Extended Galbraith's Test on the Anonymity of IBE Schemes from Higher Residuosity

Xiaopeng Zhao[1], Zhenfu Cao[1,2(✉)], Xiaolei Dong[1], and Jun Shao[3]

[1] Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, China
52164500025@stu.ecnu.edu.cn, zfcao@sei.ecnu.edu.cn
dongxiaolei@sei.ecnu.edu.cn, jinwen.zheng@foxmail.com
[2] Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen and Shanghai Institute of Intelligent Science and Technology, Tongji University, China
[3] School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou, China
chn.junshao@gmail.com

Abstract. At PKC 2019, Clear and McGoldrick presented the first identity-based encryption (IBE) scheme that supports homomorphic addition modulo a poly-sized prime e. Assuming that deciding solvability of a special system of multivariate polynomial equations is hard, they proved that their scheme for $e > 2$ is anonymous. In this paper, we review the classical Galbraith's test on the anonymity of the first pairing-free IBE scheme due to Cocks. With the eye of the reciprocity law over $\mathbb{F}_q[x]$, we can have a profound understanding of the test and naturally extend it to give a practical attack on the anonymity of the Clear-McGoldrick IBE scheme. Furthermore, we believe that our technique plays a crucial role in anonymizing IBE schemes from higher residuosity.

Keywords: reciprocity law over $\mathbb{F}_q[x]$ · identity-based encryption · Galbraith's test · anonymity

1 Introduction

Identity-based encryption (IBE), originally proposed by Shamir in 1984 [26], is an extension of the public-key encryption. The motivation for IBE is solving some of the inherently unavoidable problems associated with traditional public-key encryption technologies. For example, it replaces the *Public Key Infrastructure* with the *Public Key Generator*, thus removing the digital certificates' overload to manage public keys. So far, there are three main ways of constructing IBE; through the pairing, lattice and *quadratic residuosity* (QR). In 2001, Boneh and Franklin gave a pairing-based construction of IBE [6], which is a breakthrough in the field of realizing practical IBE. This construction has been extended to a wide range of cryptographic schemes that support different access controls. In the same year, Cocks came up with a totally different approach to construct IBE [16]. The security relies on the standard QR assumption in the random oracle. Its encryption solely includes several operations modulo an RSA modulus

and two evaluations of the Jacobi symbol. The main attractions of QR-based IBE schemes are that they provide an efficient implementation. Besides, they are inherently homomorphic [20] and support an unbounded number of homomorphic operations. However, Cocks' scheme only encrypts one bit of message into a ciphertext composed of a pair of two large integers, and hence it is used to encrypt short session keys in practice. Intuitively, encrypting more than one bit at a time can be achieved by considering higher residuosity. In 2013, Clear, Hughes, and Tewari [13] considered Cocks' scheme over the polynomial quotient ring $\mathbb{Z}_N[x]/(x^2 - R_{\mathsf{id}})$, where N is an RSA modulus and R_{id} is the IBE public key of an identity id due to the fact that 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] (BLS) 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 very large. Unfortunately, it is intractable to be optimized as any intuitive attempt at the compression fails to be secure due to the attack found by Boneh, LaVigne and Sabin [8].

The notion of *anonymity*, or *key-privacy* [3], is an essential requirement of privacy: it is infeasible for any adversary with limited computation ability to get the identity of the recipient from a ciphertext. Anonymous IBE schemes can be used to public-key encryption with keyword search [5], or anonymously broadcast messages [1]. Cocks' scheme is known not to be anonymous due to the *test* developed by Galbraith [5]. Ateniese and Gasti [2] proved that Galbraith's test is the *best* test against the anonymity of Cocks' scheme. Recently, in [28], 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. Despite the test, some researchers [2, 7, 15, 17, 20] managed to propose anonymous variants of Cocks' scheme. In 2007, Boneh, Gentry and Hamburg [7] addressed the ciphertext expansion issue and anonymity issue of Cocks' scheme; they designed a space-efficient, anonymous IBE system which merely expands an ℓ-bit message to a ciphertext about the size of $\ell + \log_2 N$. However, the encryption in their scheme is not efficient. In 2016, in virtue of rephrasing Galbraith's test using the discovery of the hidden algebraic structure behind Cocks' encryption, Joye [20] gave a constructive method of anonymizing Cocks' ciphertexts without increasing the ciphertext expansion or sacrificing the security. In 2019, Clear and McGoldrick [14] extended the BLS scheme to use a cryptographic hash function that can be securely instantiated. Their IBE schemes support a modular additive homomorphism modulo a poly-sized prime e (known as *Group Homomorphic Encryption*). Compared with lattice-based IBE schemes, their schemes have significantly smaller public parameters. Furthermore, they showed that their scheme for $e > 2$ is anonymous by additionally assuming the hardness of deciding solvability of a special system of multivariate polynomial equations. However, Galbraith's test might still work if we realize the hidden mathematical thought behind it. Specifically, we find that Galbraith's test can be deduced from the general reciprocity law over $\mathbb{F}_{\mathsf{q}}[x]$. Applying this

technique, we essentially generalize Galbraith's test and give a practical attack on the anonymity of the Clear-McGoldrick IBE scheme.

The rest of the paper is organized as follows. In Section 2, we recall Cocks' IBE scheme and the Galbraith's test. We also introduce some definitions and preliminaries about the reciprocity law over $\mathbb{F}_{\mathsf{q}}[x]$. In Section 3, we describe Clear-McGoldrick IBE scheme. In Section 4, we extend Galbraith's test and give an efficient attack on the anonymity of the Clear-McGoldrick scheme. Concluding remarks are given in Section 5.

2 Preliminaries

In this section, we review the classical identity-based encryption scheme due to Cocks and Galbraith's test. We also formally present the reciprocity law over $\mathbb{F}_{\mathsf{q}}[x]$ that we need for our attack.

2.1 General Notation

We shall write $x \xleftarrow{R} X$ for sampling at random an element x from the set X. If $\mathcal{A}$ is an algorithm, then we write $x \leftarrow \mathcal{A}(y)$ to mean: "run $\mathcal{A}$ on input y and the output is assigned to x".

Let N be a product of two RSA primes p and q. Let $\mathbb{J}_N = \left\{x \in \mathbb{Z}_N^* \;\middle|\; \left(\frac{x}{N}\right)_2 = 1\right\}$, i.e., the set of integers whose Jacobi symbols are 1. The set of (all) quadratic residues is denoted by $\mathbb{QR}_N = \left\{x \;\middle|\; \exists\, y \in \mathbb{Z}_N^*, x \equiv y^2 \pmod N\right\}$.

Let $\mathbb{F}_{\mathsf{q}}$ denote a finite field of size q. Every element in $\mathbb{F}_{\mathsf{q}}[x]$ has the form $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$. In this case we denote as $\deg(f) = n$ to say that f has degree n; we set $\mathrm{sgn}(f) = \alpha_n$ and call it the sign of f.

2.2 Identity-Based Encryption

An *identity-based encryption* (IBE) scheme is defined as a tuple of probabilistic polynomial time (PPT) algorithms $(\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$:

$\mathsf{Setup}(1^\kappa)$ The setup algorithm Setup is an algorithm that takes a security parameter 1^κ as input, and returns a tuple $(\mathsf{PP}, \mathsf{msk})$, where PP denotes the public parameters and msk denotes the master secret key. PP include a description of the message space $\mathcal{M}$, the ciphertext space $\mathcal{C}$, the identity space $\mathcal{I}$ and the master public key mpk.

$\mathsf{Extract}(\mathsf{PP}, \mathsf{msk}, \mathsf{id})$ The key derivation algorithm $\mathsf{Extract}$ is an algorithm that takes the public parameters PP, the master secret key msk and an identity $\mathsf{id} \in \mathcal{I}$ as inputs, and returns a private key $\mathsf{sk}_{\mathsf{id}}$, using the msk. The identity id is used as the public key and $\mathsf{sk}_{\mathsf{id}}$ is the corresponding secret key.

$\mathsf{Enc}(\mathsf{PP}, \mathsf{id}, m)$ The encryption algorithm Enc is an algorithm that takes the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$ and a message $m \in \mathcal{M}$ as inputs, and returns a ciphertext $C \in \mathcal{C}$.

$\mathsf{Dec}(\mathsf{PP}, \mathsf{id}, \mathsf{sk}_{\mathsf{id}}, C)$ The decryption algorithm Dec is an algorithm that takes the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$, a corresponding secret key $\mathsf{sk}_{\mathsf{id}}$ and a ciphertext $C \in \mathcal{C}$ as inputs, and returns the message m if C can be decrypted, and $\perp$ otherwise.

For any identity $\mathsf{id} \in \mathcal{I}$ and all messages $m \in \mathcal{M}$, the *correctness* property requires that $\mathsf{Dec}(\mathsf{PP}, \mathsf{id}, \mathsf{sk}_{\mathsf{id}}, C \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}, m)) = m$.

2.3 Cocks' IBE Scheme and Galbraith's Test

Cocks' IBE scheme proceeds as follows.

$\mathsf{Setup}(1^\kappa)$ Given a security parameter 1^κ, Setup generates two RSA primes p and q and their product $N = pq$. It also samples uniformly an element $\omega \in \mathbb{J}_N \setminus \mathbb{QR}_N$. Finally, it returns $\mathsf{PP} = \left\{\mathcal{M} = \{-1, 1\}, \mathcal{C} = \mathbb{Z}_N \times \mathbb{Z}_N, \mathcal{I} = \{0,1\}^*, N, \omega, \tilde{\mathsf{H}}\right\}$ and $\mathsf{msk} = \{p, q\}$, where $\tilde{\mathsf{H}}$ is assumed to be a cryptographic hash: $\{0,1\}^* \mapsto \mathbb{J}_N$.

$\mathsf{Extract}(\mathsf{PP}, \mathsf{msk}, \mathsf{id})$ Given the public parameters PP, the master secret key msk and an identity $\mathsf{id} \in \mathcal{I}$, $\mathsf{Extract}$ computes $a = \tilde{\mathsf{H}}(\mathsf{id})$. If $a \in \mathbb{QR}_N$, it then computes $r = a^{1/2} \bmod N$; otherwise, it computes $r = (\omega a)^{1/2} \bmod N$. Finally, it returns $\mathsf{sk}_{\mathsf{id}} = \{r\}$.

$\mathsf{Enc}(\mathsf{PP}, \mathsf{id}, m)$ Given the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$ and a message $m \in \mathcal{M}$, Enc computes $a = \tilde{\mathsf{H}}(\mathsf{id})$. Then, it chooses randomly $t, \bar{t} \in \mathbb{Z}_N$ such that $\left(\frac{t}{N}\right)_2 = \left(\frac{\bar{t}}{N}\right)_2 = m$. Finally, it computes

$$c = t + \frac{a}{t} \bmod N \quad \text{and} \quad \bar{c} = \bar{t} + \frac{\omega a}{\bar{t}} \bmod N$$

and returns the ciphertext $C = (c, \bar{c})$.

$\mathsf{Dec}(\mathsf{PP}, \mathsf{id}, \mathsf{sk}_{\mathsf{id}}, C)$ Given the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$, a corresponding secret key $\mathsf{sk}_{\mathsf{id}} = \{r\}$ and a ciphertext $C = (c, \bar{c}) \in \mathcal{C}$, Dec returns the message

$$m = \begin{cases} \left(\frac{c+2r}{N}\right)_2, & \text{if } r^2 \equiv a \pmod N; \\ \left(\frac{\bar{c}+2r}{N}\right)_2, & \text{otherwise.} \end{cases}$$

where $a = \tilde{\mathsf{H}}(\mathsf{id})$.

Remark 1. The above description generalizes the original Cocks' scheme [16] which only considers *Blum integers*, i.e., N is an RSA moduli with $p \equiv q \equiv 3 \pmod 4$. In this case, Cocks' scheme corresponds to the choice $\omega = -1$ in our description.

Galbraith's test for a Cocks' ciphertext $C = (c, \bar{c})$ is defined as the function $\mathsf{GT}_{N,2} : \mathbb{Z}_N \times \mathbb{Z}_N \mapsto \{-1, 0, 1\}$ given by

$$\mathsf{GT}_{N,2}(a, c) = \left(\frac{c^2 - 4a}{N}\right)_2 \quad \text{and} \quad \mathsf{GT}_{N,2}(\omega a, \bar{c}) = \left(\frac{\bar{c}^2 - 4\omega a}{N}\right)_2$$

Whenever the ciphertext $C = (c, \overline{c})$ is encrypted under an identity id, we always have $\mathsf{GT}_{N,2}(a, c) = \mathsf{GT}_{N,2}(a, \overline{c}) = 1$ or 0, but for encryptions under another identity id' this equation holds with probability negligibly close to $1/2$ [2], hence Cocks' scheme is not anonymous.

2.4 Reciprocity Law over $\mathbb{F}_{\mathsf{q}}[x]$

We start by explaining notations to be used and briefly give crucial definitions and results due to Carlitz [12]. We here refer to Chapter 3 in [24]. Let $P \in \mathbb{F}_{\mathsf{q}}[x]$ be an irreducible polynomial and e be a divisor of $\mathsf{q} - 1$. Note that there is a unique $\alpha \in \mathbb{F}_{\mathsf{q}}^*$ such that $a^{\frac{\mathsf{q}^{\deg(P)}-1}{e}} \equiv \alpha \pmod{P}$.

Definition 1. *If $a \in \mathbb{F}_{\mathsf{q}}[x]$ and P does not divide a, let $\left(\frac{a}{P}\right)_e$ be the unique element of $\mathbb{F}_{\mathsf{q}}^*$ such that*

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

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

Proposition 1. *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* $\alpha \in \mathbb{F}_{\mathsf{q}}$. *Then,* $\left(\frac{\alpha}{P}\right)_e = \alpha^{\frac{\mathsf{q}-1}{e}\deg(P)}$.

Just as for 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 $b \in \mathbb{F}_{\mathsf{q}}[x]$ with the prime decomposition $b = \mathrm{sgn}(b) Q_1^{f_1} \cdots Q_s^{f_s}$, and thus define

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

Proposition 2. *The symbol $\left(\frac{a}{b}\right)_e$ has the following properties:*

1. *If* $a_1 \equiv a_2 \pmod{b}$, *then* $\left(\frac{a_1}{b}\right)_e = \left(\frac{a_2}{b}\right)_e$.
2. $\left(\frac{a_1 a_2}{b}\right)_e = \left(\frac{a_1}{b}\right)_e \left(\frac{a_2}{b}\right)_e$.
3. $\left(\frac{a}{b_1 b_2}\right)_e = \left(\frac{a}{b_1}\right)_e \left(\frac{a}{b_2}\right)_e$.
4. $\left(\frac{a}{b}\right)_e \neq 0$ *if and only if a is relatively prime to b.*
5. *If* $x^e \equiv a \pmod{b}$ *is solvable, then* $\left(\frac{a}{b}\right)_e = 1$.

The following fascinating theorem tells the *general reciprocity law* for $\mathbb{F}_{\mathsf{q}}[x]$.

Proposition 3 (The general reciprocity law [12]). *Let $a, b \in \mathbb{F}_{\mathsf{q}}[x]$ be relatively prime, non-zero elements. Then,*

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

3 The Clear-McGoldrick IBE Scheme

Let ζ_e be an e-th primitive root of unity, i.e., $\zeta_e = \exp(2\pi i/e)$. We consider $e \geq 2$ and let $N = pq$ be a product of two RSA primes p and q such that $e|p-1$ and $e|q-1$ henceforce. Let $\mu \in \mathbb{Z}_N^*$ be a primitive root of unity modulo p and q. We obtain

$$p\mathbb{Z}[\zeta_e] = \prod_{i \in \mathbb{Z}_e^*} \mathfrak{p}_i, \;\; \mathrm{Norm}(\mathfrak{p}_i) = p \;\; (i \in \mathbb{Z}_e^*), \;\; \text{and}$$
$$q\mathbb{Z}[\zeta_e] = \prod_{j \in \mathbb{Z}_e^*} \mathfrak{q}_j, \;\; \mathrm{Norm}(\mathfrak{q}_j) = q \;\; (j \in \mathbb{Z}_e^*),$$

where $\mathfrak{p}_i = p\mathbb{Z}[\zeta_e] + (\zeta_e - \mu^i)\mathbb{Z}[\zeta_e]$ and $\mathfrak{q}_j = q\mathbb{Z}[\zeta_e] + (\zeta_e - \mu^j)\mathbb{Z}[\zeta_e]$. We use the symbol $\left(\frac{\cdot}{\cdot}\right)_e$ to denote the *e-th power residue symbol* defined in [18, Definition 4.1]. Recently, Zhao *et al.* [30] showed that computing e-th power residue symbols $\left(\frac{x}{\mathfrak{p}_1}\right)_e$ (and also $\left(\frac{x}{\mathfrak{q}_1}\right)_e$) for $x \in \mathbb{Z}$ is equivalent to solving the *discrete logarithm problem* in the cyclic subgroup $\langle\mu\rangle$ of order e in $\mathbb{Z}_p^*$ (and $\mathbb{Z}_q^*$). Let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1 = N\mathbb{Z}[\zeta_e] + (\zeta_e - \mu)\mathbb{Z}[\zeta_e]$. We define a function $\mathsf{J}_N : \mathbb{Z}_N \mapsto \{0, \ldots, e-1\}$ as follows.

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

We assume that there exists a cryptographic hash function

$$\mathsf{H} : \{0,1\}^* \mapsto \{x \in \mathbb{Z}_N \mid \mathsf{J}_N(x) = 0\}.$$

The Clear-McGoldrick IBE scheme proceeds as follows. Note that the scheme is parameterized by a prime e [4].

$\mathsf{Setup}(1^\kappa)$ Given a security parameter 1^κ. Setup generates two RSA primes p and q such that $e|p-1$ and $e|q-1$ and their product $N = pq$. It then samples uniformly an element $\omega \in \mathbb{Z}_N^*$ such that $\mathsf{J}_N(\omega) = 0$ and $\left(\frac{\omega}{\mathfrak{p}_1}\right)_e \neq 1$. For each $i \in \{0, 1, \ldots, e-1\}$, it sets $\alpha_{i+1} = \omega^i \bmod N$. It also chooses uniformly a nontrivial, non-degenerate root of unity $\mu \in \mathbb{Z}_N^*$. Finally, it returns the public parameters

$$\mathsf{PP} = \{\mathcal{M} = \{0, 1, \ldots, e-1\},$$
$$\mathcal{C} = \{(c_1(x), \ldots, c_e(x)) \mid c_i(x) \in \mathbb{Z}_N[x], \deg(c_i(x)) < e, 1 \leq i \leq e\},$$
$$\mathcal{I} = \{0,1\}^*, N, \mu, \alpha_1, \ldots, \alpha_e\}$$

and the master secret key $\mathsf{msk} = \{p, q\}$.

[4] It is better to use a small prime e because of its small message-ciphertext expansion factor. In practice, we can use the Chinese Remainder Theorem to support homomorphic addition modulo a "large" square-free modulus, see [14, Section 3.5].

$\mathsf{Extract}(\mathsf{PP}, \mathsf{msk}, \mathsf{id})$ Given the public parameters PP, the master secret key msk and an identity $\mathsf{id} \in \mathcal{I}$, $\mathsf{Extract}$ computes $a = \mathsf{H}(\mathsf{id})$ and checks which of $\alpha_1 a, \ldots, \alpha_e a$ is an e-th residue, say i. It then computes the e-th root of $\alpha_i a$ using p and q, say r. Finally, it returns $\mathsf{sk}_{\mathsf{id}} = \{i, r\}$.

$\mathsf{Enc}(\mathsf{PP}, \mathsf{id}, m)$ Given the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$ and a message $m \in \mathcal{M}$, Enc computes $a = \mathsf{H}(\mathsf{id})$ and defines the sub-algorithm $\mathcal{E}$ as follows.

Algorithm 1 $\mathcal{E}(v, m)$

Input: an integer v **and a message** $m \in \mathcal{M}$
Output: a polynomial in $\mathbb{Z}_N[x]$

1: Generate a polynomial $f(x) \xleftarrow{R} \mathbb{Z}_N[x]$ of degree $e - 1$.
2: Compute $g(x) = f(x)^e \bmod x^e - v$.
3: Choose an integer $t \xleftarrow{R} \mathbb{Z}_N^*$ such that $\mathsf{J}_N(t) = m$.
4: Output the polynomial $c(x) = t \cdot g(x)$.

Finally, it returns the ciphertext $C = (c_1(x), \ldots, c_e(x))$, where $c_i(x) \leftarrow \mathcal{E}(\alpha_i \cdot a, m)$ is obtained by running Algorithm 1 for each $1 \le i \le e$.

$\mathsf{Dec}(\mathsf{PP}, \mathsf{id}, \mathsf{sk}_{\mathsf{id}}, C)$ Given the public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$, a corresponding secret key $\mathsf{sk}_{\mathsf{id}} = \{i, r\}$ and a ciphertext $C = (c_1(x), \ldots, c_e(x)) \in \mathcal{C}$, Dec returns the message $m = \mathsf{J}_N(c_i(r))$.

Remark 2. The correctness and the additive homomorphism property of the Clear-McGoldrick scheme can be obtained from [14]. In particular, if we take $e = 2$ and choose $f(x)$ from the set $\left\{t^{-1}x + 1 \;\middle|\; t \in \mathbb{Z}_N^*, \mathsf{J}_N(t) = m\right\}$ instead of $\mathbb{Z}_N[x]$, then the ciphertext polynomial becomes

$$c_i(x) \equiv t + \frac{\alpha_i a}{t} + 2x \pmod{x^2 - \alpha_i a}, \qquad i = 1, 2.$$

This is exactly the same as Cocks' IBE scheme described in Section 2.3, corresponding to $\alpha_1 = 1$ and $\alpha_2 = \omega$, respectively.

Computing Jacobi symbols without factoring the modulus can be achieved by combining the Euclidean algorithm with quadratic reciprocity as well as the accompanying complementary laws. To some extent this method can be generalized for computing higher power residue symbols [4, 9–11, 21, 22, 25, 27, 29] (e.g., using Kummer's reciprocity law [19, pp. 289–290]). For example, the method is used to compute cubic and quintic power residue symbols in the context of higher power generalizations of the Rabin–Williams scheme [25, 29]; Caranay and Scheidler [11] developed a fast and effective algorithm for computing $\left(\frac{\alpha}{\beta}\right)_7, \gcd(\alpha, \beta) \simeq 1, \mathrm{Trace}(\beta) \not\equiv 0 \pmod 7$ in $\mathbb{Z}[\zeta_7]$, with running time linear in $\log(\mathrm{Norm}(\beta))$. Recently, the general case of computing higher power residue symbols was tackled by Squirrel [27] and Boer [4], moreover, the resulting algorithms are probabilistic.

4 Extended Galbraith's Test on the Anonymity of the Clear-McGoldrick IBE Scheme

In this section, we extend Galbraith's test and present an efficient attack on the anonymity of the Clear-McGoldrick scheme. We keep the notations as in the Clear-McGoldrick scheme described in Section 3. We first establish some notations for our attack. Let $R = \mathbb{Z}[\zeta_e]$ be the *ring of integers* of the field $\mathbb{Q}(\zeta_e)$. If $A, B \in R$ and $\mathfrak{I}$ is an ideal of R, the relation $A - B \in \mathfrak{I}$ shall be written as $A \equiv B \ (\mathfrak{I})$. Let $u(x)$ and $v(x)$ be in $\mathbb{Z}_N[x]$. We use the symbol $\left(\frac{u(x)}{v(x)}\right)_{e,\mathbb{F}_p}$ to denote the e-th power residue symbol $\left(\frac{\iota(u(x))}{\iota(v(x))}\right)_e$ defined in Section 2.4, where ι maps a polynomial $h(x) = (\beta_n/N\mathbb{Z})x^n + (\beta_{n-1}/N\mathbb{Z})x^{n-1} + \cdots + (\beta_0/N\mathbb{Z})$ in $\mathbb{Z}_N[x]$ to $\iota(h(x)) = (\beta_n/p\mathbb{Z})x^n + (\beta_{n-1}/p\mathbb{Z})x^{n-1} + \cdots + (\beta_0/p\mathbb{Z})$ in $\mathbb{F}_p[x]$. The symbol $\left(\frac{u(x)}{v(x)}\right)_{e,\mathbb{F}_q}$ can be defined analogously.

Considering the Clear-McGoldrick scheme's decryption. Given any polynomial $c_i(x)$ in the ciphertext $C = (c_1(x), \ldots, c_e(x))$, we can see that

$$c_i(x) = t \cdot g(x) \equiv t \cdot f(x)^e \pmod{x^e - \alpha_i a}, \quad i = 1, 2, \ldots, e,$$

where $\mathsf{J}_N(t)$ is equal to the message m. It follows that, for each $i = 1, 2, \ldots, e$,

$$\begin{aligned}\left(\frac{c_i(x)}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_p} &= \left(\frac{tf(x)^e}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_p} \\ &= \prod_{j=1}^{k} \left(\frac{t}{\eta_j}\right)_{e,\mathbb{F}_p}^{p_j} \\ &= \prod_{j=1}^{k} t^{\left(\frac{p-1}{e} p_j \deg(\eta_j)\right)} \equiv 1 \ \ (\mathfrak{p}_1).\end{aligned} \tag{1}$$

by Proposition 1 and 2, where $x^e - \alpha_i a = \prod_{j=1}^{k} \eta_j^{p_j}$ is the prime decomposition of $x^e - \alpha_i a$ in $\mathbb{F}_p[x]$. Similarly, we also have

$$\left(\frac{c_i(x)}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_q} \equiv 1 \ \ (\mathfrak{q}_1), \quad i = 1, 2, \ldots, e. \tag{2}$$

Next, we consider another means of computation by the general reciprocity law stated in Proposition 3. Given a polynomial $\Phi(x) \in \mathbb{Z}_N[x]$, which is prime to $x^e - \alpha_i a$, we may assume without loss of generality that $\deg(\Phi(x)) < e$. From each of the polynomials $x^e - \alpha_i a, i = 1, 2, \ldots, e$, we can recursively use the *Euclidean Algorithm* for it and $\Phi(x)$ in $\mathbb{F}_p[x]$: by successive congruences we can

write

$$\begin{aligned} x^e - \alpha_i a &\equiv \Phi_{i1}(x) \pmod{\Phi(x)} \\ \Phi(x) &\equiv \Phi_{i2}(x) \pmod{\Phi_{i1}(x)} \\ \Phi_{i1}(x) &\equiv \Phi_{i3}(x) \pmod{\Phi_{i2}(x)} \\ &\cdots \\ \Phi_{i(s_i-1)}(x) &\equiv \gamma_i \pmod{\Phi_{is_i}(x)} \end{aligned} \tag{3}$$

where γ_i is the last nonzero remainder, and

$$e > \deg(\Phi(x)) > \deg(\Phi_{i1}(x)) > \ldots > \deg(\Phi_{is_i}(x)) > 0$$

is a decreasing sequence. Let $deg_j = \deg(\Phi_{ij}(x))$ and $sgn_j = \operatorname{sgn}(\Phi_{ij}(x))$ for fixed i and each $j = 1, 2, \ldots, s_i$. From Proposition 1, 2 and 3, we have

$$\begin{aligned} \left(\frac{\Phi(x)}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_p} &= \left(\boxed{(-1)^{\deg(\Phi(x))e} \operatorname{sgn}(\Phi(x))^e}\right)^{\frac{p-1}{e}} \left(\frac{\Phi_{i1}(x)}{\Phi(x)}\right)_{e,\mathbb{F}_p} \\ \left(\frac{\Phi_{i1}(x)}{\Phi(x)}\right)_{e,\mathbb{F}_p} &= \left(\boxed{(-1)^{deg_1 \deg(\Phi(x))} sgn_1^{\deg(\Phi(x))} \operatorname{sgn}(\Phi(x))^{-deg_1}}\right)^{\frac{p-1}{e}} \left(\frac{\Phi_{i2}(x)}{\Phi_{i1}(x)}\right)_{e,\mathbb{F}_p} \\ &\cdots \\ \left(\frac{\Phi_{is_i}(x)}{\Phi_{i(s_i-1)}(x)}\right)_{e,\mathbb{F}_p} &= \left(\boxed{(-1)^{deg_{s_i} deg_{(s_i-1)}} sgn_{s_i}^{deg_{(s_i-1)}} sgn_{(s_i-1)}^{-deg_{s_i}}}\right)^{\frac{p-1}{e}} \left(\frac{\gamma_i}{\Phi_{is_i}(x)}\right)_{e,\mathbb{F}_p} \\ \left(\frac{\gamma_i}{\Phi_{is_i}(x)}\right)_{e,\mathbb{F}_p} &= \gamma_i^{deg_{s_i} \cdot \frac{p-1}{e}} \end{aligned} \tag{4}$$

Let $\lambda_{ij} \in \mathbb{F}_p^*$ be elements boxed in the j-th equation of (4) for each $j = 1, 2, \ldots, s_i + 1$. We conclude from equation (4) that, for each $i = 1, 2, \ldots, e$,

$$\begin{aligned} \left(\frac{\Phi(x)}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_p} &= \left(\gamma_i^{deg_{s_i}} \prod_{j=1}^{s_i+1} \lambda_{ij}\right)^{\frac{p-1}{e}} \\ &\equiv \left(\frac{\gamma_i^{deg_{s_i}} \prod_{j=1}^{s_i+1} \lambda_{ij}}{\mathfrak{p}_1}\right)_e \quad (\mathfrak{p}_1), \end{aligned}$$

and similarly that

$$\left(\frac{\Phi(x)}{x^e - \alpha_i a}\right)_{e,\mathbb{F}_q} \equiv \left(\frac{\delta_i^{deg_{s_i'}} \prod_{j=1}^{s_i'+1} \theta_{ij}}{\mathfrak{q}_1}\right)_e \quad (\mathfrak{q}_1)$$

for some natural number s_i' and $\delta_i \in \mathbb{F}_q, \theta_{ij} \in \mathbb{F}_q^*$.

Now, we consider the game between a challenger and an adversary $\mathcal{A}$ about anonymity. Suppose that $\mathcal{A}$ receives a challenge ciphertext $C = (c_1(x), \ldots, c_e(x))$

and tries to judge whether C is encrypted by some identity id. Although $\mathcal{A}$ does not know the factorization of N, it can perform the steps as mentioned above by the Euclidean Algorithm and Proposition 3 in $\mathbb{Z}_N[x]$ with overwhelming probability, that is, $\mathcal{A}$ is capable of obtaining an element ϑ_i in $\mathbb{Z}_N$ such that

$$\vartheta_i \equiv \gamma_i^{deg_{s_i}} \prod_{j=1}^{s_i+1} \lambda_{ij} \pmod{p}$$
$$\vartheta_i \equiv \delta_i^{deg_{s'_i}} \prod_{j=1}^{s'_i+1} \theta_{ij} \pmod{q}$$

with overwhelming probability. This indicates that

$$\begin{aligned} \mathsf{GT}_{N,e}\left(\alpha_i a, \Phi(x)\right) &= \left(\frac{\left(\frac{\Phi(x)}{x^e-\alpha_i a}\right)_{e,\mathbb{F}_p}^{\frac{e}{p-1}}}{\mathfrak{p}_1} \right)_e \left(\frac{\left(\frac{\Phi(x)}{x^e-\alpha_i a}\right)_{e,\mathbb{F}_q}^{\frac{e}{q-1}}}{\mathfrak{q}_1} \right)_e \\ &= \left(\frac{\vartheta_i}{\mathfrak{p}_1}\right)_e \left(\frac{\vartheta_i}{\mathfrak{q}_1}\right)_e \\ &= \left(\frac{\vartheta_i}{\mathfrak{a}}\right)_e \qquad\qquad i = 1, 2, \ldots, e. \end{aligned} \tag{5}$$

Thus, if the ciphertext C is generated by an identity id with $\mathsf{H}(\mathsf{id}) = a$, the values of $\left(\frac{\vartheta_i}{\mathfrak{a}}\right)_e, i = 1, 2, \ldots, e$ will always be 1 (or 0) according to the equations (1), (2) and (5); otherwise, we naturally conjecture that the values of $\left(\frac{\vartheta_i}{\mathfrak{a}}\right)_e, i = 1, 2, \ldots, e$ are statistically close to the uniform distribution on the set $\{1, \zeta_e, \ldots, \zeta_e^{e-1}\}$ (we see below that this conjecture is rational). Put another way, we have given an efficient attack on the anonymity of the Clear-McGoldrick scheme. The *extended Galbraith's test* is in the form of the equation (5).

We now show that when $e = 2$, the extended Galbraith's test corresponds exactly to the original Galbraith's test on the anonymity of Cocks' IBE scheme (see also Section 2.3). According to Remark 2, let

$$c_i(x) \equiv \overline{c_i} + 2x \pmod{x^2 - \alpha_i a}, \quad i = 1, 2,$$

where $\overline{c_i} = t + \frac{\alpha_i a}{t}$ is the ciphertext in Cocks' scheme, then we have

$$x^2 - \alpha_i a \equiv \left(2^{-1}\overline{c_i}\right)^2 - \alpha_i a \pmod{\overline{c_i} + 2x}, \quad i = 1, 2.$$

From the above attack, we learn

$$\vartheta_i = (-1)^{1\cdot 2}\left(\mathrm{sgn}(\overline{c_i} + 2x)\right)^2 \cdot \left(\left(2^{-1}\overline{c_i}\right)^2 - \alpha_i a\right) = \overline{c_i}^2 - 4\alpha_i a, \quad i = 1, 2.$$

Thus we derive the original Galbraith's test

$$\left(\frac{\vartheta_i}{\mathfrak{a}}\right)_2 = \left(\frac{\overline{c_i}^2 - 4\alpha_i a}{N}\right)_2, \quad i = 1, 2.$$

for Cocks' scheme according to Remark 1 and 2. Using Perron's result [23], Ateniese and Gasti [2, Lemma 1] proved that, given an RSA modulus and $\overline{a} \in \mathbb{J}_N$, the distribution on

$$\left\{ \left(\frac{\overline{t}^2 + \overline{a}}{N} \right)_2 \;\middle|\; \overline{t} \xleftarrow{R} \mathbb{Z}_N^* \right\}$$

is computationally indistinguishable from the uniform distribution on $\{-1, +1\}$ under the QR assumption[5]. They also argued that there is no *better* test. A natural question is whether Perron's result can be extended to the case of higher residuosity. If the answer is affirmative, we believe that these properties can also be extended to the extended Galbraith's test by applying [30, Theorem 1]]. To make the test more convincing, we finally give a toy example to illustrate how it works.

Example 1. Assume that the parameters of the Clear-McGoldrick scheme are set as in Table 1, where the value of ω is omitted since it is immaterial to our example. For simplicity, we only consider the first ciphertext polynomial $c_1(x)$ in the ciphertext $C = (c_1(x), \ldots, c_e(x))$.

Table 1. Parameters of the Clear-McGoldrick scheme in Example 1

Parameter	Value	Parameter	Value
N	4331	$\mathsf{sk}_{\mathsf{id}}$	$\{1, 67\}$
p	61	$\mathsf{H}(\mathsf{id}')$	467
q	71	$\mathsf{sk}_{\mathsf{id}'}$	$\{1, 51\}$
e	5	t	2475
μ	1900	$f(x)$	$x^4 + 2x^3 + 3x^2 + 4x + 6$
$\mathsf{H}(\mathsf{id})$	822	$c_1(x) = t \cdot f(x)^5 \bmod x^5 - \mathsf{H}(\mathsf{id})$	$3184x^4 + 3485x^3 + 1183x^2 + 3757x + 1193$

Here, the ciphertext polynomial $c_1(x)$ is generated by the identity id. To distinguish the identity of $c_1(x)$ between the identity id and id', an adversary $\mathcal{A}$ may perform the following computations in $\mathbb{Z}_N[x]$ using the Euclidean Algorithm.

[5] In [28, Theorem 3.4], the authors proved that the two distributions above are statistically indistinguishable, without any complexity assumption.

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

Next,$\mathcal{A}$ derives from the extended Galbraith's test on $x^5 - \mathsf{H}(\mathsf{id})$ that

$$\begin{aligned}\vartheta_1 &\equiv (-1)^{4\cdot 5} \cdot 3184^5 \cdot (-1)^{3\cdot 4} \cdot 3855^4 \cdot 3184^{-3} \cdot (-1)^{2\cdot 3} \cdot 29^3 \cdot 3855^{-2} \\ &\quad \cdot (-1)^{1\cdot 2} \cdot 3938^2 \cdot 29^{-1} \cdot 55 \equiv (3184 \cdot 3855 \cdot 29 \cdot 3938)^2 \cdot 55 \pmod{4331},\end{aligned}$$

and similarly from the extended Galbraith's test on $x^5 - \mathsf{H}(\mathsf{id}')$ that

$$\vartheta_1' \equiv (3184 \cdot 3855 \cdot 29 \cdot 3512)^2 \cdot 4315 \pmod{4331}.$$

Finally, $\mathcal{A}$ computes the following quintic residue symbols by applying [25, Algorithm 6.2] (note that every rational integer not divisible by $e = 5$ is *primary* [11, Definition 2.5]).

$$\left(\frac{\vartheta_1}{\mathfrak{a}}\right)_5 = 1$$
$$\left(\frac{\vartheta_1'}{\mathfrak{a}}\right)_5 = \zeta_5^3 \neq 1$$

and, in essence, captures the fact that the ciphertext C belongs to the identity id.

5 Concluding Remarks

We have shown an efficient attack on the anonymity of Clear-McGoldrick IBE scheme by extending the classical Galbraith's test. At PKC 2016, Joye [20] gave an anonymous variant of Cocks' IBE scheme on Galbraith's test. We believe that

the Clear-McGoldrick scheme can likewise be improved to achieve the anonymity by Joye's approach and the extended Galbraith's test we have investigated. For example, one can choose p and q such that $\left(\frac{-1}{\mathfrak{a}}\right)_e = \zeta_e^u$, $\gcd(u, e) = 1$, and generate a middle ciphertext $(c_1(x), \ldots, c_e(x))$ by running Clear-McGoldrick's encryption and the final ciphertext is $C = (c_1(x) \cdot x^t, \ldots, c_e(x) \cdot x^t)$ where $t \xleftarrow{R} \mathbb{Z}_e$. If we construct ciphertexts in this way, an adversary can not get the recipient's identity from the ciphertext C only by means of the extended Galbraith's test. This is because the following relation holds according to the equation (5) together with Proposition 1, 2 and 3 in Section 3.

$$\begin{aligned}
\mathsf{GT}_{N,e}\left(\alpha_i a, c_i(x) \cdot x^t\right) &= \left(\frac{-\alpha_i a}{\mathfrak{a}}\right)_e^t \cdot \mathsf{GT}_{N,e}\left(\alpha_i a, c_i(x)\right) \\
&= \zeta_e^{ut} \cdot \mathsf{GT}_{N,e}\left(\alpha_i a, c_i(x)\right) \\
&= \zeta_e^{ut} \qquad\qquad i = 1, 2, \ldots, e.
\end{aligned}$$

For decryption, the recipient needs the extended Galbraith's test to compute t to recover the message. For an anonymous construction of the case $e = 2$, please refer to [31].

Acknowledgements. This work was supported in part by the National Natural Science Foundation of China (Grant No.61632012 and 61672239), in part by the Peng Cheng Laboratory Project of Guangdong Province (Grant No. PCL2018KP004), and in part by the "Fundamental Research Funds for the Central Universities".

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. J. Cryptology **21**(3), 350–391 (2008). https://doi.org/10.1007/s00145-007-9006-6
2. Ateniese, G., Gasti, P.: Universally anonymous IBE based on the quadratic residuosity assumption. In: Fischlin, M. (ed.) Topics in Cryptology - CT-RSA 2009. LNCS, vol. 5473, pp. 32–47. Springer (2009). https://doi.org/10.1007/978-3-642-00862-7_3
3. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 566–582. Springer (2001)
4. de Boer, K.: Computing the power residue symbol. Master's thesis. Nijmegen, Radboud University. `www.koendeboer.com` (2016)
5. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer (2004). https://doi.org/10.1007/978-3-540-24676-3_30
6. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer (2001). https://doi.org/10.1007/3-540-44647-8_13

7. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption-without pairings. In: 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). pp. 647–657. IEEE (2007)
8. Boneh, D., LaVigne, R., Sabin, M.: 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. Brier, E., Ferradi, H., Joye, M., Naccache, D.: New number-theoretic cryptographic primitives. Journal of Mathematical Cryptology **14**(1), 224–235 (2020). https://doi.org/10.1515/jmc-2019-0035
10. Brier, E., Naccache, D.: The thirteenth power residue symbol. IACR Cryptology ePrint Archive **2019**, 1176 (2019), https://eprint.iacr.org/2019/1176
11. Caranay, P.C., Scheidler, R.: An efficient seventh power residue symbol algorithm. International Journal of Number Theory **6**(08), 1831–1853 (2010)
12. Carlitz, L.: On certain functions connected with polynomials in a Galois field. Duke Mathematical Journal **1**(2), 137–168 (1935)
13. Clear, M., Hughes, A., Tewari, H.: Homomorphic encryption with access policies: Characterization and new constructions. In: Youssef, A.M., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 61–87. Springer (2013). https://doi.org/10.1007/978-3-642-38553-7_4
14. Clear, M., McGoldrick, C.: Additively homomorphic IBE from higher residuosity. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11442, pp. 496–515. Springer (2019). https://doi.org/10.1007/978-3-030-17253-4_17
15. Clear, M., Tewari, H., McGoldrick, C.: Anonymous IBE from quadratic residuosity with improved performance. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 377–397. Springer (2014). https://doi.org/10.1007/978-3-319-06734-6_23
16. Cocks, C.C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding, 8th IMA International Conference, 2001, Proceedings. LNCS, vol. 2260, pp. 360–363. Springer (2001). https://doi.org/10.1007/3-540-45325-3_32
17. Crescenzo, G.D., Saraswat, V.: Public key encryption with searchable keywords based on Jacobi symbols. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 282–296. Springer (2007). https://doi.org/10.1007/978-3-540-77026-8_21
18. Freeman, D.M., Goldreich, O., Kiltz, E., Rosen, A., Segev, G.: More constructions of lossy and correlation-secure trapdoor functions. Journal of cryptology **26**(1), 39–74 (2013)
19. Hilbert, D.: The Theory of Algebraic Number Fields. Springer-Verlag, Berlin, Germany (1998)
20. Joye, M.: Identity-based cryptosystems and quadratic residuosity. In: Cheng, C., Chung, K., Persiano, G., Yang, B. (eds.) Public-Key Cryptography - PKC 2016. LNCS, vol. 9614, pp. 225–254. Springer (2016). https://doi.org/10.1007/978-3-662-49384-7_9
21. Joye, M.: Evaluating octic residue symbols. IACR Cryptology ePrint Archive **2019**, 1196 (2019), https://eprint.iacr.org/2019/1196
22. Joye, M., Lapiha, O., Nguyen, K., Naccache, D.: The eleventh power residue symbol. IACR Cryptology ePrint Archive **2019**, 870 (2019), https://eprint.iacr.org/2019/870
23. Perron, O.: Bemerkungen über die verteilung der quadratischen reste. Mathematische Zeitschrift **56**(2), 122–130 (1952)

24. Rosen, M.: Number theory in function fields, vol. 210. Springer Science & Business Media (2013)
25. Scheidler, R., Williams, H.C.: A public-key cryptosystem utilizing cyclotomic fields. Des. Codes Cryptogr. **6**(2), 117–131 (1995). https://doi.org/10.1007/BF01398010
26. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) Advances in Cryptology, Proceedings of CRYPTO '84. LNCS, vol. 196, pp. 47–53. Springer (1984). https://doi.org/10.1007/3-540-39568-7_5
27. Squirrel, D.: Computing reciprocity symbols in number fields. Undergraduate thesis, Reed College (1997)
28. Tiplea, F.L., Iftene, S., Teseleanu, G., Nica, A.: On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography. Appl. Math. Comput. **372** (2020). https://doi.org/10.1016/j.amc.2019.124993
29. Williams, H.C.: An M^3 public-key encryption scheme. In: Williams, H.C. (ed.) CRYPTO. LNCS, vol. 218, pp. 358–368. Springer (1985). https://doi.org/10.1007/3-540-39799-X_26
30. Zhao, X., Cao, Z., Dong, X., Shao, J., Wang, L., Liu, Z.: New assumptions and efficient cryptosystems from the e-th power residue symbol. In: Liu, J.K., Cui, H. (eds.) ACISP. LNCS, vol. 12248, pp. 408–424. Springer (2020). https://doi.org/10.1007/978-3-030-55304-3_21
31. Zhao, X., Cao, Z., Dong, X., Zheng, J.: Anonymous IBE from quadratic residuosity with fast encryption. IACR Cryptology ePrint Archive **2020**, 712 (2020), https://eprint.iacr.org/2020/712