「多変数署名方式とその安全性解析について」 池松さん (九大)

$F := (f_1, \cdots, f_m) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ を二次写像として, 任意の $d \in \mathbb{F}_q^m$ に対して, $F(x) = d$ は少ない計算量で解けるものを 二次中心写像 という.

- 秘密鍵:

$F: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ ：二次中心写像

$S: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$
$T: \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$
) ランダムな可逆な線形写像.

- 公開鍵:

$P := T \circ F \circ S \ : \ \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ ：二次写像

$$\begin{tikzcd} \mathbb{F}_q^n \arrow[r, "P", "\text{検証}"'] & \mathbb{F}_q^n \arrow[d, "T^{-1}"] \\ \mathbb{F}_q^n \arrow[u, "S^{-1}"] \arrow[ur, phantom, "\circlearrowleft"] & \mathbb{F}_q^m \arrow[l, "\text{署名生成}"', "F^{-1}"] \end{tikzcd}$$

Fの構造は隠れる

- UOVの一般的構成

— パラメタ: $u, o \in \mathbb{N}$, $n := u + o$.

$x := (x_1, \cdots, x_u)$, $x' := (x_{u+1}, \cdots, x_n)$
vinega 変数 　　 oil 変数

— UOV中心写像:

$$f_1(x, x') = \sum_{i,j} a_{ij}^{(1)} x_i x_{u+j} + \text{"quad poly"}$$
$$\vdots$$
$$f_o(x, x') = \sum_{i,j} a_{ij}^{(o)} x_i x_{u+j} + \text{"quad poly"}$$

§1 UOV

§2 その安全性解析.

§1.

$\mathbb{F}_q$: 有限体

$u, v, m \in \mathbb{N}_{\geq 1}$ として, $n := u + v$ とおく. これに対して,

$$\left.\begin{aligned} f_1 &:= \sum_{i=1}^{n} \sum_{j=1}^{u} a_{ij}^{(1)} x_i x_j \\ &\vdots \\ f_m &:= \sum_{i=1}^{n} \sum_{j=1}^{u} a_{ij}^{(u)} x_i x_j \end{aligned}\right\}$$

$x_{u+1}, \cdots, x_n$ に関しては 1次式 ……… ☆

$\mathbb{F} := (f_1, \cdots, f_m) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$: 2次写像

◎ Fの性質

$c_1, \cdots, c_u \in \mathbb{F}_q$, $(M_1, \cdots, M_m) \in \mathbb{F}_q^m$ に対して

$$F(c_1, \cdots, c_u, x_{u+1}, \cdots, x_m) = (M_1, \cdots, M_m) \quad \cdots\cdots (*)$$

は v-変数の mコの 1次方程式である.

$v \geq m$ として, $(*)$ の解が存在するとする.

$S \in GL_n(\mathbb{F}_q)$ として, $P = F \circ S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ を考えたとき, Sをランダムにとれば,

- 高い確率で P は ☆ の形で書けない
- Sを知っていれば, Fの性質を使うことができる.

◎ 署名方式 UOV

0. $q, u, v, m \in \mathbb{N}$ をとる.
1. 鍵生成をする. $F = (f_1, \cdots, f_m)$ と $S \in GL_n(\mathbb{F}_q)$ をランダムに生成する.
   その後, $P := F \circ S$ とおく.

   秘密鍵: F, S
   公開鍵: P

2. 署名生成をする.

M：署名をしたい文章 $\in \{0,1\}^*$

$\mathcal{H}: \{0,1\}^* \longrightarrow \mathbb{F}_q^m$ を Hash 関数とする.（逆像の計算が大変な関数.）

$P(x_1, \cdots, x_n) = \mathcal{H}(M)$ の1つの解を S としてそれを M の **署名** とする.

（$F(x_1, \cdots, x_n) = \mathcal{H}(M)$ の解 S' をとれば $S = S^{-1}(S')$ とすればよい.）1次連立方程式なので簡単.

3. 検証を行う.

これは，$P(S) = \mathcal{H}(M)$ が成り立つかを判定する. 正しければ受け入れ，そうでなければ棄却する.

◎ 安全性の議論.

(i) S を知らない状況で $F(x_1, \cdots, x_n) = \mathcal{H}(M)$ に変形することができるか？

つまり，P から F（もしくは S）を復元できるか？

(ii) 直接，$P(x_1, \cdots, x_n) = \mathcal{H}(M)$ を解くことができるか？

(i), (ii) を行えない状況にしないと方式は安全ではない.

§2.

UOV 攻撃戦略には次のようなものがある

(A) $P(x) = \mathcal{H}(M)$ の解を求める. ……**署名偽造攻撃**

(B) P の情報から (F, S) を求める. ……**鍵復元攻撃**

(A) について：Collision attack.

とにかく $P(S) = \mathcal{H}(M)$ となる (S, M) を見つけたい.

$S_1, \cdots, S_X \in \mathbb{F}_q^n$ と $M_1, \cdots, M_Y \in \{0,1\}^*$ をランダムに生成し，$P(S_i) = \mathcal{H}(M_j)$ となるかをみて，等号成立の (S_i, M_j) をとる.

$XY = q^m$ のとき，そのような組 (S_i, M_j) は $1 - \frac{1}{e}$ 程度の確率でみつかる.
おおよそ $X = Y = q^{\frac{m}{2}}$ のときが一番効率的である.

· Direct attack

与えられた M に対して， $P(x) = \mathcal{H}(M)$ を代数的に解く．

n 変数 m 個の 2次方程式

① $P = (p_1, \cdots, p_m)$， 各 p_i は $\mathbb{F}_q[x_1, \cdots, x_n]$ の元

② $I := \langle p_1, \cdots, p_m \rangle \subset \mathbb{F}_q[x_1, \cdots, x_n] =: R$ を 斉次イデアルとする．

ヒルベルト級数 $HS_{R/I}(t) := \sum_{i=0}^{\infty} \dim_{\mathbb{F}_q} (R/I)_i \cdot t^i$ とおく．

③ $k = 1, \cdots, m-1$ とする．

$Q^{(k)} := R/\langle p_1, \cdots, p_k \rangle$ として，p_k をかける写像

$$
\begin{array}{cccc}
p_k : & Q^{(k)} & \longrightarrow & Q^{(k)} \\
 & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
 & f & \longmapsto & p_k f
\end{array}
$$

をとれば，$\mathrm{coker}(p_k) = Q^{(k+1)}$ である．

$$
p_k 倍 : \quad
\begin{tikzcd}[column sep=small]
{} \arrow[dr] & Q_i^{(k)} \arrow[dr] & Q_{i+1}^{(k)} \arrow[dr] & Q_{i+2}^{(k)} \arrow[dr] & Q_{i+3}^{(k)} \arrow[dr] & \\
& Q_{i+1}^{(k)} & Q_{i+2}^{(k)} & Q_{i+3}^{(k)} & Q_{i+4}^{(k)} & Q_{i+5}^{(k)}
\end{tikzcd}
$$

(この仮定を semi-regular と呼ぶ)

すべての k で p_{k+1} 倍写像が 単射か 全射のみから構成されていると 仮定する．

このとき，

$$
\begin{aligned}
HS_{Q^{(k+1)}}(t) &= \left[HS_{Q^{(k)}}(t) - t^2 HS_{Q^{(k)}}(t) \right]_+ \\
&= \left[(1-t^2) HS_{Q^{(k)}}(t) \right]_+
\end{aligned}
$$

← 負の係数の部分はカットする．

$\because$ $HS_{R/I}(t) = \left[\dfrac{(1-t^2)^m}{(1-t)^n} \right]_+$

④. 簡単のため, $P_1 = \cdots = P_m = 0$ かつ $n = m$ であるとする.

このとき, semi-regular と考えて, その Hilbert 級数は

$$\frac{(1-t^2)^m}{(1-t)^m} = (1+t)^m = 1 + mt + \cdots + t^m$$

∵ $\langle p_1, \cdots, p_m \rangle_m \subset \mathbb{F}_q[x_1, \cdots, x_m]_m$ は codim $= 1$ である.

⇝ $x_2^m = \alpha x_1^m + \cdots \bmod \langle p_1, \cdots, p_m \rangle$

$x_3^m = \alpha x_2^m + \cdots \bmod p_1, \cdots, p_m \rangle$

⋮

とかける.

← Weideman アルゴリズムを使って $3\binom{2m-1}{m}^2\binom{m+1}{2}$ の計算量である.