Quantum-Resistant Multivariate Public Key Cryptography

Daniel Smith-Tone [1,2]

[1]National Institute of Standards and Technology

[2]University of Louisville

9th Sept., 2013

Multivariate Public Key Cryptography

Nonlinear Systems

Base the security of the cryptographic scheme on the difficulty of finding a preimage of some element in the range of a system of nonlinear equations.

Multivariate Public Key Cryptography

Nonlinear Systems

Base the security of the cryptographic scheme on the difficulty of finding a preimage of some element in the range of a system of nonlinear equations.

The fundamental problem has been studied for at least hundreds of years and seems difficult.

Systems of Quadratic Equations

We can restrict ourselves to systems of quadratic equations.

Systems of Quadratic Equations

We can restrict ourselves to systems of quadratic equations.

Key Size

A system of m quadratic equations in n unknowns consists of $m(\binom{n}{2} + n)$ monomials. Key sizes are (in general) proportional to mn^2. If $m \approx n$, key sizes scale like n^3.

Systems of Quadratic Equations

We can restrict ourselves to systems of quadratic equations.

Key Size

A system of m quadratic equations in n unknowns consists of $m(\binom{n}{2} + n)$ monomials. Key sizes are (in general) proportional to mn^2. If $m \approx n$, key sizes scale like n^3.

Underlying Problem

The $\mathcal{MQ}$ problem of solving systems of quadratic equations over a field is NP-complete.
At least there is a chance that cryptanalysis may be difficult.

Prototypical Multivariate Public Key Scheme

Butterfly Construction

Let f be an efficiently invertible (in some sense) system of m quadratic formulae in n variables over some field $\mathbb{F}_q$. Let U and T be $\mathbb{F}_q$-linear maps of dimension n and m, respectively.
Let $P = T \circ f \circ U$.

Prototypical Multivariate Public Key Scheme

Butterfly Construction

Let f be an efficiently invertible (in some sense) system of m quadratic formulae in n variables over some field $\mathbb{F}_q$. Let U and T be $\mathbb{F}_q$-linear maps of dimension n and m, respectively.
Let $P = T \circ f \circ U$.

Since P is simply a representation of f (consider choosing different bases for the input and output spaces), $y = P(x)$ is not an arbitrary instance of $\mathcal{MQ}$.

Morphisms of Polynomials

Morphism of Polynomials ($\mathcal{MP}$) Problem

Let F_q be the finite field with q elements. Let f and P be functions from F_q^n to F_q^m. Find F_q-affine maps T and U such that $P = T \circ f \circ U$.

Morphisms of Polynomials

Morphism of Polynomials ($\mathcal{MP}$) Problem

Let F_q be the finite field with q elements. Let f and P be functions from F_q^n to F_q^m. Find F_q-affine maps T and U such that $P = T \circ f \circ U$.

Isomorphism of Polynomials ($\mathcal{IP}$) Problem

Find a solution to the $\mathcal{MP}$ problem in which T and U are bijections.

Morphisms of Polynomials

Morphism of Polynomials ($\mathcal{MP}$) Problem

Let F_q be the finite field with q elements. Let f and P be functions from F_q^n to F_q^m. Find F_q-affine maps T and U such that $P = T \circ f \circ U$.

Isomorphism of Polynomials ($\mathcal{IP}$) Problem

Find a solution to the $\mathcal{MP}$ problem in which T and U are bijections.

IP 1 Secret ($\mathcal{IP}1\mathcal{S}$) Problem

Find a solution to the $\mathcal{IP}$ problem in which T is the identity.

Classical Cryptanalysis?

Algebraic Attack

Use Gröbner basis algorithms to solve the system of equations arising from an instance of the scheme. This technique amounts to trying to solve the $\mathcal{MQ}$ problem directly.

Classical Cryptanalysis?

Algebraic Attack

Use Gröbner basis algorithms to solve the system of equations arising from an instance of the scheme. This technique amounts to trying to solve the $\mathcal{MQ}$ problem directly.

Structural Attack

Utilize the special structure of the core map to perform a key recovery attack. Essentially solve a morphism problem for a subclass of maps.

Classical Cryptanalysis?

Algebraic Attack

Use Gröbner basis algorithms to solve the system of equations arising from an instance of the scheme. This technique amounts to trying to solve the $\mathcal{MQ}$ problem directly.

Alternative Algebraic Attack

Develop algorithms for specifically solving $\mathcal{MP}/\mathcal{IP}/\mathcal{IP}1\mathcal{S}$ problems.

Structural Attack

Utilize the special structure of the core map to perform a key recovery attack. Essentially solve a morphism problem for a subclass of maps.

The Complexity of Morphism Problems

$\mathcal{MP}$ is NP-hard

Poly-time reduction to 3-Tensor Rank Problem.

The Complexity of Morphism Problems

$\mathcal{MP}$ is NP-hard

Poly-time reduction to 3-Tensor Rank Problem.

$\mathcal{IP}1\mathcal{S}$ is GI-hard

Given a pair of graph presentations of length n, the existence of an isomorphism can be determined by the solution of a system of equations with $O(n^{3/2})$ variables and equations.

The Complexity of Morphism Problems

$\mathcal{MP}$ is NP-hard

Poly-time reduction to 3-Tensor Rank Problem.

$\mathcal{IP}1\mathcal{S}$ is GI-hard

Given a pair of graph presentations of length n, the existence of an isomorphism can be determined by the solution of a system of equations with $O(n^{3/2})$ variables and equations.

Deciding $\mathcal{IP}$ is not NP-hard

(Unless the poly-time hierarchy collapses.)

Rank Attacks

Low Rank Attack

Find quadratic forms in the span of the public key polynomials which have low rank.

Useful when the private key contains formulae with few variables.

Rank Attacks

Low Rank Attack

Find quadratic forms in the span of the public key polynomials which have low rank.
Useful when the private key contains formulae with few variables.

Dual Rank Attack

Find a small subspace in the kernel of much of the span of the public polynomials.
Useful when the private key contains variables occurring in very few formula.

Rank Attacks

Low Rank Attack

Find quadratic forms in the span of the public key polynomials which have low rank.
Useful when the private key contains formulae with few variables.

Dual Rank Attack

Find a small subspace in the kernel of much of the span of the public polynomials.
Useful when the private key contains variables occurring in very few formula.

Used to break triangular and “tame-like” schemes.

Differential Attacks - Discrete Differential

Definition

The *Discrete Differential* of a map $f : k \to k$ is given by:

$$Df(a, x) = f(a + x) - f(x) - f(a) + f(0).$$

Differential Attacks - Discrete Differential

Definition

The *Discrete Differential* of a map $f : k \to k$ is given by:

$$Df(a, x) = f(a + x) - f(x) - f(a) + f(0).$$

Elementary Properties

1. Linear operator.
2. Reduces complexity of a function: If f is quadratic, Df is bilinear.
3. If f is quadratic, $D(Tf(Ux + c) + d) = D(Tf(Ux))$.

Differential Attacks - Differential of Multivariate Scheme

DP

Let $P = T \circ f \circ U$. $DP(a, x) = TDf(Ua, Ux)$.

Differential Attacks - Differential of Multivariate Scheme

DP

Let $P = T \circ f \circ U$. $DP(a, x) = TDf(Ua, Ux)$.

Differential Coordinate Forms

Since P has n coordinates, DP can be split into n bilinear differential coordinate forms, $DP_i = T_i Df(La, Lx)$, where T_i represents the action of T on the ith coordinate.

Differential Attacks - Differential of Multivariate Scheme

DP

Let $P = T \circ f \circ U$. $\quad DP(a, x) = TDf(Ua, Ux)$.

Differential Coordinate Forms

Since P has n coordinates, DP can be split into n bilinear differential coordinate forms, $DP_i = T_i Df(La, Lx)$, where T_i represents the action of T on the ith coordinate.

Span of Forms

For all multivariate schemes, $Span(DP_i) \subseteq Span(D(f \circ L)_i)$.

Differential Attacks - Differential Symmetry

General Linear Differential Symmetries

$$Df(La, x) + Df(a, Lx) = \Lambda_L Df(a, x)$$

Differential Attacks - Differential Symmetry

General Linear Differential Symmetries

$$Df(La, x) + Df(a, Lx) = \Lambda_L Df(a, x)$$

Can be used to break SFLASH(C^{*-}), MI(C^{*}), SQUARE, ℓ-IC^{-},...

Differential Attacks - Differential Symmetry

General Linear Differential Symmetries

$$Df(La, x) + Df(a, Lx) = \Lambda_L Df(a, x)$$

Can be used to break SFLASH(C^{*-}), MI(C^*), SQUARE, ℓ-IC$^-$,...

Determination Possible

In principle, the space of linear maps L satisfying such a relation can be discovered (at least to live within a small subspace of the space of all linear maps).

Differential Attacks - Differential Invariants

First-Order Differential Invariants

The map f has a differential invariant if there exist V and W subspaces of F_q^n such that $dim(W) \leq dim(V)$ with the property that $Mv \in W$ for all $M \in Span(Df_i)$ and for all $v \in V$.

Differential Attacks - Differential Invariants

First-Order Differential Invariants

The map f has a differential invariant if there exist V and W subspaces of F_q^n such that $dim(W) \leq dim(V)$ with the property that $Mv \in W$ for all $M \in Span(Df_i)$ and for all $v \in V$.

Can be used to break Oil-Vinegar, as well as several schemes involving multiple-types of variables with artificial mixing.

Differential Attacks - Differential Invariants

First-Order Differential Invariants

The map f has a differential invariant if there exist V and W subspaces of F_q^n such that $dim(W) \leq dim(V)$ with the property that $Mv \in W$ for all $M \in Span(Df_i)$ and for all $v \in V$.

Can be used to break Oil-Vinegar, as well as several schemes involving multiple-types of variables with artificial mixing.

Let M_V be a projection onto V, then differential invariants induce nonlinear symmetry ($M_{W^T} M M_V = 0$ for all $M \in Span(Df_i)$).

Differential Attacks - Differential Invariants

First-Order Differential Invariants

The map f has a differential invariant if there exist V and W subspaces of F_q^n such that $dim(W) \leq dim(V)$ with the property that $Mv \in W$ for all $M \in Span(Df_i)$ and for all $v \in V$.

Can be used to break Oil-Vinegar, as well as several schemes involving multiple-types of variables with artificial mixing.
Let M_V be a projection onto V, then differential invariants induce nonlinear symmetry ($M_{W^T} M M_V = 0$ for all $M \in Span(Df_i)$).

Determination Possible

In principle, the space of linear maps M_V satisfying such a relation can be discovered (at least to live within a small subspace of the space of all linear maps).

The C^* Scheme

The C^* cryptosystem is the simplest example of a "big field" scheme.

The C^* Scheme

The C^* cryptosystem is the simplest example of a "big field" scheme.

Construction

$$\left.\begin{array}{c} k \\ | \\ \mathbb{F}_q \end{array}\right] n$$

The C^* Scheme

The C^* cryptosystem is the simplest example of a "big field" scheme.

Construction

$$\left.\begin{array}{c} k \\ | \\ \mathbb{F}_q \end{array}\right] n$$

We can identify $\mathbf{x} \in k$ with $x \in \mathbb{F}_q^n$.

The C^* Scheme

The C^* cryptosystem is the simplest example of a "big field" scheme.

Construction

$$\left.\begin{array}{c} k \\ | \\ \mathbb{F}_q \end{array}\right] n$$

We can identify $\mathbf{x} \in k$ with $x \in \mathbb{F}_q^n$.

Encryption Scheme

$$y = P(x) = (T \circ f \circ U)x \text{ where } f(x) = x^{q^\theta + 1}.$$
$$(Df(a,x) = ax^{q^\theta} + a^{q^\theta}x.)$$

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v, v) = 0$, since Df is antisymmetric.

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v, v) = 0$, since Df is antisymmetric.

We Compute...

$$0 = Df(v, v)$$

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v, v) = 0$, since Df is antisymmetric.

We Compute...

$$0 = Df(v, v)$$
$$= Df(v, u^{q^\theta+1})$$

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v, v) = 0$, since Df is antisymmetric.

We Compute...

$$\begin{aligned} 0 &= Df(v, v) \\ &= Df(v, u^{q^\theta+1}) \\ &= vu^{q^{2\theta}+q^\theta} + v^{q^\theta} u^{q^\theta+1} \end{aligned}$$

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v,v) = 0$, since Df is antisymmetric.

We Compute...

$$\begin{aligned} 0 &= Df(v,v) \\ &= Df(v, u^{q^\theta+1}) \\ &= vu^{q^{2\theta}+q^\theta} + v^{q^\theta}u^{q^\theta+1} \\ &= u^{q^\theta}\left(vu^{q^{2\theta}} + v^{q^\theta}u\right) \end{aligned}$$

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v,v) = 0$, since Df is antisymmetric.

We Compute...

$$\begin{aligned} 0 &= Df(v,v) \\ &= Df(v, u^{q^\theta+1}) \\ &= vu^{q^{2\theta}+q^\theta} + v^{q^\theta}u^{q^\theta+1} \\ &= u^{q^\theta}\left(vu^{q^{2\theta}} + v^{q^\theta}u\right) \end{aligned}$$

Therefore, $vu^{q^{2\theta}} = v^{q^\theta}u$.

Differential Attack on C^*-Patarin's Relation

Trivial Differential Relation

We know that $Df(v,v) = 0$, since Df is antisymmetric.

We Compute...

$$
\begin{aligned}
0 &= Df(v,v) \\
&= Df(v, u^{q^\theta+1}) \\
&= vu^{q^{2\theta}+q^\theta} + v^{q^\theta}u^{q^\theta+1} \\
&= u^{q^\theta}\left(vu^{q^{2\theta}} + v^{q^\theta}u\right)
\end{aligned}
$$

Therefore, $(T^{-1}y)(Ux)^{q^{2\theta}} = (T^{-1}y)^{q^\theta}(Ux)$.

HFE

Core Map

Let k be a degree n extension field of F_q and let $f : k \to k$ be defined by $f(x) = \sum_{(i,j)\in I} \alpha_{(i,j)} x^{q^i+q^j}$ where I is some index set such that the pairs satisfy some degree bound $q^i + q^j \leq d$.

HFE

Core Map

Let k be a degree n extension field of F_q and let $f : k \to k$ be defined by $f(x) = \sum_{(i,j)\in I} \alpha_{(i,j)} x^{q^i+q^j}$ where I is some index set such that the pairs satisfy some degree bound $q^i + q^j \leq d$.

Vulnerable

The original proposal can be broken with algebraic attacks involving Gröbner basis computations. This class of systems of formulae generate easy $\mathcal{MQ}$ problems.

HFE

Core Map

Let k be a degree n extension field of F_q and let $f : k \to k$ be defined by $f(x) = \sum_{(i,j)\in I} \alpha_{(i,j)} x^{q^i+q^j}$ where I is some index set such that the pairs satisfy some degree bound $q^i + q^j \leq d$.

Vulnerable

The original proposal can be broken with algebraic attacks involving Gröbner basis computations. This class of systems of formulae generate easy $\mathcal{MQ}$ problems.

We can make this more precise with degree of regularity results.

Modifiers

To secure schemes from these attacks, several modifiers have been developed.

Modifiers

To secure schemes from these attacks, several modifiers have been developed.

Most Important Modifiers

1. The minus (-) modifier: removing r of the public equations, and
2. the vinegar (v) modifier: additional variables are added to the system, the values of which are randomly assigned in the inversion process.

Multiplicative Attack on C^* and C^{*-}

Definition [*based on* Dubois et al. (2007)]

A function f has the *Multiplicative Symmetry* if:
$Df(\sigma a, x) + Df(a, \sigma x) = p(\sigma)Df(a, x)$ for all $\sigma \in k$.

Multiplicative Attack on C^* and C^{*-}

Definition [*based on* Dubois et al. (2007)]

A function f has the *Multiplicative Symmetry* if:
$Df(\sigma a, x) + Df(a, \sigma x) = p(\sigma) Df(a, x)$ for all $\sigma \in k$.

C^* monomial

$$Df(\sigma a, x) + Df(a, \sigma x) = (\sigma^{q^\theta} + \sigma) Df(a, x),$$

Multiplicative Attack on C^* and C^{*-}

Definition [*based on* Dubois et al. (2007)]

A function f has the *Multiplicative Symmetry* if:
$Df(\sigma a, x) + Df(a, \sigma x) = p(\sigma) Df(a, x)$ for all $\sigma \in k$.

C^* monomial

$$Df(\sigma a, x) + Df(a, \sigma x) = (\sigma^{q^\theta} + \sigma) Df(a, x),$$
$$DP(U^{-1}\sigma U a, x) + DP(a, U^{-1}\sigma U x) = L_\sigma DP(a, x).$$

Multiplicative Attack on C^* and C^{*-}

Definition [*based on* Dubois et al. (2007)]

A function f has the *Multiplicative Symmetry* if:
$Df(\sigma a, x) + Df(a, \sigma x) = p(\sigma)Df(a, x)$ for all $\sigma \in k$.

C^* monomial

$$Df(\sigma a, x) + Df(a, \sigma x) = (\sigma^{q^\theta} + \sigma)Df(a, x),$$
$$DP(U^{-1}\sigma Ua, x) + DP(a, U^{-1}\sigma Ux) = L_\sigma DP(a, x).$$

This relation provides a criterion for discovering the multiplicative structure of k which undermines C^*. Since this method doesn't require that T be invertible, this method works for C^{*-} as well to generate enough relations to turn it into C^*.

HFEv and HFEv-

HFEv

Let the core map be given by
$f(x,v) =$
$\sum_{i,j}(\alpha_{i,j}x^{q^i+q^j} + \beta_{i,j}x^{q^i}v^{q^j} + \gamma_{i,j}v^{q^i+q^j}) + \sum_i a_i x^{q^i} + \sum_i b_i v^{q^i} + c,$
where v is restricted to a small subspace of k.
Inversion is accomplished by fixing the values of v and then inverting the resulting set of HFE equations.

HFEv and HFEv-

HFEv

Let the core map be given by
$f(x, v) =$
$\sum_{i,j}(\alpha_{i,j}x^{q^i+q^j} + \beta_{i,j}x^{q^i}v^{q^j} + \gamma_{i,j}v^{q^i+q^j}) + \sum_i a_i x^{q^i} + \sum_i b_i v^{q^i} + c,$
where v is restricted to a small subspace of k.
Inversion is accomplished by fixing the values of v and then inverting the resulting set of HFE equations.

If we use, in addition, the minus modifier we obtain HFEv$^-$.
QUARTZ is an HFEv$^-$ scheme.

Balanced Oil-Vinegar

The Core Map

Let $f : \mathbb{F}_q^{2o} \rightarrow \mathbb{F}_q^{o}$ be a random quadratic map such that given random constants $c_1, \ldots, c_o \in \mathbb{F}_q$, $f(x_1, \ldots, x_o, c_1, \ldots, c_o)$ is affine in $x_1, \ldots, x_o$.

Balanced Oil-Vinegar

The Core Map

Let $f : \mathbb{F}_q^{2o} \rightarrow \mathbb{F}_q^o$ be a random quadratic map such that given random constants $c_1, \dots, c_o \in \mathbb{F}_q$, $f(x_1, \dots, x_o, c_1, \dots, c_o)$ is affine in $x_1, \dots, x_o$.

The Entire Map

The public map, P, is defined by $P = f \circ L$ for some affine map, L.

Balanced Oil-Vinegar

The Core Map

Let $f : \mathbb{F}_q^{2o} \to \mathbb{F}_q^o$ be a random quadratic map such that given random constants $c_1, \ldots, c_o \in \mathbb{F}_q$, $f(x_1, \ldots, x_o, c_1, \ldots, c_o)$ is affine in $x_1, \ldots, x_o$.

The Entire Map

The public map, P, is defined by $P = f \circ L$ for some affine map, L.

Inversion

Randomly choose $c_1, \ldots, c_o$, solve $y = f(x_1, \ldots, x_o, c_1, \ldots, c_o)$, compute $L^{-1}(x_1, \ldots, x_o, c_1, \ldots, c_o)^T$.

Differential Version of Kipnis-Shamir Attack

Trivial Differential Property of Core Map

Let O represent the subspace generated by the first o coordinates. For all $a, x \in O$, $Df(a, x) = 0$. Therefore each differential coordinate form, Df_i, has the form:

$$\begin{bmatrix} 0 & Df_{i1} \\ Df_{i1}^T & Df_{i2} \end{bmatrix}.$$

Differential Version of Kipnis-Shamir Attack

Trivial Differential Property of Core Map

Let O represent the subspace generated by the first o coordinates. For all $a, x \in O$, $Df(a, x) = 0$. Therefore each differential coordinate form, Df_i, has the form:

$$\begin{bmatrix} 0 & Df_{i1} \\ Df_{i1}^T & Df_{i2} \end{bmatrix}.$$

Differential Invariant

Let M_1 and M_2 be two invertible matrices in the span of the Df_i. Then $M_1^{-1}M_2$ is an O-invariant transformation of the form:

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

Broken

Find the Invariant Subspace

Since $D(f \circ L)_i = L^T Df_i L$, an attacker needs only find two invertible maps, M_1, M_2, in the span of DP_i, and find the invariant subspace of $M_1^{-1} M_2$.

Broken

Find the Invariant Subspace

Since $D(f \circ L)_i = L^T Df_i L$, an attacker needs only find two invertible maps, M_1, M_2, in the span of DP_i, and find the invariant subspace of $M_1^{-1} M_2$.

New Decryption Map

Once recovered, the attacker produces a change of basis, M, sending the basis of O to the first o standard basis vectors. The attacker can then sign a document by the same method as the legitimate user.

UOV

Unbalanced Oil-Vinegar

Increase the number of vinegar variables.

UOV

Unbalanced Oil-Vinegar

Increase the number of vinegar variables.

SIDE NOTE: There is an interesting natural parametrization within HFE and UOV.

Conclusions

- Most practical attacks are structural and work against a subclass of systems.

Conclusions

- Most practical attacks are structural and work against a subclass of systems.
- Quantum complexity theoretic results on $\mathcal{MP}/\mathcal{IP}/\mathcal{IP}1\mathcal{S}$ would be very interesting.

Conclusions

- Most practical attacks are structural and work against a subclass of systems.
- Quantum complexity theoretic results on $\mathcal{MP}/\mathcal{IP}/\mathcal{IP}1\mathcal{S}$ would be very interesting.
- Quantum algorithms for some of these generic problems?

Conclusions

- Most practical attacks are structural and work against a subclass of systems.
- Quantum complexity theoretic results on $\mathcal{MP}/\mathcal{IP}/\mathcal{IP}1\mathcal{S}$ would be very interesting.
- Quantum algorithms for some of these generic problems?
- Quantum enhancements (polynomial or exponential speedup) for structural attacks?

Done

Thanks!

I will post some references when I wake up.