SCIS 2017 2017 Symposium on
Cryptography and Information Security
Naha, Japan, Jan. 24 - 27, 2017
The Institute of Electronics,
Information and Communication Engineers

同種写像を用いた置換有理関数の生成手法
Constructing Permutation Rational Functions From Isogenies

ビソン・ガエタン * ティブシ・メディ †
Gaetan Bisson Mehdi Tibouchi

あらまし 置換有理関数とは基礎体から自信への全単射となる有限体上の有理関数である。RSA 多項式 $x \mapsto x^e$ やチェビシェフ多項式はその例であるが、非自明な置換有理関数を生成するのは容易ではない。本発表では、楕円曲線の同種写像を用いて暗号額的なサイズの有限体上でも効率よく生成する手法を紹介する。暗号への潜在用途も考察する。

キーワード 置換有理関数，同種写像，数論，公開鍵暗号

1 はじめに

有限体 $\mathbb{F}_q$ 上の（滑らかで射影的な）代数曲線の写像 $X \to Y$ は，$t = 1$ を含む無限個の t に対して $\mathbb{F}_{q^t}$ 上の点に誘導する写像 $X(\mathbb{F}_{q^t}) \to Y(\mathbb{F}_{q^t})$ が全単射となる場合は「特別被覆」（exceptional cover）という．特別被覆の構成は数論幾何学に於いて重要な課題であり [7]，暗号への応用もある．

応用の一つとしてはとくに代数曲線とそのヤコビ多様体へのハッシュ関数の構成が挙げられる．その問題について多くの論文が発表されているものの，これまで提案されてきた構成方法は系統性に欠如しており [13]，種数 2 以上の曲線に関しては部分的な結果しか得られていない [10, 4, 3]．一方，特別被覆を基にしてハッシュ関数構成へのよりプログラム的なアプローチが提言された [14]．$\mathbb{F}_q$ 上の射影直線の特別被覆 $X \to \mathbb{P}^1$ が与えられれば，非定値写像 $h\colon X \to Y$ を持つ任意の曲線 Y を対象に，全単射写像 $\mathbb{P}^1(\mathbb{F}_q) \to X(\mathbb{F}_q)$ を h と合成することにより $\mathbb{F}_q$ の元を Y の点として符号化するアルゴリズムが得られる訳である．結果として，ハッシュ関数の構成は射影直線の特別被覆の明白な構成に還元できる．

もっともシンプルな射影直線の特別被覆は種数 0 の被覆，つまり無限個の t に対して $\mathbb{P}^1(\mathbb{F}_{q^t})$ の置換を誘導する有理関数 $f \in \mathbb{F}_q(x)$ のことである．非定値写像 $\mathbb{P}^1 \to Y$ が存在するような曲線 Y は必ず有理的なのでそれらの被覆はハッシュ関数には応用できないけれども，比較的によく理解されているため [6, 8]，一般的なケースの解明への注目に値する第一歩だと考えられる．さらに Fried によると [6, 8]，それらの被覆は公開鍵暗号に於いて中心的な位置を占めている．

なぜなら，射影直線の特別被覆は RSA 多項式 $x \mapsto x^e$（但し，e が $q-1$ と互いに素）の一般化として捉えられる．実際のところ，それらの被覆はいわゆる「置換有理関数」，つまり $\mathbb{F}_q$ から自信への全単射写像を誘導する $\mathbb{F}_q$ 上の有理関数とは本質的に変わらない．確かに特別被覆 $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ が $f(\infty) = \infty$ という条件を満たせば（一次分数変換との合成を除いて必ず当てはまる），定義により置換有理関数となる．逆に，置換有理数 f の次数が q に比べて十分に小さければ，射影直線の特別被覆であると証明できる [9, 15]．

本論文の貢献. Fried による特別被覆 $\mathbb{P}^1 \to \mathbb{P}^1$ の大きな類「対合特別被覆」のモジュライ解釈 [6, Cor. 3.5] に基づいて，暗号学的サイズの有限体上では任意の固定素数次数 $\ell \geq 5$ の置換有理関数を生成する効率的アルゴリズムを考案する．なお，[7] で指摘されていた RSA との類似性を進展させて，そのアルゴリズムを用いた新たな落とし戸付き一方向性置換について考察する．

2 同種写像から置換有理数へ

票数 $2, 3$ 以外の有限体 $\mathbb{F}_q$ 上の楕円曲線 $E\colon y^2 = x^3 + ax + b$，$E'\colon y^2 = x^3 + a'x + b'$ と $\mathbb{F}_q$ 上で定義された同種写像 $\varphi\colon E \to E'$ を考えよう．同種写像 φ は -1 倍算の自己準同型写像と可換であるため，$\varphi(x, y)$ の x 座標

* フランス領ポリネシア大学大学院数理科学研究科フランス領ポリネシア BP 6570 — 98702 Faaa. Department of Mathematics, University of French Polynesia, BP 6570, 98702 Faaa, French Polynesia. bisson@gaati.org
† NTT セキュアプラットフォーム研究所〒 180–8585 東京都武蔵野市緑町 3–9–11. NTT Secure Platform Laboratories, 3–9–11 Midori-cho, Musashino-shi, Tokyo 180–8585. tibouchi.mehdi@lab.ntt.co.jp

は y の偶関数で，同様に $\varphi(x,y)$ の y 座標は y の奇関数である．そして $y^2 = x^3 + ax + b$ であるので，φ は次式の形を持つような一意の有理関数 $u_\varphi, v_\varphi \in \mathbb{F}_q(x)$ が存在する．

$$\varphi(x,y) = \big(u_\varphi(x), y \cdot v_\varphi(x)\big).$$

ある条件下で u_φ が置換有理関数である．それが本論文の基礎となる．正確には，次の定理を証明することができる．

定理 1. 上記のように，$\varphi\colon E \to E'$ が $\mathbb{F}_q$ 上で定義された素数次数 ℓ の同種写像とすると，次の各命題が同値である．

(*i*) u_φ には $\mathbb{F}_q$ 上の極がない；

(*ii*) φ の核 K は $K(\mathbb{F}_{q^2}) = \{0\}$ を満たす；

(*iii*) u_φ が置換有理関数である．

証明. *(i)* $\Rightarrow$ *(ii)*. $P = (x,y)$ が単位元以外の $K(\mathbb{F}_{q^2})$ の元としよう．P が φ の核に属するので x は u_φ の極である．さらに，x が $\mathbb{F}_q$ に属することを証明しよう．K は素数位数 ℓ の群であるため，P はその生成元である．それ故に，φ が E のフロベニウス自己準同型 F と可換であるので，F を $\mathbb{F}_\ell$-ベクトル空間 $E[\ell](\overline{\mathbb{F}_q})$ の自己準同型として見なせば P がとある固有値 λ に対する F の固有ベクトルとなる．つまり，$F(P) = [\lambda]P$．さらに，P は $E(\mathbb{F}_{q^2})$ の点なので，$F^2(P) = P$ が成り立ち，よって $\lambda = \pm 1$．結果として，$F(P) = (x, \pm y)$ である．とりわけ $x^q = x$，すなわち x が $\mathbb{F}_q$ の元であると判る．

(ii) $\Rightarrow$ *(iii)*. 有理関数 u_φ が置換有理関数となるのは，$\mathbb{F}_q$ 上の関数として単射で $\mathbb{F}_q$ での極がない時でありかつその時に限る．$K(\mathbb{F}_{q^2}) = \{0\}$ ならば，u_φ には $\mathbb{F}_q$ での極がないのは明らかだ（そのような極 x が存在すれば，E 上でのその x 座標の点 $P = (x,y)$ が $\mathbb{F}_{q^2}$ で定義されていて $\varphi(P) = 0$ が成り立つので P が単位元以外の $K(\mathbb{F}_{q^2})$ の元となる）．また，$u_\varphi(x) = u_\varphi(x')$ が成り立つような $x, x' \in \mathbb{F}_q$ が存在するとしよう．それらの x 座標の点 $P, P' \in E(\mathbb{F}_{q^2})$ を求めることができる．$u_\varphi(x) = u_\varphi(x')$ から $\varphi(P) = \pm\varphi(P')$ と推定できる．すなわち $P \mp P' \in K(\mathbb{F}_{q^2}) = \{0\}$．結果として，$P = \pm P'$，よって $x = x'$ であると判る．つまり u_φ は単射である．

(iii) $\Rightarrow$ *(i)* は自明． □

その定理を用いて，暗号学的なサイズの有限体上でも任意素数次数 $\ell \geq 5$ の置換有理関数を生成できる．そうするためには，適切な核のある同種写像を計算するのは十分である．具体的な方法を次節で説明する．

3 同種写像核の計算

Given an elliptic curve E defined over a finite field $\mathbb{F}_q$ and a prime ℓ, we now set to enumerate all subgroups K of E of order ℓ which satisfy the conditions of Theorem 1. In other words, we are looking for subgroups K defined over $\mathbb{F}_q$ that have no nontrivial point defined over $\mathbb{F}_{q^2}$.

Any such subgroup K is stable under the involution of multiplication by -1 and is thus completely determined by the set H of x-coordinates of its nontrivial points, and therefore also by its kernel polynomial $p_K(x) = \prod_{\alpha \in H}(x - \alpha)$ which is of degree $\frac{\ell-1}{2}$. Now, as ℓ is prime, all nontrivial points of K generate all others. Therefore we have a factorization

$$p_K(x) = f_1(x) f_2(x) \cdots f_{\frac{\ell-1}{2d}}(x)$$

into irreducible factors $f_i(x) \in \mathbb{F}_q[x]$ of degree $d = \deg\left(\mathbb{F}_q(x_P)/\mathbb{F}_q\right)$ where P may be any nontrivial point of K.

Recall that multiplication-by-k is an algebraic map on E:

$$P = (x,y) \longmapsto [k]P = \left(\frac{\phi_k(x)}{\psi_k(x)^2}, \frac{\omega_k(x,y)}{\psi_k(x)^3}\right)$$

where the polynomials ϕ_k, ψ_k, and ω_k are efficiently computable. It follows that $p_K(x)$ divides the so-called ℓ-division polynomial $\psi_\ell(x)$. Factoring $\psi_\ell(x)$ over $\mathbb{F}_q[x]$ is a classic computational task and it remains to identify which of its irreducible factors give polynomials $p_K(x)$ corresponding to suitable subgroups K.

補題 2. *Let $f(x)$ be a degree-d irreducible factor of $\psi_\ell(x)$, and let τ be an integer of order exactly d in $\mathbb{F}_\ell^\times/\{\pm 1\}$. There exists a subgroup K satisfying the conditions of Theorem 1 such that $f(x)$ divides $p_K(x)$ if and only if*

$$f\left(\frac{\phi_\tau(x)}{\psi_\tau(x)^2}\right) = 0 \bmod f(x).$$

In that case, the other irreducible factors of $p_K(x)$ can be obtained as $\gcd\left(\psi_\ell(x), g_\omega(x)\right)$ where

$$g_\omega(x) = \operatorname{res}_y\left(f(y), \phi_\omega(x) - \psi_\omega(x)^2 y\right)$$

for integers ω representative of classes of $\mathbb{F}_\ell^\times/\{\pm 1\}/\mu_d$.

証明. As above, let K be a subgroup satisfying the conditions of Theorem 1, and denote by ℓ its order and by d the degree of the field extension where its points are defined. The set H of x-coordinates of its nontrivial points forms a principal homogeneous space for

$\mathbb{F}_\ell^\times/\{\pm 1\}$ where $\lambda \in \mathbb{F}_\ell^\times$ acts by $x_P \mapsto x_{[\lambda]P}$. The Frobenius automorphism π of $\mathbb{F}_{q^d}/\mathbb{F}_q$ stabilizes K and thus acts as an element λ_π which satisfies $\lambda_\pi^d = 1$. Besides, since π leaves each irreducible factor $f_i(x)$ of $p_K(x)$ invariant, we find that λ_π must be a primitive d^{th} root of unity. Therefore, the group $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ embeds in $\mathbb{F}_\ell^\times/\{\pm 1\}$ as μ_d and its action partitions H into $\frac{\ell-1}{2d}$ orbits of length d, each consisting of the roots of an irreducible factor f_i. In particular, if x_P is a root of f_i, so is $x_{[\tau]P}$ for any $\tau \in \mathbb{F}_\ell^\times$ such that $\tau^d = 1$. Writing the multiplication-by-τ map with rational fractions, we obtain that roots of $f_i(x)$ are also roots of $f_i\left(\frac{\phi_\tau(x)}{\psi_\tau(x)^2}\right)$, which proves the "only if" part.

Other irreducible factors of $p_K(x)$ then correspond to other orbits of H; they are obtained through the map $x_P \mapsto x_{[\omega]P}$ for ω in $\mathbb{F}_\ell^\times/\{\pm 1\}/\mu_d$. To compute this efficiently, note that $g_\omega = f \circ (x_Q \to x_{[\omega]Q}$; for each $P \in K$ there are ω points Q such that $[\omega]Q = P$ only one of which lies in K. The others have order $\ell\omega$ and are eliminated by taking the gcd with $\psi_\ell(x)$.

Conversely, let $f(x)$ be a degree-d irreducible factor of $\psi_\ell(x)$ of which the roots are stable under the map $x_P \mapsto x_{[\tau]P}$. The polynomial

$$p(x) = \prod_{\omega \in \mathbb{F}_\ell^\times/\{\pm 1\}/\mu_d} \gcd(\psi_\ell(x), g_\omega(x))$$

vanishes at the x-coordinates of all multiples of P. It is stable under π so K is rational. □

Putting the above together we obtain Algorithm 1.

定理 3. *Heuristically, Algorithm 1 runs in $\widetilde{O}(\ell^3 \log(q)^2)$ time.*

証明. Step 1 computes the division polynomial $\psi_\ell(x) \in \mathbb{F}_q[x]$ which is of degree $\frac{\ell^2-1}{2}$. Using the formulas of [16, page 200] and an asymptotically fast method for polynomial multiplication, this takes quasi linear time in the output: $O(\ell^2 \log(q))$.

In order to find the irreducible factors of degree $d < \frac{\ell-1}{2}$ of $\psi_\ell(x)$ we use ideas from the Cantor–Zassenhaus algorithm: first we evaluate

$$r(x) = \frac{\gcd\left(\psi_\ell(x), x^{q^d} - x\right)}{\gcd\left(\psi_\ell(x), x^q - x\right)}$$

which is the product of all such factors; then we isolate those factors by iteratively splitting $r(x)$ as

$$r(x) = g(x) \cdot \frac{r(x)}{g(x)} \quad \text{where} \quad g(x) = \gcd\left(r(x), h(x)^{\frac{q^d-1}{2}}\right)$$

Algorithm 1 Compute kernel polynomials satisfying Theorem 1.

Input: an elliptic curve $E/\mathbb{F}_q$ with $q = p^\alpha$, $p \neq 2, 3$, and a prime $\ell \notin \{2, 3, p\}$.

Output: the list $\mathscr{L}$ of all kernel polynomials of ℓ-isogenies satisfying the conditions of Theorem 1.

1: compute the ℓ-division polynomial $\psi_\ell(x)$ of $E/\mathbb{F}_q$.
2: let ω denote a generator of $\mathbb{F}_\ell^\times$.
3: initialize $\mathscr{L}$ to the empty list.
4: **for** each positive divisor d of $\frac{\ell-1}{2}$ other than 1 **do**
5: compute the set $\mathscr{F}$ of degree-d irreducible factors of $\psi_\ell(x)$.
6: let τ be the smallest positive integer such that $\tau \equiv \pm\omega^{\frac{\ell-1}{2d}} \bmod \ell$.
7: **while** $\mathscr{F}$ is not empty **do**
8: remove the first element from $\mathscr{F}$ and call it f.
9: **if** $f\left(\frac{\phi_\tau(x)}{\psi_\tau(x)^2}\right) \neq 0 \bmod f(x)$ **then**
10: **continue** to the next iteration.
11: **end if**
12: let $k \leftarrow f$.
13: **for** $m = 1$ to $\frac{\ell-1}{2d} - 1$ **do**
14: let ξ be the smallest positive integer such that $\xi \equiv \pm\omega^m \bmod \ell$.
15: let $g(x) \leftarrow \mathrm{res}_y\left(f(y), \phi_\xi(x) - \psi_\xi(x)^2 y\right)$.
16: let $g(x) \leftarrow \mathrm{monic}\left(\gcd(\psi_\ell(x), g(x))\right)$.
17: let $k \leftarrow g \cdot k$.
18: remove $g(x)$ from $\mathscr{F}$.
19: **end for**
20: add $k(x)$ to the list $\mathscr{L}$.
21: **end while**
22: **end for**
23: **return** $\mathscr{L}$.

with $h(x)$ drawn uniformly at random from $\mathbb{F}_q[x]/(r(x))$. Evaluating such expressions boils down to computing $O(q^\ell)$-powers in $\mathbb{F}_q[x]/(r(x))$ which, since $r(x)$ has degree $O(\ell^2)$, gives an asymptotic complexity of $\widetilde{O}(\ell^3 \log(q)^2)$ for Step 4. □

4 置換有理数の計算

We now turn to our main algorithm. First recall that isomorphism classes of elliptic curves can be uniquely identified by their j-invariant. Under this map, pairs of ℓ-isogenous elliptic curves (E, E') are completely characterized by the equality $\Phi_\ell(j(E), j(E')) = 0$ where $\Phi_\ell(X, Y)$ denotes the ℓ-modular polynomial. Thus, to

Algorithm 2 Compute permutation rational functions.

Input: a prime power $q = p^\alpha$ with $p \neq 2, 3$ and a prime $\ell \notin \{2, 3, p\}$.

Output: permutation rational functions of degree ℓ over $\mathbb{F}_q$.

1: compute the reduction to $\mathbb{F}_q[X]$ of the ℓ-modular polynomial $\Phi_\ell(X, Y)$.
2: **loop**
3: **repeat**
4: draw an element $j \in \mathbb{F}_q$ uniformly at random.
5: **until** the polynomial $\Phi_\ell(X, j)$ has at least one root.
6: let $E/\mathbb{F}_q$ denote an elliptic curve with j-invariant j.
7: **for** each polynomial $f(x)$ output by Algorithm 1 **do**
8: compute the isogeny φ with kernel polynomial $f(x)$ using Kohel's formula.
9: **return** its x-coordinate map u_φ.
10: **end for**
11: **end loop**

select a rational ℓ-isogeny $E \to E'$, we simply draw $j(E)$ uniformly at random from $\mathbb{F}_q$ until $\Phi_\ell(X, j(E))$ has a root.

For all suitable kernel polynomials $f(x)$ found by Algorithm 1, we output the corresponding isogeny map derived using Kohel's formula [11, Section 2.4]. This gives Algorithm 2.

定理 4. *Heuristically, Algorithm 2 runs in* $\widetilde{O}(\ell^3 \log(q)^2)$ *time.*

証明. Step 1 uses the method of [2] to compute the modular polynomial in $\widetilde{O}(\ell^3 \log(q))$ operations. For Step 7 we refer to Algorithm 1. Finally, the complexity of Step 8 is quasi linear in its input.

To conclude the proof, we only need to show that the average number of loop iterations is bounded. First consider the innermost loop. The probability that a random j-invariant satisfies the condition in Step 5 is exactly that of the corresponding elliptic curve E having a rational degree-ℓ isogeny. Assuming the curve is ordinary, which only disregards finitely many j-invariants, the so-called volcano structure [11, 5] implies that, if the discriminant $\Delta(E)$ is a nonzero square modulo ℓ, then E has ℓ-maximal endomorphism ring and is connected to other such curves by a cycle of ℓ-isogenies. Therefore the probability that we so obtain a rational isogeny is $\frac{\ell-1}{2\ell}$ under the heuristic assumption that $\Delta(E)$ behaves modulo ℓ as a random integer.

The outermost loop is executed as many times as we require rational isogenies before the kernel of one admits no nontrivial rational point. Recall that the modular curves $X_0(\ell)$ and $X_1(\ell)$ essentially parametrize pairs (E, K) where K is an order-ℓ subgroup of the elliptic curve E, and pairs (E, P) where P is an order-ℓ point of E, respectively. Since $X_1(\ell) \to X_0(\ell)$ is a cyclic Galois cover of degree $\frac{\ell-1}{2}$, Chebotarev's density theorem shows that the image of $X_1(\ell)(\mathbb{F}_q) \to X_0(\ell)(\mathbb{F}_q)$ has density $\frac{2}{\ell-1} + O(q^{-1/2})$. Thus, if (E, K) is uniformly distributed, the probability that all points of K lie in $\mathbb{F}_q$ converges to $\frac{2}{\ell-1}$. In particular, if E admits a rational subgroup K of order ℓ, the probability that one such subgroup does not have nontrivial $\mathbb{F}_q$-points is asymptotically $1 - \frac{2}{\ell-1}$.

We conclude that the overall success probability of an iteration is at least $\frac{\ell-1}{2\ell}\left(1 - \frac{2}{\ell-1}\right) = \frac{\ell-3}{2\ell}$ up to the $O(q^{-1/2})$ error term, hence the expected number of iterations is less than about $\frac{2\ell}{\ell-3} \leq 5$. □

To illustrate our algorithm, take $q = 257$ and $\ell = 5$. For $j = 7$, we find that $\Phi_\ell(X, j)$ has two roots in $\mathbb{F}_q$. Thus, any elliptic curve E with $j(E) = 7$ is the domain of two rational degree-ℓ isogenies; we take $E : y^2 = x^3 + 161x + 109$, with ℓ-division polynomial

$$\begin{aligned}\psi_\ell(x) = (x + 58) \cdot (x + 106) \cdot (x^2 + 153x + 175) \cdot \\ (x^4 + 73x^3 + 117x^2 + 9x + 213) \cdot \\ (x^4 + 124x^3 + 170x^2 + 160x + 20).\end{aligned}$$

Its third irreducible factor has degree $\frac{\ell-1}{2}$ and is thus the kernel polynomial of a degree-ℓ isogeny with no rational kernel point. The x-coordinate map of that isogeny is

$$x \longmapsto \frac{x^5 + 306x^4 + 76x^3 + 192x^2 + 223x + 172}{x^4 + 49x^3 + 115x^2 + 94x + 42}$$

and one can easily verify that this rational fraction does indeed map $\mathbb{F}_q$ bijectively to itself.

Table 1 reports on running times for a simple PARI/GP [12] implementation of Algorithm 2 on a single core of an Intel Core i7–4770 CPU clocked at 3.40GHz.

5 落とし戸付き置換の類

Using the algorithm of the previous section, one can obtain a permutation rational function analogue of the

表 1: Running time in seconds for Algorithm 2.

$q =$	$2^{127}-1$	$2^{255}-19$	$2^{511}-187$	$2^{1023}-361$
$\ell = 13$	0.12	0.24	0.74	2.69
$\ell = 23$	0.76	1.21	3.29	11.88
$\ell = 37$	3.50	6.86	19.52	50.71
$\ell = 59$	22.46	35.42	107.75	292.65

RSA trapdoor permutation. Indeed, consider an RSA modulus $N = p \cdot q$. With the knowledge of the factorization of N, one can efficiently generate permutation rational functions $u = a/b \in \mathbb{F}_p(x)$ and $v = c/d \in \mathbb{F}_q(x)$ of the same prime degree ℓ, and use the Chinese Remainder Theorem to deduce polynomials $r, s \in \mathbb{Z}[x]$ of degree at most ℓ with coefficients in $(-N/2, N/2)$ such that $u = r/s \bmod p$ and $v = r/s \bmod q$.

The function $x \mapsto r(x)/s(x) \bmod N$ is then a permutation of $\mathbb{Z}/N\mathbb{Z}$ which is easy to invert with the knowledge of the factorization of N (simply reduce modulo p and q and use an algorithm like Berlekamp or Cantor–Zassenhaus to invert u and v). However, it seems hard to invert it otherwise.

This construction is somewhat less efficient in terms of public key size and evaluation efficiency than the RSA trapdoor permutation, but it seems to resist certain types of attacks better: for example, there are no obvious malleability properties, which should thwart most types of blinding attacks or related message attacks [1].

On the other hand, the security analysis is not entirely straightforward. Publishing r and s could reveal some information on the factorization of N, since its factors belong to the (presumably sparse!) set of primes p_0 such that $\lambda r + \mu s$ has exactly one root modulo p_0 for all integers λ, μ, λ coprime to N. For example, if many values of (λ, μ) provided congruence conditions on p_0, one might be able to recover p and q using the Chinese Remainder Theorem. In practice, however, the polynomial $\lambda r + \mu s \in \mathbb{Z}[x]$ will typically have Galois group S_ℓ, and so one presumably cannot hope to obtain a really effective description of the set of primes at which it has a root.

6 まとめ

We have seen that generating permutation rational functions, or exceptional covers of genus zero of the projective line, could be done quite practically using elliptic curve isogenies, even over finite fields of cryptographic size. The covers we obtain with our algorithms are (up to conjugation by linear fractional transformations) exactly the exceptional involution covers defined by Fried in [6, §3.2]. Since the classification of genus-zero exceptional covers of the projective line has been given by Guralnick et al. [8], one could ask how to effectively generate permutation rational functions from the remaining families.

Perhaps more importantly, one important open question related to this work is the construction of higher-genus exceptional covers of the projective line. At least for covers with dihedral monodromy, Fried mentions an interpretation in terms of moduli spaces of higher-genus hyperelliptic curves which may lead to a similar algorithm using isogenies of higher-dimensional abelian varieties.

Finally, an intriguing, if somewhat theoretical, question is the proper security analysis of the trapdoor permutation described in §5.

参考文献

[1] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.

[2] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012.

[3] Jean-Marc Couveignes and Reynald Lercier. The geometry of some parameterizations and encodings. *Advances in mathematics of communications*, 8(4):437–458, 2014.

[4] Pierre-Alain Fouque and Mehdi Tibouchi. Deterministic encoding and hashing to odd hyperelliptic curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277. Springer, 2010.

[5] Mireille Fouquet and Fran cois Morain. Isogeny volcanoes and the SEA algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory Symposium — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 47–62. Springer, 2002.

[6] Michael D. Fried. Global construction of general exceptional covers. In G. L. Mullen and P. J.

Shiue, editors, *Finite Fields: Theory, Applications, and Algorithms*, number 168 in Contemporary Mathematics, pages 69–100. American Mathematical Socity, 1994.

[7] Michael D. Fried. The place of exceptional covers among all diophantine relations. *Finite Fields and Their Applications*, 11:367–433, 2005.

[8] Robert M. Guralnick, Peter Müller, and Jan Saxl. *The Rational Function Analogue of a Question of Schur and Exceptionality of Permutation Representations*, volume 773 of *Memoirs of the AMS*. AMS, 2003.

[9] Robert M. Guralnick, Thomas J. Tucker, and Michael E. Zieve. Exceptional covers and bijections on rational points. *Int. Math. Res. Not.*, 2007. Article ID 004, 19 pages.

[10] Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 2010.

[11] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[12] The PARI Group. *PARI/GP*, 2016. http://pari.math.u-bordeaux.fr/.

[13] Mehdi Tibouchi. *Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA*. PhD thesis, Univ. Paris 7 and Univ. Luxembourg, 2011. Introduction in French, main matter in English.

[14] Mehdi Tibouchi. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. In Lejla Batina et al., editors, *ECC 2013*, 2013.

[15] Mehdi Tibouchi. Impossibility of surjective Icart-like encodings. In Sherman S. M. Chow, Joseph K. Liu, Lucas Chi Kwong Hui, and Siu-Ming Yiu, editors, *ProvSec 2014*, volume 8782 of *Lecture Notes in Computer Science*, pages 29–39. Springer, 2014.

[16] Heinrich Weber. *Elliptische Funktionen und Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Friedrich Vieweg und Sohn, 1891.