2F - A New Method for Constructing Efficient Multivariate Encryption Schemes

Daniel Smith-Tone[1,2]

[1]University of Louisville
[2]National Institute of Standards and Technology

29 September, 2022

Objective

Given a multivariate quadratic system of equations

$$P(\mathrm{x}) = \mathrm{y},$$

find x.

Direct Attack

- Solve directly via F4 or XL.
  (Consider the Macaulay matrix: rows = equations, columns = monomials.)
- Complexity related to homogeneous quadratic component.
- Field Equations $(x_i^q - x_i)$
- With hybrid approach we consider the Hilbert series

$$\mathcal{H}(t) = \frac{(1-t^2)^m(1-t^q)^{n-k}}{(1-t)^{n-k}}$$

Differential Attacks

Idea that broke SFLASH. (Also breaks, C^*, k-ary C^*, ℓIC-, etc.)
Discrete Differential $DP(\mathrm{a},\mathrm{x}) = P(\mathrm{a}+\mathrm{x}) - P(\mathrm{a}) - P(\mathrm{x}) + P(0)$.

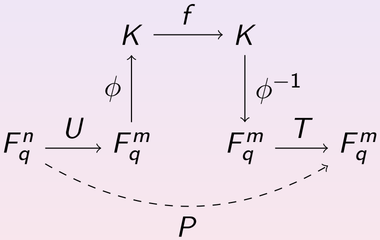
$$DP(L\mathrm{a},\mathrm{x}) + DP(\mathrm{a},L\mathrm{x}) = \Lambda_L DP(\mathrm{a},\mathrm{x})$$

Rank Attacks

Minrank: Given K matrices $\mathrm{M}_1, \ldots, \mathrm{M}_K$ of dimension $s \times t$ over the field F, find nonzero coefficients $\lambda_1, \ldots, \lambda_k$ in the field E/F such that

$$\mathrm{rank}\left(\sum_{i=1}^{K} \lambda_i \mathrm{M}_i\right) \leq r.$$

Definition of SQUARE



U is injective, $f(X) = X^2$, q odd prime-power.

Attacks

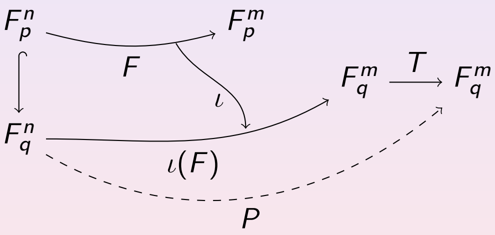
- Direct Attack
- Differential Attack (Perturb Input recover in output)
- Differential Attack (Perturb Output recover in input)
- Rank Attack (Big field "traditional")
- Rank Attack (Big field, Tao et al. style)

Linear Maps are Important

Something critical in all of these attacks (or their analyses) is the role of linear maps.

Question: Can we augment a quadratic map in a nonlinear way to disrupt these cryptanalyses?

Modulus Switching



Example

Let $p = 7$ $n = m = 3$ and $q = 331$.

$$
\begin{aligned}
v_1 &= 2x_1^2 - x_1x_2 - 2x_1x_3 + 0x_2^2 + 3x_2x_3 - x_3^2 \\
v_2 &= x_1^2 + 3x_1x_2 - x_1x_3 - 3x_2^2 + 0x_2x_3 - 2x_3^2 \\
v_3 &= -x_1^2 - 3x_1x_2 + x_1x_3 + 2x_2^2 - x_2x_3 + x_3^2
\end{aligned}
$$

Example

Let $p = 7$ $n = m = 3$ and $q = 331$.

$$v_1 = 2(1)^2 - (1)(-2) - 2(1)(2) + 0(-2)^2 + 3(-2)(2) - (2)^2$$
$$v_2 = (1)^2 + 3(1)(-2) - (1)(2) - 3(-2)^2 + 0(-2)(2) - 2(2)^2$$
$$v_3 = -(1)^2 - 3(1)(-2) + (1)(2) + 2(-2)^2 - (-2)(2) + (2)^2$$

Example

Let $p = 7$ $n = m = 3$ and $q = 331$.

$$v_1 = -2$$
$$v_2 = 1$$
$$v_3 = 2$$

Example

Let $p = 7$ $n = m = 3$ and $q = 331$.

$$v_1 = -16$$
$$v_2 = -27$$
$$v_3 = 23$$

Example

Let $p = 7$ $n = m = 3$ and $q = 331$.

$$v_1 = -16$$
$$v_2 = -27$$
$$v_3 = 23$$

$$y_1 = -153$$
$$y_2 = -83$$
$$y_3 = 109$$

Why it Works

If

$$q > \frac{(p-1)^3}{4}\binom{n+1}{2},$$

then $\mathrm{y} = T \circ \iota(F)(\mathrm{x})$ if and only if $T^{-1}(\mathrm{y}) = F(\mathrm{x}) \pmod{p}$.

Decryption Failures

$$q > \frac{(p-1)^3}{4}\binom{n+1}{2} \Rightarrow \text{no } \textit{new} \text{ decryption failures.}$$

These quadratic distributions are rather tight, so much smaller q are possible.
If we further restrict $x_i \in \{-1, 0, 1\}$, the distributions are even tighter. Can have much larger $p < q$.

Direct Attack

Instead of field equations, we have

$$g_i(x_i) = \prod_{j=\frac{1-p}{2}}^{\frac{p-1}{2}} (x_i - j).$$

$$\mathcal{H}(t) = \frac{(1-t^2)^m (1-t^p)^{n-k}}{(1-t)^{n-k}}$$

If $x_i \in \{-1, 0, 1\}$, then

$$\mathcal{H}(t) = \frac{(1-t^2)^m (1-t^3)^{n-k}}{(1-t)^{n-k}}$$

Differential Attacks

$$DP(\mathrm{La},\mathrm{x}) + DP(\mathrm{a},\mathrm{Lx}) = \Lambda_{\mathrm{L}} DP(\mathrm{a},\mathrm{x})$$

F_p-linear

Need F_p-linear

Also need F_q-linear

Rank Attacks

For small field schemes, rank structure may be preserved.
For big field schemes,

$$[H_1\ H_2\ \cdots\ H_m](M \otimes I_m) = \left[SG^{*0}S^\top\ \cdots\ SG^{*(n-1)}S^\top\right],$$

where H_i is the ith quadratic form of the hidden quadratic map.
The problem is

$$[P_1\ P_2\ \cdots\ P_m] = \left[\widetilde{H}_1\ \widetilde{H}_2\ \cdots\ \widetilde{H}_m\right](T \otimes I_m).$$

Lattice Attacks

Let P be the Macaulay matrix of the public key P.
P is $m \times \binom{n+1}{2}$.
Consider

$$\begin{bmatrix} \frac{p}{q}\mathrm{I}_m & \mathrm{P} \\ 0 & q\mathrm{I}_{\binom{n+1}{2}} \end{bmatrix}.$$

Ray Perlner has a much better lattice-based attack. (Breaks parameters from paper.)

Recall that we can restrict $x_i \in \{-1, 0, 1\}$ and use much larger p and smaller q.

Use SQUARE

Most "standard" multivariate attacks can be used to break SQUARE.

Goal: Create weakest possible target to test the 2F construction.

Parameters and Perfomance in Article

BROKEN

Scheme	PK	pt	ct	Enc.(ms)	Dec.(ms)
ABC(2^8,384,760)	54863KB	384B	760B	502	545
PCBM(149,414)	743KB	149b	414b	13	743
2FSQ$(3, 6653, 81)$	417KB	162b	129B	1.5	0.4
2FSQ$(3, 8377, 91)$	606KB	182b	148B	1.2	0.5
2FSQ$(7, 130411, 69)$	346KB	207b	147B	1.0	2.6
2FSQ$(7, 145861, 73)$	413KB	219b	157B	1.1	2.8

Performance of Secure Parameters

Slower, but still 30-40 times faster than any other multivariate decryption.

Profile

- Small ciphertexts
- Large public keys
- Fairly slow decryption

Future Directions

1) More security analysis.

2) Examine 2F applied to other schemes.