Multivariate Cryptography on Smart Cards

Mehdi-Laurent Akkar *ml.akkar@free.fr*

Jacques Patarin *j.patarin@frlv.bull.fr*

CP8, 68 route de Versailles

78431 Louveciennes, FRANCE

Public Key Cryptography

- ***Arithmetic Schemes***

  Typical operation a.b mod n

  a,b,n 512 to 2048 bits

- ***Elliptic Curves***

  Typical operation a + b on the curve

  a,b 100 to 220 bits

- ***Multivariate schemes***

  Typical operations a+b mod n / a.b mod n

  a,b,n 1 to 16 bits

- ***Others (Graphs, Lattices …)***

  often not efficient speed, size of keys …

Multivariate Cryptography (1)

- Multivariate Polynomials Cryptography
  - Degre 1: Error correcting codes schemes (Mc Eliece, Niedereiter)
  - Degre 2: $HFEV^-$ (ie. Quartz ...), C^{*--} (ie. Flash, Sflash)
  - Degre 3: Dragons of degre 3
  - Degre 4: $2R^-$

- Properties:
  - No proofs of security (indirect results)
  - Very efficien for authentificatin, signature and encryption.

Multivariate Cryptography (2)

- Multivariate Combinatorial Cryptography:
  - Non NP-Hard: IP
  - NP Hard: PKP, SD, PPP, MinRank

- Properties:
  - Good proof of security
  - Very efficient for authentification
  - Not efficient for signatures
  - No encryption

IP (Isomophisms of Polynomials)

- ***Secret of Alice (A) :***
  an isomorphism s between 2 sets of equations (X) and (Y)
  Public Key :
  (X) and (Y)

Alice	Randomly generates (Z) isomorph to (X) by t		
Bob	Send to Alice 0 or 1		
Alice	0	Send t	to bob
	1	Send $t \, o \, s^{-1}$	to Bob
Bob	0	Check that (X) is t-isomorph to (Z)	
	1	Check that (Y) is ($s^{-1} o$ t)-isomorph to (Z)	

HFE = Hidden Fields Equation

- x : cleartext (or signature), $x \in F_q^n$, $x = (x_1, \ldots, x_n)$

  ↓ s : secret affine bijection

  a

  ↓

  $b = f(a) =$ with $a,b \in F_q^n$,

  degre(b) $< d$ (< 1000

  ↓ t : secret affine bijection

  y : cyphertext (or message to sign), $y \in F_q^n$, $y = (y_1, \ldots, y_n)$

- The public key is the composition of the 3 operations.

C^{*--} = C^* scheme with missing equations & only one branch

- x : cleartext (or signature), $x \in F_q^n$, $x = (x_1, \ldots, x_n)$

  $\downarrow$ s : secret affine bijection

  a

  $\downarrow$

  $b = f(a) =$ with a F_q^n,

  $\downarrow$ t : secret affine *non bijective* fonction

  y : message to sign(no encryption) , $y \in F_q^\alpha$, $y = (y_1, \ldots, y_\alpha)$
  where $\alpha < n$ and $q^{n-\alpha} > 2^{64}$

- The public key is the composition of the 3 operations.

Example: n=8 / K=F_2

$$\left\{\begin{array}{lclcl}
y_0 & = & F^{(0)}(x_0,\ldots,x_7) & = & 1+x_0+x_3+x_0x_2+x_1x_2+x_0x_3+x_1x_3+x_2x_3+x_0x_4+x_1x_4 \\
 & & & & +x_3x_4+x_1x_5+x_4x_5+x_2x_6+x_5x_6+x_0x_7+x_2x_7+x_4x_7+x_6x_7 \\
y_1 & = & F^{(1)}(x_0,\ldots,x_7) & = & 1+x_0+x_2+x_3+x_5+x_6+x_0x_1+x_0x_2+x_1x_2+x_1x_3+x_1x_4 \\
 & & & & +x_2x_4+x_3x_4+x_0x_5+x_1x_5+x_2x_5+x_0x_6+x_4x_7+x_6x_7 \\
y_2 & = & F^{(2)}(x_0,\ldots,x_7) & = & x_2+x_3+x_5+x_6+x_2x_3+x_2x_4+x_0x_5+x_1x_5+x_0x_6+x_1x_6 \\
 & & & & +x_2x_6+x_3x_6+x_4x_6+x_2x_7+x_4x_7+x_6x_7 \\
y_3 & = & F^{(3)}(x_0,\ldots,x_7) & = & 1+x_3+x_4+x_5+x_6+x_1x_2+x_1x_3+x_2x_3+x_0x_4+x_2x_4+x_2x_5 \\
 & & & & +x_1x_6+x_2x_6+x_3x_6+x_4x_6+x_5x_6+x_0x_7+x_1x_7+x_2x_7+x_3x_7 \\
 & & & & +x_4x_7+x_5x_7 \\
y_4 & = & F^{(4)}(x_0,\ldots,x_7) & = & 1+x_5+x_0x_1+x_1x_2+x_1x_3+x_0x_4+x_2x_4+x_3x_4+x_0x_5+x_3x_5 \\
 & & & & +x_3x_6+x_5x_6+x_2x_7+x_4x_7+x_5x_7 \\
y_5 & = & F^{(5)}(x_0,\ldots,x_7) & = & x_2+x_3+x_5+x_7+x_0x_1+x_0x_2+x_0x_3+x_1x_3+x_0x_4+x_2x_4 \\
 & & & & +x_3x_4+x_1x_5+x_2x_5+x_0x_6+x_4x_6+x_5x_6+x_1x_7+x_2x_7+x_3x_7 \\
 & & & & +x_4x_7+x_5x_7+x_6x_7 \\
y_6 & = & F^{(6)}(x_0,\ldots,x_7) & = & x_0+x_0x_1+x_0x_2+x_0x_3+x_1x_3+x_0x_5+x_2x_5+x_4x_5+x_0x_6 \\
 & & & & +x_3x_6+x_1x_7+x_6x_7 \\
y_7 & = & F^{(7)}(x_0,\ldots,x_7) & = & 1+x_0+x_4+x_7+x_0x_1+x_0x_2+x_1x_2+x_2x_3+x_0x_4+x_0x_5+x_1x_5 \\
 & & & & +x_2x_5+x_4x_5+x_0x_6+x_1x_6+x_2x_6+x_4x_6+x_0x_7+x_3x_7+x_4x_7
\end{array}\right.$$

Efficiency (signature) (1)

- ***RSA 1024***

– Best known attack	10^{11} Mips year (2^{81} op.)
– RAM in secret key computations	264 bytes
– RAM in public key computations	400 bytes
– Length of the public key	128+1 bytes
– Length of the secret key	128 bytes
– ROM Code	500 bytes
– Secret key computation (CRT)	1600 basic operations
– Public key computation (e=3)	8 basic operations
– Length of the Signature	128 bytes

Efficiency (signature) (2)

- ***Quartz (HFEv- variant)***

– Best known attack	10^{13} Mips year (2^{100} op)
– RAM in secret key computations	500 bytes
– RAM in public key computations	40 bytes
– Length of the public key	71000 bytes
– Length of the scret key	3000 bytes
– ROM Code	500 bytes
– Secret key computation (CRT)	16000 basic operations
– Public key computation (e=3)	0.5 basic operations
– Length of the Signature	16 bytes

Efficiency (signature) (3)

- ***Flash (C*-- variant)***

– Best known attack	10^{13} Mips year (2^{100} op)
– RAM in secret key computations	100 bytes
– RAM in public key computations	30 bytes
– Length of the public key	18000 bytes
– Length of the scret key	2750 bytes
– ROM Code	500 bytes
– Secret key computation (CRT)	10 basic operations
– Public key computation (e=3)	1 basic operations
– Length of the Signature	37 bytes