Multivariate-quadratic signatures III

Hidden-field equatios

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

MQ signatures (typical case)

Take $F = (f_1, f_2, \ldots, f_m)$ as public key.

Let $H : \{0,1\}^* \times \{0,1\}^r \to \mathbf{F}_q^m$ be a hash function.

Signature:

Signature on $M \in \{0,1\}^*$ is $(\mathbf{X}, R)$ with

- $\mathbf{X} = (X_1, X_2, \ldots, X_n) \in \mathbf{F}_q^n$
- $R \in \{0,1\}^r$

satisfying

$$f_k(X_1, X_2, \ldots, X_n) = h_k$$

for all $1 \leq k \leq m$ and $H(M, R) = (h_1, h_2, \ldots, h_m)$.

The inclusion of R is necessary because not every system has a solution.

Notation: using bold face to indicate vectors.

Attack algorithms

If some of the equations involve only very few variables those can be easily solved / efficiently tested.

A system with a triangular shape, e.g., increasing by one variable per equation can be easily solved / efficiently tested.

Attack algorithms

If some of the equations involve only very few variables those can be easily solved / efficiently tested.

A system with a triangular shape, e.g., increasing by one variable per equation can be easily solved / efficiently tested.

The Göbner basis of a system of multivariate equations has the same solution space (formally: defines the same ideal) as the original system and has such a shape.
Göbner-basis attacks are among the most efficient attacks on MQ systems.

Attack algorithms

If some of the equations involve only very few variables those can be easily solved / efficiently tested.

A system with a triangular shape, e.g., increasing by one variable per equation can be easily solved / efficiently tested.

The Göbner basis of a system of multivariate equations has the same solution space (formally: defines the same ideal) as the original system and has such a shape.
Göbner-basis attacks are among the most efficient attacks on MQ systems.

XL (=eXtended Linearization) is an intelligent brute-force approach that fixes some variables in order to lower the degree and then solve by Gaussian elimination.
For those variables, potentially all assignments have to be tested.
Selecting the right variables requires some computation.

What do trapdoors look like?

Let S be a system of m equations in n variables over $\mathbf{F}_q$ for which finding preimages is easy.

Let $M : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and $N : \mathbf{F}_q^n \to \mathbf{F}_q^n$ be invertible linear maps.

Put

$$F = M \circ S \circ N.$$

What do trapdoors look like?

Let S be a system of m equations in n variables over $\mathbf{F}_q$ for which finding preimages is easy.

Let $M : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and $N : \mathbf{F}_q^n \to \mathbf{F}_q^n$ be invertible linear maps.

Put

$$F = M \circ S \circ N.$$

F is a system of m equations in n variables that hides S.

Given $\mathbf{y} \in \mathbf{F}_q^m$ compute $\mathbf{x} \in \mathbf{F}_q^n$:

- Compute $\mathbf{y}' = M^{-1}(\mathbf{y})$.
- Find a preimage $\mathbf{x}'$ of $\mathbf{y}'$ under S, if it exists, using the efficient algorithm for S.
- Compute $\mathbf{x} = N^{-1}(\mathbf{x}')$

What do trapdoors look like?

Let S be a system of m equations in n variables over $\mathbf{F}_q$ for which finding preimages is easy.

Let $M : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and $N : \mathbf{F}_q^n \to \mathbf{F}_q^n$ be invertible linear maps.

Put

$$F = M \circ S \circ N.$$

F is a system of m equations in n variables that hides S.

Given $\mathbf{y} \in \mathbf{F}_q^m$ compute $\mathbf{x} \in \mathbf{F}_q^n$:

- Compute $\mathbf{y}' = M^{-1}(\mathbf{y})$.
- Find a preimage $\mathbf{x}'$ of $\mathbf{y}'$ under S, if it exists, using the efficient algorithm for S.
- Compute $\mathbf{x} = N^{-1}(\mathbf{x}')$

$\mathbf{x}$ is a preimage of $\mathbf{y}$ under F because

$$F(\mathbf{x}) = M \circ S \circ N(\mathbf{x}) = M \circ S(\mathbf{x}') = M(\mathbf{y}') = \mathbf{y}.$$

What do trapdoors look like?

Let S be a system of m equations in n variables over $\mathbf{F}_q$ for which finding preimages is easy.

Let $M : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and $N : \mathbf{F}_q^n \to \mathbf{F}_q^n$ be invertible linear maps.

Put

$$F = M \circ S \circ N.$$

F is a system of m equations in n variables that hides S. *Or does it?*

Given $\mathbf{y} \in \mathbf{F}_q^m$ compute $\mathbf{x} \in \mathbf{F}_q^n$:

- Compute $\mathbf{y}' = M^{-1}(\mathbf{y})$.
- Find a preimage $\mathbf{x}'$ of $\mathbf{y}'$ under S, if it exists, using the efficient algorithm for S.
- Compute $\mathbf{x} = N^{-1}(\mathbf{x}')$

$\mathbf{x}$ is a preimage of $\mathbf{y}$ under F because

$$F(\mathbf{x}) = M \circ S \circ N(\mathbf{x}) = M \circ S(\mathbf{x}') = M(\mathbf{y}') = \mathbf{y}.$$

Hidden field equations

Let $g(z) \in \mathbf{F}_q[z]$ be a monic irreducible polynomial of degree n.
Then $\mathbf{F}_{q^n} \cong \mathbf{F}_q[z]/g(z)$.

Solving univariate equations over $\mathbf{F}_{q^n}$ can be done efficiently.

Hidden field equations

Let $g(z) \in \mathbf{F}_q[z]$ be a monic irreducible polynomial of degree n.
Then $\mathbf{F}_{q^n} \cong \mathbf{F}_q[z]/g(z)$.

Solving univariate equations over $\mathbf{F}_{q^n}$ can be done efficiently.

For $m = n$:

- Pick an explicit basis for $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.
- Let $\phi : \mathbf{F}_{q^n} \to \mathbf{F}_q^n$ obtain the coefficients wrt this basis.
- Let
$$s(X) = \sum_{\substack{0 \leq i \leq < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leq i < n \\ q^i < D}} \beta_i X^{q^i} + \gamma,$$
for $\alpha_{i,j}, \beta_i, \gamma \in \mathbf{F}_{q^n}$ and some degree bound D.

Hidden field equations

Let $g(z) \in \mathbf{F}_q[z]$ be a monic irreducible polynomial of degree n.
Then $\mathbf{F}_{q^n} \cong \mathbf{F}_q[z]/g(z)$.

Solving univariate equations over $\mathbf{F}_{q^n}$ can be done efficiently.

For $m = n$:

- Pick an explicit basis for $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.
- Let $\phi : \mathbf{F}_{q^n} \to \mathbf{F}_q^n$ obtain the coefficients wrt this basis.
- Let
$$s(X) = \sum_{\substack{0 \le i \le < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i < n \\ q^i < D}} \beta_i X^{q^i} + \gamma,$$
for $\alpha_{i,j}, \beta_i, \gamma \in \mathbf{F}_{q^n}$ and some degree bound D.
- $S = \phi \circ s \circ \phi^{-1} : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a quadratic system of equations

Hidden field equations

Let $g(z) \in \mathbf{F}_q[z]$ be a monic irreducible polynomial of degree n.
Then $\mathbf{F}_{q^n} \cong \mathbf{F}_q[z]/g(z)$.

Solving univariate equations over $\mathbf{F}_{q^n}$ can be done efficiently.

For $m = n$:

- Pick an explicit basis for $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.
- Let $\phi : \mathbf{F}_{q^n} \to \mathbf{F}_q^n$ obtain the coefficients wrt this basis.
- Let
$$s(X) = \sum_{\substack{0 \le i \le < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i < n \\ q^i < D}} \beta_i X^{q^i} + \gamma,$$
  for $\alpha_{i,j}, \beta_i, \gamma \in \mathbf{F}_{q^n}$ and some degree bound D.
- $S = \phi \circ s \circ \phi^{-1} : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a quadratic system of equations because q-th power is linear, thus $X^{q^i + q^j}$ is a product of linear maps.
- Define F, M and N as before.

Hidden field equations

Let $g(z) \in \mathbf{F}_q[z]$ be a monic irreducible polynomial of degree n.
Then $\mathbf{F}_{q^n} \cong \mathbf{F}_q[z]/g(z)$.

Solving univariate equations over $\mathbf{F}_{q^n}$ can be done efficiently.

For $m = n$:

- Pick an explicit basis for $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.
- Let $\phi : \mathbf{F}_{q^n} \to \mathbf{F}_q^n$ obtain the coefficients wrt this basis.
- Let
$$s(X) = \sum_{\substack{0 \le i \le < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i < n \\ q^i < D}} \beta_i X^{q^i} + \gamma,$$
  for $\alpha_{i,j}, \beta_i, \gamma \in \mathbf{F}_{q^n}$ and some degree bound D.
- $S = \phi \circ s \circ \phi^{-1} : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a quadratic system of equations because q-th power is linear, thus $X^{q^i + q^j}$ is a product of linear maps.
- Define F, M and N as before.
- To find a preimage of $\mathbf{y}$ compute $Y = \phi^{-1}(M^{-1}(\mathbf{y})) \in \mathbf{F}_{q^n}$.
  Compute X with $s(X) = Y$, if it exists. Complexity depends on D.
  Output $\mathbf{x} = N^{-1}(\phi(X))$.

HFE systems

- Matsumoto–Imai C^* scheme used $s(X) = X^{q^i+1}$.
  This makes s bijective for $\gcd(q^i + 1, q^n - 1) = 1$
- C^* was broken by Patarin observing linear properties.
- Patarin proposed HFE the same year.
  Downside: s no longer bijective; benefit: direct attack stopped
- Still some attack surface to detecting the structure.

HFE systems

- Matsumoto–Imai C^* scheme used $s(X) = X^{q^i+1}$.
  This makes s bijective for $\gcd(q^i + 1, q^n - 1) = 1$
- C^* was broken by Patarin observing linear properties.
- Patarin proposed HFE the same year.
  Downside: s no longer bijective; benefit: direct attack stopped
- Still some attack surface to detecting the structure.
- $-$ tweak: remove equations, define $M : \mathbf{F}_q^n \to \mathbf{F}_q^m$ of rank m.

HFE systems

- Matsumoto–Imai C^* scheme used $s(X) = X^{q^i+1}$.
  This makes s bijective for $\gcd(q^i + 1, q^n - 1) = 1$
- C^* was broken by Patarin observing linear properties.
- Patarin proposed HFE the same year.
  Downside: s no longer bijective; benefit: direct attack stopped
- Still some attack surface to detecting the structure.
- $-$ tweak: remove equations, define $M : \mathbf{F}_q^n \to \mathbf{F}_q^m$ of rank m.
  "Inverse" has solution space of dimension $n - m$.

HFE systems

- Matsumoto–Imai C^* scheme used $s(X) = X^{q^i+1}$.
  This makes s bijective for $\gcd(q^i + 1, q^n - 1) = 1$
- C^* was broken by Patarin observing linear properties.
- Patarin proposed HFE the same year.
  Downside: s no longer bijective; benefit: direct attack stopped
- Still some attack surface to detecting the structure.
- $-$ tweak: remove equations, define $M : \mathbf{F}_q^n \to \mathbf{F}_q^m$ of rank m.
  "Inverse" has solution space of dimension $n - m$.
- vinegar tweak: include extra variables that do not mix:
  Let $n' = n + v, N' : \mathbf{F}_q^{n'} \to \mathbf{F}_q^{n'}$ and $\beta_i, \gamma : \mathbf{F}_q^v \to \mathbf{F}_{q^n}$ be affine maps.
  Let $\mathbf{t} = (t_1, t_2, \ldots, t_v)$ and

$$s_{\mathbf{t}}(X) = \sum_{\substack{0 \le i \le < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i < n \\ q^i < D}} \beta_i(t_1, t_2, \ldots, t_v) X^{q^i} + \gamma(t_1, t_2, \ldots, t_v),$$

Then $S = \phi \circ s_{\mathbf{t}} \circ (\phi^{-1} \times \mathrm{id}_v) : \mathbf{F}_q^{n+v} \to \mathbf{F}_q^n$.

HFE systems

- Matsumoto–Imai C^* scheme used $s(X) = X^{q^i+1}$.
  This makes s bijective for $\gcd(q^i+1, q^n-1) = 1$
- C^* was broken by Patarin observing linear properties.
- Patarin proposed HFE the same year.
  Downside: s no longer bijective; benefit: direct attack stopped
- Still some attack surface to detecting the structure.
- $-$ tweak: remove equations, define $M : \mathbf{F}_q^n \to \mathbf{F}_q^m$ of rank m.
  "Inverse" has solution space of dimension $n-m$.
- vinegar tweak: include extra variables that do not mix:
  Let $n' = n + v, N' : \mathbf{F}_q^{n'} \to \mathbf{F}_q^{n'}$ and $\beta_i, \gamma : \mathbf{F}_q^v \to \mathbf{F}_{q^n}$ be affine maps.
  Let $\mathbf{t} = (t_1, t_2, \ldots, t_v)$ and

  $$s_{\mathbf{t}}(X) = \sum_{\substack{0 \le i \le < n \\ q^i + q^j < D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{0 \le i < n \\ q^i < D}} \beta_i(t_1, t_2, \ldots, t_v) X^{q^i} + \gamma(t_1, t_2, \ldots, t_v),$$

  Then $S = \phi \circ s_{\mathbf{t}} \circ (\phi^{-1} \times \mathrm{id}_v) : \mathbf{F}_q^{n+v} \to \mathbf{F}_q^n$.
  To compute preimage, pick random $\mathbf{t} = (t_1, t_2, \ldots, t_v)$,
  solve $s_{\mathbf{t}}(X) = Y$ for X (if possible, else repeat with different choice).
  Output $N'^{-1}(x_1, x_2, \ldots, x_n, t_1, t_2, \ldots, t_v)$ as preimage.
- HVEv- uses both of these tweaks.