Identity-Based Encryption from e-th Power Residue Symbols

Xiaopeng Zhao[1], Jinwen Zheng[1], Zhenfu Cao[1] **, Xiaolei Dong[1], and Jun Shao[2]

[1] School of Computer Science and Software Engineering, East China Normal University, Shanghai, China
52164500025@stu.ecnu.edu.cn,jinwen.zheng@foxmail.com
zfcao@sei.ecnu.edu.cn,dongxiaolei@sei.ecnu.edu.cn
[2] School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou, China
jshao@zjgsu.edu.cn

Abstract. Designing an identity-based encryption (IBE) scheme supporting additive homomorphism modulo a large integer is not an easy job. At PKC 2019, Clear and McGoldrick (CM) proposed the first such IBE scheme based on the IBE scheme of Boneh, LaVigne and Sabin (BLS). In this paper, we further improve the CM scheme. In particular, 1) we improve the efficiency by removing the evaluation of e-th power residue symbols in the encryption process; when $e = 2$, this modification even makes the encryption considerably efficient than that in Cocks scheme. We also construct an anonymous IBE scheme without sacrificing the encryption speed. 2) our construction widens the BLS scheme and the CM scheme to the case that e is square-free. Furthermore, we have two results that may be of independent interests. 1) We generalize the notable Galbraith's test by introducing the general reciprocity law over function fields. With the help of the generalized Galbraith's test, we show the BLS scheme is not anonymous in general). 2) We also provide some new methods for computing the e-th power residue symbols, which can be used to generalize the public key encryption scheme due to Joye and Libert proposed at CRYPTO 2013.

Keywords: identity-based encryption · e-th power residue symbol · the general reciprocity law over function fields · anonymity.

1 Introduction

Identity-based encryption (IBE), originally proposed by Shamir in 1984 [34], is an extension of the public key encryption. The motivation of IBE is to solve some existing but unavoidable problems in classic public key encryption systems. For example, it substitutes the *Public Key Generator* (PKG) for *Public Key Infrastructure* (PKI), and thus removes the overload of the certificate management. So far, there have been three practical ways to construct IBE; the pairing-based one, the lattice-based one and the *quadratic residuosity* (QR)-based one. In 2001, Boneh and Franklin gave a pairing-based construction of IBE [6], which is a breakthrough work realizing practical IBE. In 2008, Gentry, Peikert and Vaikuntanathan proposed a lattice-based IBE [20]. These two constructions have been extended to substantial cryptographic schemes that support different access controls. Back towards the year 2001, Clifford Cocks came up with a totally different construction of IBE [16], whose security relies on the *standard QR assumption*. Its encryption solely includes several operations modulo an RSA modulus and two evaluations of the Jacobi symbol. As we all know, QR-based IBE is more efficient than the lattice-based one. In addition, it is additively homomorphic, supporting an unbounded number of homomorphic operations. Although additively homomorphic pairing-based IBE can be transformed from a multiplicatively homomorphic one, the number of operations is bounded. Due to its unique functionality, QR-based IBE captures some researchers' attention. However, Cocks scheme encrypts one bit plaintext into a ciphertext composed of a pair of two large integers, and hence is used to encrypt short session keys in practice. Intuitively, encryption of more than one bit at a time can be achieved by introducing higher-power residue symbols.

1.1 Related Work

The notion of *key-privacy* was put forward by Bellare *et al.* [4] as an additional security requirement of an encryption scheme; if an adversary learns nothing about the identity of a ciphertext, we call this scheme anonymous. Halevi gave a sufficient condition for *key-privacy* in a short note [22]. In 2005, Abdalla *et*

** Corresponding author

al. [1] led into the conception of AIBE (Anonymous Identity-Based Encryption). Cocks scheme is known not to be anonymous due to the test developed by Galbraith [5]. In 2007, Boneh, Gentry and Hamburg [7] addressed the ciphertext expansion issue and *anonymity* issue, they designed an anonymous IBE system (BGH) which merely expands an ℓ-bit plaintext to a ciphertext about a size of $\ell + \log_2 N$. However, the encryption in their scheme is not efficient. In [24], Jhanwar and Barua presented a scheme which is more time efficient, but larger ciphertext expansion than BGH scheme. Next, Susilo *et al.* [18] gave an improvement of Jhanwar-Barua scheme. However, neither of the two schemes are IND-ID-CPA secure due to the security flaw discovered by Schipor [33].

In 2013, Clear, Hughes, and Tewari [14] considered Cocks scheme over the polynomial quotient ring $\mathbb{Z}_N[x]/(x^2 - R_{id})$ because it is natural and convenient to view ciphertexts as elements in it. With the help of this sharp observation, they constructed a strongly XOR-homomorphic IBE scheme. In the same year, Boneh, LaVigne and Sabin [8] generalized Cocks scheme to e^{th} residuosity so that it can encrypt more than one bit in a message. The downside of this generalization is that the ciphertext expansion is massive, which is intractable to optimize yet because any intuitive attempt of compression fails to be secure due to the attack found by Boneh, LaVigne and Sabin [14]. Recently, Clear and McGoldrick [15] extended BLS scheme so that it can use a hash function which can be securely instantiated.

Constructing cryptosystems from higher-power residue symbols has been explored in several studies by researchers. For example, Cao [10] proposed a type of extension of the Goldwasser-Micali QR-based cryptosystem [21]. His scheme is based upon k^{th}-power residues and enables segment encryption instead of bit encryption. In 2013, Joye and Libert [26] revisited the Goldwasser-Micali QR-based cryptosystem using 2^k-th power residue symbols and described a more efficient lossy trapdoor function based upon the k-QR assumption, k-Squared Jacobi Symbol assumption and DDH assumption. Subsequently, Cao [11] proposed a type of extension of Joye-Libert cryptosystem based upon k^{th}-power residues. The extended scheme is more efficient than Joye-Libert cryptosystem in decryption speed. Recently, Brier *et al.* [9] introduced new $p^r q$-based one-way functions and companion signature schemes which replace the Jacobi symbol with higher-power residue symbols.

1.2 Our Contributions

In this work, we investigate BLS scheme [8] as well as CM scheme [15], and make the following contributions.

Our first contribution is to improve these two schemes in the following two aspects:

1. We omit the superfluous computation of e-th power residue symbols, a very time-consuming part in the encryption phase of BLS scheme. Also, this modification does not influence the security. It is worth mentioning that in the case $e = 2$, our improved scheme can be *anonymous* and is much more efficient in encryption, while its ciphertext extension is increased by a factor of 2, compared with Cocks scheme.
2. In BLS scheme, e must be a prime number. We leverage knowledge of classical number theory to extend BLS scheme to the case e is a square-free number, which strengthens its flexibility.

Our second contribution is to reformulate the analyses on the incompressibility of BLS scheme in [8] rigorously by introducing the general reciprocity law over function fields. Applying this technique, we fully generalize the famous Galbraith's test to the case $e > 2$ and show that BLS scheme is not anonymous in general.

Our third contribution is to provide methods for computing e-th power residue symbols. We correct a theorem proposed in [19] and give an analogous conclusion with the same effect. Furthermore, we focus on computing e-th power residue symbols in a particular condition. The results can be utilized to extend Joye-Libert cryptosystem [26].

2 Preliminaries

2.1 Notations

If X is a finite set, the notation $\#X$ means the cardinality of X, writing $x \xleftarrow{\$} X$ to indicate that x is an element sampled from the uniform distribution over X. If $\mathscr{A}$ is an algorithm, then we write $x \leftarrow \mathscr{A}(y)$

to mean: "run $\mathscr{A}$ on input y and the output is assigned to x". PPT is short for "probabilistic polynomial time".

For a group $\mathbb{G}$, the subgroup of $\mathbb{G}$ generated by the set X is denoted by $\langle X \rangle$. If R is a ring, $a, b \in R$ and $\mathfrak{I}$ is an ideal of R, the relation $a - b \in \mathfrak{I}$ is written $a \equiv b \ (\mathfrak{I})$. A finite field of size q is denoted by $\mathbb{F}_q$. For a polynomial f, we denote as $deg(f) = n$ to say f has degree n. log stands for the binary logarithm. $\left(\frac{\cdot}{\cdot}\right)$ stands for Jacobi symbol. φ denotes the Euler's totient function.

2.2 Identity-Based Encryption

An identity-based encryption scheme is defined as a tuple of PPT algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

$\mathsf{Setup}(\mathbf{1}^\lambda)$ The setup algorithm Setup is a randomized algorithm that takes a security parameter $\mathbf{1}^\lambda$ as input, and outputs a tuple (mpk, msk), where the mpk denotes the public parameters and msk denotes the master secret key.

$\mathsf{KeyGen}\,(mpk, msk, id)$ The key generation algorithm KeyGen is a deterministic algorithm that takes msk and an identity id as inputs, and outputs a decryption key sk_{id} associated with the identity id.

$\mathsf{Enc}\,(mpk, id, m)$ The encryption algorithm Enc is a randomized algorithm that takes mpk, id and a plaintext m as inputs, and outputs a ciphertext c. That is, we encrypt plaintext m with an identity id and achieve a ciphertext c.

$\mathsf{Dec}(mpk, sk_{id}, c)$ The decryption algorithm Dec is a deterministic algorithm that takes mpk, sk_{id}, c as inputs, and outputs the corresponding plaintext m if c is a valid ciphertext, and $\perp$ otherwise.

2.3 Security Notions

Correctness The *correctness* property states that any valid ciphertext can be decrypted to recover the corresponding plaintext. For a formal definition, we denotes $\mathsf{M}, \mathsf{ID}, \mathsf{C}$ as the plaintext space, the identity space and the ciphertext space respectively. An IBE scheme $\Sigma = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is said *correct* if $\forall m \in \mathsf{M},\ \forall id \in \mathsf{ID}$, it satisfies

$$\Pr[\mathsf{Dec}\,(mpk, sk_{id}, \mathsf{Enc}\,(mpk, id, m)) = m] = \mathbf{1}.$$

where mpk, id, sk_{id} are obtained from Setup and KeyGen.

Semantic Security The semantic security property states that it is infeasible for any adversary with the limited computation ability to get any information of plaintext if it is given the corresponding ciphertext. The behaviors of an adversary $\mathcal{A}$ can be simulated by a pair of probabilistic PPT algorithms $(\mathcal{A}_1, \mathcal{A}_2)$. The game between the adversary and the challenger contains the following five phases:

Initialization phase: The challenger runs the algorithm Setup and keeps the master secret key msk and gives the public parameters mpk to the adversary.

The first query phase: After receiving mpk, the adversary chooses a subset $\mathsf{ID_1} \subseteq \mathsf{ID}$ and issues the key generation queries and obtains the private key corresponding to each identity in $\mathsf{ID_1}$. The queries can be asked adaptively so the adversary can update and enrich its knowledge about the scheme, which is denoted by the state s.

Challenge phase: The adversary chooses a challenge identity $id^* \notin \mathsf{ID_1}$ and two different plaintexts $m_{\mathbf{0}},\ m_{\mathbf{1}} \in \mathsf{M}$ of the same length. It sends them to the challenger.

The second query phase: This phase is the same as *the first query phase* except that the query identity subset $\mathsf{ID_2} \subseteq \mathsf{ID}$ cannot contain id^*.

Guess phase: The challenger chooses a random bit b and encrypts m_b with mpk, id^*. It then sends the corresponding ciphertext $c \in \mathsf{C}$ to the adversary. The adversary tries to guess the bit b. It wins the game (carries a successful attack) if the guess is right.

Formally, an IBE scheme Σ is said to be semantically secure if

$$\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\Sigma}(\lambda) = \left| \Pr \left[\begin{array}{l} (mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda) \\ (id^*, m_0, m_1, s) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(mpk,msk,\cdot)} \\ b \xleftarrow{\$} \{0,1\},\ c \leftarrow \mathsf{Enc}(mpk, id^*, m_b) \end{array} : \mathcal{A}_2^{\mathsf{KeyGen}(mpk,msk,\cdot)}(s,c) = b \right] - \frac{1}{2} \right|$$

is negligible, where $\mathcal{A}_1$ denotes the behaviors of the adversary in two query phases and in the *Challenge phase*, $\mathcal{A}_2$ denotes the behaviors of the adversary in the *Guess phase*. Because the adversary can adaptively choose the challenge identity and challenge plaintexts and attempts to distinguish them, the semantic security can also be called indistinguishable chosen-identity chosen-plaintext security (IND-ID-CPA).

Anonymity Generally, an IND-ID-CPA secure IBE scheme may not possess *anonymity*. To formally define this property combined with IBE, we should modify the behaviors of $\mathcal{A}$ in the last three phases as:

Challenge phase: The adversary chooses two different challenge identities id_0^*, $id_1^* \notin \mathsf{ID}_1$ and a plaintext $m \in \mathsf{M}$. It sends them to the challenger.

The second query phase: This phase is the same as *the first query phase* except that the query identity subset $\mathsf{ID}_2 \subseteq \mathsf{ID}$ cannot contain id_0^* and id_1^*.

Guess phase: The challenger chooses a random bit b and encrypts $r \xleftarrow{\$} \mathsf{M}$ ($|r|_2 = |m|_2$) with mpk, id_b^*. It then sends the corresponding ciphertext $c \in \mathsf{C}$ to the adversary. The adversary tries to guess the bit b. It wins the game (carries a successful attack) if the guess is right.

Formally, an IND-ID-CPA secure IBE scheme Σ is said to be *anonymous* (ANO-IND-ID-CPA) if

$$\mathsf{Adv}^{\mathsf{ANO\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\Sigma}(\lambda) = \left| \Pr \left[\begin{array}{l} (mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^\lambda) \\ (id_0^*, id_1^*, m, s) \leftarrow \mathcal{A}_1^{\mathsf{KeyGen}(mpk,msk,\cdot)} \\ b \xleftarrow{\$} \{0,1\},\ r \xleftarrow{\$} \mathsf{M}\ (|r|_2 = |m|_2) \\ c \leftarrow \mathsf{Enc}(mpk, id_b^*, r) \end{array} : \mathcal{A}_2^{\mathsf{KeyGen}(mpk,msk,\cdot)}(s,c) = b \right] - \frac{1}{2} \right|$$

is negligible.

2.4 e-th Power Residue Symbol

Let K be a number field, and $\mathcal{O}_K$ be the ring of integers in K, and $e \geq 1$ be an integer. We say a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is relatively prime to e if $\mathfrak{p} \nmid e\mathcal{O}_K$. It is easy to see that $\mathfrak{p}$ is relatively prime to e if and only if $\gcd(q, e) = 1$, where $q = p^f = \mathrm{Norm}(\mathfrak{p})$ for some $f \in \mathbb{N}$. For every $\alpha \in \mathcal{O}_K$, $\alpha \notin \mathfrak{p}$, we have

$$\alpha^{q-1} \equiv 1 \pmod{\mathfrak{p}}$$

Let $\zeta_e = \exp(2\pi i/e)$ be an e-th root of unity. If $\zeta_e \in K$ and $\mathfrak{p}$ is relatively prime to e, the order of the subgroup of $\left(\frac{\mathcal{O}_K}{\mathfrak{p}}\right)^\times$ generated by $\zeta_e \bmod \mathfrak{p}$ is e. This indicates that e divides $q-1$, hence we can define the e-th power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_e$ as follows:

1. $\left(\frac{\alpha}{\mathfrak{p}}\right)_e = 0$ if $\alpha \in \mathfrak{p}$.
2. If $\alpha \notin \mathfrak{p}$, $\left(\frac{\alpha}{\mathfrak{p}}\right)_e$ is the unique e-th root of unity such that $\alpha^{\frac{\mathrm{Norm}(\mathfrak{p})-1}{e}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_e \pmod{\mathfrak{p}}$.

Next, we extend the symbol multiplicatively to all ideals. Suppose $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal prime to e. Let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m$ be the prime decomposition of $\mathfrak{a}$. For $\alpha \in \mathcal{O}_K$ define $\left(\frac{\alpha}{\mathfrak{a}}\right)_e = \prod_{i=1}^m \left(\frac{\alpha}{\mathfrak{p}_i}\right)_e$. If $\beta \in \mathcal{O}_K$ and

β is prime to e, we define $\left(\frac{\alpha}{\beta}\right)_e = \left(\frac{\alpha}{(\beta)}\right)_e$. See [23, 28, 29] for more properties about e-th power residue symbols.

From here on we only consider the case $K = \mathbb{Q}(\zeta_e)$. It's well-known that $\mathcal{O}_K = \mathbb{Z}[\zeta_e]$. Let $N = pq$ be a product of two distinct primes satisfying $p \equiv \mathtt{1} \pmod{e}$, $q \equiv \mathtt{1} \pmod{e}$, then both p and q split completely in K. Suppose that $\mu \in \mathbb{Z}_N^*$ is a primitive e-th root of unity modulo p and modulo q, we say it a *non-degenerate* primitive e-th root of unity modulo N. The following lemma is crucial for the instance of schemes based upon higher-power residue.

Lemma 1 (Freeman *et al.* [19]). *Let e be a positive integer, $N = pq$ be a product of two distinct primes p, q with $p \equiv q \equiv \mathtt{1}$ mod e. Let $\mu \in \mathbb{Z}_N^*$ be a* non-degenerate *primitive e-th root of unity modulo N. For each $i \in \mathbb{Z}_e^*$, let $\mathfrak{a}_i = N\mathcal{O}_K + (\zeta_e - \mu^i)\mathcal{O}_K$, $\mathfrak{p}_i = p\mathcal{O}_K + (\zeta_e - \mu^i)\mathcal{O}_K$ and $\mathfrak{q}_i = q\mathcal{O}_K + (\zeta_e - \mu^i)\mathcal{O}_K$. Then, we have* $\mathrm{Norm}(\mathfrak{a}_i) = N$, $\mathfrak{a}_i = \mathfrak{p}_i\mathfrak{q}_i$ *for each $i \in \mathbb{Z}_e^*$ and $p\mathcal{O}_K = \prod_{i\in\mathbb{Z}_e^*} \mathfrak{p}_i$, $q\mathcal{O}_K = \prod_{i\in\mathbb{Z}_e^*} \mathfrak{q}_i$, $N\mathcal{O}_K = \prod_{i\in\mathbb{Z}_e^*} \mathfrak{a}_i$.*

3 Security Assumption and Properties of e-th Power Residue Symbols

In this section, we define the security assumption related to our new schemes and prove some properties about e-th power residue symbols.

3.1 Security Assumption

For a better understanding of the schemes based upon higher-power residue, we first give definitions of the notations to be used. Then, we describe the security assumption our proposed schemes rely on.

We define a function $\mathscr{J}_{N,e} : \mathbb{Z}_N \mapsto \{\mathtt{0}, \ldots, e - \mathtt{1}\}$ as follows:

$$\mathscr{J}_{N,e}(x) = \begin{cases} \mathtt{0}, & \text{if } \gcd(x, N) \neq \mathtt{1}; \\ i, & \text{if } \gcd(x, N) = \mathtt{1} \text{ and } \left(\frac{x}{\mathfrak{a}_\mathtt{1}}\right)_e = \zeta_e^i. \end{cases}$$

It is easy to check that, if $x, y \in \mathbb{Z}_N^*$, then $\mathscr{J}_{N,e}(xy) = \mathscr{J}_{N,e}(x)\,\mathscr{J}_{N,e}(y)$.

Squirrel [37] gave a polynomial algorithm with expensive precomputations to compute the e-th power residue symbols. Although Boer [17] managed to propose an improved algorithm that does not rely on heavy precomputations and runs fast in experiments, he could not give a rigorous proof to verify that it runs in polynomial time.

For $e \geq \mathtt{2}$, we say an integer $x \in \mathbb{Z}_N^*$ is an *e-th residue* modulo N if there exists an integer $y \in \mathbb{Z}_N^*$ such that $y^e \equiv x \pmod{N}$. Note that if x is an *e-th residue*, then $\left(\frac{x}{\mathfrak{p}_i}\right)_e = \left(\frac{x}{\mathfrak{q}_i}\right)_e = \mathtt{1}$ holds for each $i \in \mathbb{Z}_e^*$. We denote the set of all *e-th residues* in $\mathbb{Z}_N^*$ by $\mathcal{ER}_{N,e}$. Correspondingly, $\mathcal{J}_{N,e}^k$ is denoted as

$$\mathcal{J}_{N,e}^k = \begin{cases} \left\{ x \in \mathbb{Z}_N^* \;\middle|\; \left(\frac{x}{\mathfrak{a}_\mathtt{1}}\right)_e = \mathtt{1} \right\} & k = \mathtt{0}; \\ \left\{ x \in \mathbb{Z}_N^* \;\middle|\; \left(\frac{x}{\mathfrak{a}_\mathtt{1}}\right)_e = \mathtt{1},\ \left(\frac{x}{\mathfrak{p}_\mathtt{1}}\right)_e \text{ and } \left(\frac{x}{\mathfrak{q}_\mathtt{1}}\right)_e \text{ are primitive} \right\} \bigcup \mathcal{ER}_{N,e} & k = \mathtt{1}. \end{cases}$$

We alter the *MER assumption* defined in [8] as follows.

Definition 1 (Modified e-th Residue (MER_e^i, $i \in \{\mathtt{0}, \mathtt{1}\}$) Assumption). *A* PPT *algorithm* $\mathsf{RSAgen}(\lambda)$ *generates two equally sized primes p, q and a square-free integer e such that $p \equiv q \equiv \mathtt{1}$ mod e and* $\gcd(\frac{p+q-\mathtt{2}}{e}, e) = \mathtt{1}$, *then picks a random number $u \in \mathcal{J}_{N,e}^i \setminus \mathcal{ER}_{N,e}$ and $\mu \in \mathbb{Z}_N^*$ a* non-degenerate *primitive e-th root of unity to $N = pq$. We define the following two distributions relative to* $\mathsf{RSAgen}(\lambda)$ *as:*

$$\mathbb{D}_{ER}^i : \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\lambda),\ v \xleftarrow{\$} \mathcal{ER}_{N,e} \right\}$$

$$\mathbb{D}_{ENR}^i : \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\lambda),\ v \xleftarrow{\$} \mathcal{J}_{N,e}^i \setminus \mathcal{ER}_{N,e} \right\}$$

The MER_e^i *assumption relative to* $\mathsf{RSAgen}(\lambda)$ *asserts that the advantage* $\mathsf{Adv}^{\mathsf{MER}_e^i}_{\mathcal{A},\mathsf{RSAgen}}(\lambda)$ *defined as*

$$\left|\Pr\left[\mathcal{A}(N,v,e,\mu,u)=\mathtt{1}\;\middle|\;(N,v,e,\mu)\xleftarrow{\$}\mathbb{D}^i_{ER}(\lambda)\right]-\Pr\left[\mathcal{A}(N,v,e,\mu,u)=\mathtt{1}\;\middle|\;(N,v,e,\mu)\xleftarrow{\$}\mathbb{D}^i_{ENR}(\lambda)\right]\right|$$

is negligible for any PPT *adversary* $\mathcal{A}$.

Both of the two assumptions are natural extensions to the *standard QR assumption* [25] (when $e=\mathtt{2}$, we have $\zeta_{\mathtt{2}}=\mu=-\mathtt{1}$, so $\mathsf{MER}_{\mathtt{2}}^{\mathtt{0}}=\mathsf{MER}_{\mathtt{2}}^{\mathtt{1}}$ are equivalent to the *standard QR assumption* except for the choices of the RSA modulus and u). Therefore, we believe that it is intractable to break both of them. Obviously, $\mathsf{MER}_e^{\mathtt{1}}$ implies $\mathsf{MER}_e^{\mathtt{0}}$. The next subsection may be helpful for illuminating the relation between the two assumptions.

3.2 Properties of e-th Power Residue Symbols

Now, we investigate more properties of e-th power residue symbols.

Theorem 1. $\#\mathcal{J}^{\mathtt{0}}_{N,e}=\dfrac{\varphi(N)}{e},\ \#\mathcal{J}^{\mathtt{1}}_{N,e}=(\varphi(e)+\mathtt{1})\dfrac{\varphi(N)}{e^{\mathtt{2}}}$

Proof. Let $\mathscr{U}=\left\{\mathtt{1},\zeta_e,\ldots,\zeta_e^{e-\mathtt{1}}\right\}$ denotes the subgroup of roots of unity in $\mathcal{O}_K$. The map $\theta:\mathbb{Z}_p^*\to\mathscr{U}$ given by $x\mapsto\left(\dfrac{x}{\mathfrak{p}_{\mathtt{1}}}\right)_e$ is an homomorphism. Let

$$\mathcal{ER}_{p,e}=\left\{y\in\mathbb{Z}_p^*\mid y\equiv x^e \bmod p \text{ for some } x\in\mathbb{Z}_p^*\right\}$$

be the subgroup composed of *e-th residues* in $\mathbb{Z}_p^*$. It's an easy matter to check that the cardinality of $\mathcal{ER}_{p,e}$ is $\dfrac{p-\mathtt{1}}{e}$. Therefore, an integer $z\in\mathbb{Z}_p^*$ satisfying $\left(\dfrac{z}{\mathfrak{p}_{\mathtt{1}}}\right)_e=\mathtt{1}$ must be in $\mathcal{ER}_{p,e}$. Hence the kernel of θ is exactly $\mathcal{ER}_{p,e}$ and we have the following isomorphic

$$\frac{\mathbb{Z}_p^*}{\mathcal{ER}_{p,e}}\ \cong\ \mathscr{U}$$

due to the equality of cardinality. Of course, elements in different cosets of $\mathcal{ER}_{p,e}$ in $\mathbb{Z}_p^*$ have different e-th power residue symbols, whence there is a one to one correspondence between cosets of $\mathcal{ER}_{p,e}$ in $\mathbb{Z}_p^*$ and e-th roots of unity via the e-th power residue symbol. Note that the above arguments are also valid for $\mathbb{Z}_q^*$. As a result, we derive

$$\#\mathcal{J}^{\mathtt{0}}_{N,e}=e\frac{\varphi(N)}{e^{\mathtt{2}}}=\frac{\varphi(N)}{e}$$
$$\#\mathcal{J}^{\mathtt{1}}_{N,e}=(\varphi(e)+\mathtt{1})\frac{\varphi(N)}{e^{\mathtt{2}}}$$

■

We are now in a position to describe the core theorem to the follow-up security proof.

Theorem 2. *Let* e *be a prime number,* $t\in\mathbb{Z}_N^*$ *a transport key,* R *an element in* $\mathbb{Z}_N^*$ *such that* $\left(\dfrac{R}{\mathfrak{p}_{\mathtt{1}}}\right)_e=\zeta_e^{i_R}$, $\left(\dfrac{R}{\mathfrak{q}_{\mathtt{1}}}\right)_e=\zeta_e^{j_R}$ *where* i_R, j_R *are relatively prime to* e. *If* $c(x)=\dfrac{f(x)^e}{t}\ mod\ (x^e-R)$ *for some* $f(x)\xleftarrow{\$}\mathbb{Z}_N^*[x]$ *is a polynomial of degree* $e-\mathtt{1}$, *then the sets*

$$\Omega_k=\left\{g(x)\in\mathbb{Z}_N^*[x]\;\middle|\;\deg g(x)=e-\mathtt{1},\ \frac{g(x)^e}{k}\ mod\ (x^e-R)=c(x)\right\}$$

are of the same cardinality for each transport key $k\in\mathbb{Z}_N^*$.

Proof. Consider the two sets $\Omega_t, \Omega_{\bar{t}}$, to prove the theorem, it suffices to prove that $\#\Omega_t = \#\Omega_{\bar{t}}$ for any $\bar{t} \in \mathbb{Z}_N^*$. Suppose that $\left(\frac{t\bar{t}^{-1}}{\mathfrak{p}_1}\right)_e = \zeta_e^{i_t}, \left(\frac{t\bar{t}^{-1}}{\mathfrak{q}_1}\right)_e = \zeta_e^{j_t}$. Since

$$\left(\frac{R^{i_R^{-1} i_t}}{\mathfrak{p}_1}\right)_e = \left(\frac{t\bar{t}^{-1}}{\mathfrak{p}_1}\right)_e, \quad \left(\frac{R^{j_R^{-1} j_t}}{\mathfrak{q}_1}\right)_e = \left(\frac{t\bar{t}^{-1}}{\mathfrak{q}_1}\right)_e,$$

by the proof of Theorem 1, there exist $W_p \in \mathbb{Z}_p^*$ and $W_q \in \mathbb{Z}_q^*$ such that

$$W_p^e R^{i_R^{-1} i_t} \equiv t\bar{t}^{-1} \pmod{p}, \quad W_q^e R^{j_R^{-1} j_t} \equiv t\bar{t}^{-1} \pmod{q}.$$

According to the Chinese remainder theorem, we have

$$\frac{\mathbb{Z}_N[x]}{(x^e - R)} \cong \frac{\mathbb{Z}_p[x]}{(x^e - R)} \oplus \frac{\mathbb{Z}_q[x]}{(x^e - R)}.$$

Therefore, the map $\phi : \Omega_t \to \Omega_{\bar{t}}$ given by $h(x) \mapsto g(x)$ where

$$g(x) \equiv W_p x^{i_R^{-1} i_t} h(x) \pmod{p}$$
$$g(x) \equiv W_q x^{j_R^{-1} j_t} h(x) \pmod{q}$$

is well defined for a fixed $\bar{t}$. In the other direction, the inverse map $\psi : \Omega_{\bar{t}} \to \Omega_t$ is given by $g(x) \mapsto h(x)$ where

$$h(x) \equiv W_p^{-1} \left(R^{-1} x^{e-1}\right)^{i_R^{-1} i_t} g(x) \pmod{p}$$
$$h(x) \equiv W_q^{-1} \left(R^{-1} x^{e-1}\right)^{j_R^{-1} j_t} g(x) \pmod{q}$$

It is straightforward to verify $\psi \circ \phi = \mathbf{1}_{\Omega_t}$ and $\phi \circ \psi = \mathbf{1}_{\Omega_{\bar{t}}}$ where $\mathbf{1}_{\Omega_t}$ and $\mathbf{1}_{\Omega_{\bar{t}}}$ denote the identity maps on Ω_t and on $\Omega_{\bar{t}}$ respectively. ■

We close this section by showing that the precondition of Proposition 4.3 proposed in [19] can be relaxed as follows.

Proposition 1. *Let e be an integer. Let $N = pq$ where $p \equiv q \equiv 1 \pmod{e}$. Suppose that $\gcd(\frac{p-1}{e}, e) = \gcd(\frac{q-1}{e}, e)$. Then there is a ν such that*

1. *ν is a* non-degenerate *primitive e-th root of unity modulo N.*
2. *$\left(\frac{\nu}{\mathfrak{a}_i}\right)_e = 1$ for every ideal $\mathfrak{a}_i \subset \mathcal{O}_K$ as in Lemma 1.*

Proof. The condition $\gcd(\frac{p-1}{e}, e) = \gcd(\frac{q-1}{e}, e)$ implies that there exist integers s_p, t_p, s_q, t_q such that $s_p \frac{p-1}{e} + t_p e = s_q \frac{p-1}{e} + t_q e$. Let $\mu_p = \mu \bmod p$ and $\mu_q = \mu \bmod q$. Observe that every primitive e-th root of unity in $\mathbb{Z}_p$ has the form μ_p^i for some $i \in \mathbb{Z}_e^*$. It follows that

$$\left(\frac{\mu_p^{s_p}}{\mathfrak{p}_1}\right)_e = \left(\frac{\zeta_e^{s_p}}{\mathfrak{p}_1}\right)_e = \zeta_e^{\frac{p-1}{e} s_p}$$

Similarly,

$$\left(\frac{\mu_q^{-s_q}}{\mathfrak{q}_1}\right)_e = \left(\frac{\zeta_e^{-s_q}}{\mathfrak{q}_1}\right)_e = \zeta_e^{-\frac{q-1}{e} s_q}$$

Hence, letting ν be the integer congruent to $\mu_p^{s_p}$ modulo p and $\mu_q^{-s_q}$ modulo q. Then,

$$\left(\frac{\nu}{\mathfrak{a}_1}\right)_e = \left(\frac{\nu}{\mathfrak{p}_1}\right)_e \left(\frac{\nu}{\mathfrak{q}_1}\right)_e = \zeta_e^{s_p \frac{p-1}{e} - s_q \frac{q-1}{e}} = 1$$

Since $\nu \in \mathbb{Z}$, the result $\left(\frac{\nu}{\mathfrak{a}_i}\right)_e = 1$ follows from Galois-equivalence of the e-th power residue symbol. ■

4 Identity-Based Encryption from e-th Power Residue Symbols

BLS scheme naturally generalizes Cocks scheme to e-th residuosity so that it encrypts more than one bit at a time, whereas it is less efficient and bandwidth-wise than Cocks scheme. In this section, we first review BLS scheme. Then, we present a scheme that makes the encryption much more efficient than BLS scheme's, and even than Cocks scheme's. Our scheme also enables BLS scheme to support the case e is square-free.

4.1 Review of BLS Scheme

We now describe the IBE scheme presented by Boneh, LaVigne and Sabin [8]. The scheme allows encrypting multiple bits at a time.

$\mathsf{Setup}(\mathtt{1}^\lambda)$ Given a security parameter λ, Setup selects a prime e, then generates an RSA modulus $N = pq$ a product of two large primes p and q such that $e \mid p-\mathtt{1}, e \mid q-\mathtt{1}$. The public parameters are $mpk = \{N, e, \mu, \mathscr{H}\}$ where μ is a *non-degenerate* primitive e-th root of unity in $\mathbb{Z}_N$, $\mathscr{H}$ is a publicly available cryptographic hash function mapping an arbitrary binary string to an *e-th residue* in $\mathbb{Z}_N^*$. The master secret key is $msk = \{p, q\}$.

$\mathsf{KeyGen}(mpk, msk, id)$ Using the hash function $\mathscr{H}$ and p, q, KeyGen sets $R_{id} = \mathscr{H}(id)$, then calculates $r_{id} = \mathscr{H}(id)^{\frac{1}{e}} \mod N$. Finally, KeyGen returns $sk_{id} = \{r_{id}\}$ as user's private key.

$\mathsf{Enc}(mpk, id, m)$ To encrypt a message $m \in \{\mathtt{0}, \ldots, e-\mathtt{1}\}$ for a user with identity id, Enc derives the hash value $R_{id} = \mathscr{H}(id)$. It then chooses a random polynomial f of degree $e-\mathtt{1}$ from $\mathbb{Z}_N[x]$ and calculates $g(x) = f(x)^e \mod (x^e - R_{id}) = \sum_{i=\mathtt{0}}^{e-\mathtt{1}} a_i x^i$. Next, it chooses a transport key $t \xleftarrow{\$} \mathbb{Z}_N^*$. The returned ciphertext is

$$C = \left\{ \frac{a_{\mathtt{0}}}{t}, \frac{a_{\mathtt{1}}}{t}, \ldots, \frac{a_{e-\mathtt{1}}}{t}, (m + \mathscr{J}_{N,e}(t)) \mod e \right\}.$$

$\mathsf{Dec}(mpk, sk_{id}, C)$ When a user with $sk_{id} = \{r_{id}\}$ receives a ciphertext set C, it parses C as $\{c_{\mathtt{0}}, c_{\mathtt{1}}, \ldots, c_{e-\mathtt{1}}, c\}$, Dec recovers the plaintext m as

$$m = \left(\mathscr{J}_{N,e} \left(\sum_{i=\mathtt{0}}^{e-\mathtt{1}} c_i r_{id}^i \right) + c \right) \pmod e$$

Remark 1. BLS scheme ingeniously extends Cocks scheme to higher-power residue case. To understand the point just pick $e = \mathtt{2}$ and $f(x) = t + x$ with $\left(\frac{t}{N}\right) = (-\mathtt{1})^m$, the ciphertext polynomial is $\frac{g(x)}{t} = t + \frac{R_{id}}{t} + \mathtt{2}x$, which agrees with the construction of Cocks scheme.

Remark 2. In Cocks scheme, the PKG can easily derive a user's secret key by several efficient probabilistic algorithms taking square roots in finite fields, such as Cipolla-Lehmer [27] algorithm, Tonelli-Shanks [35] algorithm and Adleman-Manders-Miller [2] algorithm. Fortunately, these methods can also be applied to general situations, e.g. [12], the extended Adleman-Manders-Miller algorithm can extract an e-th root modulo a prime p in $\mathcal{O}\left(\log^4 p + e \log^3 p\right)$ time complexity.

Since it's tough to implement such a hash function $\mathscr{H}$ without leaking information about msk, BLS scheme was not given a formally security proof in the original paper. In [15], the authors proposed an approach which is akin to Cocks scheme to circumventing the issue, but at the cost of a lower efficiency and a larger ciphertext extension.

4.2 Our IBE Scheme

We perceive that it is redundant to compute e-th power residue symbols during the encryption process in BLS scheme. To clearly describe our improved scheme with this method, we first give the construction in the specific case $e = \mathtt{2}$ (also is the most commonly used), namely $\Pi_{\mathtt{2}}$, and make a comparison of $\Pi_{\mathtt{2}}$ and Cocks scheme.

Construction in the Case $e = 2$

$\mathsf{Setup}(\mathbf{1}^\lambda)$ Given a security parameter λ, Setup generates an RSA modulus $N = pq$ a product of two distinct large primes p and q such that $\frac{p+q}{2}$ is even and an element $u \in \mathcal{J}^{\mathbf{0}}_{N,\mathbf{2}} \setminus \mathcal{ER}_{N,\mathbf{2}}$. The public parameters are $mpk = \{N, u, \mathscr{H}\}$ where $\mathscr{H}$ is a publicly available cryptographic hash function mapping an arbitrary binary string to $\mathcal{J}^{\mathbf{0}}_{N,\mathbf{2}}$. The master secret key is $msk = \{p, q\}$.

$\mathsf{KeyGen}(mpk, msk, id)$ Using the hash function $\mathscr{H}$ and p, q, KeyGen sets $R_{id} = \mathscr{H}(id)$. If $R_{id} \in \mathcal{ER}_{N,\mathbf{2}}$, KeyGen calculates $r_{id} = \mathscr{H}(id)^{\frac{1}{2}} \mod N$; otherwise it calculates $r_{id} = (u\mathscr{H}(id))^{\frac{1}{2}} \mod N$. Finally, KeyGen returns $sk_{id} = \{r_{id}\}$ as user's private key.

$\mathsf{Enc}(mpk, id, m)$ To encrypt a message $m \in \{\mathtt{0}, \mathtt{1}\}$ for a user with identity id, Enc derives the hash value $R_{id} = \mathscr{H}(id)$. It then chooses two random polynomials $f_{\mathbf{1}}, f_{\mathbf{2}}$ of degree $\mathbf{1}$ from $\mathbb{Z}_N[x]$ and calculates $g_{\mathbf{1}}(x) = f_{\mathbf{1}}(x)^{\mathbf{2}} \mod (x^2 - R_{id}) = a_{\mathbf{1}}x + a_{\mathbf{0}}$ and $g_{\mathbf{2}}(x) = f_{\mathbf{2}}(x)^{\mathbf{2}} \mod (x^2 - uR_{id}) = b_{\mathbf{1}}x + b_{\mathbf{0}}$. The returned ciphertext is

$$C = \begin{cases} \{a_{\mathbf{0}}, a_{\mathbf{1}}, b_{\mathbf{0}}, b_{\mathbf{1}}\}, & \text{if } m = \mathbf{0}; \\ \{N - a_{\mathbf{0}}, N - a_{\mathbf{1}}, N - b_{\mathbf{0}}, N - b_{\mathbf{1}}\}, & \text{if } m = \mathbf{1}. \end{cases}$$

$\mathsf{Dec}(mpk, sk_{id}, C)$ When a user with $R_{id} = \mathscr{H}(id)$ and $sk_{id} = \{r_{id}\}$ receives a ciphertext set $C = \{c_{\mathbf{1}}, c_{\mathbf{2}}, c_{\mathbf{3}}, c_{\mathbf{4}}\}$, it parses C as $g_{\mathbf{1}}(x) = c_{\mathbf{1}} + c_{\mathbf{2}}x$ and $g_{\mathbf{2}}(x) = c_{\mathbf{3}} + c_{\mathbf{4}}x$. If $r^2_{id} \equiv R_{id} \mod N$, Dec sets $h(x) = g_{\mathbf{1}}(x)$; otherwise it sets $h(x) = g_{\mathbf{2}}(x)$. Finally, Dec recovers the plaintext m as $m = \mathscr{J}_{N,\mathbf{2}}(h(r_{id}))$.

Clearly, the ciphertext in the scheme above is twice the length of that in Cocks scheme, whereas encryption operations just amounts to several multiplications in contrast to the heavy computations about the modular multiplicative inverse and the Jacobi symbol in Cocks scheme. In fact, this space-time trade-off method makes encryption considerably efficient. Also, $\Pi_{\mathbf{2}}$'s security is guaranteed by the following theorem whose proof is similar to the proof of Proposition 1 in [25].

Theorem 3. *Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary against the* IND-ID-CPA *security of our scheme $\Pi_{\mathbf{2}}$, making at most $q_{\mathscr{H}}$ queries to the random oracle $\mathscr{H}$ and a single query to the* Challenge phase. *Then, there exists an adversary $\mathcal{B}$ against the $\mathsf{MER}^{\mathbf{0}}_{\mathbf{2}}$ assumption such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\Pi_{\mathbf{2}}}(\lambda) = \frac{q_{\mathscr{H}}}{\mathbf{2}} \cdot \mathsf{Adv}^{\mathsf{MER}^{\mathbf{0}}_{\mathbf{2}}}_{\mathcal{B},RSAgen}(\lambda)$$

Proof. Suppose that the adversary $\mathcal{B}$ is given an RSA modulus N from the algorithm RSAgen(λ), a random element $w \in \mathcal{J}^{\mathbf{0}}_{N,\mathbf{2}}$ and $u \in \mathcal{J}^{\mathbf{0}}_{N,\mathbf{2}} \setminus \mathcal{ER}_{N,\mathbf{2}}$ and is asked to determine whether $w \in \mathcal{J}^{\mathbf{0}}_{N,\mathbf{2}} \setminus \mathcal{ER}_{N,\mathbf{2}}$. $\mathcal{B}$ sets $mpk = \{N, u, \mathscr{H}\}$ and gives it to $\mathcal{A}_{\mathbf{1}}$, who has oracle access to hash queries and extraction queries (i.e., ask the private key corresponding to each identity in the chosen set $\mathsf{ID}_{\mathbf{1}}$). $\mathcal{B}$ answers the oracle queries as follows:

Hash queries Initially, $\mathcal{B}$ maintains a counter $ctr = \mathbf{0}$ and a list $\mathcal{S}_{\mathscr{H}} \leftarrow \varnothing$ whose entry is in the form of $\{id, R_{id}, r_{id}\}$. In addition, $\mathcal{B}$ selects $i^* \xleftarrow{\$} \{\mathbf{1}, \ldots, q_{\mathscr{H}}\}$.
When $\mathcal{A}$ queries oracle $\mathscr{H}$ on an identity id, $\mathcal{B}$ increments ctr and checks whether there is an entry whose first component is id. If so, it returns R_{id}; otherwise, if $ctr = i^*$, it returns w and appends $\{id, w, \perp\}$ to $\mathcal{S}_{\mathscr{H}}$; else, it sets $h = u^{-j}r^{\mathbf{2}} \mod N$ with $r \xleftarrow{\$} \mathbb{Z}^*_N$ and $j \xleftarrow{\$} \{\mathtt{0}, \mathtt{1}\}$ and appends $\{id, h, r\}$ to $\mathcal{S}_{\mathscr{H}}$.

Extraction queries When $\mathcal{A}$ queries the secret key on id, $\mathcal{B}$ first checks whether there is an entry whose first component is id. If not, it invokes $\mathscr{H}(id)$ to generate an entry (id, R_{id}, r_{id}). Finally, if $r_{id} = \perp$, it aborts; otherwise, it returns r_{id}.

Afterward, $\mathcal{A}_{\mathbf{1}}$ selects a challenge identity $id^* \notin \mathsf{ID}_{\mathbf{1}}$. If $\mathscr{H}(id^*) \neq w$, $\mathcal{B}$ returns a random bit $b \in \{\mathtt{0}, \mathtt{1}\}$ to $\mathcal{A}$; otherwise, $\mathcal{B}$ does the following process:

1. Choose $b \xleftarrow{\$} \{0,1\}$ and two random polynomials f_1, f_2 of degree $\mathbf{1}$ from $\mathbb{Z}_N[x]$, and calculate $g_1(x) = f_1(x)^2 \bmod (x^2 - w) = a_1 x + a_0$ and $g_2(x) = f_2(x)^2 \bmod (x^2 - uw) = b_1 x + b_0$. The corresponding ciphertext is
$$C_b = \begin{cases} \{a_0, a_1, N - b_0, N - b_1\}, & \text{if } b = 0; \\ \{N - a_0, N - a_1, b_0, b_1\}, & \text{otherwise.} \end{cases}$$
2. Give C_b to $\mathcal{A}_2$ —— $\mathcal{A}_2$ may issue more hash queries and extraction queries except that the query identity subset ID_2 cannot contain id^*. Finally, $\mathcal{A}_2$ returns a bit b'.
3. If $b = b'$ return 1; otherwise return 0.

We shall only analyze the success probability of $\mathcal{B}$ solving the MER_2^0 assumption in the subcase $w = \mathscr{H}(id^*) \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}$ as the analyses of the other subcases are analogous to those in the proof of Proposition 1 in [25]. From $\mathscr{H}(id^*) \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}$ and Theorem 2, we conclude that C_b is a valid ciphertext for $(-1)^{1-b}$. Hence, $\mathcal{B}$ returns $\mathbf{1}$ if and only if $\mathcal{A}$ loses the game. Let ϵ be the probability that $\mathcal{A}$ can break the IND-ID-CPA security of Π_2, thus we have

$$\begin{aligned} \mathsf{Adv}^{\mathsf{MER}_2^0}_{\mathcal{B},\mathrm{RSAgen}}(\lambda) &= \left|\Pr\left[\mathcal{B}(N,w,u) = 1 \mid w \in \mathcal{ER}_{N,2}\right] - \Pr\left[\mathcal{B}(N,w,u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \setminus \mathcal{ER}_{N,2}\right]\right| = \\ &\left|\Pr[w = \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N,w,u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \wedge w = \mathscr{H}(id^*)\right] + \right. \\ &\Pr[w \neq \mathscr{H}(id^*)] \cdot \Pr\left[\mathcal{B}(N,w,u) = 1 \mid w \in \mathcal{J}_{N,2}^0 \wedge w \neq \mathscr{H}(id^*)\right] - \left.\left(\frac{1-\epsilon}{q_{\mathscr{H}}} + \frac{1 - \frac{1}{q_{\mathscr{H}}}}{2}\right)\right| = \\ &\left|\frac{\epsilon}{q_{\mathscr{H}}} + \left(1 - \frac{1}{q_{\mathscr{H}}}\right) \cdot \frac{1}{2} - \frac{1}{2} - \frac{\frac{1}{2} - \epsilon}{q_{\mathscr{H}}}\right| = \frac{2}{q_{\mathscr{H}}} \cdot \mathsf{Adv}^{\text{IND-ID-CPA}}_{\mathcal{A},\Pi_2}(\lambda) \end{aligned}$$

■

Construction for Square-free Integer e For ease of description, we suppose that there exists a hash function $\mathscr{H}$ mapping an arbitrary binary string to an *e-th residue* in $\mathbb{Z}_N^*$, our IBE scheme Π_e for a square-free integer e is defined as follows:

$\mathsf{Setup}(1^\lambda)$ Given a security parameter λ, Setup generates an RSA modulus $N = pq$ a product of two distinct large primes p and q, and selects a square-free integer e with the prime decomposition $e = \prod_{i=1}^{\ell} e_i$ such that $e \mid p - 1$, $e \mid q - 1$ and $\gcd(\frac{p+q-2}{e}, e) = 1$. The settings of μ is the same as for in BLS scheme. The public parameters are $mpk = \{N, e, \mu, \mathscr{J}_{N,e}(\mu), \mathscr{H}\}$. The master secret key is $msk = \{p, q\}$.

$\mathsf{KeyGen}(mpk, msk, id)$ Using the hash function $\mathscr{H}$ and p, q, KeyGen sets $R_{id} = \mathscr{H}(id)$, then calculates $r_{id} = \mathscr{H}(id)^{\frac{1}{e}} \bmod N$. Finally, KeyGen returns $sk_{id} = \{r_{id}\}$ as user's private key.

$\mathsf{Enc}(mpk, id, m)$ To encrypt a message $m \in \{0, \ldots, e-1\}$ for a user with identity id, Enc first derives the hash value $R_{id} = \mathscr{H}(id)$. Then, it generates a transport key $t = \mu^k$ where $k \xleftarrow{\$} \{0, \ldots, e-1\}$. We define the sub-algorithm $\mathcal{E}$ which takes as inputs a prime number $\mathscr{P}$ and a public key R_{id} as Algorithm 1.

Algorithm 1 $\mathcal{E}$

Input: a prime number $\mathcal{P}$, a public key R_{id}
Output: a polynomial

1: Generate a uniform random polynomial $f(x) \xleftarrow{\$} \mathbb{Z}_N^*[x]$ of degree $\mathcal{P} - 1$
2: Compute $g(x) \leftarrow f(x)^{\mathcal{P}} \bmod x^{\mathcal{P}} - R_{id}$
3: Output the polynomial $c(x) = \frac{g(x)}{\mu^{k \bmod \mathcal{P}}}$

The returned ciphertext is

$$C = \{\mathcal{E}(e_1), \ldots, \mathcal{E}(e_\ell), (m + \mathscr{J}_{N,e}(t)) \bmod e\}.$$

$\mathsf{Dec}(mpk, sk_{id}, C)$ When a user with $sk_{id} = \{r_{id}\}$ receives a ciphertext set C, it parses C as $\{c_1(x), \ldots, c_\ell(x), c\}$, Dec recovers the plaintext m as

$$m = \left(\mathscr{J}_{N,e} \left(\prod_{i=1}^{\ell} c_i (r_{id}^{\frac{e}{e_i}})^{\frac{e}{e_i}} \bmod N \right) + c \right) \bmod e$$

Remark 3. The condition $\gcd(\frac{p+q-2}{e}, e) = 1$ ensures that $\mathscr{J}_{N,e}(\mu)$ is primitive through the proof of Proposition 1. In the encryption phase, computing $\mathscr{J}_{N,e}(t) = k\,\mathscr{J}_{N,e}(\mu) \bmod e$ can be very convenient.

Correctness *Correctness* can be verified directly as follows.

$$\begin{aligned}
\mathsf{Dec}(mpk, sk_{id}, (\mathsf{Enc}(id, m))) &\equiv \sum_{i=1}^{\ell} \mathscr{J}_{N,e} \left(c_i (r_{id}^{\frac{e}{e_i}})^{\frac{e}{e_i}} \right) + m + \mathscr{J}_{N,e}(\mu^k) \\
&\equiv \sum_{i=1}^{\ell} \mathscr{J}_{N,e} \left(\frac{1}{\mu^{(k \bmod e_i)\frac{e}{e_i}}} \right) + m + \mathscr{J}_{N,e}(\mu^k) \\
&\equiv \mathscr{J}_{N,e} \left(\frac{\mu^k}{\mu^{\sum_{i=1}^{\ell} (k \bmod e_i)\frac{e}{e_i}}} \right) + m \\
&\equiv m \pmod{e}
\end{aligned}$$

Theorem 4. *Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary against the* IND-ID-CPA *security of our scheme Π_e, making at most $q_{\mathscr{H}}$ queries to the random oracle $\mathscr{H}$ and a single query to the* Challenge phase. *Then, there exists an adversary $\mathcal{B}$ against the MER_e^1 assumption such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\Pi_e}(\lambda) = q_{\mathscr{H}} \cdot \mathsf{Adv}^{\mathsf{MER}^1_e}_{\mathcal{B},RSAgen}(\lambda)$$

Proof. We prove it by defining a sequence of three games. For simplicity, we omit the procedure of Enc in the *Challenge phase*.

$\mathsf{Game}_1^{\mathcal{A}}(\lambda)$**:** This game is the real attack against our IBE scheme.

$\mathsf{Game}_2^{\mathcal{A}}(\lambda)$**:** In this game, we guess the number of the challenge identity and abort the game if the guess is wrong.

$\mathsf{Game}_3^{\mathcal{A}}(\lambda)$**:** We change the simulation of the H phase so that it returns a random element in $\mathcal{J}^1_{N,e} \setminus \mathcal{ER}_{N,e}$ for the i^*-th query.

$\mathsf{Game}_1^{\mathcal{A}}(\lambda)$	$\mathsf{Game}_2^{\mathcal{A}}(\lambda)$ $\boxed{\mathsf{Game}_3^{\mathcal{A}}(\lambda)}$
phase Setup(λ)	**phase Setup**(λ)
$b \xleftarrow{\$} \{0,1\}$	$b \xleftarrow{\$} \{0,1\}$
	$i^* \xleftarrow{\$} \{1,\ldots,q_{\mathcal{H}}\}$
$\mathcal{S}_{\mathcal{H}} \leftarrow \varnothing$; $ctr \leftarrow 0$	$\mathcal{S}_{\mathcal{H}} \leftarrow \varnothing$; $ctr \leftarrow 0$
$msk \leftarrow \{p,q\}$	$msk \leftarrow \{p,q\}$
$mpk \leftarrow \{N, e, \mu, \mathscr{J}_{N,e}(\mu), \ell, e_1, \ldots, e_\ell\}$	$mpk \leftarrow \{N, e, \mu, \mathscr{J}_{N,e}(\mu), \ell, e_1, \ldots, e_\ell\}$
return mpk	**return** mpk
phase KeyGen(id)	**phase KeyGen**(id)
if $(ctr, id, R_{id}, \cdot) \notin \mathcal{S}_{\mathcal{H}}$ $\mathbf{H}(id)$	**if** $(ctr, id, R_{id}, r_{id}) \notin \mathcal{S}_{\mathcal{H}}$ $\mathbf{H}(id)$
read $(ctr, id, R_{id}, \cdot) \in \mathcal{S}_{\mathcal{H}}$	read $(ctr, id, R_{id}, r_{id}) \in \mathcal{S}_{\mathcal{H}}$
	if $r_{id} = \perp$ **abort**
$\mathsf{usk} \leftarrow R_{id}^{\frac{1}{e}} \bmod N$	$\mathsf{usk} \leftarrow r_{id}$
return usk	**return** usk
phase H(id)	**phase H**(id)
if $(ctr, id, R_{id}, \cdot) \in \mathcal{S}_{\mathcal{H}}$ **return** R_{id}	**if** $(ctr, id, R_{id}, r_{id}) \in \mathcal{S}_{\mathcal{H}}$ **return** R_{id}
$ctr \leftarrow ctr + 1$	$ctr \leftarrow ctr + 1$
	if $ctr = i^*$
$R_{id} \xleftarrow{\$} \mathcal{ER}_{N,e}$	$r_{id} \xleftarrow{\$} \mathbb{Z}_N^*$; $R_{id} = r_{id}^e \bmod N$ $\boxed{R_{id} \xleftarrow{\$} \mathcal{J}^1_{N,e} \setminus \mathcal{ER}_{N,e}}$
$\mathcal{S}_{\mathcal{H}} \leftarrow \mathcal{S}_{\mathcal{H}} \cup \{(ctr, id, R_{id}, \perp)\}$	$\mathcal{S}_{\mathcal{H}} \leftarrow \mathcal{S}_{\mathcal{H}} \cup \{(ctr, id, R_{id}, \perp)\}$
	else
	$r_{id} \xleftarrow{\$} \mathbb{Z}_N^*$; $R_{id} = r_{id}^e \bmod N$
	$\mathcal{S}_{\mathcal{H}} \leftarrow \mathcal{S}_{\mathcal{H}} \cup \{(ctr, id, R_{id}, r_{id})\}$
return R_{id}	**return** R_{id}
phase Challenge(id^*, m_0, m_1)	**phase Challenge**(id^*, m_0, m_1)
	if $(i^*, id, R_{id}, r_{id}) \in \mathcal{S}_{\mathcal{H}}$ and $id = id^*$
$C \leftarrow \mathsf{Enc}(mpk, id^*, m_b)$	$C \leftarrow \mathsf{Enc}(mpk, id^*, m_b)$
	else abort
return C	**return** C
phase Guess(b')	**phase Guess**(b')
return $b' = b$	**return** $b' = b$

We claim:

Claim 1: $\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\Pi_e}(\lambda) = \left| \Pr\left[\mathsf{Game}_1^{\mathcal{A}}(\lambda) = true\right] - \frac{1}{2}\right|$.

Claim 2: $\Pr\left[\mathsf{Game}_2^{\mathcal{A}}(\lambda) = true\right] = \frac{1}{2}(1 - \frac{1}{q_{\mathcal{H}}}) + \frac{1}{q_{\mathcal{H}}} \Pr\left[\mathsf{Game}_1^{\mathcal{A}}(\lambda) = true\right]$.

Claim 3: $\left| \Pr\left[\mathsf{Game}_3^{\mathcal{A}}(\lambda) = true\right] - \Pr\left[\mathsf{Game}_2^{\mathcal{A}}(\lambda) = true\right] \right| \leq \mathsf{Adv}^{\mathsf{MER}^1_e}_{\mathcal{B},\mathrm{RSAgen}}(\lambda)$.

Claim 4: $\Pr\left[\mathsf{Game}_3^{\mathcal{A}}(\lambda) = true\right] = \frac{1}{2}$.

Proof. *Claim 1* follows immediately by the definition of semantic security. *Claim 2* is derived from Bayes' theorem. *Claim 3* follows from Difference Lemma [36]. If the public key R_{id^*} of the challenge identity id^* is chosen from $\mathcal{J}^1_{N,e} \setminus \mathcal{ER}_{N,e}$, then $\left(\frac{R_{id^*}}{\mathfrak{p}_1}\right)_{e_j}$ and $\left(\frac{R_{id^*}}{\mathfrak{q}_1}\right)_{e_j}$ are both primitive e_j-th roots of unity

for each $\mathtt{1} \le j \le \ell$. Since $\left(\frac{\mu}{\mathfrak{a}_\mathtt{1}}\right)_e$ is primitive, the set

$$\left\{ \left\{ \left(\frac{\mu^{k \bmod e_1}}{\mathfrak{a}_\mathtt{1}}\right)_{e_1}, \ldots, \left(\frac{\mu^{k \bmod e_\ell}}{\mathfrak{a}_\mathtt{1}}\right)_{e_\ell} \right\} \;\middle|\; \mathtt{0} \le k < e \right\}$$

takes over combinations of all e_j-th roots of unity for each $\mathtt{1} \le j \le \ell$. Hence, by Theorem 2, ciphertexts are statistically indistinguishable to an adversary, which completes the proof of *Claim 4*. ■

Combining all above claims gives this theorem. ■

5 Anonymity

In this section, we review the basic theory of the reciprocity law over function fields, and then extend the Galbraith's test [5] to e-th power residue situation in order to prove that BLS scheme is not *anonymous* when e is small. Some attempts to extend Cocks scheme to achieve *anonymity* have been proposed by several researchers, e.g., in [3,7,25,32]. These methods may be adaptive to BLS scheme and ours as they share many common features with Cocks scheme. In particular, we utilize the methodology originated from Joye [25] to make our scheme $\Pi_\mathtt{2}$ satisfy ANO-IND-ID-CPA security. Moreover, the new scheme $\Pi_\mathtt{2}^{\mathsf{ANO}}$ does not sacrifice the efficiency of encryption.

5.1 Reciprocity Law over Function Fields

We start by explaining notation to be used and briefly give crucial definitions and results due to Carlitz [13]. We here refer to Chapter 3 in [31].

Every element in $\mathbb{F}_q[t]$ has the form $f(t) = \alpha_n t^n + \alpha_{n-\mathtt{1}} t^{n-\mathtt{1}} + \cdots + \alpha_\mathtt{0}$. In this case we set $sgn(f) = \alpha_n$ and call it the sign of f. Let $P \in \mathbb{F}_q[t]$ of degree γ be an irreducible polynomial and e a divisor of $q - \mathtt{1}$. Note that there is a unique $\alpha \in \mathbb{F}_q^*$ such that $a^{\frac{q^\gamma - \mathtt{1}}{e}} \equiv \alpha \pmod P$.

Definition 2. *If $a \in \mathbb{F}_q[t]$ and P does not divide a, let $\left(\frac{a}{P}\right)_e$ be the unique element of $\mathbb{F}_q^*$ such that*

$$a^{\frac{q^\gamma - \mathtt{1}}{e}} \equiv \left(\frac{a}{P}\right)_e \pmod P.$$

If $P \mid a$ define $\left(\frac{a}{P}\right)_e = \mathtt{0}$. The symbol $\left(\frac{a}{P}\right)_e$ is called the e-th power residue symbol.

Proposition 2. *The e-th power residue symbol has the following properties:*

1. $\left(\frac{a}{P}\right)_e = \left(\frac{b}{P}\right)_e$ *if* $a \equiv b \pmod P$.
2. $\left(\frac{ab}{P}\right)_e = \left(\frac{a}{P}\right)_e \left(\frac{b}{P}\right)_e$.
3. *Let $\alpha \in \mathbb{F}_q$. Then,* $\left(\frac{\alpha}{P}\right)_e = \alpha^{\frac{q-\mathtt{1}}{e}\gamma}$.

Just as the Jacobi symbol, the definition of the e-th power residue symbol can be extended to the case that P is an arbitrary non-zero element $b \in \mathbb{F}_q[t]$ with the prime decomposition $b = sgn(b) Q_\mathtt{1}^{f_\mathtt{1}} \cdots Q_s^{f_s}$, and thus define

$$\left(\frac{a}{b}\right)_e = \prod_{j=\mathtt{1}}^{s} \left(\frac{a}{Q_j}\right)_e^{f_j}.$$

Proposition 3. *The symbol $\left(\frac{a}{b}\right)_e$ has the following properties:*

1. *If* $a_\mathtt{1} \equiv a_\mathtt{2} \pmod b$, *then* $\left(\frac{a_\mathtt{1}}{b}\right)_e = \left(\frac{a_\mathtt{2}}{b}\right)_e$.
2. $\left(\frac{a_\mathtt{1} a_\mathtt{2}}{b}\right)_e = \left(\frac{a_\mathtt{1}}{b}\right)_e \left(\frac{a_\mathtt{2}}{b}\right)_e$.
3. $\left(\frac{a}{b_\mathtt{1} b_\mathtt{2}}\right)_e = \left(\frac{a}{b_\mathtt{1}}\right)_e \left(\frac{a}{b_\mathtt{2}}\right)_e$.
4. $\left(\frac{a}{b}\right)_e \neq \mathtt{0}$ *if and only if a is relatively prime to b.*
5. *If* $x^e \equiv a \pmod b$ *is solvable, then* $\left(\frac{a}{b}\right)_e = \mathtt{1}$.

The following fascinating theorem tells the general reciprocity law for $\mathbb{F}_q[t]$.

Theorem 5. *[**The general reciprocity law [13]**] Let $a, b \in \mathbb{F}_q[t]$ be relatively prime, non-zero elements. Then,*

$$\left(\frac{a}{b}\right)_e = \left(\frac{b}{a}\right)_e \left((-\mathtt{1})^{deg(a)deg(b)} sgn(a)^{deg(b)} sgn(b)^{-deg(a)}\right)^{\frac{q-\mathtt{1}}{e}}$$

5.2 Galbraith's Test on Higher-power Residues

Let $a = H(id), N, c$ be the public key of a user id, an RSA modulus and a ciphertext as in Cocks scheme respectively. Here, we consider a as a quadratic residue modulo N. Galbraith constructed the following elegant test

$$\mathscr{GT}(a, c) = \left(\frac{c^2 - 4a}{N}\right)$$

to distinguish the identity of a ciphertext. The reason it can be successful is: if the ciphertext c is generated by the user id with public key a, then $c^2 - 4a$ must be a square, but is not always the case if the public key a is replaced by another one. In [3], Ateniese and Gasti proved that Galbraith's test is the best test against the *anonymity* of Cocks scheme. Recently, in [38], the authors developed exact formulas for the distributions of quadratic residues and non-residues on special sets and rigorously made deep analyses on Galbraith's test. Equivalently, in BLS scheme, if $g(x) = f(x)^e \bmod (x^e - R_{id})$ is a ciphertext polynomial encrypted by the user id, it is uncertain whether $g(x)$ can be obtained by another user id' if the modulus $x^e - R_{id}$ is replaced by $x^e - R_{id'}$.

In BLS scheme, an adversary who intercepts ciphertexts has the ability of recreating the polynomial

$$\frac{g(x)}{t} = \frac{f(x)^e}{t} \bmod (x^e - R_{id}).$$

Let $x^e - R_{id} = \prod_{j=1}^{m} \eta_j^{p_j}$ be the prime decomposition of $x^e - R_{id}$ in $\mathbb{F}_p[x]$. There is

$$\left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_p} = \left(\frac{t^{-1}f(x)^e}{x^e - R_{id}}\right)_{e,\mathbb{F}_p} = \prod_{j=1}^{m}\left(\frac{t^{-1}}{\eta_j}\right)_{e,\mathbb{F}_p}^{p_j} = \prod_{j=1}^{m} t^{-\frac{p-1}{e}p_j deg(\eta_j)} = t^{-\frac{p-1}{e}e} \equiv 1 \quad (\mathfrak{p}_1). \quad (1)$$

Similarly,

$$\left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_q} \equiv 1 \quad (\mathfrak{q}_1). \quad (2)$$

Notice that all the following three situations occur with overwhelming probability.

1. $\gcd(x^e - R_{id}, f(x)) = 1$.
2. The *leading term* x^{e-1} of $\frac{g(x)}{t}$ has non-zero coefficient.
3. All terms in each polynomial in process have coefficients relatively prime to N.

Therefore, we may assume that all of them hold by default. By continuously applying Theorem 5 until the process terminates, i.e., modulo a polynomial of degree 1, one can get

$$\left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_p} \equiv \left(\frac{c_p}{\mathfrak{p}_1}\right)_e \left(\frac{\alpha_p}{\Phi(x)}\right)_{e,\mathbb{F}_p} \quad (\mathfrak{p}_1), \quad \left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_q} \equiv \left(\frac{c_q}{\mathfrak{q}_1}\right)_e \left(\frac{\beta_q}{\Psi(x)}\right)_{e,\mathbb{F}_q} \quad (\mathfrak{q}_1) \quad (3)$$

where $\alpha_p, c_p \in \mathbb{F}_p$, $\beta_q, c_q \in \mathbb{F}_q$ and $\Phi(x) \in \mathbb{F}_p[x]$, $\Psi(x) \in \mathbb{F}_q[x]$, $deg(\Phi(x)) = deg(\Psi(x)) = 1$. An adversary can perform the above steps as well, but in $\mathbb{Z}_N[x]$. In other words, it can, however obtain c_N, γ_N and $\Theta(x)$ such that

$$\begin{array}{lll} c_N \equiv c_p \pmod{p} & \gamma_N \equiv \alpha_p \pmod{p} & \Theta(x) \equiv \Phi(x) \pmod{p} \\ c_N \equiv c_q \pmod{q} & \gamma_N \equiv \beta_q \pmod{q} & \Theta(x) \equiv \Psi(x) \pmod{q} \end{array}$$

With this terminology, we define the *e-th Galbraith's test* as

$$\mathscr{GT}(R_{id}, C)_e = \left(\frac{c_N\gamma_N}{\mathfrak{a}_1}\right)_e = \left(\frac{\left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_p}^{\frac{e}{p-1}}}{\mathfrak{p}_1}\right)_e \left(\frac{\left(\frac{t^{-1}g(x)}{x^e - R_{id}}\right)_{e,\mathbb{F}_q}^{\frac{e}{q-1}}}{\mathfrak{q}_1}\right)_e.$$

Now that the ciphertext C is generated by the user id, the equation $\mathscr{GT}(R_{id}, C)_e = 1$ must hold with all but negligible probability. While for another user id', we conjecture that the value $\mathscr{GT}(R_{id'}, C)_e$ is statistically close to the uniform distribution on $\left\{\zeta_e^i \;\middle|\; i \in \{0, 1, \ldots, e-1\}\right\}$. Furthermore, we naturally conjecture that the *e-th Galbraith's test* is the most effective test against the *anonymity* of BLS scheme.

Remark 4. When $e = 2$, let $c_0, c_1 \in \mathbb{Z}_N^*$ and $c(x) = c_1 x + c_0$ be the ciphertext polynomial, then

$$x^2 - R_{id} \equiv (c_1^{-1} c_0)^2 - R_{id} \pmod{c_1 x + c_0}.$$

By Theorem 5, $c_N = c_1^2$ and $\gamma_N = (c_1^{-1} c_0)^2 - R_{id}$. Hence, the 2-*th Galbraith's test* simplifies to

$$\mathscr{GT}(R_{id}, C)_2 = \left(\frac{c_N \gamma_N}{a_1}\right)_2 = \left(\frac{c_0^2 - c_1^2 R_{id}}{N}\right),$$

as mentioned in [14]. Substituting c for c_0 and 2 for c_1 into $\mathscr{GT}(R_{id}, C)_2$, we derive the original form of Galbraith's test on Cocks scheme.

Finally, we give an example to demonstrate how the e-*th Galbraith's test* works.

Example 1. Assume that all parameters of BLS scheme are set as in Table 1:

Table 1. Parameters of BLS scheme in *Example 1*

Parameter	*Value*	*Parameter*	*Value*
N	4331	r_{id}	67
p	61	$R_{id'}$	467
q	71	$r_{id'}$	51
e	5	t	7
μ	1900	$f(x)$	$x^4 + 2x^3 + 3x^2 + 4x + 6$
R_{id}	822	$\frac{g(x)}{t}$	$3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193$

Here, the ciphertext polynomial $\frac{g(x)}{t}$ is generated by the user id. To distinguish the identity of $\frac{g(x)}{t}$ between id and id', an adversary may perform the following calculations:

$\boxed{R_{id} = 822}$
$x^5 - 822 \equiv 3855x^3 + 649x^2 + 1331x + 1525 \pmod{3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193}$
$3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193 \equiv 29x^2 + 460x + 1742 \pmod{3855x^3 + 649x^2 + 1331x + 1525}$
$3855x^3 + 649x^2 + 1331x + 1525 \equiv 3938x + 951 \pmod{29x^2 + 460x + 1742}$
$29x^2 + 460x + 1742 \equiv 55 \pmod{3938x + 951}$
$\boxed{R_{id'} = 467}$
$x^5 - 467 \equiv 3855x^3 + 649x^2 + 1331x + 1880 \pmod{3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193}$
$3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193 \equiv 29x^2 + 105x + 3020 \pmod{3855x^3 + 649x^2 + 1331x + 1880}$
$3855x^3 + 649x^2 + 1331x + 1880 \equiv 3512x + 99 \pmod{29x^2 + 105x + 3020}$
$29x^2 + 105x + 3020 \equiv 4315 \pmod{3512x + 99}$

Next, it derives

$$c_N = (3184 \times 3855 \times 29 \times 3938)^2 \bmod 4331 \qquad c'_N = (3184 \times 3855 \times 29 \times 3512)^2 \bmod 4331$$
$$\gamma_N = 55 \qquad \gamma'_N = 4315$$

and computes $\left(\frac{c_N \gamma_N}{a_1}\right)_5 = 1$ and $\left(\frac{c'_N \gamma'_N}{a_1}\right)_5 = \zeta_5^3 \neq 1$. Finally, it captures the fact that the ciphertext polynomial $\frac{g(x)}{t}$ belongs to the identity id. Indeed, there is $\left(\frac{c_N \gamma_N}{p_1}\right)_5 = \left(\frac{c_N \gamma_N}{q_1}\right)_5 = 1$.

5.3 An Anonymous Scheme

To avoid our scheme Π_2 from being attacked against the *anonymity* by the $\mathtt{2}$-*th Galbraith's test*, one should generate two types of ciphertexts with values $\{\pm\mathtt{1}\}$ when taking them to do the $\mathtt{2}$-*th Galbraith's test*. Obviously, multiplying the ciphertext polynomial by a scalar doesn't work as the $\mathtt{2}$-*th Galbraith's test* doesn't change. What about multiplying a polynomial? In fact, x is suitable as

$$\mathscr{G}\mathscr{T}(R_{id}, x)_{\mathtt{2}} = \left(\frac{(-\mathtt{1})^{\mathtt{2}} \cdot -\mathtt{1}}{N}\right) = -\mathtt{1}.$$

Therefore, inspired by the anonymous IBE scheme Γ without ciphertext expansion from [Section 6.2, [25]], we construct the following anonymous IBE scheme Π_2^{ANO} with fast encryption.

$\mathsf{Setup}(\mathtt{1}^\lambda)$ Given a security parameter λ, Setup generates an RSA modulus $N = pq$ a product of two distinct large primes p and q such that $\dfrac{p+q}{\mathtt{2}}$ is even and an element $u \in \mathcal{J}^{\mathtt{0}}_{N,\mathtt{2}} \setminus \mathcal{ER}_{N,\mathtt{2}}$. The public parameters are $mpk = \{N, u, \mathscr{H}\}$ where $\mathscr{H}$ is a publicly available cryptographic hash function mapping an arbitrary binary string to $\mathcal{J}^{\mathtt{0}}_{N,\mathtt{2}}$. The master secret key is $msk = \{p, q\}$.

$\mathsf{KeyGen}(mpk, msk, id)$ Using the hash function $\mathscr{H}$ and p, q, KeyGen sets $R_{id} = \mathscr{H}(id)$. If $R_{id} \in \mathcal{ER}_{N,\mathtt{2}}$, KeyGen calculates $r_{id} = \mathscr{H}(id)^{\frac{1}{\mathtt{2}}} \mod N$; otherwise it calculates $r_{id} = (u\mathscr{H}(id))^{\frac{1}{\mathtt{2}}} \mod N$. Finally, KeyGen returns $sk_{id} = \{r_{id}\}$ as user's private key.

$\mathsf{Enc}(mpk, id, m)$ To encrypt a message $m \in \{\mathtt{0}, \mathtt{1}\}$ for a user with identity id, Enc derives the hash value $R_{id} = \mathscr{H}(id)$. It then chooses two random polynomials $f_{\mathtt{1}}, f_{\mathtt{2}}$ of degree $\mathtt{1}$ from $\mathbb{Z}_N[x]$ and lets

$$g_{\mathtt{1}}(x)^{\mathtt{0}} = (-\mathtt{1})^m f_{\mathtt{1}}(x)^{\mathtt{2}} \bmod (x^{\mathtt{2}} - R_{id}), \quad g_{\mathtt{1}}(x)^{\mathtt{1}} = (-\mathtt{1})^m x \cdot f_{\mathtt{1}}(x)^{\mathtt{2}} \bmod (x^{\mathtt{2}} - R_{id})$$
$$g_{\mathtt{2}}(x)^{\mathtt{0}} = (-\mathtt{1})^m f_{\mathtt{2}}(x)^{\mathtt{2}} \bmod (x^{\mathtt{2}} - uR_{id}), \quad g_{\mathtt{2}}(x)^{\mathtt{1}} = (-\mathtt{1})^m x \cdot f_{\mathtt{2}}(x)^{\mathtt{2}} \bmod (x^{\mathtt{2}} - uR_{id})$$

It also chooses at random two bits $\beta_{\mathtt{1}}, \beta_{\mathtt{2}} \in \{\mathtt{0}, \mathtt{1}\}$. The returned ciphertext is

$$C = \{g_{\mathtt{1}}(x)^{\beta_{\mathtt{1}}}, g_{\mathtt{2}}(x)^{\beta_{\mathtt{2}}}\}$$

$\mathsf{Dec}(mpk, sk_{id}, C)$ When a user with $R_{id} = \mathscr{H}(id)$ and $sk_{id} = \{r_{id}\}$ receives a ciphertext polynomial set $C = \{c_{\mathtt{1}}(x), c_{\mathtt{2}}(x)\}$. If $r_{id}^{\mathtt{2}} \equiv R_{id} \bmod N$, Dec sets $h(x) = c_{\mathtt{1}}(x)$, $\triangle = R_{id}$; otherwise it sets $h(x) = c_{\mathtt{2}}(x)$, $\triangle = uR_{id}$. Next, it computes $\sigma = \mathscr{G}\mathscr{T}(\triangle, h(x))_{\mathtt{2}}$. Finally, Dec recovers the plaintext m as $m = \mathscr{J}_{N,\mathtt{2}}((-\mathtt{1})^\sigma h(r_{id}))$.

Remark 5. Note that when taken $f_{\mathtt{1}} = x + t_{\mathtt{1}}$, $f_{\mathtt{2}} = x + t_{\mathtt{2}}$ with $\left(\frac{t_{\mathtt{1}}}{N}\right) = \left(\frac{t_{\mathtt{2}}}{N}\right) = (-\mathtt{1})^m$, Π_2^{ANO} is identical to Γ in the case $d = \mathtt{0}$ where d is the hash index in Γ.

6 Computing $\left(\dfrac{\cdot}{\mathfrak{a}_{\mathtt{1}}}\right)_e$

In this section, we first develop a method for computing $\left(\frac{\cdot}{\mathfrak{a}_{\mathtt{1}}}\right)_e$ for large values of e, and then show that computing $\left(\frac{\cdot}{\mathfrak{a}_{\mathtt{1}}}\right)_e$ becomes much easier if the factorization $\mathfrak{a}_{\mathtt{1}} = \mathfrak{p}_{\mathtt{1}}\mathfrak{q}_{\mathtt{1}}$ is already known. Finally, we extend Joye-Libert cryptosystem [26] to the higher-power residue case.

6.1 Computing $\left(\dfrac{\cdot}{\mathfrak{a}_{\mathtt{1}}}\right)_e$ for Large Values of e

In [19], to compute the e-th power residue symbol, the authors constructed a "compatibility" identity and claimed that it holds for all ideals in $\mathbb{Z}[\zeta_e]$. But this is not correct, e.g., If $\mathfrak{U}$ is a prime ideal in $\mathbb{Z}[\zeta_e]$ and $\mathfrak{B} = \mathfrak{U} \cap \mathbb{Z}[\zeta_f]$ is a prime ideal in $\mathbb{Z}[\zeta_f]$ where $f \mid e$, the argument $\mathrm{Norm}_{\mathbb{Z}[\zeta_e]}(\mathfrak{U}) = \mathrm{Norm}_{\mathbb{Z}[\zeta_f]}(\mathfrak{B})$ is not always true. In fact, when $\mathfrak{B}$ is singular, the local-global principle makes the "compatibility" identity hold, see Chapter 1 in [17]. Furthermore, note that in the case $\mathrm{Norm}_{\mathbb{Z}[\zeta_e]}(\mathfrak{U}) = p - \mathtt{1}$, it also holds due to the inclusion map $\iota : \dfrac{\mathbb{Z}[\zeta_e]}{\mathfrak{U}} \mapsto \dfrac{\mathbb{Z}[\zeta_f]}{\mathfrak{B}}$. Hence, we formalize the following revised theorem.

Theorem 6. *Let e, f be integers with $f \mid e$. Let $\mathfrak{p}_1$ be as Lemma 1, and let $x \in \mathbb{Z}[\zeta_e]$. Then*

$$\left(\frac{x}{\mathfrak{p}_1 \cap \mathbb{Z}[\zeta_f]}\right)_f = \left(\frac{x}{\mathfrak{p}_1}\right)_e^{\frac{e}{f}}.$$

It follows readily that $\mathfrak{p}_1 \cap \mathbb{Z}[\zeta_f] = p\mathbb{Z}[\zeta_f] + (\zeta_f - \mu^{\frac{e}{f}})\mathbb{Z}[\zeta_f]$ due to the fact that $\mu^{\frac{e}{f}}$ is a *non-degenerate* primitive f-th root of unity modulo N. Therefore, we are able to learn the value of $\left(\frac{x}{\mathfrak{a}_1}\right)_e$ by computing $\left(\frac{x}{N\mathbb{Z}[\zeta_f] + (\zeta_f - \mu^{\frac{e}{f}})\mathbb{Z}[\zeta_f]}\right)_f$ for each prime factor f of e and applying the Chinese remainder theorem.

6.2 Computing $\left(\frac{\cdot}{\mathfrak{a}_1}\right)_e$ if the Factorization $\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{q}_1$ is Known

The following simple theorem demonstrates that computing $\left(\frac{\cdot}{\mathfrak{p}_1}\right)_e$ is related to solving the discrete logarithm problem in a certain cyclic group. Recall that the *discrete logarithm problem* (DLP) is defined as: given a finite cyclic group $\mathbb{G}$ of order n with a generator α and an element $\beta \in \mathbb{G}$, find the integer $x \in \mathbb{Z}_n$ such that $\alpha^x = \beta$.

Theorem 7. $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$ *if and only if* $\mu^x = y^{\frac{p-1}{e}}$ *in* $\mathbb{Z}_p^*$. *Therefore, the solution to the* DLP *in the finite cyclic subgroup* $\langle\mu\rangle$ *of order* e *allows the computation of* $\left(\frac{\cdot}{\mathfrak{p}_1}\right)_e$.

Proof. $\Leftarrow$ If $\mu^x = y^{\frac{p-1}{e}}$, then $y^{\frac{p-1}{e}} - \zeta_e^x = \mu^x - \zeta_e^x \in \mathfrak{p}_1$. It follows that $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$.

$\Rightarrow$ If $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$ for some $x \in \mathbb{Z}_e$, that is $y^{\frac{p-1}{e}} - \zeta_e^x \in \mathfrak{p}_1$. As the order of $y^{\frac{p-1}{e}}$ divides e, $y^{\frac{p-1}{e}}$ can be expressed as μ^z with an integer $z \in \mathbb{Z}_e$, which implies $\mu^x - \mu^z \in \mathfrak{p}_1$. The fact that the order of μ is e forces $x = z$. ■

Although the *DLP* is considered to be intractable in general, it can be quickly solved in a few particular cases, e.g., if the order of $\mathbb{G}$ is smooth, the Pohlig-Hellman algorithm [30] turns out to be quite efficient. Taking advantage of the discovery above, Joye-Libert scheme [26] which generalizes Goldwasser-Micali cryptosystem using 2^k-th power residue symbols can be extended and rephrased as follows:

$\mathsf{KeyGen}\,(\mathbf{1}^\kappa)$ Given a security parameter κ. KeyGen selects arbitrary $e = \prod_{i=1}^{\ell} e_i^{f_i}$ a product of small prime numbers, then generates an RSA modulus $N = pq$ a product of two large primes p and q such that $e \mid p - \mathbf{1}, e \mid q - \mathbf{1}$ and picks at random $\mu \in \mathbb{Z}_N^*$ a *non-degenerate* primitive e-th root of unity to N and $y \in \mathcal{J}_{N,e}^{\mathbf{1}} \setminus \mathcal{ER}_{N,e}$. The public and private keys are $pk = \{N, e, y\}$ and $sk = \{p, \mu\}$.

$\mathsf{Enc}\,(pk, m)$ To encrypt a message $m \in \mathbb{Z}_e$, Enc picks a random $x \in \mathbb{Z}_N^*$ and returns the ciphertext

$$c = y^m x^e \bmod N.$$

$\mathsf{Dec}\,(sk, c)$ Given the ciphertext c and the private key $sk = \{p, \mu\}$, Dec first computes $\left(\frac{c}{\mathfrak{p}_1}\right)_e = \zeta_e^z$ and then recovers the plaintext as $m = zk^{-\mathbf{1}} \bmod e$ where $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^k$.

The above scheme has the similar security proof as Goldwasser-Micali cryptosystem's, i.e., by the proof of Theorem 1, it is $\mathsf{IND\text{-}CPA}$ secure under the ER_e assumption defined as:

Definition 3 (e-th Residue (ER_e) Assumption). *A* PPT *algorithm* $\mathsf{RSAgen}(\lambda)$ *generates two equally sized primes* p, q *and an integer* e *such that* $p \equiv q \equiv \mathbf{1}$ *mod* e*, and chooses at random* $\mu \in \mathbb{Z}_N^*$ *a* non-degenerate *primitive* e*-th root of unity to* $N = pq$*. We define the following two distributions relative to* $\mathsf{RSAgen}(\kappa)$ *as:*

$$\mathbb{D}_{ER}: \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\kappa),\ v \xleftarrow{\$} \mathcal{ER}_{N,e} \right\}$$

$$\mathbb{D}_{ENR}: \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\kappa),\ v \xleftarrow{\$} \mathcal{J}^{\mathbf{1}}_{N,e} \setminus \mathcal{ER}_{N,e} \right\}$$

The ER_e *assumption relative to* $\mathsf{RSAgen}(\kappa)$ *asserts that the advantage* $\mathsf{Adv}^{\mathsf{ER}_e}_{\mathcal{A},\mathsf{RSAgen}}(\kappa)$ *defined as*

$$\left| \Pr\left[\mathcal{A}(N, v, e) = \mathbf{1} \;\middle|\; (N, v, e, \mu) \xleftarrow{\$} \mathbb{D}_{ER}(\kappa) \right] - \Pr\left[\mathcal{A}(N, v, e) = \mathbf{1} \;\middle|\; (N, v, e, \mu) \xleftarrow{\$} \mathbb{D}_{ENR}(\kappa) \right] \right|$$

is negligible for any PPT *adversary* $\mathcal{A}$*.*

Note that when $e = \mathbf{2}^k$ for an integer k, ER_e assumption holds if and only if the k-QR *assumption* (Definition 2, [26]) holds since $\left(\frac{a}{p}\right) = -\mathbf{1}$ if and only if $\left(\frac{a}{\mathfrak{p}_1}\right)_e$ is primitive (for a fixed p and arbitrary μ). Therefore, the above scheme for $e = \mathbf{2}^k$ (Joye-Libert scheme) is $\mathsf{IND\text{-}CPA}$ secure under the k-QR *assumption.*

References

1. Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In *Annual International Cryptology Conference*, pages 205–222. Springer, 2005.
2. Leonard Adleman, Kenneth Manders, and Gary Miller. On taking roots in finite fields. In *18th Annual Symposium on Foundations of Computer Science (SFCS 1977)*, pages 175–178. IEEE, 1977.
3. Giuseppe Ateniese and Paolo Gasti. Universally anonymous ibe based on the quadratic residuosity assumption. In *Cryptographers' Track at the RSA Conference*, pages 32–47. Springer, 2009.
4. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 566–582. Springer, 2001.
5. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer, 2004.
6. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.
7. Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryptionwithout pairings. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 647–657. IEEE, 2007.
8. Dan Boneh, Rio LaVigne, and Manuel Sabin. Identity-based encryption with e^{th} residuosity and its incompressibility. In *Autumn 2013 TRUST Conference. Washington DC (Oct 9-10, 2013), poster presentation*, 2013.
9. Eric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. Cryptology ePrint Archive, Report 2019/484, 2019. `https://eprint.iacr.org/2019/484`.
10. Zhenfu Cao. A new public-key cryptosystem based on k^{th}-power residues (full version). *Journal of the China Institute of Communications*, 11(2):80–83, 1990.
11. Zhenfu Cao, Xiaolei Dong, Licheng Wang, and Jun Shao. More efficient cryptosystems from k-th power residues. *IACR Cryptology ePrint Archive*, 2013:569, 2013.
12. Zhengjun Cao, Qian Sha, and Xiao Fan. Adleman-manders-miller root extraction method revisited. In *International Conference on Information Security and Cryptology*, pages 77–85. Springer, 2011.
13. Leonard Carlitz et al. On certain functions connected with polynomials in a galois field. *Duke Mathematical Journal*, 1(2):137–168, 1935.
14. Michael Clear, Arthur Hughes, and Hitesh Tewari. Homomorphic encryption with access policies: Characterization and new constructions. In *International Conference on Cryptology in Africa*, pages 61–87. Springer, 2013.

15. Michael Clear and Ciaran McGoldrick. Additively homomorphic ibe from higher residuosity. In *IACR International Workshop on Public Key Cryptography*, pages 496–515. Springer, 2019.
16. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *IMA International Conference on Cryptography and Coding*, pages 360–363. Springer, 2001.
17. Koen de Boer. *Computing the power residue symbol*. PhD thesis, Master's thesis. Nijmegen, Radboud University. `www.koendeboer.com`, 2016.
18. Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-barua's identity-based encryption revisited. In *International Conference on Network and System Security*, pages 271–284. Springer, 2015.
19. David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev. More constructions of lossy and correlation-secure trapdoor functions. *Journal of cryptology*, 26(1):39–74, 2013.
20. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.
21. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.
22. Shai Halevi. A sufficient condition for key-privacy. *IACR Cryptology ePrint Archive*, 2005:5, 2005.
23. Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.
24. Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In *International Conference on Information Security and Cryptology*, pages 314–331. Springer, 2008.
25. Marc Joye. Identity-based cryptosystems and quadratic residuosity. In *Public-Key Cryptography–PKC 2016*, pages 225–254. Springer, 2016.
26. Marc Joye and Benoit Libert. Efficient cryptosystems from $\mathsf{2}^k$-th power residue symbols. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 76–92. Springer, 2013.
27. Derrick H Lehmer. Computer technology applied to the theory of numbers. *Studies in number theory*, pages 117–151, 1969.
28. Franz Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein*. Springer Science & Business Media, 2013.
29. Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
30. Stephen Pohlig and Martin Hellman. An improved algorithm for computing logarithms over $\mathbb{GF}(p)$ and its cryptographic significance. *IEEE Transactions on information Theory*, 24(1):106–110, 1978.
31. Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.
32. Adrian G. Schipor. On the anonymization of cocks ibe scheme. In *International Conference on Cryptography and Information Security in the Balkans*, pages 194–202. Springer, 2014.
33. Adrian G. Schipor. On the security of jhanwar-barua identity-based encryption scheme. In *International Conference on Security for Information Technology and Communications*, pages 368–375. Springer, 2018.
34. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.
35. Daniel Shanks. Five number-theoretic algorithms. In *Proceedings of the Second Manitoba Conference on Numerical Mathematics (Winnipeg), 1973*, 1973.
36. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.
37. Douglas Squirrel. Computing reciprocity symbols in number fields, 1997. *Undergraduate thesis, Reed College*.
38. F.L. Tiplea, S. Iftene, G. Teseleanu, and A.-M. Nica. On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography. Cryptology ePrint Archive, Report 2019/638, 2019. `https://eprint.iacr.org/2019/638`.

A Incompressibility of BLS Scheme

BLS scheme has a space-efficient variation (see [8]) that seems to work. If a trusted PKG sets the user's secret key to the root of $x^\delta - R_{id}$ for some δ satisfying $2 \le \delta < e$ with some prime e, and operations of polynomials are performed in the quotient ring $\frac{\mathbb{Z}_N[x]}{(x^\delta - R_{id})}$ in the encryption phase, then the number of elements in the ciphertext can be significantly reduced to $\delta + 1$. However, this ambitious method makes the scheme insecure. Moreover, there even exists an attack that recovers the decrypted messages with the help of the reciprocity law over $\mathbb{F}_q[t]$, the polynomial ring over some finite field $\mathbb{F}_q$. This attack also shows that it is incompressible for any generalization of similar methods, and as a result it hinders the progress of Cocks scheme. We next employ the notations and terminology in section 5 to demonstrate this attack.

An adversary who intercepts ciphertexts has the ability of recreating the polynomial

$$\frac{g(x)}{t} = \frac{f(x)^e}{t} \bmod \left(x^\delta - R_{id}\right).$$

Let $x^\delta - R_{id} = \prod_{j=1}^{m} \eta_j^{p_j}$ be the prime decomposition of $x^\delta - R_{id}$ in $\mathbb{F}_p[x]$. There are

$$\left(\frac{t^{-1}g(x)}{x^\delta - R_{id}}\right)_{e,\mathbb{F}_p} \equiv \left(\frac{t^{-1}}{\mathfrak{p}_1}\right)_e^\delta \ (\mathfrak{p}_1), \tag{4}$$

$$\left(\frac{t^{-1}g(x)}{x^\delta - R_{id}}\right)_{e,\mathbb{F}_q} \equiv \left(\frac{t^{-1}}{\mathfrak{q}_1}\right)_e^\delta \ (\mathfrak{q}_1). \tag{5}$$

Combining with the formulas above and (3) yields

$$\left(\frac{t^{-1}}{\mathfrak{p}_1}\right)_e^\delta = \left(\frac{c_p}{\mathfrak{p}_1}\right)_e \left(\frac{\alpha}{\mathfrak{p}_1}\right)_e, \quad \left(\frac{t^{-1}}{\mathfrak{q}_1}\right)_e^\delta = \left(\frac{c_q}{\mathfrak{q}_1}\right)_e \left(\frac{\beta}{\mathfrak{q}_1}\right)_e. \tag{6}$$

Since an adversary can find c_N and γ_N, it then gains $\left(\frac{t^{-1}}{\mathfrak{a}_1}\right)_e$ by computing $\left(\frac{c_N\gamma_N}{\mathfrak{a}_1}\right)_e^{\delta^{e-2} \bmod e}$.

Example 2. Finally, we give a toy example to demonstrate how an adversary attacks the space-efficient variation of BLS scheme. Assume that all parameters are set as in Table 2.

Table 2. Parameters of the space-efficient variation of BLS scheme in *Example 2*

Parameter	*Value*	*Parameter*	*Value*
N	4331	R_{id}	158
p	61	r_{id}	67
q	71	$f(x)$	$x^4 + 2x^3 + 3x^2 + 4x + 6$
e	5	t	7
μ	1900	$\frac{g(x)}{t}$	$2102x + 3769$
δ	2		

By calculation, we learn $\left(\frac{7}{\mathfrak{p}_1}\right)_5 = \zeta_5^4$, $\left(\frac{7}{\mathfrak{q}_1}\right)_5 = \zeta_5$. An adversary first analyzes as

$$x^2 - 158 \equiv 2102^{-2}3769^2 - 158 = 1416 \pmod{2102x + 3769},$$

then gets $c_N = \left((-1)^2 2102^2\right)$, $\gamma_N = 1416$, and finally discloses the plaintext $\left(\frac{c_N\gamma_N}{\mathfrak{a}_1}\right)_5^3 = 1 = \left(\frac{7^{-1}}{\mathfrak{a}_1}\right)_5$. Actually, one can check that $\left(\frac{c_N\gamma_N}{\mathfrak{p}_1}\right)_5 = \left(\frac{7}{\mathfrak{p}_1}\right)_5^3 = \zeta_5^2$, $\left(\frac{c_N\gamma_N}{\mathfrak{q}_1}\right)_5 = \left(\frac{7}{\mathfrak{q}_1}\right)_5^3 = \zeta_5^3$.