Reusable Fuzzy Extractor from Isogeny

Yu Zhou[1,2][0000−0003−3452−7831], Shengli Liu[1,2(✉)][0000−0003−1366−8256], and Shuai Han[2,3][0000−0002−8156−7089]

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] School of Cyber Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{zhouyusjtu2019,slliu,dalen17}@sjtu.edu.cn

Abstract. We propose the *first* reuasble fuzzy extractor (rFE) scheme from isogeny. Our rFE scheme supports linear fraction of errors. The reusability is based on the weak pseudorandomness of CSI-FiSh (Beullens et al., Asiacrypt 2019) in the standard model, and allows multiple extractions from the fuzzy source, which admits many applications of rFE with the same source.

Keywords: Reusable fuzzy extractor · Isogeny-based cryptography · Weak pseudorandomness.

1 Introduction

In physical world, there are fuzzy sources which have high entropy and samplings from a fuzzy source result in close samples. Common fuzzy sources include biometric features like faces, fingerprints, palmprint, voice etc. [21,17,23]), physical unclonable functions (PUFs) [18,28], and quantum bits [9,4]. Extracting uniformly random strings from fuzzy sources is known as *fuzzy extractor (FE)*, a primitive first proposed by Dodis et al. [15].

A traditional FE is captured by two algorithms: the generation algorithm Gen and the reproduction algorithm Rep. One can sample a reading $\mathbf{x} \leftarrow X$ from the fuzzy source X, and then use $\mathsf{Gen}(\mathbf{x})$ to extract a string R and output public helper string P. Later, one can sample another reading $\mathbf{x}' \leftarrow X$, then use the reproduction algorithm $\mathsf{Rep}(\mathbf{x}', \mathsf{P})$ to output an extracted string R'. As long as $\mathbf{x}$ and $\mathbf{x}'$ are close enough, then the reproduce algorithm will successfully recover $\mathsf{R}' = \mathsf{R}$. The security of FE requires that R is uniformly distributed even when P is disclosed.

Reusable Fuzzy Extractor. FE is inherently limited to a single extraction, and this prevents FE from wide applications. In [8], Boyen introduced the concept of *reusable fuzzy extractor (rFE)*. rFE relaxes the uniformity of the extracted string to a pseudo-random one but allows multiple extractions from the same fuzzy source, which is captured by reusability of rFE. Boyen [8] also proposed

a reusable FE scheme in the random oracle (RO) model. Later, Canetti et al. [10] and Alamélou et al. [2] proposed reusable FE schemes for the low-entropy source, which also relied on the RO model. In [32], Wen et al. proposed the first reusable FE scheme in the standard model from the DDH assumption.

To pursue post-quamtum security, Apon et al. [3] introduced the first reusable FE scheme from the learning with errors (LWE) assumption. However, their scheme only tolerates logarithmic fraction of errors. In 2018, Wen et al. [31] overcame this limitation by presenting the first reusable FE scheme which is capable of tolerating linear fraction of errors under the LWE assumption. Both works of [3] and [31] assume that the manipulation between two readings of the same source is adaptively controlled by a PPT adversary.

Isogeny-Based Cryptography. Another promising candidate for post-quantum security is isogeny-based cryptography, which can be traced back to 1997 by Couveignes. In 2006, Couveignes proposed authentication and key exchange schemes from isogeny [14]. In the mean time, Rostovtsev and Stolbunov [26] independently discovered these results. The Couveignes-Rostovtsev-Stolbunov scheme relies on the action of ideal class groups on ordinary elliptic curves as its foundation. However, its efficiency is far from practical, and it is vulnerable to a subexponential-time attack [13]. To seek efficiency, Jao and De Feo [19] turned to supersingular elliptic curves and proposed a Diffie-Hellman like key agreement protocol, known as the Supersingular Isogeny Diffie Hellman (SIDH). However, recent works [11,24] has shown that SIDH is no longer secure.

The well-accepted secure key-exchange protocol is the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) protocol, due to Castryck et al. [12]. By leveraging isogeny over supersingular elliptic curves instead of ordinary elliptic curves, CSIDH becomes a practical protocol. Up to now, CSIDH is believed to have post-quantum security since it avoids the leakage of some sensitive points. Later, Beullens et al. [7] constructed CSI-FiSh by computing the structure of the ideal class group for CSIDH-512.

In 2020, Alamati et al. [1] introduced the concept called *cryptographic group action*, which enabled the generalization of the work of CSIDH and CSI-FiSh, resulting in ranges of isogeny-based schemes [22,16,6]. However, up to now, there does not exist isogeny-based rFE scheme. It naturally arises a question:

How to construct an efficient reusable fuzzy extractor from isogeny-based assumptions?

1.1 Our Contributions

In this paper, we answer this question in the affirmative.

- We construct the *first* isogeny-based reusable fuzzy extractor in the standard model. Our rFE supports linear fraction of errors.
- The reusability of our construction is tightly reduced to the weak pseudorandomness of CSI-FiSh [7].

- Our construction is simple and efficient. Only one group action operation is involved in both generation and reproduction algorithm.

In Sect. 4, we present our isogeny-based rFE scheme $\mathsf{rFE}_{\mathsf{Isogeny}}$. We provide a comparison between our $\mathsf{rFE}_{\mathsf{Isogeny}}$ and some known rFE schemes in Table 1.

rFE Schemes	Linear Error Rate	Assumptions	Reusability	Source Requirement
Boy04 [8]	✓	–	weak	$\widetilde{\mathbf{H}}_\infty(W_i\|\Delta W_{i,j}) = \mathbf{H}_\infty(W_i)$
ABCG16 [2]	✓	DDH	strong	$\widetilde{\mathbf{H}}_\infty(W_i[j]\|(W_i/W_i[j]))$ is high enough
CFPRS16 [10]	✘	strong DDH	strong	$\widetilde{\mathbf{H}}_\infty(W_i[j_1],\ldots,W_i[j_k]\|j_1,\ldots,j_k)$ is high enough
ACEK17 [3]	✘	LWE	strong	W follows the error distribution of LWE
WLH18 [32]	✓	DDH	strong	(m,ρ)-correlated
WL18 [31]	✓	LWE	strong	$\Delta W_{i,j}$ is chosen by PPT adversary $\mathcal{A}$
Our $\mathsf{rFE}_{\mathsf{Isogeny}}$	✓	Isogeny	strong	$\Delta W_{i,j}$ is chosen by PPT adversary $\mathcal{A}$

Table 1. Comparison with some known reusable fuzzy extractor schemes. Each source reading is denoted by W_i for $i \in [Q]$. Let $\Delta W_{i,j}$ denote $W_j - W_i$. Let $W_i[j]$ denotes the j-th element of W_i. "Linear Error Rate" denotes whether the scheme tolerates linear fraction of errors. "Source Requirement" denotes the requirements for the fuzzy source. "$-$" means the scheme is an information theoretical one. "weak" means that it is difficult for any PPT adversary to distinguish R_i from a uniform one solely based on observing public helper strings $\{\mathsf{P}_j\}_{j\in[Q]}$. "strong" means that it is difficult for any PPT adversary to distinguish R_i from a uniform one when given both $\{\mathsf{P}_j\}_{j\in[Q]}$ and $\{\mathsf{R}_j\}_{j\neq i, j\in[Q]}$.

2 Preliminaries

Notation. Let λ denote the security parameter throughout this paper, and all algorithms, distributions, functions and adversaries take 1^λ as an implicit input. We use normal and bold letters like x, $\mathbf{x}$ to denote elements and column vectors respectively. For a set $\mathcal{X}$, $x \leftarrow\!\!\$\ \mathcal{X}$ denotes the process of sampling x uniformly from $\mathcal{X}$. For a distribution X, $x \leftarrow X$ denotes the process of sampling x according to X. PPT abbreviates probabilistic polynomial time. Denote by negl some negligible function. For $n \in \mathbb{N}$, define $[n] := \{1, 2, ..., n\}$.

For two distributions X and Y, the min-entropy of X is defined by $\mathbf{H}_\infty(X) := -\log(\max_x \Pr[X = x])$, and the average min-entropy of X given Y is defined by $\widetilde{\mathbf{H}}_\infty(X|Y) := -\log(\mathbb{E}_{y\leftarrow Y}[\max_x \Pr[X = x|Y = y]])$. The statistical distance between X and Y is defined by $\mathsf{SD}(X, Y) := \frac{1}{2}\sum_u |\Pr[X = u] - \Pr[Y = u]|$. We denote $X \overset{s}{\approx}_\varepsilon Y$ if $\mathsf{SD}(X, Y) \leq \varepsilon$. We denote $X \overset{c}{\approx}_\varepsilon Y$ if $|\Pr[\mathcal{D}(X) = 1] - \Pr[\mathcal{D}(Y) = 1]| \leq \varepsilon$ for all PPT distinguishers $\mathcal{D}$. When $\varepsilon = \mathsf{negl}(\lambda)$, we simply denote $X \overset{s}{\approx} Y$ or $X \overset{c}{\approx} Y$.

For a primitive XX and a security notion YY, by $\mathsf{Exp}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\lambda) \Rightarrow 1$, we mean that the security experiment outputs 1 after interacting with an adversary $\mathcal{A}$, and by $\mathbf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\lambda)$, we denote the advantage of $\mathcal{A}$ in the security experiment. Finally, we define $\mathbf{Adv}^{\mathrm{YY}}_{\mathrm{XX}}(\lambda) := \max_{\mathrm{PPT}\mathcal{A}} \mathbf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\lambda)$.

2.1 Fuzzy Source and Secure Sketch

A *metric space* is a set $\mathcal{M}$ equipped with a distance function $\mathsf{dis} : \mathcal{M} \times \mathcal{M} \to [0, \infty)$. Especially, let $\mathsf{dis}(\mathbf{w}) := \mathsf{dis}(\mathbf{w}, \mathbf{0})$. Now we present the definitions of fuzzy source and secure sketch.

Definition 1 ($(\mathcal{M}, m)$-Fuzzy Source). *Let W be a random variable over $\mathcal{M}$. If $\mathbf{H}_\infty(W) \geq m$, then W is called an $(\mathcal{M}, m)$-fuzzy source.*

Definition 2 (Secure Sketch [15]). *An $(\mathcal{M}, \mathcal{S}, m, \widetilde{m}, t)$-secure sketch for a metric space $\mathcal{M}$ consists a pair of PPT algorithms $\mathsf{SS} = (\mathsf{SS.Gen}, \mathsf{SS.Rec})$:*

- $\mathbf{s} \leftarrow \mathsf{SS.Gen}(\mathbf{w})$: *Taking $\mathbf{w} \in \mathcal{M}$ as input, it outputs a sketch $\mathbf{s} \in \mathcal{S}$.*
- $\hat{\mathbf{w}} \leftarrow \mathsf{SS.Rec}(\mathbf{w}', \mathbf{s})$: *Taking as input $\mathbf{w}' \in \mathcal{M}$ and $\mathbf{s} \in \mathcal{S}$, it outputs $\hat{\mathbf{w}}$.*

Moreover, it satisfies the following two properties.

- **Correctness.** *For any $\mathbf{w}, \mathbf{w}' \in \mathcal{M}$, if $\mathsf{dis}(\mathbf{w}, \mathbf{w}') \leq t$, then we have $\mathbf{w} = \mathsf{SS.Rec}(\mathbf{w}', \mathsf{SS.Gen}(\mathbf{w}))$.*
- **Privacy.** *For any distribution W over $\mathcal{M}$, if $\mathbf{H}_\infty(W) \geq m$, then we have $\widetilde{\mathbf{H}}_\infty(W|\mathsf{SS.Gen}(W)) \geq \widetilde{m}$.*

Moreover, a secure sketch is homomorphic if for any $\mathbf{w}, \mathbf{w}' \in \mathcal{M}$, it holds that $\mathsf{SS.Gen}(\mathbf{w} + \mathbf{w}') = \mathsf{SS.Gen}(\mathbf{w}) + \mathsf{SS.Gen}(\mathbf{w}')$.

2.2 Extractor

In this subsection, we recall the definition of average-case strong extractor, along with its homomorphic property.

Definition 3 (Average-Case Strong Extractor [15]). *An efficiently computable function $\mathsf{Ext} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is an average-case $(\widetilde{m}, \varepsilon)$-strong extractor, if for any variable X over $\mathcal{X}$ and any variable Z such that $\widetilde{\mathbf{H}}_\infty(X|Z) \geq \widetilde{m}$, it holds that $\mathsf{SD}((\mathsf{Ext}(K, X), K, Z), (U, K, Z)) \leq \varepsilon$, where K and U are uniformly distributed over $\mathcal{K}$ and $\mathcal{Y}$, respectively.*

Definition 4 (Homomorphic Average-Case Strong Extractor). *An average-case $(\widetilde{m}, \varepsilon)$-strong extractor $\mathsf{Ext} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is homomorphic, if for any $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}$ and all $\mathbf{k} \in \mathcal{K}$, we have $\mathsf{Ext}(\mathbf{k}, \mathbf{x}_1 + \mathbf{x}_2) = \mathsf{Ext}(\mathbf{k}, \mathbf{x}_1) \oplus \mathsf{Ext}(\mathbf{k}, \mathbf{x}_2)$, where $(\mathcal{X}, +)$ and $(\mathcal{Y}, \oplus)$ are both groups.*

2.3 Isogenies, Ideal Class Group Actions and CSI-FiSh

In this subsection, we provide a brief overview of the concepts and syntax of ideal class group action. Meanwhile, we present some essential results from CSI-FiSh [7]. Instead of recalling the background on elliptic curves over finite fields and isogenies, we refer the readers to [29,27] for more details.

Set of isomorphism classes of elliptic curves $\mathcal{E}(\mathcal{O})$. Let $\mathbb{F}_p$ be a prime field and E an elliptic curve defined over $\mathbb{F}_p$. Let $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E)$ denote the set of

the endomorphisms defined over $\mathbb{F}_p$, which is only an order in the imaginary quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{-p})$. Define $\mathcal{E}(\mathcal{O})$ as the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves with $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O}$.

Ideal class group $Cl(\mathcal{O})$ and group action $\star$. The ideal class group of $\mathcal{O}$, denoted by $Cl(\mathcal{O})$, is the quotient of the group of fractional invertable ideals in $\mathcal{O}$ by the principal fractional invertable ideals.

For any $[\mathfrak{a}] \in Cl(\mathcal{O})$ and $E \in \mathcal{E}(\mathcal{O})$, a group action $\star$ can be defined by $[\mathfrak{a}] \star E = E/\mathfrak{a}$ such that there exists an isogeny $\phi : E \to E'$ with $ker(\phi) = \cap_{\alpha\in[\mathfrak{a}]}\{P \in E(\overline{\mathbb{F}}_p)|\alpha(P) = 0\}$. The image curve of $[\mathfrak{a}]\star E$ is well-defined up to $\mathbb{F}_p$-isomorphism. Moreover, the ideal class group $Cl(\mathcal{O})$ acts freely and transitively on $\mathcal{E}(\mathcal{O})$, which gives us a regular abelian group operation according to [30].

CSI-FiSh. Given $p = 4 \times \ell_1 \times \cdots \times \ell_n - 1$ where ℓ_i are small odd primes. In this case, $p = 3 \mod 8$, then for any supersingular elliptic curve E defined over $\mathbb{F}_p$, the ring $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ if and only if E is $\mathbb{F}_p$-isomorphic to $E_A : y^2 = x^3 + Ax^2 + x$ for some unique $A \in \mathbb{F}_p$. Then we can use the coefficient A to identify the isomorphism class of a curve $E_A : y^2 = x^3 + Ax^2 + x$. Now we simply denote

$$\mathcal{E}(\mathcal{O}) = \mathcal{E}(\mathbb{Z}[\sqrt{-p}]) = \{E_A \mid A \in \mathbb{F}_p \text{ and } E_A : y^2 = x^3 + Ax^2 + x \text{ is supersingular}\}. \tag{1}$$

In 2019, Beullens et al. [7] introduced CSI-FiSh, in which they proposed a method for precomputing the structure of the group $Cl(\mathcal{O}) = Cl(\mathbb{Z}[\sqrt{-p}])$ for CSIDH-512 [12]. This is achieved by representing it as a relation lattice of low norm generators. In this way, CSI-FiSh admits unique representation of group element and enables efficient uniform sampling from the group. Furthermore, they computed the group order $N = O(\sqrt{p})$ and obtained the generator $[\mathfrak{g}]$ of $Cl(\mathbb{Z}[\sqrt{-p}])$. In this way, any ideal $[\mathfrak{a}] \in Cl(\mathbb{Z}[\sqrt{-p}])$ can be represented by $[\mathfrak{g}]^a$ with $a \in \mathbb{Z}_N$, and the group action is given by

$$\begin{aligned} \star : Cl(\mathbb{Z}[\sqrt{-p}]) \times \mathcal{E}(\mathbb{Z}[\sqrt{-p}]) &\to \mathcal{E}(\mathbb{Z}[\sqrt{-p}]) \\ ([\mathfrak{g}]^a, E) &\mapsto [\mathfrak{g}]^a \star E. \end{aligned} \tag{2}$$

Based on CSIDH, Beullens et al. exploited a practical algorithm to compute the group action $[\mathfrak{g}]^a \star E$ from $[\mathfrak{g}], a, E$.

According to [1] and [25], the group action $\star$ from CSI-FiSh is believed to have weak pseudorandomness. That is, for $Q = \mathsf{poly}(\lambda)$,

$$\{E_i, [\mathfrak{g}]^a \star E_i\}_{i\in[Q]} \overset{c}{\approx} \{E_i, F_i\}_{i\in[Q]}, \tag{3}$$

where $a \leftarrow_\$ \mathbb{Z}_N$, $E_i, F_i \leftarrow_\$ \mathcal{E}(\mathbb{Z}[\sqrt{-p}])$, and $[\mathfrak{g}]$ is the generator of $Cl(\mathbb{Z}[\sqrt{-p}])$.

3 Reusable Fuzzy Extractor

In this section, we recall the definition of *reusable fuzzy extractor (rFE)*.

Definition 5 (Reusable Fuzzy Extractor (rFE)). *An $(\mathcal{M}, m, \mathcal{R}, t)$-reusable Fuzzy Extractor (rFE) for a metric space $\mathcal{M}$ consists of three PPT algorithms* $\mathsf{rFE} = (\mathsf{rFE.Setup}, \mathsf{rFE.Gen}, \mathsf{rFE.Rep})$*:*

- $\mathsf{crs} \leftarrow \mathsf{rFE.Setup}$: *The setup algorithm outputs a common reference string* crs.
- $(\mathsf{P}, \mathsf{R}) \leftarrow \mathsf{rFE.Gen}(\mathsf{crs}, \mathbf{w})$: *Taking as input* crs *and an element* $\mathbf{w} \in \mathcal{M}$*, it outputs a public helper string* P *and an extracted string* $\mathsf{R} \in \mathcal{R}$.
- $\mathsf{R}/\perp \leftarrow \mathsf{rFE.Rep}(\mathsf{crs}, \mathbf{w}', \mathsf{P})$: *Taking as input* crs*, an element* $\mathbf{w}' \in \mathcal{M}$ *and the public helper string* P*, it outputs an extracted string* R *or a rejection symbol* $\perp$.

Moreover, it satisfies the following properties.

- **Correctness.** *For any* $\mathbf{w}, \mathbf{w}' \in \mathcal{M}$*, if* $\mathsf{dis}(\mathbf{w}, \mathbf{w}') \leq t$*, then for all* $\mathsf{crs} \leftarrow \mathsf{rFE.Setup}$*,* $(\mathsf{P}, \mathsf{R}) \leftarrow \mathsf{rFE.Gen}(\mathsf{crs}, \mathbf{w})$ *and* $\mathsf{R}' \leftarrow \mathsf{rFE.Rep}(\mathsf{crs}, \mathbf{w}', \mathsf{P})$*, we have* $\mathsf{R}' = \mathsf{R}$.
- **Reusability.** *For any distribution* W *over* $\mathcal{M}$ *such that* $\mathbf{H}_\infty(W) \geq m$ *and any PPT adversary* $\mathcal{A}$*, it holds that*

$$\mathbf{Adv}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda) := |\Pr[\mathsf{Exp}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda) \Rightarrow 1] - 1/2| \leq \mathsf{negl}(\lambda),$$

where $\mathsf{Exp}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda)$ *describes the reusability experiment played between* $\mathcal{A}$ *and a challenger* $\mathcal{C}$ *is shown in Fig. 1.*

$\underline{\mathsf{Exp}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda)}$:	$\underline{\mathcal{O}^b_{\mathsf{Gen}}(\delta_i \in \mathcal{M})}$:
$b \leftarrow\!\!\$\ \{0,1\}$, $\mathsf{crs} \leftarrow \mathsf{rFE.Setup}$.	If $\mathsf{dis}(\delta_i) > t$, return $\perp$.
$\mathbf{w} \leftarrow W$.	$(\mathsf{P}_i, \mathsf{R}_i^{(1)}) \leftarrow \mathsf{rFE.Gen}(\mathsf{crs}, \mathbf{w} + \delta_i)$.
$b' \leftarrow \mathcal{A}^{\mathcal{O}^b_{\mathsf{Gen}}(\delta_i)}(\mathsf{crs})$.	$\mathsf{R}_i^{(0)} \leftarrow\!\!\$\ \mathcal{R}$.
Return 1 iff $b' = b$.	Return $(\mathsf{P}_i, \mathsf{R}_i^{(b)})$.

Fig. 1. The reusability experiment $\mathsf{Exp}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda)$.

In the above formalization of reusability, we assume that the adversary controls the differences δ between any two different readings of the source W, following Wen et al. [31].

4 Construction of Reusable Fuzzy Extractor from CSI-FiSh

In this section, we present our construction of isogeny-based reusable fuzzy extractor $\mathsf{rFE}_{\mathsf{Isogeny}}$, which uses the following building blocks.

- Let $\mathsf{SS} = (\mathsf{SS.Gen}, \mathsf{SS.Rec})$ be a homomorphic $(\mathcal{M}, \mathcal{S}, m, \widetilde{m}, t)$-secure sketch.
- Let $\mathsf{Ext} : \{0,1\}^\ell \times \mathcal{M} \to \mathbb{Z}_N$ be a homomorphic average-case $(\widetilde{m}, \varepsilon = \mathsf{negl}(\lambda))$-strong extractor.
- The group action $\star$ defined in CSI-FiSh (cf. Eq. (2) in Subsect. 2.3), that is

$$\begin{aligned} \star : Cl(\mathbb{Z}[\sqrt{-p}]) \times \mathcal{E}(\mathbb{Z}[\sqrt{-p}]) &\to \mathcal{E}(\mathbb{Z}[\sqrt{-p}]) \\ ([\mathfrak{g}]^a, E) &\mapsto [\mathfrak{g}]^a \star E, \end{aligned}$$

where the group $Cl(\mathbb{Z}[\sqrt{-p}])$ is cyclic of order N with generator $[\mathfrak{g}]$, and the set $\mathcal{E}(\mathbb{Z}[\sqrt{-p}])$ is defined in Eq. (1).

The resulting isogeny-based rFE scheme $\mathsf{rFE}_{\mathsf{Isogeny}}$ is shown in Fig. 2.

$\underline{\mathsf{rFE.Setup}}$:	$\underline{\mathsf{rFE.Gen}(\mathsf{crs}, \mathbf{w})}$:	$\underline{\mathsf{rFE.Rep}(\mathsf{crs}, \mathbf{w}', \mathsf{P})}$:
$\mathsf{k}_{\mathsf{ext}} \leftarrow\!\!\$\ \{0,1\}^{\ell}$.	Parse $\mathsf{crs} = (p, [\mathfrak{g}], N, \mathsf{k}_{\mathsf{ext}})$.	Parse $\mathsf{crs} = (p, [\mathfrak{g}], N, \mathsf{k}_{\mathsf{ext}})$.
Return $\mathsf{crs} := (p, [\mathfrak{g}], N, \mathsf{k}_{\mathsf{ext}})$.	$\mathbf{s} \leftarrow \mathsf{SS.Gen}(\mathbf{w})$.	Parse $\mathsf{P} = (\mathbf{s}, E)$.
	$k \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w})$.	$\hat{\mathbf{w}}' \leftarrow \mathsf{SS.Rec}(\mathbf{w}', \mathbf{s})$.
	$E \leftarrow\!\!\$\ \mathcal{E}(\mathbb{Z}[\sqrt{-p}])$.	If $\mathsf{dis}(\hat{\mathbf{w}}', \mathbf{w}') > t$: return $\perp$.
	$\mathsf{R} := [\mathfrak{g}]^k \star E$.	$k \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \hat{\mathbf{w}}')$.
	Return $(\mathsf{P} := (\mathbf{s}, E), \mathsf{R})$.	$\mathsf{R} \leftarrow [\mathfrak{g}]^k \star E$.
		Return R.

Fig. 2. The isogeny-based reusable fuzzy extractor $\mathsf{rFE}_{\mathsf{Isogeny}}$.

Theorem 1. *Let W be an $(\mathcal{M}, m)$-fuzzy source. Then the scheme $\mathsf{rFE}_{\mathsf{Isogeny}}$ proposed in Fig. 2 is an $(\mathcal{M}, m, \mathcal{R}, t)$-reusable fuzzy extractor, where $\mathcal{R} := \mathcal{E}(\mathbb{Z}[\sqrt{-p}])$.*

Proof. We prove the reusability of $\mathsf{rFE}_{\mathsf{Isogeny}}$ by a sequence of games. Denoted by $\Pr[\mathsf{G}_j \Rightarrow 1]$ the probability that $\mathcal{A}$ wins (i.e., $b = b'$) in G_j.

Game G_0 : This is exactly the reusability experiment $\mathsf{Exp}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda)$ (cf. Definition 5). Then we have $\mathbf{Adv}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda) = |\Pr[\mathsf{G}_0 \Rightarrow 1] - 1/2|$.

Game G_1 : G_1 is the same as G_0, except that when answering $\mathcal{A}$'s oracle query $\mathcal{O}^b_{\mathsf{Gen}}(\delta_i)$, $\mathcal{O}^b_{\mathsf{Gen}}(\delta_i)$ will generate $\mathbf{s}_i := \mathsf{SS.Gen}(\mathbf{w}) + \mathsf{SS.Gen}(\delta_i)$ and $k_i := \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w}) + \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \delta_i)$ instead of generating $\mathbf{s}_i \leftarrow \mathsf{SS.Gen}(\mathbf{w} + \delta_i)$ and $k_i \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w} + \delta_i)$ directly.

According to the homomorphic properties of SS and Ext, these changes are only conceptional. Thus, $\Pr[\mathsf{G}_0 \Rightarrow 1] = \Pr[\mathsf{G}_1 \Rightarrow 1]$.

Game G_2 : G_2 is the same as G_1, except that $k \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w})$ in G_1 is changed to $k \leftarrow\!\!\$\ \mathbb{Z}_N$ during step 2.

Note that when computing $\mathbf{s}_i := \mathbf{s} + \mathsf{SS.Gen}(\delta_i)$ and $k_i := k + \Delta k_i$, only $\mathbf{s} \leftarrow \mathsf{SS.Gen}(\mathbf{w})$ and $k \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w})$ may leak information of $\mathbf{w}$. Due to the fact that $\mathbf{H}_\infty(W) \geq m$ and the privacy of SS, we have $\widetilde{\mathbf{H}}_\infty(W \,|\, \mathbf{s}) \geq \widetilde{m}$. Moreover, Ext is an average-case $(\widetilde{m}, \varepsilon = \mathsf{negl}(\lambda))$-strong extractor, it holds that $\mathsf{SD}((k, \mathsf{k}_{\mathsf{ext}}, \mathbf{s}), (u, \mathsf{k}_{\mathsf{ext}}, \mathbf{s})) \leq \varepsilon$, where $k \leftarrow \mathsf{Ext}(\mathsf{k}_{\mathsf{ext}}, \mathbf{w})$ and $u \leftarrow\!\!\$\ \mathbb{Z}_N$. Thus, $|\Pr[\mathsf{G}_1 \Rightarrow 1] - \Pr[\mathsf{G}_2 \Rightarrow 1]| \leq \varepsilon = \mathsf{negl}(\lambda)$.

Game G_3 : G_3 is the same as G_2, except that when answering $\mathcal{A}$'s oracle query, $\mathsf{R}^{(1)}_i \leftarrow [\mathfrak{g}]^{k_i} \star E_i$ is replaced with $\mathsf{R}^{(1)}_i \leftarrow [\mathfrak{g}]^{\Delta k_i} \star ([\mathfrak{g}]^k \star E_i)$.

Since $Cl(\mathbb{Z}[\sqrt{-p}])$ is a cyclic group, in G_2, $\mathsf{R}^{(1)}_i$ can be rewritten as $[\mathfrak{g}]^{k_i} \star E_i = [\mathfrak{g}]^{k+\Delta k_i} \star E_i = [\mathfrak{g}]^{\Delta k_i} \star ([\mathfrak{g}]^k \star E_i)$. These changes are just conceptional. Thus, $\Pr[\mathsf{G}_2 \Rightarrow 1] = \Pr[\mathsf{G}_3 \Rightarrow 1]$.

Game G_4 : G_4 is the same as G_3, except that when generating $\mathsf{R}^{(1)}_i$, $\mathcal{C}$ samples $\mathsf{R}^{(1)}_i \leftarrow\!\!\$\ \mathcal{E}(\mathbb{Z}[\sqrt{-p}])$, instead of invoking $\mathsf{R}^{(1)}_i \leftarrow [\mathfrak{g}]^{\Delta k_i} \star ([\mathfrak{g}]^k \star E_i)$.

According to the weak pseudorandomness of CSI-FiSh (cf. Eq. (3)), given elements $\{E_i \leftarrow\!\!\$\ \mathcal{E}(\mathbb{Z}[\sqrt{-p}])\}_{i\in[Q]}$, the distribution of $\{\mathsf{R}^{(1)}_i \leftarrow\!\!\$\ \mathcal{E}(\mathbb{Z}[\sqrt{-p}])\}_{i\in[Q]}$ is

computationally indistinguishable to the distribution of $\{\mathsf{R}_i^{(1)} \leftarrow [\mathfrak{g}]^{\Delta k_i} \star ([\mathfrak{g}]^k \star E_i)$, where $k \leftarrow_\$ \mathbb{Z}_N$. If $\mathcal{A}$ can distinguish G_3 and G_4 with a non-negligible probability, then we can construct a PPT adversary $\mathcal{B}$ to break the weak pseudorandomness of CSI-FiSh. As a result, $|\Pr[\mathsf{G}_3 \Rightarrow 1] - \Pr[\mathsf{G}_4 \Rightarrow 1]| \leq \mathsf{negl}(\lambda)$.

Finally, both $\mathsf{R}_i^{(0)}$ and $\mathsf{R}_i^{(1)}$ are sampled uniformly at random from $\mathcal{E}(\mathbb{Z}[\sqrt{-p}])$ in G_4. Thus, the challenge bit b is completely hidden to $\mathcal{A}$, and $\Pr[\mathsf{G}_4 \Rightarrow 1] = \frac{1}{2}$.

Taking all things together, we obtain the result that $\mathbf{Adv}^{\mathsf{reu}}_{\mathsf{rFE},W,\mathcal{A}}(\lambda) := |\Pr[\mathsf{G}_0 \Rightarrow 1] - 1/2| \leq \mathsf{negl}(\lambda)$. Consequently, Theorem 1 follows. □

5 Efficiency Analysis

Firstly, we show how to instantiate our isgogeny-based rFE scheme $\mathsf{rFE}_{\mathsf{Isogeny}}$.

- For the homomorphic secure sketch, we utilize a syndrome-based secure sketch [15].
- For the average-case strong extractor, we employ the Toeplitz matrix, which is a simple and straightforward tool for extracting uniform strings. Previous works [32,20] also make use of Toplitz matrix as their extractors.
- We implement the CSI-FiSh group action with the code package on GitHub [5].

	Time of SS.Gen (ms)	**Time of** SS.Rec (ms)	**Time of** Ext (ms)	**Time of Sampling** E (ms)	**Time of Group Action** $\star$ (ms)	**Total Time** (ms)
rFE.Gen-256	0.001	–	0.003	147.054	92.587	239.679
rFE.Rep-256	–	0.002	0.003	–	90.243	90.256
rFE.Gen-1024	0.001	–	0.019	153.868	335.611	489.527
rFE.Rep-1024	–	0.003	0.024	–	351.111	351.160

Table 2. Efficiency of our rFE scheme. "rFE.Gen-256 (resp., rFE.Rep-256)" denotes the rFE's generation (resp., reproduction) algorithm processing 256-bit readings of fuzzy source. "rFE.Gen-1024 (resp., rFE.Rep-1024)" denotes the generation (resp., reproduction) algorithm processing 1024-bit readings of fuzzy source. "Time of Algorithms" denotes the average running time of Algorithms, where Algorithms $\in$ {SS.Gen, SS.Rec, Ext, sampling E, group action $\star$}. "Total time" denotes the average running time of a whole rFE's generation or reproduction processing.

Next, we present the efficiency of our scheme with simulated experiments. We consider the fuzzy sources with two cases: one case is 256 bit readings from fuzzy sources, and the other is 1024 bit readings. In our experiments, we test the average running time of each building block and the total processing on platform of Apple M3 Pro. The results are shown in Table 2.

Notice that both our SS and Ext are implemented using information-theoretical cryptographic primitives, resulting in high efficiency. Therefore, the main factors affecting the performance of our scheme lie in the computations involving elliptic curves and group actions. Nevertheless, the total time for a single generation or reproduction process is still low, thanks to the work of [7], which saves us

significant overhead in computing the relation lattice and the reduced basis. Additionally, the random sampling of elliptic curve E in the generation algorithm also consumes considerable time, reflected in more running time of $\mathsf{rFE.Gen}$ than $\mathsf{rFE.Rep}$.

6 Conclusion

In this work, we propose the first isogeny-based reusable fuzzy extractor from CSI-FiSh in the standard model. The proposed rFE scheme is simple, since only one group action is involved in either the rFE's generation algorithm or the reproduction algorithm. Besides, it tolerates linear fraction of errors. Our simulation experiments show that our rFE from CSI-FiSh is practical with running time hundreds of milliseconds. Our work provides the first practical solution to rFE from isogeny.

Acknowledgments. Yu Zhou and Shengli Liu were partially sponsored by Guangdong Major Project of Basic and Applied Basic Research under Grant (No. 2019B030302008), National Natural Science Foundation of China under Grant (No. 61925207) and the National Key R&D Program of China under Grant (No. 2022YFB2701500). Shuai Han was partially supported by National Natural Science Foundation of China under Grant (No. 62372292), and Young Elite Scientists Sponsorship Program by China Association for Science and Technology under Grant (No. YESS20200185).

References

1. Alamati, N., Feo, L.D., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: ASIACRYPT 2020. vol. 12492, pp. 411–439 (2020)
2. Alamélou, Q., Berthier, P., Cachet, C., Cauchie, S., Fuller, B., Gaborit, P., Simhadri, S.: Pseudoentropic isometries: A new framework for fuzzy extractor reusability. In: AsiaCCS 2018. pp. 673–684 (2018)
3. Apon, D., Cho, C., Eldefrawy, K., Katz, J.: Efficient, reusable fuzzy extractors from LWE. In: CSCML 2017. pp. 1–18 (2017)
4. Bennett, C.H., Brassard, G., Robert, J.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
5. Beullens, W.: Csi-fish: Github repository (2019), https://github.com/KULeuven-COSIC/CSI-FiSh/tree/master/implementation
6. Beullens, W., Dobson, S., Katsumata, S., Lai, Y., Pintore, F.: Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In: EUROCRYPT 2022. vol. 13276, pp. 95–126 (2022)
7. Beullens, W., Kleinjung, T., Vercauteren, F.: Csi-fish: Efficient isogeny based signatures through class group computations. In: ASIACRYPT 2019. vol. 11921, pp. 227–247 (2019)
8. Boyen, X.: Reusable cryptographic fuzzy extractors. In: CCS 2004. pp. 82–91. ACM (2004)
9. Briët, J., Perdrix, S.: Quantum computation and information - introduction to the special theme. ERCIM News **2018**(112) (2018)

10. Canetti, R., Fuller, B., Paneth, O., Reyzin, L., Smith, A.D.: Reusable fuzzy extractors for low-entropy distributions. In: EUROCRYPT 2016. vol. 9665, pp. 117–146 (2016)
11. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: EUROCRYPT 2023. vol. 14008, pp. 423–447 (2023)
12. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: ASIACRYPT 2018. vol. 11274, pp. 395–427 (2018)
13. Childs, A.M., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. J. Math. Cryptol. **8**(1), 1–29 (2014)
14. Couveignes, J.M.: Hard homogeneous spaces. IACR Cryptol. ePrint Arch. p. 291 (2006)
15. Dodis, Y., Reyzin, L., Smith, A.D.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: EUROCRYPT 2004. vol. 3027, pp. 523–540 (2004)
16. Feo, L.D., Galbraith, S.D.: Seasign: Compact isogeny signatures from class group actions. In: EUROCRYPT 2019. vol. 11478, pp. 759–789 (2019)
17. Golic, J.D., Baltatu, M.: Entropy analysis and new constructions of biometric key generation systems. IEEE Trans. Inf. Theory **54**(5), 2026–2040 (2008)
18. Herder, C., Yu, M.M., Koushanfar, F., Devadas, S.: Physical unclonable functions and applications: A tutorial. Proc. IEEE **102**(8), 1126–1141 (2014)
19. Jao, D., Feo, L.D.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: PQCrypto 2011. vol. 7071, pp. 19–34 (2011)
20. Jiang, M., Liu, S., Lyu, Y., Zhou, Y.: Face-based authentication using computational secure sketch. IEEE Trans. Mob. Comput. **22**(12), 7172–7187 (2023)
21. Kelkboom, E.J.C., Breebaart, J., Buhan, I., Veldhuis, R.N.J.: Maximum key size and classification performance of fuzzy commitment for gaussian modeled biometric sources. IEEE Trans. Inf. Forensics Secur. **7**(4), 1225–1241 (2012)
22. Lai, Y., Galbraith, S.D., de Saint Guilhem, C.D.: Compact, efficient and uc-secure isogeny-based oblivious transfer. In: EUROCRYPT 2021. vol. 12696, pp. 213–241 (2021)
23. Li, N., Guo, F., Mu, Y., Susilo, W., Nepal, S.: Fuzzy extractors for biometric identification. In: ICDCS 2017. pp. 667–677 (2017)
24. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: EUROCRYPT 2023. vol. 14008, pp. 448–471 (2023)
25. Montgomery, H., Zhandry, M.: Full quantum equivalence of group action dlog and cdh, and more. In: ASIACRYPT 2022. vol. 13791, pp. 3–32 (2022)
26. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. IACR Cryptol. ePrint Arch. p. 145 (2006)
27. Silverman, J.H.: The arithmetic of elliptic curves, Graduate texts in mathematics, vol. 106 (1986)
28. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: DAC 2007. pp. 9–14 (2007)
29. Washington, L.C.: Elliptic curves: number theory and cryptography (2008)
30. Waterhouse, W.C.: Abelian varieties over finite fields. In: Annales scientifiques de l'École normale supérieure. vol. 2, pp. 521–560 (1969)
31. Wen, Y., Liu, S.: Reusable fuzzy extractor from LWE. In: ACISP 2018. vol. 10946, pp. 13–27 (2018)
32. Wen, Y., Liu, S., Han, S.: Reusable fuzzy extractor from the decisional diffie-hellman assumption. Des. Codes Cryptogr. **86**(11), 2495–2512 (2018)