SCIENCE CHINA
Information Sciences

• LETTER •

May 2022, Vol. 65 159101:1–159101:3
https://doi.org/10.1007/s11432-019-2669-6

Pseudorandom number generator based on supersingular elliptic curve isogenies

Yan HUANG[1], Fangguo ZHANG[2,3*], Zhijie LIU[2] & Haibo TIAN[2,3]

[1]*School of Electronic and Information Engineering, Sun Yat-sen University, Guangzhou* 510006*, China;*
[2]*School of Data and Computer Science, Sun Yat-sen University, Guangzhou* 510006*, China;*
[3]*Guangdong Key Laboratory of Information Security, Guangzhou* 510006*, China*

Received 5 July 2019/Accepted 24 September 2019/Published online 26 May 2021

Citation Huang Y, Zhang F G, Liu Z J, et al. Pseudorandom number generator based on supersingular elliptic curve isogenies. Sci China Inf Sci, 2022, 65(5): 159101, https://doi.org/10.1007/s11432-019-2669-6

Dear editor,

Pseudorandom number generator (PRNG) is very important for the randomness study in some cryptographic algorithms. A PRNG is a deterministic function that takes a uniform random bit string as input and outputs a longer bit string. The pseudorandom sequence cannot be distinguished from a uniform random string in any polynomial time. Håstad et al. [1] showed that PRNGs exist if and only if one-way functions exist. In what follows, we mainly focus on provably secure PRNGs. Classical PRNGs are based on the hardness of the discrete-log problem (DLP) or the integer factorization problem. Nevertheless, Shor [2] provided an efficient quantum algorithm to solve the DLP and the integer factorization problem in polynomial time, which makes the PRNGs unsafe with the advent of quantum computers, thus attracting considerable attentions in constructing efficient quantum-resistant PRNGs. Up to now, PRNGs based on lattices [3] and coding theory [4] have been proposed.

Note that Jao et al. [5] proposed a Diffie-Hellman protocol based on supersingular elliptic curve isogenies and Biasse et al. [6] showed that computing supersingular isogenies over an extension field $\mathbb{F}_{p^2}$ needs quantum exponential time, it is interesting to construct the quantum-resistant PRNG based on supersingular isogenies.

Decisional supersingular product (*DSP*). Jao et al. [5] proposed the computational supersingular isogeny problem, the computational Diffie-Hellman problem and the decisional Diffie-Hellman problem based on supersingular isogenies. Galbraith et al. [7] presented a DSP problem, which is a variant of the Diffie-Hellman assumption. The explicit description is as follows.

Let $\mathcal{G}$ be a polynomial algorithm that takes 1^λ as input and outputs $(\mathbb{F}_{p^2}, E_0, (P_A, Q_A))$ where $p = \ell_A^{e_A}\ell_B^{e_B} f - 1$ is a large prime such that $\ell_A^{e_A} \approx \ell_B^{e_B}$, and P_A, Q_A are two independent points of order $\ell_A^{e_A}$ on a random curve E_0 over $\mathbb{F}_{p^2}$. E_0, E_B are two supersingular elliptic curves over $\mathbb{F}_{p^2}$ such that there exists an isogeny $\phi_B : E_0 \to E_B$ of degree $\ell_B^{e_B}$. Suppose $\phi_B(P_A)$ and $\phi_B(Q_A)$ are the isogenous points for the generator points $P_A, Q_A \in E_0[\ell_A^{e_A}]$ under the mapping ϕ_B, respectively. Consider the two distributions of pairs (E_A, E_{AB}) and (E'_A, E'_{AB}), respectively. The first distribution for the pair (E_A, E_{AB}) is that s_A is chosen at random in the set $\{1, \ldots, \ell_A^{e_A} - 1\}$ such that $E_A \cong E_0/\langle P_A + s_A Q_A\rangle$ and $E_{AB} \cong E_B/\langle \phi_B(P_A) + s_A\phi_B(Q_A)\rangle$. The second distribution for the pair (E'_A, E'_{AB}) is that E'_A is chosen at random among the curves having the same cardinality as E_0, and $\phi' : E'_A \to E'_{AB}$ is a random $\ell_B^{e_B}$-isogeny.

The problem is given (E_0, E_B) and the auxiliary points $P_A, Q_A, \phi_B(P_A), \phi_B(Q_A)$ plus a pair (E_A, E_{AB}) (or (E'_A, E'_{AB})), to determine from which distribution the pair is sampled.

The construction of pseudorandom generator based on supersingular isogenies. The public parameters in Algorithm 1 are a finite field $\mathbb{F}_{p^2}$ with a large prime $p = \ell_A^{e_A}\ell_B^{e_B} f - 1$, an initial supersingular curve E_0 over $\mathbb{F}_{p^2}$, and two pairs of independent points (P_A, Q_A) of order $\ell_A^{e_A}$ and (P_B, Q_B) of order $\ell_B^{e_B}$ on E_0. Algorithm 1 takes as input a seed $s_0 \in \{0,1\}^{\frac{\lambda}{2}}$ with $\lceil \log_2 p \rceil = \lambda$, an upper bound N of pseudorandom numbers such that $\log_2 N \leqslant \log_2 \lceil \frac{p}{12} \rceil$ and their numbers n, and outputs n pseudorandom numbers, which are stored in the set L.

Algorithm 1 $\sum_n : (\{0,1\}^{\frac{\lambda}{2}}, [0, N-1], F_{E_0, P_A, Q_A, \ell_A^{e_A}}, F_{E_B, \phi_B(P_A), \phi_B(Q_A), N}, s_0)$

Require: $\mathbb{F}_{p^2}$, $(E_0, P_A, Q_A, P_B, Q_B)$, s_0, N, n.
Ensure: L.
1: $r_0 \leftarrow \mathrm{SHA}_3(s_0, N) \mod \ell_B^{e_B}$;
2: $R_B = P_B + r_0 \cdot Q_B$;
3: $\phi_B : E_0 \to E_B \cong E_0/\langle R_B\rangle$;
4: Compute $\phi_B(P_A)$ and $\phi_B(Q_A)$;
5: $\emptyset \leftarrow L$;
6: for $k = 1$ to n
7: $s_k \leftarrow F_{E_0, P_A, Q_A, \ell_A^{e_A}}(s_{k-1})$;
8: $r_k \leftarrow F_{E_B, \phi_B(P_A), \phi_B(Q_A), N}(s_k)$;
9: Add r_k to L;
10: Return L.

* Corresponding author (email: isszhfg@mail.sysu.edu.cn)

The standard SHA3 algorithm in Step 1 takes as input s_0 and the modulus N, and outputs a secret value r_0. Steps 2 and 3 compute a kernel generated point R_B and an $\ell_B^{e_B}$-isogeny ϕ_B which corresponds to the kernel $\langle R_B\rangle$. Step 4 evaluates two points P_A and Q_A under the isogeny ϕ_B. Steps 1–4 can be precomputed, because these steps are not included in the iterative process described in Steps 6–9. Furthermore, $E_B, \phi_B(P_A)$ and $\phi_B(Q_A)$ are only used as the fixed parameters of function $F_{E_B,\phi_B(P_A),\phi_B(Q_A),N}(s_k)$ in Step 8. Step 5 creates a set L storing pseudorandom numbers. Steps 6–9 first iteratively generate each internal state s_k by the function $F_{E_0,P_A,Q_A,\ell_A^{e_A}}(s_{k-1})$, and compute each pseudorandom number r_k by the function $F_{E_B,\phi_B(P_A),\phi_B(Q_A),N}(s_k)$, and then add it into the set L. The function $F_{E_0,P_A,Q_A,\ell_A^{e_A}}(s_{k-1})$ is defined by taking as input an internal state s_{k-1} and public parameters $E_0, P_A, Q_A, \ell_A^{e_A}$, computing the kernel generated point $R_A = P_A + s_{k-1}\cdot Q_A$ and the isogeny $\phi_A : E_0 \to E_A$ which corresponds to the kernel $\langle R_A\rangle$, and then outputting s_k such that $s_k = a'||b' \mod \ell_A^{e_A}$ where $j(E_A) = a' + b'\cdot \mathrm{i}$. The computation of function $F_{E_B,\phi_B(P_A),\phi_B(Q_A),N}(s_k)$ is similar to that of $F_{E_0,P_A,Q_A,\ell_A^{e_A}}(s_{k-1})$. The difference is that the function $F_{E_0,P_A,Q_A,\ell_A^{e_A}}(s_k)$ is used to change the internal state while the function $F_{E_B,\phi_B(P_A),\phi_B(Q_A),N}(s_k)$ is used to generate pseudo-random numbers (thus we can also call it output function). Both of them are based on computational supersingular elliptic curve isogenies problem which lays the security foundation of the PRNG $\sum_n$. Nevertheless, the security of the PRNG can be based on the weaker assumption, i.e., the DSP assumption, which will be proved later.

Remark 1. Note that the assumption $\log_2 N \leqslant \log_2\lceil\frac{p}{12}\rceil$ above is necessary, which can ensure that these numbers represented j-invariants with length of $2\log_2 p$ bits, are approximately uniformly distributed in the set $\{0,\ldots,N-1\}$ under the action of modulo N, because there are about $\log_2\lceil\frac{p}{12}\rceil$ supersingular j-invariants over $\mathbb{F}_{p^2}$. On the condition of $\log_2 N > \log_2\lceil\frac{p}{12}\rceil$, there might be some numbers in the set $\{0,\ldots,N-1\}$ that have no corresponding j-invariants mapping to themselves under the action of modulo N. Upon $\log_2 N \geqslant 2\log_2 p$, our PRNG is easily broken by the adversary distinguishing the random numbers generated by the scheme $\sum_n$ from those chosen randomly in the set $\{0,\ldots,N-1\}$ by the supersingularity.

Indistinguishability. For the convenience of the proof of the scheme $\sum_n : \big(\{0,1\}^{\frac{\lambda}{2}}, [0,N-1], F_{E_0,P_A,Q_A,\ell_A^{e_A}}, F_{E_B,\phi_B(P_A),\phi_B(Q_A),N}, s_0\big)$, we first consider the subscheme Π_n of $\sum_n$ that outputs random supersingular curves, namely,

$$\Pi_n : (\{0,1\}^{\frac{\lambda}{2}}, [0,N-1], F_{E_0,P_A,Q_A,\ell_A^{e_A}}, G_{E_B,\phi_B(P_A),\phi_B(Q_A)}, s_0),$$

where the output function $G_{E_B,\phi_B(P_A),\phi_B(Q_A)}$ can be defined by computing $R_{ABk} = \phi_B(P_A) + s_k\phi_B(Q_A)$, $\phi_{ABk} : E_B \to E_{ABk} \cong E_B/\langle R_{ABk}\rangle$, and $r_k = E_{ABk}$, for $k = 1,\ldots,n$. We first consider the indistinguishability of Π_n, then show the indistinguishability of Σ_n.

Theorem 1. If there exists a polynomial time algorithm that distinguishes the output of Π_n from the sequence which is generated by choosing n random curves with the same cardinality as the initial curve in Π_n and computing random $l_B^{e_B}$-isogenies with the advantage of ε, then the DSP problem can be solved in polynomial time with the advantage of $\frac{\varepsilon}{n}$.

Proof. Denote the sequence $Z_0 = (E^*_{AB1,0},\ldots, E^*_{ABn,0})$ which is generated by choosing n random curves with the same cardinality as the initial curve in Π_n and computing random $l_B^{e_B}$-isogenies, and the sequence $Z_n = (E^*_{AB1,1},\ldots,E^*_{ABn,1})$ which is generated by Π_n. If there exists a polynomial time algorithm $\mathcal{D}$ that distinguishes Z_n from Z_0 with the advantage of ε, that is,

$$|\Pr[\mathcal{D}(Z_0)=1] - \Pr[\mathcal{D}(Z_n)=1]| \geqslant \varepsilon.$$

Owing to the classical hybrid argument as in [8],

$$|\Pr[\mathcal{D}(Z_k)=1] - \Pr[\mathcal{D}(Z_{k+1})=1]| \geqslant \frac{\varepsilon}{n},$$

where $Z_k = (E^*_{AB1,0},\ldots,E^*_{AB(k-1),0}, E^*_{ABk,1}, E^*_{AB(k+1),1},\ldots,E^*_{ABn,1})$ and $Z_{k+1} = (E^*_{AB1,0},\ldots, E^*_{AB(k-1),0}, E^*_{ABk,0}, E^*_{AB(k+1),1},\ldots,E^*_{ABn,1})$. The probability is taken not only over internal coin flips of $\mathcal{D}$ but also over the choice of k.

Now, we show how to solve the DSP problem using the distinguisher $\mathcal{D}$ as the building block. Let $((E_0,E_B^*),(P_A,Q_A,\phi_B^*(P_A),\ \phi_B^*(Q_A)),\ (E_A^*,\ E^*_{AB,b}))$ be a DSP instance. The distribution of the pair $(E_A^*,\ E^*_{AB,1})$ is that s_A is chosen by computing the j-invariant $j(E) = a+b\mathrm{i}$ of a random supersingular curve E and performing the modular operation $s_A = a||b \mod \ell_A^{e_A}$ such that $E_A^* \cong E_0/\langle P_A + s_A Q_A\rangle$ and $E^*_{AB,1} \cong E_B^*/\langle\phi_B^*(P_A) + s_A\phi_B^*(Q_A)\rangle$. The distribution of the pair $(E_A^*,\ E^*_{AB,0})$ is that E_A^* is chosen at random among the curves having the same cardinality as E_0, and $E^*_{AB,0}$ is a random $\ell_B^{e_B}$-isogeny curve. A solver for the DSP problem decides from which distribution the pair $(E_A^*, E^*_{AB,b})$ is sampled as Algorithm 2.

Algorithm 2 is given $((E_0,E_B^*),(P_A,Q_A,\phi_B^*(P_A),\ \phi_B^*(Q_A)),(E_A^*,E^*_{AB,b}))$ as input.

Algorithm 2

1: Select $k \leftarrow \{1,\ldots,n\}$;
2: Select random curves $E^*_{AB1,0},\ldots,E^*_{AB(k-1),0}$ as the way above;
3: Set $s_k \leftarrow a_k \parallel b_k \mod \ell_A^{e_A}$ such that $j(E_A^*) = a_k + b_k\cdot\mathrm{i}$;
4: for $t = k+1$ to n do
5: Set $s_t \leftarrow F_{E_0,P_A,Q_A,\ell_A^{e_A}}(s_{t-1})$;
6: Set $E^*_{ABt,1} \leftarrow G_{E_B,\phi_B(P_A),\phi_B(Q_A)}(s_t)$;
7: end for
8: Set $Z \leftarrow (E^*_{AB1,0},\ldots,E^*_{AB(k-1),0}, E^*_{AB,b}, E^*_{AB(k+1),1}, E^*_{AB(k+2),1},\ldots,E^*_{ABn,1})$;
9: Return $D(Z)$.

If there exists s_A such that $E_A^* \cong E_0/\langle P_A + s_A Q_A\rangle$ and $E^*_{AB,b} \cong E_B^*/\langle\phi_B^*(P_A) + s_A\phi_B^*(Q_A)\rangle$ then $b=1$, and $E^*_{AB,1} = E^*_{ABk,1}$, so Z is distributed as Z_k. Otherwise, if E_A^* is chosen at random among the curves having the same cardinality as E_0, and $E^*_{AB,b}$ is a random $\ell_B^{e_B}$-isogeny curve, then $b=0$, and $E^*_{AB,0} = E^*_{ABk,0}$, so Z is distributed as Z_{k+1}. Therefore, the above algorithm solves the DSP problem in polynomial time with the advantage of $\frac{\varepsilon}{n}$.

We have proved that the scheme Π_n has the property of indistinguishability. The scheme $\sum_n$ that translates every output curve $E_{ABt,1}$ into a random number $r_t \in \{0,\ldots,N-1\}$ by computing $j(E_{ABt,1}) = a_t + b_t\cdot\mathrm{i}$, $R_t = a_t||b_t$, and $r_t = R_t \mod N$ for $t \in \{1,\ldots,n\}$ also has the property. Because $\log_2 N \leqslant \log_2\lceil\frac{p}{12}\rceil \leqslant \log_2\lceil R_t\rceil$, it follows that r_t is approximately random in the set $\{0,\ldots,N-1\}$. Hence, the scheme $\sum_n$ has the property of indistinguishability.

Conclusion. We proposed a PRNG based on supersingular elliptic curve isogenies for the first time and presented the security analysis under the assumption of the DSP assumption. Whether the PRNG based on supersingular elliptic curve isogenies is more efficient compared with other post-quantum PRNGs is a topic we will study further. Besides, the randomness can further be tested by the statistical tests such as the optimized discrete Fourier transform way [9].

Acknowledgements Fangguo ZHANG was supported by National Key R&D Program of China (Grant No. 2017YFB0802500) and National Natural Science Foundation of China (Grant Nos. 61672550, 61972429). Haibo TIAN was supported by Natural Science Foundation of Guangdong Province of China (Grant No. 2018A0303130133).

References

1 Håstad J, Impagliazzo R, Levin L A, et al. A pseudorandom generator from any one-way function. SIAM J Comput, 1999, 28: 1364–1396
2 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994. 124–134
3 Banerjee A, Peikert C, Rosen A. Pseudorandom functions and lattices. In: Advances in Cryptology—EUROCRYPT 2012. Berlin: Springer, 2012. 7237: 719–737
4 Gaborit P, Hauteville A, Tillich J P. RankSynd a PRNG based on rank metric. In: Post-Quantum Cryptography. Berlin: Springer, 2016. 9606: 18–28
5 Jao D, de Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Post-Quantum Cryptography. Berlin: Springer, 2011. 7071: 19–34
6 Biasse J F, Jao D, Sankar A. A quantum algorithm for computing isogenies between supersingular elliptic curves. In: Progress in Cryptology—INDOCRYPT 2014. Berlin: Springer, 2014. 8885: 428–442
7 Galbraith S D, Petit C, Silva J. Identification protocols and signature schemes based on supersingular isogeny problems. In: Advances in Cryptology—ASIACRYPT 2017. Berlin: Springer, 2017. 10624: 3–33
8 Farashahi R R, Schoenmakers B, Sidorenko A. Efficient pseudorandom generators based on the DDH assumption. In: Public Key Cryptography—PKC 2007. Berlin: Springer, 2007. 4450: 426–441
9 Chen M H, Chen H, Fan L M, et al. A new discrete Fourier transform randomness test. Sci China Inf Sci, 2019, 62: 032107