Constructing Permutation Rational Functions From Isogenies

Gaetan Bisson[1] and Mehdi Tibouchi[2]

[1] University of French Polynesia
[2] NTT Secure Platform Laboratories

Abstract. A *permutation rational function* $f \in \mathbb{F}_q(x)$ is a rational function that induces a bijection on $\mathbb{F}_q$, that is, for all $y \in \mathbb{F}_q$ there exists exactly one $x \in \mathbb{F}_q$ such that $f(x) = y$. Permutation rational functions are intimately related to exceptional rational functions, and, more generally, exceptional covers of the projective line, of which they form the first important example.

In this paper, we show how to efficiently generate many permutation rational functions over large finite fields using isogenies of elliptic curves, and discuss some cryptographic applications. Our algorithm is based on Fried's modular interpretation of certain dihedral exceptional covers of the projective line [7].

1 Introduction

A map $X \to Y$ of (smooth, projective) algebraic curves over a finite field $\mathbb{F}_q$ is called an *exceptional cover* when the induced map on $\mathbb{F}_{q^t}$-points $X(\mathbb{F}_{q^t}) \to Y(\mathbb{F}_{q^t})$ is a bijection for infinitely many values of t (necessarily including $t = 1$). The construction of exceptional covers is an important problem in arithmetic algebraic geometry [8], which also has applications to cryptography.

One can, in particular, mention the construction of hash functions with values in algebraic curves and their Jacobians: while there already is abundant literature on the subject, the construction techniques proposed so far have been somewhat ad hoc and unsystematic [15], and only partial results have been obtained for curves of genus ≥ 2 [11,5,4]. A more programmatic approach has been suggested in [16] based on the observation that, given an exceptional cover $X \to \mathbb{P}^1$ of the projective line over $\mathbb{F}_q$, one can obtain encodings of elements of $\mathbb{F}_q$ to all curves Y with a nonconstant map $h : X \to Y$ simply by composing the bijection $\mathbb{P}^1(\mathbb{F}_q) \to X(\mathbb{F}_q)$ with h. The construction of hash functions is thus reduced to obtaining explicit exceptional covers of the projective line.

The simplest such exceptional covers are those of genus zero, namely, rational functions $f \in \mathbb{F}_q(x)$ inducing a permutation of $\mathbb{P}^1(\mathbb{F}_{q^t})$ for infinitely many t. They are not directly applicable to hashing (since any curve Y with a nonconstant map $\mathbb{P}^1 \to Y$ is rational), but they are comparably well understood [7,9] and an interesting first step towards the general case. Fried [8, §4] also suggested that these exceptional covers should play an important role in public-key cryptography.

Indeed, exceptional covers are essentially the same objects as *permutation rational functions*, i.e. rational functions over $\mathbb{F}_q$ inducing a bijection of $\mathbb{F}_q$ to itself: clearly, an exceptional cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ satisfying $f(\infty) = \infty$ (which can always be satisfied up to a linear fractional transformation) is a permutation rational function, and one can show that if the degree of f is small compared to q, the converse also holds [10,17]. In particular, we can see these rational functions as generalizations of the RSA polynomials x^e with e coprime to $q - 1$.

Our contributions. Based on Fried's modular interpretation of a large class of exceptional covers $\mathbb{P}^1 \to \mathbb{P}^1$ called exceptional involution covers [7, Cor. 3.5], we describe an algorithm to generate permutation rational functions of any constant prime degree $\ell \geq 5$ (which are, in fact, exceptional covers) over large finite fields and show that it is efficient and practical. We also expand upon the RSA analogy alluded to in [8] and discuss how our algorithm might indeed be used to obtain new factoring-related trapdoor permutations that behave better than the RSA trapdoor permutation against certain classes of attacks.

2 Permutation rational functions from isogenies

Consider two elliptic curves $E\colon y^2 = x^3 + ax + b$ and $E'\colon y^2 = x^3 + a'x + b'$ over a finite field $\mathbb{F}_q$ of characteristic $\neq 2, 3$ and an isogeny $\varphi\colon E \to E'$ defined over $\mathbb{F}_q$. Since φ commutes to the involution of multiplication by -1, the x-coordinate (resp. y-coordinate) of $\varphi(x, y)$ is an even (resp. odd) function of y. And since $y^2 = x^3 + ax + b$, this means that there exist unique rational functions $u_\varphi, v_\varphi \in \mathbb{F}_q(x)$ such that φ has the form

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

This paper is based on the following observation.

Theorem 1. *Let $\varphi\colon E \to E'$ as above be an isogeny defined over $\mathbb{F}_q$ of prime degree ℓ. The following conditions are equivalent:*

(*i*) *u_φ has no $\mathbb{F}_q$-rational pole;*
(*ii*) *the kernel K of φ satisfies $K(\mathbb{F}_{q^2}) = \{0\}$;*
(*iii*) *u_φ is a permutation rational function.*

Proof. (i) $\Rightarrow$ (ii). Let $P = (x, y)$ be a nonidentity element of $K(\mathbb{F}_{q^2})$. We know that x is a pole of u_φ (as $P \in K$) and will now show that $x \in \mathbb{F}_q$. First note that P is a generator of K since that group has prime order ℓ. As a result, in view of the fact that φ commutes with the Frobenius, P must be an eigenvector of the Frobenius F of E for some eigenvalue λ (when we view F as a linear endomorphism of the $\mathbb{F}_\ell$-vector space $E[\ell](\overline{\mathbb{F}_q})$). Moreover, since P is in $E(\mathbb{F}_{q^2})$, we have $F^2(P) = P$, hence, $\lambda = \pm 1$. Therefore, $F(P) = (x, \pm y)$ and, in particular, $x^q = x$, that is, $x \in \mathbb{F}_q$. Thus, x is an $\mathbb{F}_q$-rational pole of u_φ.

(ii) $\Rightarrow$ (iii). The rational fraction u_φ is a permutation rational function if and only if it has no rational pole and is injective. Assuming $K(\mathbb{F}_{q^2}) = \{0\}$, u_φ cannot have a rational pole: indeed, if x were such a pole, a point P on E with that x-coordinate would be defined over $\mathbb{F}_{q^2}$ and satisfy $\varphi(P) = 0$. Suppose now that there exist $x, x' \in \mathbb{F}_q$ such that $u_\varphi(x) = u_\varphi(x')$. Take two points $P, P' \in E(\mathbb{F}_{q^2})$ having these values as their respective x-coordinates. Since $u_\varphi(x) = u_\varphi(x')$, we have $\varphi(P) = \pm\varphi(P')$, and so $P \mp P' \in K(\mathbb{F}_{q^2}) = \{0\}$. This implies that $P = \pm P'$ and thus $x = x'$. Therefore u_φ is injective.

(iii) $\Rightarrow$ (i) is clear. □

We note that the conditions in the above theorem can only be satisfied for $\ell \geq 5$. Indeed, since the kernel of φ consists of ℓ points including the point at infinity, the denominator of u_φ is of degree $\ell - 1$. In particular, for $\ell = 2$, it is linear and thus does have a rational root.

Moreover, for ℓ odd, the nonzero kernel points come in pairs $\{\pm P\}$ of distinct points with the same x-coordinate, so the denominator of u_φ is actually the square of a polynomial of degree $(\ell-1)/2$. This again implies that u_φ has a rational pole for $\ell = 3$. On the other hand, we will be able to construct examples of the situation in the theorem for any $\ell \geq 5$.

Note also that under the conditions of the theorem, u_φ is in fact an exceptional cover $\mathbb{P}^1 \to \mathbb{P}^1$. This follows from the fact that $K(\mathbb{F}_{q^{2t}})$ remains trivial for any t coprime to the degree of the finite extension of $\mathbb{F}_q$ over which the points of K are defined.

The above theorem enables us to efficiently construct permutation rational functions of given prime degree $\ell \geq 5$ over prescribed finite fields $\mathbb{F}_q$ of cryptographic size. To do so, we proceed as follows.

3 Computing isogeny kernels

As before, let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Denote by P a point of prime order ℓ and by K the subgroup it generates. The isogeny $E \to E/K$ satisfies the conditions of Theorem 1 if and only if K is rational and $K(\mathbb{F}_{q^2}) = \{0\}$. The second condition is easy to test: since ℓ is prime, all nontrivial points of K generate all others; it thus suffices to verify that P is not defined over $\mathbb{F}_{q^2}$. To efficiently test whether K is rational we use the following criterion.

Lemma 1. *Let P be a point of prime order ℓ on E. Denote by d the degree of the field extension $\mathbb{F}_q(x_P)/\mathbb{F}_q$. Let τ be an integer of order exactly d in $\mathbb{F}_\ell^\times/\{\pm 1\}$. The subgroup K generated by P is rational if and only $x_{[\tau]P}$ is a Galois conjugate of x_P.*

Proof. The 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, which 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 H and thus acts as an element λ_π. Now let e denote the degree of the smallest extension of $\mathbb{F}_q$ over which H is defined. Note that $\mathbb{F}_{q^e}$ is also the field of definition of K since this subgroup has odd order. Then λ_π is of order exactly d/e. Therefore, the group $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ embeds in $\mathbb{F}_\ell^\times/\{\pm 1\}$ as $\mu_{d/e}$ and its action partitions H into orbits of length d/e. The stabilizer of P's orbit is then $\mu_{d/e}$. In particular, $e = 1$ if and only if $x_{[\tau]P}$ lies in the same orbit as x_P. □

To make the above criterion explicit, 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 x-coordinates of ℓ-torsion points are roots of the so-called ℓ-division polynomial $\psi_\ell(x)$. If $f(x)$ is a degree-d irreducible factor of $\psi_\ell(x)$, we can test whether its roots are the x-coordinates of points P such that $f(x_{[\tau]P}) = 0$ by checking whether

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

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: using a remainder tree, compute $a_f = \phi_\tau(x)/\psi_\tau(x)^2 \bmod f(x)$ for each $f \in \mathscr{F}$.
8: **while** $\mathscr{F}$ is not empty **do**
9: remove the first element from $\mathscr{F}$ and call it f.
10: **if** $f(a_f) \neq 0 \bmod f(x)$ **then**
11: **continue** to the next iteration.
12: **end if**
13: let $k \leftarrow f$.
14: **for** $m = 1$ to $\frac{\ell-1}{2d} - 1$ **do**
15: let ρ be the smallest positive integer such that $\rho \equiv \pm\omega^m \bmod \ell$.
16: let $g(x) \leftarrow \mathrm{res}_y\big(f(y), \phi_\rho(x) - \psi_\rho(x)^2 y\big)$.
17: let $g(x) \leftarrow \mathrm{monic}(\gcd(\psi_\ell(x), g(x)))$.
18: let $k \leftarrow g \cdot k$.
19: remove $g(x)$ from $\mathscr{F}$.
20: **end for**
21: add $k(x)$ to the list $\mathscr{L}$.
22: **end while**
23: **end for**
24: **return** $\mathscr{L}$.

In that case, the x-coordinates of other points of K are obtained through the map $x_P \mapsto x_{[\rho]P}$ for ρ in $\mathbb{F}_\ell^\times/\{\pm 1\}/\mu_d$. We can compute them as the roots of

$$\gcd\big(\psi_\ell(x), g_\rho(x)\big) \qquad \text{where} \qquad g_\rho(x) = \mathrm{res}_y\big(f(y), \phi_\rho(x) - \psi_\rho(x)^2 y\big).$$

Indeed, for each $P \in K$ there are ρ^2 points Q such that $[\rho]Q = P$, only one of which lies in K; the others have order $\ell\rho$ and are eliminated by taking the gcd with $\psi_\ell(x)$.

Remark 1. Note that the above is unnecessary for $d = \frac{\ell-1}{2}$. In that case, the condition of the lemma always holds and degree-d irreducible factors of $\psi_\ell(x)$ are directly kernel polynomials of rational degree-ℓ isogenies.

Putting the above together we obtain Algorithm 1.

Theorem 2. *Algorithm 1 has a probabilistic running time of* $\widetilde{O}(\ell^{4+\epsilon}\log(q)^2)$.

Proof. 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 [18, page 200] and an asymptotically fast method for polynomial multiplication, this takes quasi-linear time in the output: $O(\ell^2\log(q))$.

The loop from step 4 runs a maximum of $O(\ell^\epsilon)$ iterations, for any $\epsilon > 0$ thanks to the bound on the number of divisors from [1, Theorem 13.12].

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

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

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 5.

Step 7 takes at most $\ell^{2+\epsilon}$ elementary operations in $\mathbb{F}_q$ using [13].

Both steps 16 and 17 use $O(d\,\ell^2)$ operations over $\mathbb{F}_q$. They run at most once per element $f \in \mathscr{F}$, which gives an overall contribution of $\widetilde{O}(\ell^4 \log(q))$ to the running time. This dominates the loop from steps 8 to 22. □

4 Computing permutation rational functions

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 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 [12, Section 2.4]. This gives Algorithm 2.

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

Proof. Step 1 uses the method of [3] 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 [12,6] implies that, if the discriminant $\Delta(E)$ is a nonzero square modulo ℓ, then E has an 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.

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 $\mathbb{F}_q$.

```
compute the reduction to F_q[X] of the ℓ-modular polynomial Φ_ℓ(X, Y).
loop
    repeat
        draw an element j ∈ F_q uniformly at random.
    until the polynomial Φ_ℓ(X, j) has at least one root.
    let E/F_q denote an elliptic curve with j-invariant j.
    for each polynomial f(x) output by Algorithm 1 do
        compute the isogeny φ with kernel polynomial f(x) using Kohel's formula.
        return its x-coordinate map u_φ.
    end for
end loop
```

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. Similarly, one can consider the modular curve associated with the congruence subgroup

$$\Gamma_1'(\ell) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \pm 1 & * \\ 0 & * \end{bmatrix} \pmod{\ell} \right\}$$

whose associated modular curve parametrizes pairs $(E, \pm P)$ consisting of an elliptic curve and a point of order ℓ up to sign. The natural map $X_1(\ell) \to X\left(\Gamma_1'(\ell)\right)$ is actually an isomorphism, and 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 $X\left(\Gamma_1'(\ell)\right)(\mathbb{F}_q) \to X_0(\ell)(\mathbb{F}_q)$ has density $\frac{2}{\ell-1} + O(q^{-1/2})$. Thus, if (E, K) is uniformly distributed, the probability that all points P of K are defined over $\mathbb{F}_{q^2}$ (which is equivalent to saying that $\{\pm P\}$ is defined over $\mathbb{F}_q$) 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 $\mathbb{F}_{q^2}$-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 $\frac{2\ell}{\ell-3} \leq 5$. □

Example 1. Take $q = 127$ and $\ell = 13$. For $j = 60$ we find that $\Phi_\ell(X, j)$ has two roots in $\mathbb{F}_q$. Thus, any elliptic curve E with $j(E) = 60$ is the domain of two rational degree-ℓ isogenies; we take $E : y^2 = x^3 + 25x + 58$, of which the ℓ-division polynomial factors as $\psi_\ell(x) = f_1(x) f_2(x) f_3(x) Q(x)$ with

$$\begin{aligned} f_1(x) &= x^3 + 88x^2 + 60x + 59, \\ f_2(x) &= x^3 + 91x^2 + 14x + 57, \\ f_3(x) &= x^6 + 36x^5 + 17x^4 + 73x^3 + 88x^2 + 11x + 31, \end{aligned}$$

and $Q(x)$ is the product of six irreducible polynomials of degree twelve.

Since $f_3(x)$ has degree $\frac{\ell-1}{2}$, it is the kernel polynomial of a degree-ℓ isogeny with no rational kernel point. The x-coordinate map of that isogeny provides a first permutation rational fraction:

$$x \longmapsto \big(x^{13} + 72x^{12} + 84x^{11} + 72x^{10} + 2x^9 + 15x^8 + 91x^7 \\ +94x^6 + 4x^5 + 66x^4 + 17x^3 + 49x^2 + 48x + 53\big) \big/ f_3(x)^2.$$

Now consider $f_1(x)$. We take $\omega = 2$ as a generator of $\mathbb{F}_\ell^\times$ and deduce $\tau = 4$. The condition $f_1\left(\frac{\phi_\tau(x)}{\phi_\tau(x)^2}\right) = 0 \bmod f_1(x)$ holds and, therefore, $f_1(x)$ is a factor of the kernel polynomial of a rational degree-ℓ isogeny. We compute the other factor as steps 15–17 in Algorithm 1 with $m = 1$ and find $g(x) = f_2(x)$. We then compute the isogeny with kernel polynomial $f_1(x)f_2(x)$ and obtain a second permutation rational fraction as its x-coordinate map:

$$x \longmapsto \big(x^{13} + 67x^{12} + 13x^{11} + 61x^{10} + 83x^9 + 50x^8 + 49x^7 \\ +80x^6 + 75x^5 + 88x^4 + 7x^3 + 41x^2 + 38x + 7\big) \big/ \big(f_1(x)f_2(x)\big)^2.$$

Table 1 reports on running times for a simple PARI/GP [14] implementation of Algorithm 2 on a single core of an Intel Xeon E3-1275 CPU.

Additionally, Table 2 gives the average density of computed kernel polynomials which are not irreducible, that is, for which $d < \frac{\ell-1}{2}$. It shows that, for certain values of ℓ, although the special case discussed in Remark 1 greatly simplifies our algorithms, it significantly restricts the range of permutation rational fractions found. Note that a density of zero is expected for $\ell = 23$ and $\ell = 59$ since in that case $\frac{\ell-1}{2}$ is exactly twice a prime number p, so all isogenies of degree $d = 2, p$ have rational kernel points.

$q =$	$2^{127}-1$	$2^{255}-19$	$2^{511}-187$	$2^{1023}-361$
$\ell = 13$	0.13	0.24	0.57	2.53
$\ell = 23$	0.68	1.28	2.98	9.81
$\ell = 37$	3.25	5.99	15.48	43.14
$\ell = 59$	21.38	35.02	89.05	227.20

Table 1. Average running time in seconds for Algorithm 2.

5 A family of candidate trapdoor permutations

Using the algorithm of the previous section, one can obtain a permutation rational function analogue of the 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 $v = r/s \bmod q$.

$q =$	$2^{127}-1$	$2^{255}-19$	$2^{511}-187$	$2^{1023}-361$
$\ell = 13$	0.55	0.40	0.55	0.50
$\ell = 23$	—	—	—	—
$\ell = 37$	0.70	0.80	0.55	0.60
$\ell = 59$	—	—	—	—

Table 2. Density of computed kernel polynomials with $d < \frac{\ell-1}{2}$.

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 [2].

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 Conclusion and open problems

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 [7, §3.2]. Since the classification of genus-zero exceptional covers of the projective line has been given by Guralnick et al. [9], 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.

References

1. T. M. Apostol. *Introduction to analytic number theory*. Springer, 1976.
2. D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.
3. R. Bröker, K. Lauter, and A. V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012.
4. J.-M. Couveignes and R. Lercier. The geometry of some parameterizations and encodings. *Advances in mathematics of communications*, 8(4):437–458, 2014.
5. P.-A. Fouque and M. Tibouchi. Deterministic encoding and hashing to odd hyperelliptic curves. In *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277. Springer, 2010.
6. M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory Symposium — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 47–62. Springer, 2002.
7. M. 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.
8. M. D. Fried. The place of exceptional covers among all diophantine relations. *Finite Fields and Their Applications*, 11:367–433, 2005.
9. R. M. Guralnick, P. Müller, and J. Saxl. *The Rational Function Analogue of a Question of Schur and Exceptionality of Permutation Representations*, volume 773 of *Memoirs of the AMS*. AMS, 2003.
10. R. M. Guralnick, T. J. Tucker, and M. E. Zieve. Exceptional covers and bijections on rational points. *Int. Math. Res. Not.*, 2007. Article ID 004, 19 pages.
11. J.-G. Kammerer, R. Lercier, and G. Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 2010.
12. D. R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.
13. R. T. Moenck and A. B. Borodin. Fast modular transforms via division. In *IEEE 13th Annual Symposium on Switching and Automata Theory*, pages 90–96. IEEE Press, 1972.
14. The PARI Group. *PARI/GP*, 2016. `http://pari.math.u-bordeaux.fr/`.
15. M. 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.
16. M. Tibouchi. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. In L. Batina et al., editors, *ECC 2013*, 2013.
17. M. Tibouchi. Impossibility of surjective Icart-like encodings. In S. S. M. Chow, J. K. Liu, L. C. K. Hui, and S. Yiu, editors, *ProvSec 2014*, volume 8782 of *Lecture Notes in Computer Science*, pages 29–39. Springer, 2014.
18. H. Weber. *Elliptische Funktionen und Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Friedrich Vieweg und Sohn, 1891.