

$F := (f_1, \dots, f_m) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ を二次写像とし、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:

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

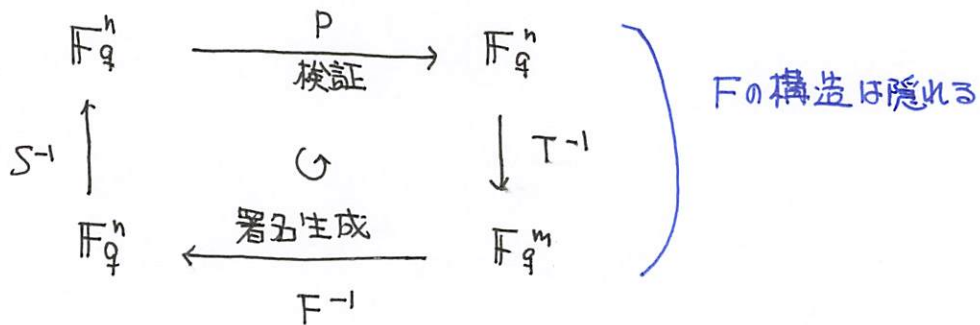
$S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$

$T : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m$

) ランダムな可逆な線形写像.

◦ 公開鍵:

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



◦ UOVの一般的構成

— パラメータ: $u, v \in \mathbb{N}$, $n := u + v$.

$x := (x_1, \dots, x_u)$, $x' := (x_{u+1}, \dots, x_n)$

vinegar 変数

oil 変数

— UOV中心写像:

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

$f_2(x, x') = \sum_{i,j} a_{ij}^{(2)} x_i x_{u+j} + \text{"quad poly"}$

§1 UOV

§2 zの安全性解析.

§1.

\mathbb{F}_q : 有限体

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

$$f_1 := \sum_{i=1}^n \sum_{j=1}^u a_{ij}^{(1)} x_i x_j$$

⋮

$$f_m := \sum_{i=1}^n \sum_{j=1}^u a_{ij}^{(u)} x_i x_j$$

} x_{u+1}, \dots, x_n に関しては 1次式 ----- (★)

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

◎ Fの性質

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

$$F(c_1, \dots, c_u, x_{u+1}, \dots, x_n) = (M_1, \dots, M_m) \dots (*)$$

は ϑ -変数の m 本の 1次方程式 である.

$\vartheta \geq m$ とし、(*) の 解が 存在する とする.

$S \in GL_n(\mathbb{F}_q)$ とし、 $P = F \circ S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ を 考えれば、 S を ランダム に 与えれば、

- 高い確率で P は (★) の形 で 書ける
- 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. $q, u, \vartheta, m \in \mathbb{N}$ とする.

1. 鍵生成をする. $F = (f_1, \dots, f_m)$ 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 ε した文章 $\in \{0,1\}^*$ (逆像の計算が大変な関数.)
 $\mathcal{H}: \{0,1\}^* \rightarrow \mathbb{F}_q^m$ ε Hash 関数とする.

$P(x_1, \dots, x_n) = \mathcal{H}(M)$ の 1 つの解 ε を S として ε が M の **署名** とする.

↑
 1-次元連立方程式なので簡単.

$$\left(\begin{array}{l} F(x_1, \dots, x_n) = \mathcal{H}(M) \text{ の解 } S' \text{ が見つかる} \\ S = S^{-1}(S') \text{ とすればよい.} \end{array} \right)$$

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. 正しい場合は受け入れ, 正しいでなければ棄却する.

o 安全性の議論.

- (i) S を知らない状態で $F(x_1, \dots, x_n) = \mathcal{H}(M)$ 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, $P(x_1, \dots, x_n) = \mathcal{H}(M)$ を解くことができるか?
- (i), (ii) を行えない状況にした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 $P(S) = \mathcal{H}(M)$ とする (S, M) を見つけたい.

$S_1, \dots, S_x \in \mathbb{F}_q^m$ と $M_1, \dots, M_r \in \{0,1\}^*$ をランダムに生成し, $P(S_i) = \mathcal{H}(M_j)$ となるかを見て, 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 $1 - \frac{1}{q}$ 程度の確率で見つかる.
 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, $P(x) = A(M)$ を代数的に解く.

n 変数 m 個の 2 次方程式

- ① $P = (P_1, \dots, P_m)$, 各 P_i は $\mathbb{F}_q[x_1, \dots, x_n]$ の元
- ② $I := \langle P_1, \dots, P_m \rangle \subset \mathbb{F}_q[x_1, \dots, x_n] =: R$ を斉次イデアルとする.

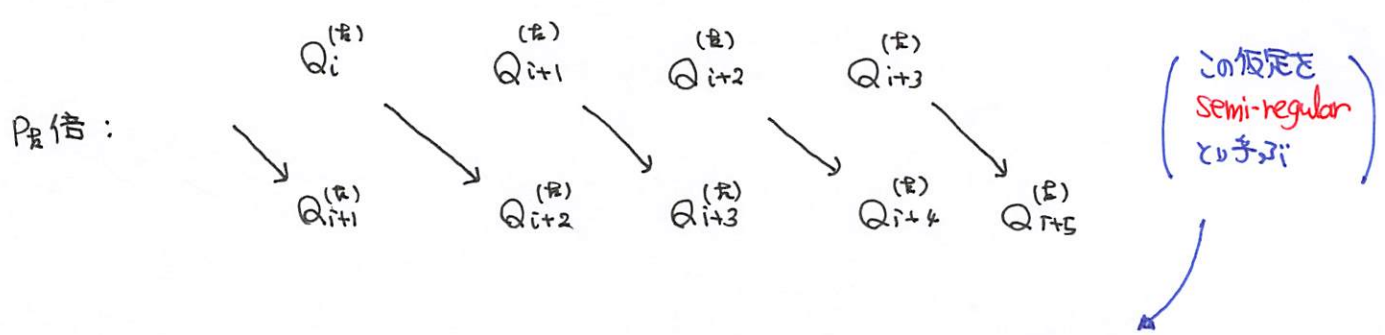
ヒルバート級数 $HS_{R/I}(t) := \sum_{i=0}^{\infty} \dim_{\mathbb{F}_q}(R/I)_i \cdot t^i$ とおく.

- ③ $k = 1, \dots, m-1$ とする.

$Q^{(k)} := R / \langle P_1, \dots, P_k \rangle$ として, P_{k+1} をかける写像

$$P_{k+1} : \begin{array}{ccc} Q^{(k)} & \longrightarrow & Q^{(k)} \\ \cup & & \cup \\ f & \longmapsto & P_{k+1}f \end{array}$$

をかける, $\text{coker}(P_{k+1}) = Q^{(k+1)}$ とある.



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,

$$HS_{Q^{(k+1)}}(t) = [HS_{Q^{(k)}}(t) - t^2 HS_{Q^{(k)}}(t)]_+ \leftarrow \text{負の係数の部分はカットする.}$$

$$= [(1-t^2) HS_{Q^{(k)}}(t)]_+$$

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

④. 簡単のため, $P_1 = \dots = P_m = 0$ かつ $n=m$ とする.

このとき, semi-regular と考え, \cong の Hilbert 級数は

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

⑤ $\langle P_1, \dots, P_m \rangle_m \subset \mathbb{F}_3[x_1, \dots, x_m]_m$ は $\text{codim} = 1$ とある.

$\rightsquigarrow x_2^m = d x_1^m + \dots \pmod{\langle P_1, \dots, P_m \rangle}$
 $x_3^m = d x_2^m + \dots \pmod{\langle P_1, \dots, P_m \rangle}$
 \vdots
とかける.

Weideman アルゴリズムを用いて
 $3 \binom{2m-1}{m}^2 \binom{m+1}{2}$
の計算量がある.