Differential Cryptanalysis for Multivariate Schemes

Jacques Stern

Joint work with P. A. Fouque and L. Granboulan

École normale supérieure

MI Cryptosystem

- $\mathbb{F}_q$ a finite field of characteristic 2
- Secret Key : $\boldsymbol{S}$, $\boldsymbol{T}$ two affine bijections in $(\mathbb{F}_q)^n$
- $\boldsymbol{F}$ is defined as $F(X) = X^{q^\ell+1}$ in $\mathbb{F}_{q^n}$ and is thus a quadratic map from $(\mathbb{F}_q)^n$ to $(\mathbb{F}_q)^n$
- Public key : the system $\boldsymbol{E}$ of equations in $(\mathbb{F}_q)^n$

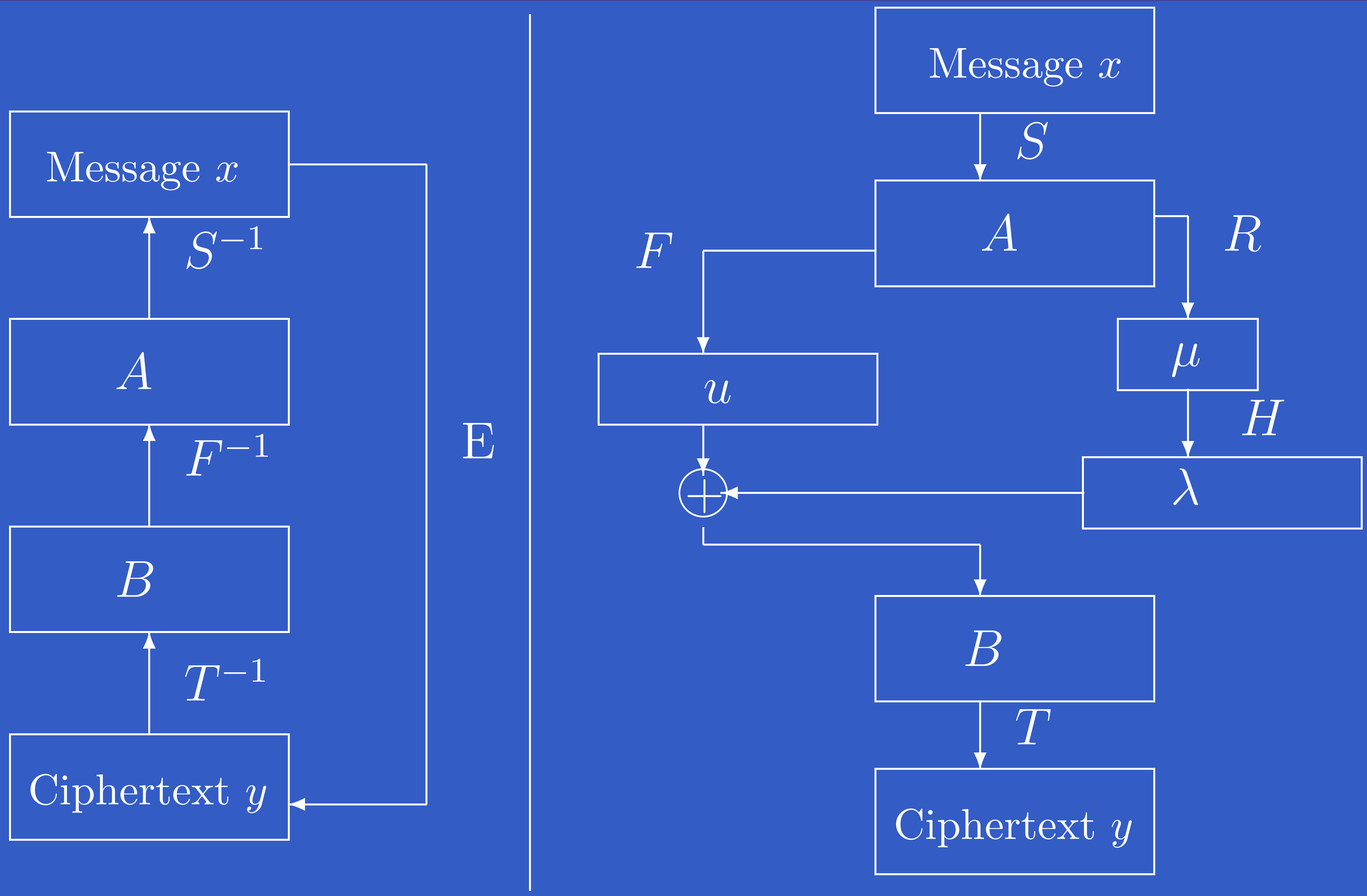
$$\boldsymbol{E} = \boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{S}$$

- Decryption function : invert $\boldsymbol{T}$, compute F^{-1} by raising to the power $(q^\ell + 1)^{-1} \bmod (q^n - 1)$, and invert $\boldsymbol{S}$

Perturbated MI Cryptosystem (PMI)

- $\boldsymbol{R}$ linear map from $(\mathbb{F}_q)^n$ to $(\mathbb{F}_q)^r$ with $r \ll n$
- $\boldsymbol{H}$ quadratic function from $(\mathbb{F}_q)^r$ to $(\mathbb{F}_q)^n$
- $\boldsymbol{E'} = \boldsymbol{T} \circ (\boldsymbol{F} + \boldsymbol{H} \circ \boldsymbol{R}) \circ \boldsymbol{S} = \boldsymbol{E} + \boldsymbol{T} \circ \boldsymbol{H} \circ \boldsymbol{R} \circ \boldsymbol{S}$
- The PMI scheme $\boldsymbol{E'}$ is the MI scheme $\boldsymbol{E}$ plus a random-looking quadratic term $\boldsymbol{T} \circ \boldsymbol{H} \circ \boldsymbol{R} \circ \boldsymbol{S}$
- q^r must be small so that exhaustive search on q^r is efficient, otherwise decryption is slow
- Secret key : $(\boldsymbol{S}, \boldsymbol{T}, P)$ where P is a table storing $(\boldsymbol{\lambda}, \boldsymbol{\mu})$ pairs s.t. $\boldsymbol{H}(\boldsymbol{\mu}) = \boldsymbol{\lambda}$

MI and PMI Cryptosystems



PMI Decryption Algorithm

- Input : y ciphertext
- Output : x plaintext s.t. $y = E'(x)$
- Compute $B = T^{-1}(y)$
- For the q^r pairs (λ, μ), compute

$$A_\lambda = F^{-1}(B - \lambda) \text{ until } R(A_\lambda) = \mu$$

- Return $x_\lambda = S^{-1}(A_\lambda)$
- If many pairs (λ, μ) are possible, redundancy is added to the plaintext

PMI schemes and variants

- Ding's practical cryptosystem
  - $q = 2$, $n = 136$, $\ell = 40$ and $r = 6$
  - so $F(X) = X^{2^{40}+1}$, $R : (\mathbb{F}_2)^{136} \longrightarrow (\mathbb{F}_2)^6$ and $H : (\mathbb{F}_2)^6 \longrightarrow (\mathbb{F}_2)^{136}$
  - $\gcd(2^{136} - 1, 2^{40} - 1) = 2^{\gcd(136,40)} - 1 = 2^8 - 1$

The variant of PMI when $\gcd(n, \ell) = 8$ is called "Ding's scheme"

The variant of PMI when $\gcd(n, \ell) = 1$ is called "Generalized scheme"

Patarin attack on MI

- Search n bilinear relations $(B_i)_{1\leq i\leq n}$ between the plaintext $\boldsymbol{x}$ and the ciphertext $\boldsymbol{y}$
- Recover the coefficients of the bilinear relations using $O(n^2)$ plaintext/ciphertext pairs
- Given a ciphertext $\boldsymbol{y}$, solve the system of the n bilinear relations to find the plaintext $\boldsymbol{x}$
- However, the system is not invertible ($\Rightarrow$ exhaustive search to uniquely recover $\boldsymbol{x}$)

Patarin attack on (2)

- Let $A = \boldsymbol{S}(\boldsymbol{x}) \in \mathbb{F}_{q^n}$ and $B = \boldsymbol{T}^{-1}(\boldsymbol{y}) \in \mathbb{F}_{q^n}$
- Since $F(A) = B$, we have $B = A^{q^\ell+1}$
- By raising to the power $q^\ell - 1$ and multiplying by AB, we get a bilinear expression

$$A \cdot B^{q^\ell} = A^{q^{2\ell}} \cdot B$$

- Rewriting this equation in the variables $\boldsymbol{x}$ and $\boldsymbol{y}$ and projeting into $(\mathbb{F}_q)^n$, we get n bilinear relations between the plaintext and ciphertext

Breaking the PMI scheme

- $\boldsymbol{E'} = \boldsymbol{E} + \boldsymbol{T} \circ \boldsymbol{H} \circ \boldsymbol{R} \circ \boldsymbol{S}$
- Here, constants of affine maps are erased (see paper)
- If $k \in \mathcal{K} = \ker(R \circ S)$, then $\boldsymbol{E'(k) = E(k)}$
- On the subspace $\mathcal{K}$, Patarin's attack can be applied
- Goal : decrypting all PMI ciphertexts
  - when $x \in \mathcal{K}$ whose dimension $(n - r)$ is large
  - for all x

Detecting membership in $\mathcal{K}$ using differential cryptanalysis

The use of differentials

- Let G be a quadratic map, its differential is linear

$$\boldsymbol{L_{G,k}} \; : x \mapsto G(x+k) - G(x) - G(k) + G(0)$$

- The constant term disappears thanks to $G(0)$, and so $\boldsymbol{L_{G,k}}$ is a linear map and not an affine one
- Let $X = \boldsymbol{S}(\boldsymbol{x})$ and $K = \boldsymbol{S}(\boldsymbol{k})$
- Differential of a composition of functions : if $E = T \circ F \circ S$, then $L_{E,k}(x) = T \circ L_{F,K}(X)$
- Since $\boldsymbol{S}$ and $\boldsymbol{T}$ are bijection, $\dim(\ker(\boldsymbol{L_{E,k}})) = \dim(\ker(\boldsymbol{L_{F,K}}))$

Expression of $L_{F,K}$

$$\begin{aligned}
L_{F,K}(X) &= F(X+K) - F(X) - F(K) + F(0) \\
&= (X+K)^{q^\ell} \cdot (X+K) - X^{q^\ell+1} - K^{q^\ell+1} \\
&= (X^{q^\ell} + K^{q^\ell}) \cdot (X+K) - X^{q^\ell+1} - K^{q^\ell+1} \\
&= K^{q^\ell} \cdot X + X^{q^\ell} \cdot K = K^{q^\ell+1} \cdot \left(\frac{X}{K} + \left(\frac{X}{K}\right)^{q^\ell} \right)
\end{aligned}$$

$X \mapsto L_{F,K}(X)$ is a linear map

Kernel's dimension of the differential in MI

- X is in the kernel of $L_{F,K}$

$$
\begin{aligned}
L_{F,K}(X) = 0 \quad & \iff \quad Y + Y^{q^\ell} = 0 \text{ where } Y = \frac{X}{K} \\
& \iff \quad Y(1 + Y^{q^\ell - 1}) = 0 \\
& \iff \quad Y^{q^\ell - 1} = 1 \text{ since } \mathrm{char}(\mathbb{F}_q) = 2
\end{aligned}
$$

- $Y = 1 \Rightarrow K \in \ker L_{F,K} \iff k \in \ker L_{E,k}$
- The equation $Y^{q^\ell - 1} = 1$ has $q^{\gcd(\ell,n)} - 1$ solutions
- Therefore, $\dim(\ker L_{E,k}) = \dim(\ker L_{F,K}) = \gcd(\ell, n)$

Kernel's dimension of the differential in PMI

- What is the contribution of $\boldsymbol{H} \circ \boldsymbol{R}$ on the kernel's dimension ?
- Since $\boldsymbol{H}$ is quadratic, its differential is $\boldsymbol{L}_{\boldsymbol{H}\circ\boldsymbol{R},\boldsymbol{K}}(X) = \sum_{i,j=1}^{r} \alpha_{i,j}[R_i(X)R_j(K) + R_i(K)R_j(X)]$
- K is always in $\ker(\boldsymbol{L}_{\boldsymbol{H}\circ\boldsymbol{R},\boldsymbol{K}})$ and $\dim(\ker(L_{E',K})) \geq 1$
- Since $\boldsymbol{H}$ is random, $L_{H\circ R,K}$ is a random linear map and $L_{E',k}$ is also a random linear map
- Consequently, $\dim(\ker L_{E',k})$ follows the distribution of random linear map

Breaking Ding's scheme

- In the proposed system, $\gcd(\ell, n) = 8$
- The probability that a linear map has a kernel of dimension 8 is small $(\leq 1/2^{20})$
- We devise the following test :
  - if $\dim(\ker(L_{E',k})) = \gcd(\ell, n)$, then decide $k \in \mathcal{K}$
  - otherwise decide $k \notin \mathcal{K}$

Total Break of Ding's scheme

- $\mathcal{K}$ can be recovered by collecting $n-r$ independent vectors as well as the bilinear relations of Patarin's attack when $k \in \mathcal{K}$
- On this subspace, we can invert any ciphertext $\boldsymbol{y}$ s.t. $\boldsymbol{x} \in \mathcal{K}$ where $\boldsymbol{y} = \boldsymbol{E}'(\boldsymbol{x})$ which holds with probability $1/q^r$
- The entire space can be divided into q^r affine subspaces parallel to the $\mathcal{K}$ direction
- The same attack can be mounted in parallel on all these subspaces to recover any ciphertext $\boldsymbol{y}$

Breaking the Generalized scheme

- When $\gcd(\ell, n) = 1$, the previous test cannot be applied since $\dim(\ker L_{E',k}) = \gcd(\ell, n) = 1$ with high probability even if $k \notin \mathcal{K}$
- Therefore,
  - if $\dim(\ker L_{E',k}) = 1$, k may or not be in $\mathcal{K}$
  - if $\dim(\ker L_{E',k}) > 1$, $k \notin \mathcal{K}$ with probability 1
- We need to filter bad values k s.t.

$$\dim(\ker L_{E',k}) = 1 \text{ and } k \notin \mathcal{K}$$

Filtering the bad values k

- Since $\mathcal{K}$ is a linear space, if $k, k' \in \mathcal{K}$, then $k + k' \in \mathcal{K}$
- To decide if $k \in \mathcal{K}$, which holds with probability $1/q^r$, take different k' s.t. $\dim(\ker L_{E',k'}) = 1$ and compute the distribution of $\dim(L_{E',k+k'})$
- The distributions of $\dim(L_{E',k+k'})$ when $k \in \mathcal{K}$ and when $k \notin \mathcal{K}$ are different and can be distinguished by statistic experiments

New Attack on the MI cryptosystem

- This new attack finds two bilinear relations C and D of n coordinates :
  - C is between a vector f_k of the kernel of the transpose matrix of $L_{E,k}$ and the ciphertext $\boldsymbol{y}$ corresponding to $E(\boldsymbol{k})$
  - D is between the vector f_k and the corresponding plaintext $\boldsymbol{k}$

Decomposition of $L_{E,k}$

- Since $L_{F,K}(X) = K^{q^\ell+1} \cdot \left(\frac{X}{K} + \left(\frac{X}{K}\right)^{q^\ell}\right)$, $L_{E,k} = T \circ L_{F,K} \circ S$ can be written as

$$T \circ \mu_K \circ \psi \circ \theta_K \circ S$$

where μ_K, ψ and θ_K are the linear maps and $K = S(k)$ and $X = S(x)$:

$$\begin{aligned} \theta_K &: X \mapsto \frac{X}{K} \\ \psi &: Y \mapsto Y + Y^{q^\ell} \text{ independent of } K \\ \mu_K &: Z \mapsto K^{q^\ell+1} \cdot Z \end{aligned}$$

f_k in the kernel of transpose of $L_{E,k}$

- T, μ_K, ψ, θ_K and S are $n \times n$ matrices, and (f_k) is a row vector in $L_{E,k}^{\top}$ s.t.

$$(f_k)(T.\mu_K.\psi.\theta_K.S) = 0$$

- Since θ_K and S invertible matrices,

$$(f_k)(T.\mu_K) \in \ker \psi$$

- If $\gcd(\ell, n) = 1$, then $\dim(\ker \psi) = 1$ and if $q = 2$

$$(f_k)(T.\mu_K) = (\hat{f})$$

The two bilinear relations C and D

- $\mu_K(Z) = F(K) \cdot Z$ is linear in $F(K)$
- Since $F(K) = T^{-1}(E(k))$, then μ_K is linear in the ciphertext $E(k)$
- So $(f_k)(T.\mu_K) = (\hat{f})$ is a bilinear relation C between $E(k)$ and f_k which can be projected to the n coordinates
- Finally, as $(f_k)(L_{E,k}) = 0$ and $L_{E,k}$ is linear in k, then there is a bilinear relation D between f_k and the plaintext k

The new attack against MI

Precomputation stage :

- Using many plaintexts k, compute f_k (kernel of $L_{E,k}^{\top}$) and the corresponding ciphertexts $E(k)$ and
  - recover the bilinear relations $C(f_k, E(k))$
  - recover the bilinear relations $D(f_k, k)$

On-line stage :

- Given a ciphertext $E(k)$,
  - recover the vector f_k using C and
  - decrypt using D and f_k

Conclusion

- We show that differential cryptanalysis is a nice tool which can be adapted to successfully attack multivariate schemes
- We apply this novel cryptanalytic method in order to propose
  - A new attack against the MI original scheme
  - An attack against a recently proposed variant of MI called PMI