ is a valid signature since $\Pi \circ \mathcal{P}(\sigma) = m$

Parameters (n, θ) must define a bijective C^*

$$\mathcal{Q}(x) = x^{1+q^\theta}$$

- $\mathcal{Q}$ is bijective when $\gcd(q^\theta + 1, q^n - 1) = 1 \quad (q = 2^k)$
- This condition is equivalent to n/d odd where $d = \gcd(n, \theta)$

$q^r \geq 2^b$ to avoid a possible recomposing attack

Skew-Symmetry: C^{*-} Attack by Dubois (2007)

First attack requires $d = \gcd(n, \theta) > 1$, but isn't necessary

Take any $\zeta \in (\mathbb{F}_{q^n})^*$, then $D\mathcal{Q}(\zeta a, x) + D\mathcal{Q}(a, \zeta x) = L(\zeta) D\mathcal{Q}(a, x)$, implying that if $\mathrm{M}_\zeta = S^{-1} \circ M_\zeta \circ S$, where M_ζ means multiplying by ζ, then if H_i are symmetric matrices of the public key polynomials p_i, we should have

$$\mathrm{span}\{\mathrm{M}_\zeta^T H_i + H_i \mathrm{M}_\zeta : i = 1 \cdots n\} = \mathrm{span}\{H_i : i = 1 \cdots n\}.$$

Heuristic Argument by Shamir et al

pick three random linear combinations $\sum_{i=1}^{n-r} b_i (\mathrm{M}_\zeta^T H_i + H_i \mathrm{M}_\zeta)$ and demand that they fall in $S = \mathrm{span}\{H_i : i = 1 \cdots n - r\}$, then

1. there is a good chance to find a nontrivial M_ζ
2. this matrix really correspond to a multiplication by ζ in $\mathbb{F}_{q^n}$;
3. the skew-symmetric action of this M_ζ on the H_i leads to matrices in $\mathrm{span}\{H_i : i = 1 \cdots n\} \backslash S$.

Net Result of Differential Attacks

End of SFLASH

The heuristic argument holds under comprehensive tests and SFLASH and in fact all C^{*-} are comprehensively broken!! Later a slightly more complex but very similar argument was used to break the similar ℓIR signature scheme (PKC 2008) by Fouque et al.

A Defense In One Sentence

When we restrict to a subspace H of $\mathbb{F}_{q^n}$, the only maps that satisfy the symmetry properties (required of the differential attacks) happens to be the same ones in $\mathbb{F}_{q^n}$ that leaves H invariant.

Projections block differential attacks

All symmetry disappears from hyperplane-restricted C^{*-}'s. Differential Attacks verified not to work. This is further studied by Smith et al.

Prefixed C^{*-} signature scheme

Natural restriction of $\mathcal{Q}$ to hyperplane = set coordinate to 0

Start from a C^* scheme with $\mathcal{Q}(x) = x^{1+q^\theta}$ with secret linear maps S and T. Let r and s be two integers between 0 and n. Let T^- be the projection of T on the last r coordinates and S^- be the restriction of S to the first $n-s$ coordinates. $\mathcal{P} = T^- \circ \mathcal{Q} \circ S^-$ is the public key and S^{-1} and T^{-1} are used as the secret key.

Prefixed C^{*-} signature scheme

Natural restriction of $\mathcal{Q}$ to hyperplane = set coordinate to 0

Start from a C^* scheme with $\mathcal{Q}(x) = x^{1+q^\theta}$ with secret linear maps S and T. Let r and s be two integers between 0 and n. Let T^- be the projection of T on the last r coordinates and S^- be the restriction of S to the first $n-s$ coordinates. $\mathcal{P} = T^- \circ \mathcal{Q} \circ S^-$ is the public key and S^{-1} and T^{-1} are used as the secret key.

Inversion

To find $\mathcal{P}^{-1}(m)$ for $m \in \mathbb{F}_q^{n-r}$, the legitimate user first pads m with a random vector m' of $(\mathbb{F})^r$ and compute the preimage of (m, m') by $T^{-1} \circ \mathcal{Q}^{-1} \circ S^{-1}$. If this element has its last s coordinates to 0, then its $n-s$ first coordinates are a valid signature for m. Otherwise, he discards this element and tries with another m'. When $r > s$, the process ends with probability 1 and costs on average q^s inversions of $\mathcal{Q}$.

pFLASH (C^{*-} p, prefixed C^{*-})

Choosing Parameters

n, θ, r are chosen following the rationales for C^{*-} schemes. As signing is q^s times slower, we prefer $s = 1$ and q small. However, if q is chosen small, at constant blocksize this requires a larger value of n and therefore larger keys.

Realistic 80-bit Parameters: pFLASH($\mathbb{F}_{16}$,62-1,40)

As a possible trade-off, the original proposers suggested pFLASH with $q = 2^4$, $n = 74$, $\theta = 11$, $r = 22$ and $s = 1$ (we call this pFLASH($\mathbb{F}_{16}$,74-1,56)). It has (as expected) a bigger secret key of 5.4kB and signs in line with expectations of $\sim 16\times$ time of SFLASH. Currently Smith et al suggests pFLASH($\mathbb{F}_{16}$,62-1,40).
One big plus for $q = 2^4$ is to compute over $\mathbb{F}_{2^8}$ until the last step.

Larger pFLASH Parameters at 128 and 256 bits

We suggest pFLASH($\mathbb{F}_{16}$,96-1,64) and pFLASH($\mathbb{F}_{16}$,192-1,128).

The HFE Cryptosystem [Pa96]

- " Hidden Field Equations", proposed by Patarin in 1995
- BigField Scheme, can be used both for encryption and signatures
- finite field $\mathbb{F}$, extension field $\mathbb{E}$ of degree n, isomorphism $\phi : \mathbb{F}^n \to \mathbb{E}$

Original HFE

- central map $\mathcal{Q} : \mathbb{E} \to \mathbb{E}$ (not bijective, invert using Berlekamp Algorithm).

$$\mathcal{Q}(X) = \sum_{0 \le i \le j}^{q^i + q^j \le D} \alpha_{ij} X^{q^i + q^j} + \sum_{i=0}^{q^i \le D} \beta_i \cdot X^{q^i} + \gamma$$

  $\Rightarrow \bar{\mathcal{Q}} = \phi^{-1} \circ \mathcal{Q} \circ \phi : \mathbb{F}^n \to \mathbb{F}^n$ quadratic

- degree bound D needed for efficient decryption / signature generation
- linear maps $\mathcal{S}, \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{T} \circ \bar{\mathcal{Q}} \circ \mathcal{S} : \mathbb{F}^n \to \mathbb{F}^n$
- *private key*: $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{T}$

Decryption and Signature Generation

Signing message d

1. Use hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}^n$ to compute $\mathbf{z} = \mathcal{H}(d)$
2. Compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{z}) \in \mathbb{F}^n$ and $Y = \phi(\mathbf{y}) \in \mathbb{E}$
3. Solve $\mathcal{Q}(X) = Y$ over $\mathbb{E}$ via Berlekamp's algorithm
4. Compute $\mathbf{x} = \phi^{-1}(X) \in \mathbb{F}^n$ and $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{x})$

Signature: $\mathbf{w} \in \mathbb{F}^n$.

Decryption proceeds similarly, but ...

- Signature generation process does not output a signature for every input message $\Rightarrow$ need to append a counter to the message d
- Decryption is not unique $\Rightarrow$ need disambiguation in the plaintext.

MinRank Attack against HFE

Look in extemsion field $\mathbb{E}$ (Kipnis and Shamir [KS99])

- the linear maps $\mathcal{S}$ and $\mathcal{T}$ relate to univariate maps $\mathcal{S}^\star(X) = \sum_{i=1}^{n-1} s_i \cdot X^{q^i}$ amd $\mathcal{T}^\star(X) = \sum_{i=1}^{n-1} t_i \cdot X^{q^i}$, with $s_i,\ t_i \in \mathbb{E}$.
- the public key $\mathcal{P}^\star$ can be expressed as $\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} p_{ij}^\star X^{q^i+q^j} = \underline{X} \cdot P^\star \cdot \underline{X}^T$,
- Components of $P^\star$ can be found by polynomial interpolation.
- Solve MinRank problem over $\mathbb{E}$.

No need to look in $\mathbb{E}$ (Bettale et al)

Perform the MinRank attack without recovering $\mathcal{P}^\star \Rightarrow$ HFE can be broken by using a MinRank problem over the base field $\mathbb{F}$.

$$\text{Complexity}_{\text{MinRank}} = \binom{n+r}{r}^\omega$$

with $2 < \omega \leq 3$ and $r = \lfloor \log_q(D-1) \rfloor + 1$.

Direct Attacks

- J-C Faugère solved HFE Challenge 1 (HFE over GF2, $d = 96$) in 2002
- Empirically HFE systems can be solved much faster than random
- Ding-Hodges Upper bound for d_{reg}

$$d_{reg} \leq \begin{cases} \frac{(q-1)\cdot(r-1)}{2} + 2 & q \text{ even and } r \text{ odd}, \\ \frac{(q-1)\cdot r}{2} + 2 & \text{otherwise.} \end{cases},$$

with $r = \lfloor \log_q(D-1) \rfloor + 1$.

$\Rightarrow$ Basic version of HFE is not secure

Variant Schemes

- Encryption Schemes IPHFE+ (inefficient), ZHFE (broken here).
- Signature Schemes HFEv- (QUARTZ/GUI), MHFEv- (talk here)

HFEv-

- finite field $\mathbb{F}$, extension field $\mathbb{E}$ of degree n, isomorphism $\phi : \mathbb{F}^n \to \mathbb{E}$
- central map $\mathcal{Q} : \mathbb{F}^v \times \mathbb{E} \to \mathbb{E}$, where the β_i and γ are affine.

$$\mathcal{Q}(X) = \sum_{0 \le i \le j}^{q^i + q^j \le D} \alpha_{ij} X^{q^i + q^j} + \sum_{i=0}^{q^i \le D} \beta_i(v_1, \ldots, v_v) \cdot X^{q^i} + \gamma(v_1, \ldots, v_v)$$

$\Rightarrow \bar{\mathcal{Q}} = \phi^{-1} \circ \mathcal{Q} \circ (\phi \times \mathrm{id}_v)$ quadratic map: $\mathbb{F}^{n+v} \to \mathbb{F}^n$

- linear maps $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^{n-a}$ and $\mathcal{S} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ of maximal rank
- *public key*: $\mathcal{P} = \mathcal{T} \circ \bar{\mathcal{Q}} \circ \mathcal{S} : \mathbb{F}^{n+v} \to \mathbb{F}^{n-a}$
- *private key*: $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{T}$

Signing Message digest z

1. Compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{z}) \in \mathbb{F}^n$ and $Y = \phi(\mathbf{y}) \in \mathbb{E}$
2. Choose random values for the vinegar variables $v_1, \ldots, v_v$
   Solve $\mathcal{Q}_{v_1,\ldots,v_v}(X) = Y$ over $\mathbb{E}$ via Berlekamps algorithm.
   Repeat this step until there is a unique solution.
3. Compute $\mathbf{x} = \phi^{-1}(X) \in \mathbb{F}^n$ and signature $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{x}||v_1|| \ldots ||v_v)$.

Security vs. Efficiency

Main Attacks

- MinRank Attack $\mathrm{Rank}(F) = r + a + v$

  $$\Rightarrow \mathrm{Compl}_{\mathrm{MinRank}} = \binom{n + r + a + v}{r + a + v}^{\omega}$$

- Direct attack [DY13]

$$d_{reg} \leq \begin{cases} \frac{(q-1)\cdot(r+a+v-1)}{2} + 2 & q \text{ even and } r + a \text{ odd}, \\ \frac{(q-1)\cdot(r+a+v)}{2} + 2 & \text{otherwise.} \end{cases},$$

with $r = \lfloor \log_q(D-1) \rfloor + 1$ and $2 < \omega \leq 3$.

Efficiency

Rate determining step: solving X from a univariate equation of degree D.

$$\mathrm{Complexity}_{\mathrm{Berlekamp}} = \mathcal{O}(D^3 + n \cdot D^2)$$

How to define a HFEv- like scheme over $\mathbb{F}_2$ [PCY+15]?

Collision Resistance of the hash function

To cover a hash value of k bit, the public key of a pure HFEv- scheme has to contain at least k equations over $\mathbb{F}_2$. $\Rightarrow$ public key $> k^3/2$ bits

security level	80	100	128	192	256
# equations	100	200	256	384	512
pubkey size (kB)	>250	> 500	> 1000	> 3000	> 8000

QUARTZ

- standardized by Courtois, Patarin in 2002
- HFEv$^-$ with $\mathbb{F} = \mathrm{GF}(2)$, $n = 103$, $D = 129$, $a = 3$ and $v = 4$
- public key: quadratic map $\mathcal{P} = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S} : \mathrm{GF}(2)^{107} \to \mathrm{GF}(2)^{100}$
- Prevent birthday attacks $\Rightarrow$ Generate four HFEv$^-$ signatures
  (for $\mathbf{w}$, $\mathcal{H}(\mathbf{w}|00)$, $\mathcal{H}(\mathbf{w}|01)$ and $\mathcal{H}(\mathbf{w}|11)$)
- Combine them to a single signature of length
  $(n - a) + 4 \cdot (a + v) = 128$ bit

GUI (Generalization of QUARTZ) Signature Generation

Input: HFEv- private key $(\mathcal{S}, \mathcal{Q}, \mathcal{T})$ message $\mathbf{d}$, repetition factor k
Output: signature $\sigma \in \mathbb{F}_2^{(n-a)+k(a+v)}$

1: $\mathbf{h} \leftarrow$ SHA-256($\mathbf{d}$)
2: $S_0 \leftarrow \mathbf{0} \in \mathrm{GF}(2)^{n-a}$
3: **for** $i = 1$ to k **do**
4: $\quad D_i \leftarrow$ first $n - a$ bits of $\mathbf{h}$
5: $\quad (S_i, X_i) \leftarrow \mathrm{HFEv}-^{-1}(D_i \oplus S_{i-1})$
6: $\quad \mathbf{h} \leftarrow$ SHA-256($\mathbf{h}$)
7: **end for**
8: $\sigma \leftarrow (S_k||X_k|| \ldots ||X_1)$
9: **return** σ

Note that if the equation has zero or more than 2 equations, then we discard those vinegars and try again.

Signature Verification

Input: HFEv- public key $\mathcal{P}$, message **d**, repetition factor k, signature $\sigma \in \mathbb{F}_2^{(n-a)+k(a+v)}$

Output: **TRUE** or **FALSE**

1: $\mathbf{h} \leftarrow$ SHA-256(**d**)
2: $(S_k, X_k, \ldots, X_1) \leftarrow \sigma$
3: **for** $i = 1$ to k **do**
4: $\quad D_i \leftarrow$ first $n - a$ bits of **h**
5: $\quad \mathbf{h} \leftarrow$ SHA-256(**h**)
6: **end for**
7: **for** $i = k - 1$ to 0 **do**
8: $\quad S_i \leftarrow \mathcal{P}(S_{i+1}||X_{i+1}) \oplus D_{i+1}$
9: **end for**
10: **if** $S_0 = \mathbf{0}$ **then**
11: $\quad$ **return TRUE**
12: **else**
13: $\quad$ **return FALSE**
14: **end if**

Parameters for HFEv- (GUI) over $\mathbb{F}_2$?

Parameters are set by the complexity of MinRank and direct attacks

- For the complexity of the MinRank attack we have a concrete formula
- For the direct attack, we only have an upper bound on d_{reg}.

$$d_{reg} \leq \begin{cases} \frac{(q-1)\cdot(r+a+v-1)}{2} + 2 & q \text{ even and } r+a \text{ odd}, \\ \frac{(q-1)\cdot(r+a+v)}{2} + 2 & \text{otherwise.} \end{cases} \quad (\star)$$

Experiments show that these estimate for d_{reg} is reasonably tight.

Parameter Choice of HFEv- over $\mathbb{F}_2$

Efficiency $\Rightarrow$ Choose D as small as possible

- $D = 5 \Rightarrow r = \lfloor \log_2(D-1) \rfloor + 1 = 3$
- $D = 9 \Rightarrow r = \lfloor \log_2(D-1) \rfloor + 1 = 4$
- $D = 17 \Rightarrow r = \lfloor \log_2(D-1) \rfloor + 1 = 5$

Increase a and v to reach the required security level

Choose a and v as equal as possible, i.e. $0 \leq v - a \leq 1$.

Quantum Attacks and Impact

A determined multivariate system of m equations over $\mathbb{F}_2$ can be solved using $2^{m/2} \cdot 2 \cdot m^3$ operations using a quantum computer.

- This does not affect signatures in general because the hashes are typically twice as wide as the design security.
- Alas, this wipes out nearly all GUI's gains.

$\Rightarrow$ very large public key size

security level	80	100	128	192	256
min # equations	117	155	208	332	457

Minimal Conservative Quantum-Safe Parameters

quantum security level (bit)		public key size (kB)	private key size (kB)	signature size (bit)
80	Gui ($\mathbb{F}_2$,120,9,3,3,2)	110.7	3.8	129
100	Gui ($\mathbb{F}_2$,161,9,6,7,2)	271.8	7.5	181
128	Gui ($\mathbb{F}_2$,219,9,11,11,2)	680.4	14.5	252
192	Gui ($\mathbb{F}_2$,350,9,18,19,2)	2,781.6	40.9	406
256	Gui ($\mathbb{F}_2$,483,9,26,26,2)	7,269.2	82.8	561

HFEv- - Summary

- very short (pre-quantum) signatures
- security well respected
- conflict between security and efficiency
- restricted to very small fields, hence very large keys

HMFEv- (Hidden Medium Field Equations vinegar minus)

Central map is a random $\mathbb{E}^k \mapsto \mathbb{E}^k$ quadratic map.

- shown by J-C Faugère et al to act like a HFE with rank k
- basic scheme is breakable the same way.
- Can build HMFEv- just like HFEv-
- key size is roughly proportional to field size
- Please attend talk by Albrecht Petzoldt (shameless plug).

References

KS99 A. Kipnis, A. Shamir: Cryptanalysis of the HFE Public Key Cryptosystem. CRYPTO 99, LNCS vol. 1666, pp. 19 - 30. Springer 1999.

DDY+08 J. Ding, V. Dubois, B.-Y. Yang, C.-H. Chen, and C.-M. Cheng. Can SFLASH be Repaired?, ICALP 2008 - Part 2, LNCS 5126, pp. 691-701.

PCY+15 A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: Design Principles for HFEv- based Signature Schemes. ASIACRYPT 2015 - Part 1, LNCS vol. 9452, pp. 311-334. Springer, 2015.

DY13 J. Ding, B.Y. Yang: Degree of regularity for HFEv and HFEv-. PQCrypto 2013, LNCS vol. 7932, pp. 52 - 66. Springer, 2013.