Skew-Frobenius 写像を利用した超楕円曲線上の整数倍算について

IISEC 小崎 俊二, 松尾和人

2008 年 7 月 5 日

Frobenius 写像を利用した高速な超楕円曲線暗号系

曲線 $C/\mathbb{F}_p$ に対する Jacobian $\mathbb{J}_C(\mathbb{F}_{p^n})$ の Frobenius 写像 ϕ_p を利用

- ϕ_p は群演算と比較して効率的に計算可能
- $\mathbb{Z}[\phi_p] \subset \mathrm{End}(\mathbb{J}_C)$ における整数の ϕ_p 展開

→ 整数倍算における群演算量の削減

- $\mathbb{J}_C(\mathbb{F}_p) \subset \mathbb{J}_C(\mathbb{F}_{p^n})$ より、$\sharp(\mathbb{J}_C(\mathbb{F}_{p^n})/\mathbb{J}_C(\mathbb{F}_p)) \approx p^{g(n-1)}$
- $g \geq 2$, p のサイズが大きい場合

→ 拡大次数 n が小 $\Rightarrow$ $\mathbb{J}_C(\mathbb{F}_p)$ によるロス大

超楕円曲線の skew-Frobenius 写像

楕円曲線の skew-Frobenius **写像** [Iijima, Matsuo, Chao and Tsujii SCIS2002]

$C/\mathbb{F}_p : Y^2 = F(X)$ **の** $\mathbb{F}_{p^n}$ **上 2 次ツイスト**, $c \in \mathbb{F}_{p^n}$ **の平方非剰余**:

$$C_t/\mathbb{F}_{p^n} : Y^2 = F_t(X),\ F_t(X) = c^{2g+1} F(c^{-1}X)$$

Skew-Frobenius **写像**: $\tilde{\phi}_p : \mathbb{J}_{C_t} \xrightarrow[\tau]{\sim} \mathbb{J}_C \xrightarrow[\phi_p]{\sim} \mathbb{J}_C \xrightarrow[\tau^{-1}]{\sim} \mathbb{J}_{C_t}$

$$(U, V) \mapsto (\bar{U}, \bar{V})\ ;\ \mathbb{J}_{C_t} \text{の Mumford 表現}$$

$$\begin{cases} U = X^\ell + \sum_{i=0}^{\ell-1} u_i X^i \\ V = \sum_{i=0}^{k} v_i X^i \end{cases} \mapsto \begin{cases} \bar{U} = X^\ell + \sum_{i=0}^{\ell-1} c^{(1-p)(\ell-i)} u_i^p X^i \\ \bar{V} = \sum_{i=0}^{k} c^{(1-p)\left(\frac{2g+1}{2}-i\right)} v_i^p X^i \end{cases}$$

- $\tilde{\phi}_p$ **は効率的に計算可能 (高々** $2g$ **回の** p **乗算と** $\mathbb{F}_{p^n}$ **乗算)**
- $\tilde{\phi}_p$ **は** ϕ_p **と同一の特性多項式を満足**
- $n = 2^i$ **の場合に** $\sharp\mathbb{J}_{C_t}(\mathbb{F}_{p^n})$ **が素数となる** C_t **が存在**

Skew-Frobenius 展開

整数 $k \approx p^{ng}$ に対する $\tilde{\phi}_p$ 展開:

$$k\mathcal{D} = \sum_{i=0}^{n-1} k_i \tilde{\phi}_p^i(\mathcal{D}),\ \max_{0 \le i < n} \left(\lceil |k_i| \rceil\right) \approx p^g$$

$\mathcal{D} \in \mathbb{J}_{C_t}(\mathbb{F}_{p^n})$ に対して、$\tilde{\phi}_p^n(\mathcal{D}) = -\mathcal{D}$

例：$g = 3, n = 2, p = 2^7 - 1$

$$\tilde{\phi}_p^6 - 13\tilde{\phi}_p^5 - 55\tilde{\phi}_p^4 + 2003\tilde{\phi}_p^3 - 6985\tilde{\phi}_p^2 - 209677\tilde{\phi}_p + 2048383 = 0$$

$$3457660716925\mathcal{D} = 1892989\mathcal{D} - 2091980\tilde{\phi}_p(\mathcal{D})$$

Skew-Frobenius 展開を利用した整数倍算

$\mathcal{D}, \tilde{\phi}_p^1(\mathcal{D}), \ldots, \tilde{\phi}_p^{n-1}(\mathcal{D})$ を独立した n 個の元として、

$$k\mathcal{D} = k_0\mathcal{D} + k_1\tilde{\phi}_p^1(\mathcal{D}) + \cdots + k_{n-1}\tilde{\phi}_p^{n-1}(\mathcal{D})$$

→ $(k_0, k_1, \ldots, k_{n-1})$ について multi-exponentiation を適用して計算

- Interleave 法 [Möller SAC 2001]
  + Width w Non Adjacent Form (NAF$_w$) [Miyaji, Ono and Cohen ICICS 1997, Solinas CRYPTO 1997]
- Simultaneous 法 [Yen, Laih and Lenstra IEE Proc. Comput. Digit. Tech 1994, Straus Amer. Math. Montly 1964]
  + Colexicographically Minimal Integer Representation (CMR$_w$) [Heuberger and Muir J. Math. Cryptol. 2007]

$n = 2, 4$、skew-Frobenius 展開の整数倍算に対する事前計算量を削減

→ Interleave 法と simultaneous 法の群演算量を評価・比較

Interleave 法

Input: $(k_0, \ldots, k_{n-1}) \in \mathbb{Z}^n$, $\mathcal{D}_0, \ldots, \mathcal{D}_{n-1} \in \mathbb{J}_{C_t}(\mathbb{F}_{p^n})$, $w \in \mathbb{N}_{>1}$

Output: $\sum_{i=0}^{n-1} k_i \mathcal{D}_i \in \mathbb{J}_{C_t}(\mathbb{F}_{p^n})$

1: $(k_{i,j})_{0 \le j < \ell_i} \leftarrow k_i$ の NAF$_w$ 表現, $\ell \leftarrow \max_{0 \le i \le n-1} \ell_i$
2: $\{\mathcal{D}_0, 3\mathcal{D}_0, \ldots, (2^{(w-1)}-1)\mathcal{D}_0, \ldots, \mathcal{D}_{n-1}, \ldots, (2^{(w-1)}-1)\mathcal{D}_{n-1}\}$
3: $\mathcal{D}' \leftarrow \mathsf{sign}(k_{m,\ell-1})|k_{m,\ell-1}|\mathcal{D}_m$, m s.t. $k_{i,\ell-1} = 0$, $i < m$
4: **for** $i = m$ to $n-1$ **do**
5: **if** $k_{i,\ell-1} \neq 0$ **then**
6: $\mathcal{D}' \leftarrow \mathcal{D}' + \mathsf{sign}(k_{i,\ell-1})(|k_{i,\ell-1}|\mathcal{D}_i)$ /* 事前計算利用 */
7: **for** $j = \ell - 2$ down to 0 **do**
8: $\mathcal{D}' \leftarrow 2\mathcal{D}'$
9: **for** $i = 0$ to $n-1$ **do**
10: **if** $k_{i,j} \neq 0$ **then**
11: $\mathcal{D}' \leftarrow \mathcal{D}' + \mathsf{sign}(k_{i,j})(|k_{i,j}|\mathcal{D}_i)$ /* 事前計算利用 */
12: **return** $\mathcal{D}'$

例 -Interleave 法-

$$3457660716925\mathcal{D} = 1892989\mathcal{D} - 2091980\tilde{\phi}_p(\mathcal{D}),$$

$w = 4$

$$\begin{pmatrix} 1892989 \\ -2091980 \end{pmatrix} = \begin{pmatrix} (0007000070000050000003\bar{3})_{\mathsf{NAF}_4} \\ (\bar{1}000000000050001000\bar{3}00)_{\mathsf{NAF}_4} \end{pmatrix}$$

事前計算：

$$\left\{\mathcal{D}, 3\mathcal{D}, 5\mathcal{D}, 7\mathcal{D}, \tilde{\phi}_p(\mathcal{D}), 3\tilde{\phi}_p(\mathcal{D}), 5\tilde{\phi}_p(\mathcal{D}), 7\tilde{\phi}_p(\mathcal{D})\right\}$$

メイン：

$$2 \cdot 2\left(\left(\cdots\left(2 \cdot 2 \cdot 2\left(-\tilde{\phi}_p(\mathcal{D})\right) + 7\mathcal{D}\right)\cdots\right) - 3\tilde{\phi}_p(\mathcal{D})\right) - 3\mathcal{D}$$

Interleave 法の群演算量

$m\tilde{\phi}_p^i(\mathcal{D}) = \tilde{\phi}_p^i(m\mathcal{D})$ より、$m\tilde{\phi}_p^i(\mathcal{D})$ $(1 \leq i < n)$ は事前計算不要

$$\{\mathcal{D}, 3\mathcal{D}, \ldots, (2^{w-1}-1)\mathcal{D}, \ldots, \tilde{\phi}_p^{n-1}(\mathcal{D}), \ldots, (2^{w-1}-1)\tilde{\phi}_p^{n-1}(\mathcal{D})\}$$
$$\rightarrow \{\mathcal{D}, 3\mathcal{D}, \ldots, (2^{w-1}-1)\mathcal{D}\}$$

事前計算：2 倍算 1 回、加算 $2^{w-1}-2$ 回

ℓ ビット整数の NAF_w 表現に対する平均 Hamming weight は $\frac{\ell}{w+1}$

メイン：加算 $\dfrac{n\ell - 1}{w+1}$ 回、2 倍算 $\ell - 1$ 回

Simultaneous 法

Input: $(k_0, \ldots, k_{n-1}) \in \mathbb{Z}^n$, $\mathcal{D}_0, \ldots, \mathcal{D}_{n-1} \in \mathbb{J}_{C_t}(\mathbb{F}_{p^n})$, $w \in \mathbb{N}_{>1}$

Output: $\sum_{i=0}^{n-1} k_i \mathcal{D}_i \in \mathbb{J}_{C_t}(\mathbb{F}_{p^n})$

1: $((k_{i,j})_{0 \le j < \ell})_{0 \le i < n} \leftarrow (k_i)_{0 \le i < n}$ の CMR$_w$ 表現
   /* 事前計算 */
2: $\left\{ \sum_{m \le i < n} d_i \mathcal{D}_i \mid 0 \le m < n-1,\ |d_i| < 2^{w-1},\ d_m > 0 \right\}$
   /* メイン */
3: $\mathcal{D}' \leftarrow \mathsf{sign}(k_{m,\ell-1}) \sum_{m \le i < n} k_{i,\ell-1} \mathcal{D}_0$
4: **for** $j = \ell - 2$ down to 0 **do**
5: $\quad \mathcal{D}' \leftarrow 2\mathcal{D}'$
6: $\quad$ **if** $(k_{0,j}, \ldots, k_{n-1,j}) \neq (0, \ldots, 0)$ **then**
7: $\quad\quad \mathcal{D}' \leftarrow \mathcal{D}' + \mathsf{sign}(k_{m,j}) \sum_{m \le i < n} k_{i,j} \mathcal{D}_i$ /* 事前計算利用 */
8: **return** $\mathcal{D}'$

例 -Simultaneous 法-

$$3457660716925\mathcal{D} = 1892989\mathcal{D} - 2091980\tilde{\phi}_p(\mathcal{D}),$$

$$w = 3$$

$$\begin{pmatrix} 1892989 \\ -2091980 \end{pmatrix} = \begin{pmatrix} 10000\bar{3}000\bar{2}00100200\bar{0}\bar{1}01 \\ \bar{1}0000000010020010003\bar{0}0 \end{pmatrix}_{\mathsf{CMR_3}}$$

事前計算：
$$\left\{ \begin{array}{l} \mathcal{D}, 2\mathcal{D}, 3\mathcal{D}, \tilde{\phi}_p(\mathcal{D}), 2\tilde{\phi}_p(\mathcal{D}), 3\tilde{\phi}_p(\mathcal{D}), \\ \mathcal{D} \pm \tilde{\phi}_p(\mathcal{D}), \mathcal{D} \pm 2\tilde{\phi}_p(\mathcal{D}), \mathcal{D} \pm 3\tilde{\phi}_p(\mathcal{D}), \\ \ldots, 3\mathcal{D} \pm \tilde{\phi}_p(\mathcal{D}), 3\mathcal{D} \pm 2\tilde{\phi}_p(\mathcal{D}), 3\mathcal{D} \pm 3\tilde{\phi}_p(\mathcal{D}) \end{array} \right\}$$

メイン：

$$2 \cdot 2 \left(\left(\cdots \left(\mathcal{D} - \tilde{\phi}_p(\mathcal{D}) \right) \cdots \right) - \left(\mathcal{D} + 3\tilde{\phi}_p(\mathcal{D}) \right) \right) + \mathcal{D}$$

Simultaneous 法の事前計算量削減 $n = 2$

$\tilde{\phi}_p^2(\mathcal{D}) = -\mathcal{D}$ を利用

$$\begin{array}{ccc} i\mathcal{D} + j\tilde{\phi}_p(\mathcal{D}) & \overset{\tilde{\phi}_p}{\longmapsto} & -j\mathcal{D} + i\tilde{\phi}_p(\mathcal{D}), \\ -\updownarrow & & -\updownarrow \\ -i\mathcal{D} - j\tilde{\phi}_p(\mathcal{D}) & \overset{\tilde{\phi}_p}{\longmapsto} & j\mathcal{D} - i\tilde{\phi}_p(\mathcal{D}) \end{array}$$

$0 \le i, j \le 2^{w-1} - 1$ に対する $i\mathcal{D} + j\tilde{\phi}_p(\mathcal{D})$ を事前計算すれば十分

$\{\mathcal{D}, 2\mathcal{D}, \ldots, (2^{w-1} - 1)\mathcal{D}\}$: 加算 $2^{w-1} - 2$ 回

$\cup \left\{ i\mathcal{D} + \tilde{\phi}_p(j\mathcal{D}) \mid 1 \le i, j \le 2^{w-1} - 1 \right\}$: 加算 $(2^{w-1} - 1)^2$ 回

事前計算量: 加算 $(2^{w-1})^2 - 2^{w-1} - 1$ 回

メイン: CMR_w の平均 joint Hamming Weight を利用して加算回数を評価

整数倍算に要する群演算回数 $n = 2$

	事前計算		メイン	
	加算	2 倍算	加算	2 倍算
Inter.	$2^{w-2} - 1$	1	$\dfrac{2\ell - 1}{w + 1}$	$\ell - 1$
Simul.	$2^{2w-2} - 2^{w-1} - 1$	0	$\dfrac{(3 \cdot 2^w + 4)(\ell - 1)}{3w2^w + 2^w + 4w - 4}$	$\ell - 1$

Simultaneous 法の事前計算量削減 $n = 4$

$\tilde{\phi}_p^4(\mathcal{D}) = -\mathcal{D}$ を利用、

$i\mathcal{D} + j\tilde{\phi}_p(\mathcal{D}) + k\tilde{\phi}_p^2(\mathcal{D}) + l\tilde{\phi}_p^3(\mathcal{D}),\ -2^{w-1} < i, j, k, l < 2^{w-1}$

$$\pm \begin{pmatrix} i \\ j \\ k \\ l \end{pmatrix} \overset{\tilde{\phi}_p}{\longmapsto} \pm \begin{pmatrix} -l \\ i \\ j \\ k \end{pmatrix} \overset{\tilde{\phi}_p}{\longmapsto} \pm \begin{pmatrix} -k \\ -l \\ i \\ j \end{pmatrix} \overset{\tilde{\phi}_p}{\longmapsto} \pm \begin{pmatrix} -j \\ -k \\ -l \\ i \end{pmatrix}$$

事前計算: 加算 $\frac{1}{8}((2^w - 1)^4 - 1) - 1$ 回

メイン: CMR_w の平均 joint Hamming Weight を利用して加算回数を評価

整数倍算に要する群演算回数 $n = 4$

	事前計算		メイン	
	加算	倍算	加算	倍算
Inter.	$(2^{w-2} - 1)$	1	$\frac{4\ell - 1}{w + 1}$	$\ell - 1$
Simul.	$\frac{1}{8}((2^w - 1)^4 - 9)$	0	※	$\ell - 1$

cf. ※ http://www.opt.math.tu-graz.ac.at/~cheub/publications/colexi/Expectation_d_4_l_odd_u_odd.txt を利用

パラメータ設定

$g = 3$ の場合、[Nagao JJIAM 2007, Gaudry, Thomé, Thériault and Diem Math. Comp. 2007] の Double large prime attack を考慮

		g	
		2	3
k	160 ビット	$n = 2, \log_2 p = 40$ $n = 4, \log_2 p = 20$	$n = 2, \log_2 p = 30$ $n = 4, \log_2 p = 15$
	224 ビット	$n = 2, \log_2 p = 56$ $n = 4, \log_2 p = 28$	$n = 2, \log_2 p = 42$ $n = 4, \log_2 p = 21$

→ $\ell = \log_2 p^g$ として群演算量を評価

k: 160 ビット, $g = 2$ の群演算回数

		事前計算		メイン		合計
		加算	2 倍算	加算	2 倍算	
$n = 2$	Interleave	8		105.5		113.5
	$w = 5$	7	1	26.5	79	
	Simultaneous	11		104.1		115.1
	$w = 3$	11	0	25.1	79	
$n = 4$	Interleave	8		65.5		73.5
	$w = 5$	7	1	26.5	39	
	Simultaneous	9		64.1		73.1
	$w = 2$	9	0	25.1	39	

k: 160 ビットに対する整数倍算の群演算回数

		g	
		2	3
$n = 2$	Interleave $w = 5$	113.5	126.8
	Simultaneous $w = 3$	115.1	128.3
$n = 4$	Interleave $w = 5$	73.5	81.8
	Simultaneous $w = 2$	73.1	81.3

k に対して NAF$_w$ 表現を利用した場合の整数倍算の群演算回数: 193.5

k: 224 ビットに対する整数倍算の群演算回数

		g	
		2	3
$n = 2$	Interleave $w = 5$	156.2	174.8
	Simultaneous $w = 3$	157.3	175.8
$n = 4$	Interleave $w = 5$	100.2	111.8
	Simultaneous $w = 2$	99.3	110.8

k に対して NAF$_w$ 表現を利用した場合の整数倍算の群演算回数: 268.2

まとめ

- 拡大次数 $n = 2, 4$ に対する Interleave 法と Simultaneous 法それぞれの事前計算量を skew-Frobenius 写像の性質を利用して削減
- Interleave 法と Simultaneous 法それぞれについて最適なウィンドウ幅 w に対する整数倍算の群演算量を評価
- k: 160 ビット,224 ビットに対して、Interleave 法と Simultaneous 法は同程度の群演算量