Key Recovery on Hidden Monomial Multivariate Schemes

P.-A. Fouque, J. Stern — ENS
G. Macario-Rat — Orange Labs

April 2008

Multivariate Cryptography

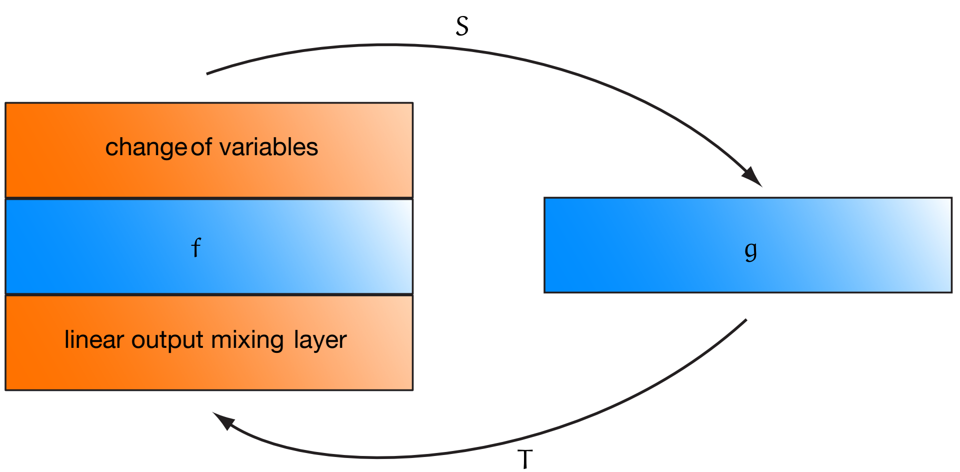
- MQ: Multivariate Quadratic systems

  solving quadratic systems in many variables

  - NP-hard
- Gröbner basis algorithms
  - exponential complexity in time and space
- easy instances hidden using linear mappings
- efficient cryptographic schemes
  - C^*, SFLASH, C^{*-}
  - “Minus” scheme contermeasure against Patarin’s attack

IP: Isomorphism of Polynomials

- Patarin in 1996
- IP with two secrets
  - given f and g two polynomial systems, find if any, two linear isomorphisms S and T such as $T \circ f = g \circ S$
  - possible equivalent keys for C^*, HFE, etc.
  - central problem in the Traitor Tracing Scheme



C^* Scheme

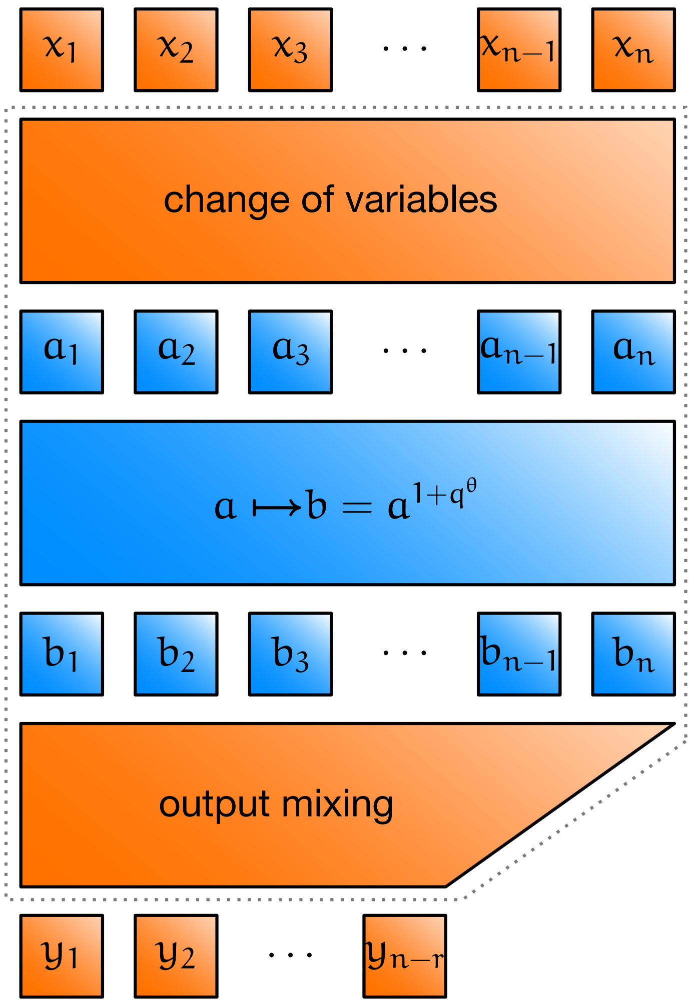
✔

- Matsumoto and Imai 1985
- n unknowns over the finite field $GF(q)$
- uses an embedding

$$\Phi : GF(q)^n \longrightarrow GF(q^n)$$

- the internal mapping is $a \mapsto a^{1+q^\theta}$
- cryptanalysis: Patarin 1995
  - $ab^{q^\theta} = a^{q^{2\theta}} b$
- decryption

SFLASH



- Patarin, Goubin, and Courtois in 1998
- C^* with Minus scheme
  - contermeasure against Patarin's cryptanalysis
  - r equations removed, complexity q^r
- cryptanalysis
  - Dubois, Fouque, Shamir, and Stern
  - use of the differential
  - attack of the Minus scheme

Differential

- differential of first order

$$D_X(f) = f(X) - f(0)$$

- differential of second order

$$\begin{aligned} D_{X,Y}(f) &= D_X(D_Y(f(X+Y)) \\ &= f(X+Y) - f(X) - f(Y) + f(0) \end{aligned}$$

- differential of higher order

$$D_{X_1,X_2,\ldots,X_\ell}(f) = D_{X_1}(D_{X_2}(\ldots(D_{X_\ell}(f(X_1+X_2+\ldots+X_\ell)))\ldots))$$

- symmetric in all its variables, easy to compute

Properties of the differential

- for f of degree d
  - for $\ell > d$, $D_{X_1,X_2,\ldots,X_\ell}(f) = 0$
  - for $\ell = d$, $D_{X_1,X_2,\ldots,X_\ell}(f)$ is $(X_1, X_2, \ldots, X_\ell)$ -linear
- product of two linear functions f and g (fg is quadratic)
  - $D_{X,Y}(fg) = f(X)g(Y) + f(Y)g(X)$
- multiplicative property when f and g are multiplicative

  i.e. $f(XY) = f(X)f(Y)$, $g(XY) = g(X)g(Y)$
  - $D_{XZ,Y}(fg) + D_{X,YZ}(fg) = (f(Z) + g(Z))D_{X,Y}(fg)$

Characteristic property

- from central mapping to public key

  $P = T \circ f \circ S$ public equations

  $D_{X,Y}(T \circ f \circ S) = T \circ D_{S(X),S(Y)}(f)$

- characteristic property of multiplications

  linear mappings M and M' such that
  $D_{M(X),Y}(f) + D_{X,M(Y)}(f) = M'(D_{X,Y}(f))$ are multiplications

  linear mappings L and L' such that
  $D_{L(X),Y}(P) + D_{X,L(Y)}(P) = L'(D_{X,Y}(P))$ are
  $L = S^{-1} \circ M_Z \circ S$ for some Z where $M_Z(X) = ZX$

Key recovery

- from multiplication to multiplier
  - $L = S^{-1} \circ M_Z \circ S$ and M_Z are conjuguate
  - same minimal polynomial, Z is one of its roots
- retreiving S

  $S \circ L = M_Z \circ S$ is linear in S coordinates
- retreiving T

  $T = P \circ S^{-1} \circ f^{-1}$

Practical attack

- considered central mappings are monomials
  - $f = X^{1+q^{\theta_1}+\ldots+q^{\theta_{d-1}}}$
  - all $X^{q^{\theta_i}}$ are linear and multiplicative
- equivalent keys

  multiplications and Frobenius traverse the central mapping
  - $(T, f, S) \equiv (T \circ M_{f(Z)^{-1}}, f, M_Z \circ S)$
  - $(T, f, S) \equiv (T \circ (Z^{q^i})^{-1}, f, Z^{q^i} \circ S)$
- complexity
  - $d!n^{d+1} + n^{d+4} + n^6$

Experimental results

- non homogeneous public key
  - extra computations still possible
- comparison with Faugère's and Perret's works
  - Gröbner basis algorithms : $n \leqslant 20\,,\ d_0 = 2$
  - deals directly with monomial of highest degree
- timings

d	q	n	t_{gen}	t_{sol}
2	2^7	37	6s.	23s.
2	2^7	67	60s.	12m.
3	2^9	12	26s.	15s.
4	2^{16}	9	1.4s.	0.3s.
4	2^8	12	32s.	80s.