ℓIC 方式への Fouque 等の攻撃法について

小椋 直樹, 内山 成憲

首都大学東京 大学院理工学研究科 数理情報科学専攻

2008 年 7 月 5 日

目的

- ℓIC / ℓIC- (MQ 問題に基づく署名方式) への FGPS 攻撃法と異なる効率的な攻撃法の提案
  - ℓ が偶数の場合についても実装
    - ★ [FGPS 08] の実装は ℓ が奇数の場合のみ
  - ℓ が偶奇各々の実装実験/計算量評価

FGPS = Fouque, Gilles, Perret, Stern

目次

目次

ℓIC(1/4)

- Ding, Wolf, Yang **によって提案** (2007)
- **多変数連立２次方程式の求解** (MQ **問題**) **に安全性の根拠をおく**
  - NP-hard
  - **量子多項式時間アルゴリズムも知られていない**
- **署名の生成/検証が高速**
- Fouque **等による攻撃法の提案** (2008)
  - SFLASH **への攻撃法のうち**, Patarin attack **を利用せず**
  - F_4 **アルゴリズム** (Gröbner **基底を使った一般的な攻撃法**)

ℓIC(2/4)

[鍵生成]

秘密鍵: $(S,\ T)$

1. 全単射 Affine 変換 $S : {F_q}^n \to {F_q}^n$ を構成
   (n 次正則行列 S_L と n 次元ベクトル S_C を選び,
   $S(x) = S_L \cdot x + S_C$)
2. 全単射 Affine 変換 $T : {F_q}^n \to {F_q}^n$
   (行列 T_L とベクトル T_C) を構成

ℓIC(3/4)

[鍵生成]

公開鍵: P

1. $P = T \circ F \circ S$ **を構成**
   ただし, $A = (A_1, A_2, \ldots, A_\ell) \in {F_{q^{n/\ell}}}^{\ell}$ **について**,
   F **は** Cremona **変換の拡張**

$$F(A) = \begin{cases} (A_1A_2,\ A_2A_3, \ldots, A_\ell A_1) & [\ell : \text{odd}] \\ (A_1^2A_2,\ A_2A_3, \ldots, A_\ell A_1) & [\ell : \text{even}] \end{cases}$$

($ {F_{q^{n/\ell}}}^{\ell}$ **と** ${F_q}^n$ **を同一視**)

ℓIC(4/4)

[署名]

メッセージダイジェスト $V \in {F_q}^n$

1. **V に対し, 署名を $P^{-1}(V) = S^{-1}(F^{-1}(T^{-1}(V)))$ とする**

[検証]

メッセージダイジェスト $V \in {F_q}^n$, 署名 Y

1. **$P(Y)$ が, V と一致するか確認**

射影 $\Pi : {F_q}^n \to {F_q}^{n-r}$ によって, $\Pi P = \Pi \circ P$ を構成
P の代わりに ΠP を公開鍵とする

提案パラメータは以下の通り

- $q = 2^8, n = 30, \ell = 3, k = 10, r = 10$
- $q = 2^8, n = 36, \ell = 3, k = 12, r = 12$
- $q = 2^8, n = 48, \ell = 3, k = 16, r = 16$

目次

FGPS 攻撃法

- Patarin attack を用いず, Gröbner 基底アルゴリズム F_4 を適用
- 効率的な実装
  ($q = 2^8$, $n = 30$, $\ell = 3$, $k = 10$ で 0.7 秒)
- 計算量 $O(n^{4\omega})$ $(2 \leq \omega < 3)$ (実験結果からの推測)
- 秘密鍵として線形変換を仮定
- ℓ が偶数の場合を実装せず

提案攻撃法

- Patarin attack を応用
- 実用的
- 厳密に計算量を評価 (ℓ 小なら n の多項式時間)
- 秘密鍵として一般の Affine 変換とする
- ℓ が偶奇各々の場合を実装

目次

ℓIC への攻撃法

1. Affine **変換を線形変換へと変換** [GSB 01]
2. **偽署名生成式による署名の偽造** [Patarin 95]

ℓIC への攻撃アルゴリズム

入力: 公開鍵関数 P, パラメータ $q, n, \ell,$ メッセージ m
出力: V に対する正当な署名

{(線形変換への帰着)}
$\{v_j\} \leftarrow P$ の線形部
$\{\zeta_{ij}\} \leftarrow P$ の双線形部
$v$space $\leftarrow v_j$ の Kernel
$v \leftarrow v$space のうち v が満たす方程式の解ベクトル
$P_L(x) := P(x - v) - P(-v)$
{(署名の偽造)}
$\{\gamma^{(k)}, \gamma'^{(k)}\} \leftarrow$ 偽署名生成式を満たす $\{\gamma^{(k)}, \gamma'^{(k)}\}$ 空間
$V \leftarrow m$ にハッシュ関数を適用して生成した K^n の元
$y \leftarrow V - P(v)$
$x$space $\leftarrow y$ に対して, 偽署名生成式を満たす x の空間
$x \leftarrow x$space のうち, $y = P_L(x)$ を満たすベクトル
return $x - v$

線形変換への帰着

Affine 変換を, 線形変換に帰着

$$S(x) = S_L \cdot x + S_C$$

$$\Downarrow$$

$$S(x - v) := S_L \cdot x$$

以下の式から, $K \neq F_2$ である限り, v の計算が可能

$$\sum_j {v_j}^{(k)} x_j - \sum_{1 \leq i < j \leq n} {\zeta_{ij}}^{(k)} (v_i x_j + v_j x_i) = 0$$

$({v_j}^{(k)}, {\zeta_{ij}}^{(k)}$ は, 公開鍵 P から分かる F_q の元)

よって, S, T は線形変換としてよい

署名の偽造

ℓ: even の場合:

$$\begin{aligned}(B_1, \ldots, B_\ell) &= F((A_1, \ldots, A_\ell)) \\ &= (A_1{}^2 A_2,\ A_2 A_3, \ldots, A_\ell A_1)\end{aligned}$$

⇓(Linearization)

$$A_3 B_1 - A_1{}^2 B_2 = 0, \ldots, A_2 B_\ell{}^2 - A_\ell{}^2 B_1 = 0$$

よって, $y = P(x)$ について,

$$\sum_{i,\ j} \gamma_{ij} x_i y_j + \sum_i (\alpha_i x_i + \beta_i y_i) + \delta = 0$$

なる $\gamma_{ij}, \alpha_i, \beta_i, \delta$ が存在
この式から署名の偽造が可能

目次

ℓIC- への攻撃法

1. Affine **変換を線形変換へと変換** [GSB 01]
2. **差分による射影除去部分の補完** [DFSS 07]
3. **偽署名生成式による署名の偽造** [Patarin 95]

ℓIC- 攻撃アルゴリズム (1/2)

入力: 公開鍵関数 ΠP, パラメータ q, n, θ, r,
メッセージダイジェスト V
出力: V に対する正当な署名

{(線形変換への帰着)}
$\{v_j\} \leftarrow \Pi P$ の線形部
$\{\zeta_{ij}\} \leftarrow \Pi P$ の双線形部
$v$space $\leftarrow v_j$ の Kernel
$v \leftarrow v$space のうち v が満たす方程式の解ベクトル
$\Pi P_L(x) := \Pi P(x - v) - \Pi P(v)$
{(差分による射影除去部分の補完)}
$\Pi DP_L(a,\ x) := \Pi P_L(x + a) - \Pi P_L(x) - \Pi P_L(a) + \Pi P_L(0)$
Nspace $\leftarrow \Pi DP_L$ からなる方程式を満たす空間

ℓIC- 攻撃アルゴリズム (2/2)

while true do
　　{(署名の偽造)}
　$N_\xi \leftarrow N$space のうち, スカラー行列でない正則行列
　$P_f \leftarrow \Pi P_L$ に加えて, $(\Pi P_L) \circ N_\xi$ を使って,
　　full rank に戻した ${F_q}^n \rightarrow {F_q}^n$ 関数
　γspace $\leftarrow$ 偽署名生成式を満たす $\{\gamma^{(k)}, \gamma'^{(k)}\}$ 空間
　if rank(γspace) $\leq n$ then
　　$\{\gamma^{(k)}, \gamma'^{(k)}\} \leftarrow \gamma$space
　　break
　end if
end while
$y \leftarrow V - \Pi P(v)$ に適当に座標を加えて作った ${F_q}^n$ の元
$x$space $\leftarrow y$ に対して, 偽署名生成式を満たす x の空間
$x \leftarrow x$space のうち, $y = P_f(x)$ を満たすベクトル
return $x - v$

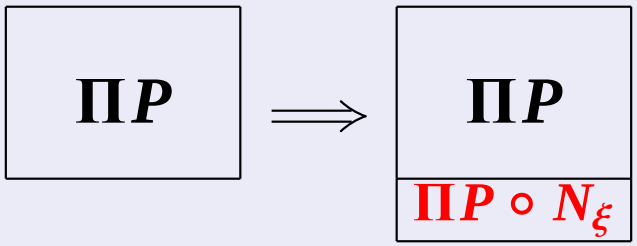
差分による射影除去部分の補完 (1/4)

$$\Pi P = \Pi T \circ F \circ S$$

に対して,

$$\Pi P \circ N_\xi = \Pi T_\xi \circ F \circ S$$

なる N_ξ を見つけて, 射影 Π の除去部分を補完



差分による射影除去部分の補完 (2/4)

N_ξ を求めるために, 以下の**差分**を使用

$$DP(A,\ B) := P(A + B) - P(A) - P(B) + P(0)$$

S, T が**線形変換**のとき,

$$DP(A,\ B) = T \circ DF(S(A),\ S(B))$$

$F(A) = (A_1{}^{q^{\lambda_1}} A_2,\ A_2{}^{q^{\lambda_2}} A_3, \ldots, A_\ell{}^{q^{\lambda_\ell}} A_1)$ について,

$$DF(A,\ B) = (A_1{}^{q^{\lambda_1}} B_2 + B_1{}^{q^{\lambda_1}} A_2, \ldots, A_\ell{}^{q^{\lambda_\ell}} B_1 + B_\ell{}^{q^{\lambda_\ell}} A_1)$$

となるから, 次の式が導ける

差分による射影除去部分の補完 (3/4)

$$BS^{(k)}_{N_\xi} = DP^{(k)}(N_\xi(A),\ B) + DP^{(k)}(A,\ N_\xi(B))$$

について,

$$BS^{(k)}_{N_\xi} \in \mathrm{Span}\{DP^{(1)},\ \ldots,\ DP^{(n)}\}$$

このままでは射影 Π で消える $DP^{(n-r+1)}, \ldots$ が含まれてしまう

差分による射影除去部分の補完 (4/4)

ℓ: even の場合:

$$BS_{N_\xi}^{(k)} \in \mathrm{Span}\{DP^{(1)}, \ldots, DP^{(n)}\}$$

を,

$$BS_{N_\xi}{}^{(k)} \in \mathrm{Span}\{DP^{(1)}, \ldots, DP^{(n-r)}\}$$

で計算

$k = 1, 2, 3$ として方程式を解くことで実際に N_ξ の導出に成功

目次

実装環境

	FGPS 実験	本実験
実装状況	ℓ:odd のみ	ℓ:even & odd
ℓIC への攻撃	F_4 アルゴリズム	Patarin's attack
CPU	2GHz Opteron	同等
ソフトウエア	Magma	Magma
秘密鍵	線形のみ	Affine

実験結果 (1/2)

evenIC に対する攻撃 ($q = 2$)

ℓ	2	2	4	6
n	120	240	240	240
k	60	120	60	40
time[s]	327.1	5630.3	5618.9	5668.3

実験結果 (2/2)

3IC-に対する攻撃 ($q = 2^8$)

n	30	36	48
k	10	12	16
r	10	12	16
time[s]	34.1	79.3	321.6

計算量 & 考察

計算量は, 偽署名生成式を生成する step **が中心**

$$\begin{cases} O(n^{3(\ell+1)/2} \lg^2 q) & [\ell : \text{odd}] \\ O(n^6 \lg^2 q) & [\ell : \text{even}] \end{cases}$$

- **3IC-で** $q = 2^8$, $n = 48$ **でも** 5 **分半で解読**
- FGPS **より遅いが, 実用的であり, 実装も容易**

まとめ

- **今回の結果**
  - ℓIC / ℓIC- **への** FGPS **とは異なる攻撃法の提案**
  - ℓ **が偶奇各々について実装実験**
  - **実用性を確認**
- **今後の課題**
  - **一般の** MQ **問題に適用される範囲の解析**
    - ★ HFE^{-}, Quartz **等**

署名の偽造 (ℓ:odd) (1/2)

$$
\begin{aligned}
(B_1, \ldots, B_\ell) &= F((A_1, \ldots, A_\ell)) \\
&= (A_1A_2,\ A_2A_3, \ldots, A_\ell A_1)
\end{aligned}
$$

$\Downarrow$(Linearization)

$$A_3B_1 - A_1B_2 = 0, \ldots, A_2B_\ell - A_\ell B_1 = 0$$

先と同様に, $y = P(x)$ について, x と y の関係式を生成
線形従属関係を含んでいるので, 最悪 $2^{n/\ell}$ 個の探索が必要

署名の偽造 (ℓ:odd) (2/2)

$$
\begin{aligned}
(B_1, \ldots, B_\ell) &= F((A_1, \ldots, A_\ell)) \\
&= (A_1A_2,\ A_2A_3, \ldots, A_\ell A_1)
\end{aligned}
$$

$$\Downarrow \text{(Linearization)}$$

$$
\begin{aligned}
B_1B_3 \ldots B_\ell &- A_1{}^2B_2B_4 \ldots B_{\ell-1} = 0 \\
&\vdots \\
B_\ell B_2 \ldots B_{\ell-1} &- A_\ell{}^2B_1B_3 \ldots B_{\ell-2} = 0
\end{aligned}
$$

先と同様に, $y = P(x)$ について, x と y の関係式を生成
この式から署名の偽造が可能

N_ξ の計算 (ℓ:odd)

$$BS^{(k)}_{N_\xi} \in \mathrm{Span}\{DP^{(1)}, \ldots, DP^{(n)}\}$$

を,

$$BS_{N_\xi}{}^{(k)} = 0$$

で計算

全ての k について方程式を解いて N_ξ を導出可能

実験結果 (oddIC)

oddIC に対する攻撃 ($q = 2^8$)

ℓ	3	3	5
n	69	138	35
k	23	46	7
time[s]	1353.1	73814.7	82309.1

実験結果 (2IC-)

(線形)2IC-に対する攻撃 ($q = 2$)

n	40	60	80
k	20	30	40
r	10	15	20
time[s]	317.3	2021.3	7725.6