On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography

Ferucio Laurenţiu Ţiplea[1,3], Sorin Iftene[1], George Teşeleanu[1,2], Anca-Maria Nica[1]

[1] Department of Computer Science
"Alexandru Ioan Cuza" University of Iaşi 700505 Iaşi, Romania
{ferucio.tiplea,siftene}@uaic.ro
contact@ancamarianica.ro
[2] Advanced Technologies Institute
021101 Bucharest, Romania
tgeorge@dcti.ro
[3] Simion Stoilow Institute of Mathematics of the Romanian Academy
010702 Bucharest, Romania

Abstract. We develop exact formulas for the distribution of quadratic residues and non-residues in sets of the form $a + X = \{(a + x) \bmod n \mid x \in X\}$, where n is a prime or the product of two primes and X is a subset of integers with given Jacobi symbols modulo prime factors of n. We then present applications of these formulas to Cocks' identity-based encryption scheme and statistical indistinguishability.

Keywords: Jacobi symbol, probability distribution, statistical distance, identity-based encryption

1 Introduction and Preliminaries

The theory of quadratic residues has proved to be very useful in cryptography. Two classic and notable achievements in this direction are the Rabin public-key cryptosystem [22] and the Goldwasser-Micali probabilistic public-key cryptosystem [15]. The Rabin cryptosystem encrypts messages by quadratic residues, while the Goldwasser-Micali cryptosystem encrypts one-bit messages by multiplying random quadratic residues by a public quadratic non-residue whose Jacobi symbol in one, raised to the message power. In both cases, the computation is performed modulo a product of two primes. Another notable achievement is the Blum-Blum-Shub pseudo-random number generator [3]. The initial state of this generator is a random quadratic residue modulo a Blum integer. At each iteration, the current state is squared and the least significant bit is outputted.

Identity-based encryption (IBE) is another sub-field of cryptography where quadratic residues have proved to be very useful. Thus, in 2001, Cocks proposed the first identity-based encryption scheme based on quadratic residues [8]. The scheme encrypts messages bit by bit and each encrypted bit is a pair of two integers. The decryption consists of computing the Jacobi symbol of one of the two integers in each pair. Although Cocks' IBE scheme is efficient only for small messages, it is very elegant and *per se* revolutionary. The scheme attracted the interest of many researchers [6,1,7,17].

A careful analysis of [8,6,1,7,17] shows that integers of the form $a+r$, where a is an integer and r is a quadratic residue (modulo a given integer n), play an important role in these papers. Particularly, it turns out to be important to know the distribution of quadratic residues among all integers of the form $a+r$. A study in this direction was initiated by Perron [21] for the case of a prime modulus p. However, most applications of quadratic residues to cryptography require the use of a composite modulus $n = pq$. We are thus faced with the need to extend Perron's results to composite moduli. The same was advocated in [1] (see Section 2.3 in [1]). Here, the authors avoided the extension of Perron's results to composite moduli with the price of weaker indistinguishability results (this will be fully discussed in Section 3.2).

Contributions and Structure of the Paper The contributions of this paper are structured into two parts. The first part (the entire Section 2) considers sets of the form $a+X = \{(a+x) \bmod n \mid x \in X\}$, where n is a prime or the product of two primes $n = pq$, and X is a subset of $\mathbb{Z}_n^*$ whose elements have some given Jacobi symbols modulo prime factors of n. For instance, X may be the set of all integers in $\mathbb{Z}_n^*$ whose Jacobi symbol modulo p is 1 and Jacobi symbol modulo q is -1 (assuming $n = pq$); we say that the *Jacobi pattern* of the integers in X, in this case, is "$+-$". Then, given a set $a+X$, we look for the distribution of the quadratic residues, quadratic non-residues, etc., in $a+X$. We develop complete results for all the Jacobi patterns of length one, + and - (this corresponds to quadratic residues and non-residues modulo a prime) and Jacobi patterns of length two, $++$, $--$, $+-$, and $-+$ (this corresponds to moduli that are product of two distinct primes).

The second part of the paper's contribution (the entire Section 3) points out some applications of the results developed in the first part (Section 2). There are two main applications discussed here. The first one relates to Galbraith's test for Cocks' IBE scheme. This test was briefly described in several papers such us [4,1,17], except that some claims were not rigorously formulated and/or proved. Based on the results developed in Section 2, we were able to make a deep analysis of some distributions related to Cocks' IBE scheme and Galbraith's test, providing thus rigorous proofs for Galbraith's test.

The second application discussed in Section 3 relates to the computational indistinguishability of some distributions in [1,7,17], under the quadratic residuosity assumption. Based on the results developed in Section 2, we were able to prove statistical indistinguishability of those distributions (without any assumption).

In addition to the applications already mentioned in the paper, we believe that our study in Section 2 is important also because it contributes to a better understanding of the structure of $\mathbb{Z}_n^*$ with respect to Jacobi patterns of length at most two, which are frequently employed in cryptography.

Related Work Our work in Section 2 is a major extension of Perron's result [21], where only the distribution of quadratic residues in the set $a + QR_p$, where p is a prime, has been considered. Related studies to the one in our paper were performed in [9,10,20,18], where the problem is to calculate the probability that

$$J_p(a)J_p(a+1)\cdots J_p(a+\ell-1)$$

meets some Jacobi residuosity modulo p, a priori given, for the ℓ elements, when a is chosen uniformly at random from $a \in \mathbb{Z}_p^*$ (p is a prime). Thus, in [20] it was shown that the number of integers a with the property above is in between $p\frac{1}{2^\ell} - \epsilon$ and $p\frac{1}{2^\ell} + \epsilon$, where $\epsilon = \ell(3 + \sqrt{p})$. Dividing these two bounds by p we obtain the probability that an integer a induces a given Jacobi residuosity for the ℓ consecutive elements. A direct extension of this result to the case of RSA moduli may lead to "much larger bound" than ϵ. In [18], an extension to RSA moduli has been proposed by generalizing [10]. Thus, it was shown that the number of integers a with the property above is $n\frac{1}{2^\ell} + \mathcal{O}(\sqrt{n} \cdot \log^2 n)$, where n is an RSA modulus and $1 \leq \ell \leq (1/2 - \delta)\log_2 n$, for some $0 < \delta < 1/2$.

The results developed in our paper are different than those mentioned above for at least two main reasons. First of all, we have developed exact and not approximate formulas for the number of integers with a given Jacobi pattern in sets $a + X$. Secondly, the increment factor is arbitrary in all our studies, while it is one in all the results mentioned above.

Preliminaries We recall now the basic notation and terminology that is going to be used in the paper.

The set of integers is denoted by $\mathbb{Z}$. The gcd of two integers a and b is denoted (a, b) (the distinction between gcd and the utilization of parenthesis for pairing will be clear from context). The integers a and b are called *co-prime* if $(a, b) = 1$. If n is an integer, then a and b are called *congruent modulo n*, denoted $a \equiv b \bmod n$ or $a \equiv_n b$, if n divides $a - b$. The quotient and remainder of the integer division of a by n, assuming $n \neq 0$, are denoted $a \operatorname{div} n$ and $(a)_n$, respectively. Positive integers $n = pq$ that are product of two distinct primes p and q will be usually called *RSA integers* or *RSA moduli*. As a convention, we assume $p < q$ for all RSA moduli $n = pq$.

Given a positive integer n, $\mathbb{Z}_n$ stands for $\{0, \ldots, n-1\}$ and $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$. An integer a co-prime with n is a *quadratic residue modulo n* if $a \equiv_n x^2$, for some integer x; the integer x is called a *square root* of a modulo n. $SQRT_n(A)$ stands for the set of all square roots $x \in \mathbb{Z}_n$ of integers $a \in A$, where $A \subseteq \mathbb{Z}$. We will sometimes write $SQRT_n(a_1, \ldots, a_m)$ instead of $SQRT_n(A)$, if $A = \{a_1, \ldots, a_m\}$.

The *Chinese Remainder Theorem* (CRT) [19,25] states that the system of congruences

$$x \equiv b_i \bmod m_i \quad \text{for all } 1 \leq i \leq n$$

in the non-determinate x has a unique solution in $\mathbb{Z}_{m_1 \cdots m_n}$, if $m_1, \ldots, m_n$ are pairwise co-prime.

Let p be a prime. The *Legendre symbol* of an integer a modulo p, denoted $J_p(a)$, is defined by $J_p(a) = 1$, if a is a quadratic residue modulo p, $J_p(a) = 0$, if p divides a, and $J_p(a) = -1$, otherwise (the notation $\left(\frac{a}{p}\right)$ is also used but for the sake of simplicity we prefer to use $J_p(a)$). The *Jacobi symbol* extends the Legendre symbol to composite moduli. If $n = p_1^{e_1} \cdots p_m^{e_m}$ is the prime factorization of the positive integer n, then the Jacobi symbol of a modulo n is

$$J_n(a) = J_{p_1}(a)^{e_1} \cdots J_{p_m}(a)^{e_m}$$

For the sake of simplicity we will use the terminology of Jacobi symbol in both cases (prime or composite moduli). For details regarding basic properties of the Jacobi symbol the reader is referred to [19,25].

Given a positive integer n and a subset $A \subseteq \mathbb{Z}_n^*$, $QR_n(A)$ ($QNR_n(A)$, $J_n^+(A)$, $J_n^-(A)$) stands for the set of quadratic residues (quadratic non-residues, integers with the Jacobi symbol $+1$, integers with the Jacobi symbol -1, respectively) modulo n from A. When $A = \mathbb{Z}_n^*$, the notation will be simplified to QR_n (QNR_n, J_n^+, J_n^-, respectively). When n is a prime, $QR_n(A) = J_n^+(A)$ and $QNR_n(A) = J_n^-(A)$.

Assume now that $n = pq$ is an RSA modulus and $p < q$. Given $A \subseteq \mathbb{Z}_n^*$, define the sets $J_n^{\pm}(A) = \{a \in A \mid J_p(a) = +1,\ J_q(a) = -1\}$ and $J_n^{\mp}(A) = \{a \in A \mid J_p(a) = -1,\ J_q(a) = +1\}$.

The *quadratic residuosity* (QR) *problem* is the problem to decide, given an RSA modulus $n = pq$ and $a \in J_n^+$, where p and q are unknown, whether a is a quadratic residue or not.

Let $RSAgen(\lambda)$ be a probabilistic polynomial-time (PPT) algorithm that, given a security parameter λ, outputs a triple (n, p, q), where $n = pq$ is an RSA modulus. The *QR assumption* holds for $RSAgen(\lambda)$ if the distance

$$|P(\mathcal{D}(a,n) = 1\ :\ (n,p,q) \leftarrow RSAgen(\lambda),\ a \leftarrow QR_n) -$$

$$P(\mathcal{D}(a,n) = 1\ :\ (n,p,q) \leftarrow RSAgen(\lambda),\ a \leftarrow J_n^+ \setminus QR_n)|,$$

as a function of λ, is negligible for all PPT algorithms $\mathcal{D}$.

2 The set $a + \mathbb{Z}_n^*$

In [21], Perron studied the set $\{(a + r)_p \mid r \in QR_p\}$, where $p > 2$ is a prime and $a \in \mathbb{Z}_p^*$, in order to establish how many of its elements are still quadratic residues modulo p. In this section we extend Perron's study to sets

$$a + X = \{(a + x)_n \mid x \in X\}$$

where n is a prime or an RSA modulus, $a \in \mathbb{Z}_n^*$, and $X \subseteq \mathbb{Z}_n^*$. When n is a prime, X will be $\mathbb{Z}_n^*$, QR_n, and QNR_n; when n is an RSA modulus, X will be $\mathbb{Z}_n^*$, J_n^+, J_n^-, QR_n, QNR_n, $J_n^+ \setminus QR_n$, $J_n^{\pm}$, and $J_n^{\mp}$.

Given a set $A = a + X$ as above, we will partition $A^* = A \cap \mathbb{Z}_n^*$ into two subsets

- $QR_n(A) = A^* \cap QR_n$ and
- $QNR_n(A) = A^* \cap QNR_n$,

if n is a prime, and into four subsets

- $QR_n(A) = A^* \cap QR_n$,
- $(J_n^+ \setminus QR_n)(A) = A^* \cap (J_n^+ \setminus QR_n)$,
- $J_n^\pm(A) = A^* \cap J_n^\pm$, and
- $J_n^\mp(A) = A^* \cap J_n^\mp$,

if n is an RSA modulus. Moreover, in this last case, we will also consider $J_n^+(A) = A^* \cap J_n^+$ and $J_n^-(A) = A^* \cap J_n^-$. The diagram in Figure 1 provides a pictorial view of this case.

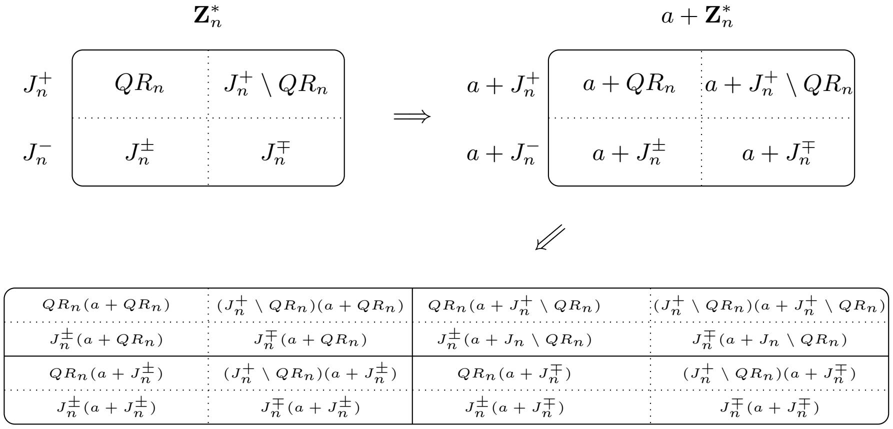

Fig. 1. Partitioning the set $a + \mathbb{Z}_n^*$ when n is an RSA modulus

Now, our goal is to estimate the cardinalities of these subsets of $\mathbb{Z}_n^*$ and then to compute probability distributions on them, such as $P(x \in QR_n : x \leftarrow a + J_n^\mp)$ (this is the probability that x is a quadratic residue when it is uniformly at random sampled from $a + J_n^\mp$).

Perron's study developed in [21] corresponds, although not exactly in the form we use in our paper, to the case of the set $QR_n(a + QR_n)$ with a prime n.

2.1 Prime moduli

We will focus in this sub-section on the calculation of the cardinalities of the sets defined above, when $n > 2$ is a prime. Recall that, in this case, $QR_n = J_n^+$, $QNR_n = J_n^-$, and $\mathbb{Z}_n^*$ is the disjoint union of the sets QR_n and QNR_n.

Proposition 1. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then,*

1. *$a + \mathbb{Z}_p = \mathbb{Z}_p$ and $|(a + \mathbb{Z}_p)^*| = |\mathbb{Z}_p^*| = p - 1$;*
2. *$a + \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{a\}$ and $|(a + \mathbb{Z}_p^*)^*| = |\mathbb{Z}_p^* \setminus \{a\}| = p - 2$.*

Proof. Both (1) and (2) are straightforward from definitions. However, we will provide some details for the first part of (2).

Given $x \in \mathbb{Z}_p^*$, the integer $(a + x)_p$ is different from a. Therefore, it is in $\mathbb{Z}_p \setminus \{a\}$. Moreover, for any $y \in \mathbb{Z}_p \setminus \{a\}$ there exists $x \in \mathbb{Z}_p^*$ such that $(a+x)_p = y$.

Proposition 2. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then,*

$$|(a + QR_p)^*| = \frac{p - 2 - J_p(-a)}{2}$$

and

$$|(a + QNR_p)^*| = \frac{p - 2 + J_p(-a)}{2}$$

Proof. Let $\alpha \in QR_p$. Clearly, $(a + \alpha)_p$ is co-prime to p iff $\alpha \neq (-a)_p$. Therefore, if $(-a)_p \in QNR_p$ then $\alpha \neq (-a)_p$ because $\alpha \in QR_p$ and, as a conclusion, all integers in $a + QR_p$ are co-prime to p.

If $(-a)_p \in QR_p$, exactly one integer in $a + QR_p$, namely $(a + (-a)_p)_p = 0$, is not co-prime to p.

If we add to these remarks the fact that $|QR_p| = (p - 1)/2$, we obtain the first part of the proposition.

The second part of this proposition follows a similar proof line to its first part. Alternatively, it can be obtained from the set partitioning

$$(a + \mathbb{Z}_p^*)^* = (a + QR_p)^* \cup (a + QNR_p)^*,$$

Proposition 1, and the formula for $|(a + QR_p)^*|$.

Corollary 1. *Let $p > 2$ be a prime and $a, b \in \mathbb{Z}_p^*$.*

1. *If a and b are of the same quadratic residuosity, then*
   (a) *$|(a + QR_p)^*| = |(b + QR_p)^*|$ and*
   (b) *$|(a + QNR_p)^*| = |(b + QNR_p)^*|$;*
2. *If a and b are of opposite quadratic residuosities, then*

$$|(a + QR_p)^*| = |(b + QNR_p)^*|.$$

Proof. All the equalities simply follow from Proposition 2 and from the fact that $(-a)_p$ and $(-b)_p$ are of the same quadratic residuosity in the first case, and are of opposite quadratic residuosities in the second case.

We go further to estimate $|QR_p(A)|$ and $|QNR_p(A)|$ for the aforementioned values of A. We begin with the case of $A = a + \mathbb{Z}_p^*$, which simply follows from Proposition 1 and from the fact that $|QR_p| = |QNR_p| = (p-1)/2$ [19,25].

Corollary 2. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then,*

$$|QR_p(a + \mathbb{Z}_p^*)| = \frac{p - 2 - J_p(a)}{2}$$

and

$$|QNR_p(a + \mathbb{Z}_p^*)| = \frac{p - 2 + J_p(a)}{2}$$

Proof. By Proposition 1(2), $QR_p(a + \mathbb{Z}_p^*) = QR_p(\mathbb{Z}_p^* \setminus \{a\})$. If $a \in QR_p$, then $|QR_p(\mathbb{Z}_p^* \setminus \{a\})| = |QR_p(\mathbb{Z}_p^*)| - 1$; otherwise, $|QR_p(\mathbb{Z}_p^* \setminus \{a\})| = |QR_p(\mathbb{Z}_p^*)|$. By taking into account that $|QR_p| = (p-1)/2$, we obtain the first part of the proposition.

The second part of the proposition follows a similar proof line to its first part. Alternatively, one may partition $(a + \mathbb{Z}_p^*)^*$ into $QR_p(a + \mathbb{Z}_p^*)$ and $QNR_p(a + \mathbb{Z}_p^*)$, and then use Proposition 1 and the first part of this corollary.

In [21], Perron proposed a very useful characterization of the quadratic residues in the set $a + QR_p$. However, he considered the integer 0 as a quadratic residue, which is not the case in our paper. For this reason and for the sake of uniformity and completeness of the paper we recall and adapt Perron's results to fit our case.

Lemma 1. *Let $p > 2$ be a prime, $a \in \mathbb{Z}_p^*$, and $r \in QR_p$. Then, $(a + r)_p \in QR_p$ if and only if there exists $u \in \mathbb{Z}_p^* \setminus SQRT_p(a, -a)$ such that $r \equiv_p \frac{1}{4}\left(u - \frac{a}{u}\right)^2$.*

Proof. Let $p > 2$ be a prime, $a \in \mathbb{Z}_p^*$, and $r \in QR_p$.

Assume first that $r \equiv_p \frac{1}{4}\left(u - \frac{a}{u}\right)^2$ for some $u \in \mathbb{Z}_p^* \setminus SQRT_p(a, -a)$. We remark that $r \not\equiv_p 0$ since u is not a square root of a. Then, the following congruences hold:

$$\begin{aligned} a + r &\equiv_p a + \tfrac{1}{4}\left(u - \tfrac{a}{u}\right)^2 \\ &\equiv_p a + \tfrac{1}{4}\left(u^2 - 2a + \tfrac{a^2}{u^2}\right) \\ &\equiv_p \tfrac{1}{4}\left(u^2 + 2a + \tfrac{a^2}{u^2}\right) \\ &\equiv_p \tfrac{1}{4}\left(u + \tfrac{a}{u}\right)^2. \end{aligned}$$

As u is not a square root of $-a$ modulo p, we deduce that $a + r \not\equiv_p 0$ and, therefore, $(a + r)_p \in QR_p$.

Conversely, assume that $(a + r)_p \in QR_p$. Therefore, there exists $t \in \mathbb{Z}_p^*$ such that $a + r \equiv_p t^2$. As $r \in QR_p$, there exists $s \in \mathbb{Z}_p^*$ such that $r \equiv_p s^2$. Combining the two congruences we obtain

$$(s - t)(s + t) \equiv_p -a.$$

As $a \in \mathbb{Z}_p^*$ it follows that $(-a)_p \in \mathbb{Z}_p^*$ and, therefore, $(s+t)$ cannot be divisible by p. So, we may write

$$s - t \equiv_p -\frac{a}{s+t}$$

which leads to

$$s \equiv_p \frac{1}{2}\left((s+t) - \frac{a}{s+t}\right).$$

Now, we take $u = (s+t)_p$. It follows that $u \in \mathbb{Z}_p^*$ and

$$r \equiv_p s^2 \equiv_p \frac{1}{4}\left(u - \frac{a}{u}\right)^2.$$

It remains to prove that $u \notin SQRT_p(a, -a)$.

Because $r \in QR_p$, it follows that $r \not\equiv_p 0$, which leads to the fact that u cannot be a square root of a modulo p. Similarly, because $(a+r)_p \in QR_p$ it follows that $a + r \not\equiv_p 0$. As

$$a + r \equiv_p \frac{1}{4}\left(u + \frac{a}{u}\right)^2,$$

we deduce that u cannot be a square root of $-a$ modulo p.

Remark 1. One may reformulate Lemma 1 as follows:

> Let $p > 2$ be a prime, $a \in \mathbb{Z}_p^*$, and $r \in QR_p$. Then, $(a+r)_p \in QR_p$ if and only if $r \equiv_p \frac{(s-a)^2}{4s}$, for some $s \in QR_p \setminus \{a, -a\}$.

This reformulation shows that $(a+r)_p$ is a quadratic residue modulo p if and only if the quadratic residue r can be written as an expression that depends of another quadratic residue modulo p.

Lemma 2. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then, the function $\psi_a : \mathbb{Z}_p^* \setminus SQRT_p(a, -a) \to QR_p$ given by*

$$\psi_a(u) = \frac{1}{4}\left(u - \frac{a}{u}\right)^2 \bmod p,$$

for all $u \in \mathbb{Z}_p^* \setminus SQRT_p(a, -a)$, is a four-to-one map. Moreover, $(a + \psi_a(u))_p \in QR_p(a + QR_p)$, for all $u \in \mathbb{Z}_p^* \setminus SQRT_p(a, -a)$.

Proof. Let $a \in \mathbb{Z}_p^*$ and $u \in \mathbb{Z}_p^* \setminus SQRT_p(a, -a)$. The form of $\psi_a(u)$ together with the fact that u is not a square root of a modulo p show that $\psi_a(u) \in QR_p$. Therefore, the function ψ_a is well-defined.

The congruence

$$\left(x - \frac{a}{x}\right)^2 \equiv_p \left(u - \frac{a}{u}\right)^2$$

has four solutions in $\mathbb{Z}_p^*$ in the nondeterminate x, namely u, $(-u)_p$, $(a/u)_p$, and $(-a/u)_p$. If we prove that the four solutions above are pairwise incongruent modulo p, then ψ_a is a four-to-one map.

Due to the fact that $p > 2$ and $(u,p) = 1$, we obtain $u \not\equiv_p -u$. In a similar way and taking into consideration that $(a,p) = 1$, we obtain $a/u \not\equiv_p -a/u$. Finally, the hypothesis $u \notin SQRT_p(a,-a)$ leads to the fact that neither u nor $-u$ can be congruent to a/u or $-a/u$ modulo p. Therefore, the four integers u, $(-u)_p$, $(a/u)_p$, and $(-a/u)_p$ are pairwise incongruent modulo p.

A simple computation (see also the proof of Lemma 1) shows that

$$a + \psi_a(u) \equiv_p \frac{1}{4}\left(u + \frac{a}{u}\right)^2.$$

Combining this with the fact that $u \notin SQRT_p(-a)$, we obtain $(a + \psi_a(u))_p \in QR_p(a + QR_p)$, for all $u \in \mathbb{Z}_p^* \setminus SQRT_p(a,-a)$.

The two lemmata proved above lead directly to the following very important result.

Theorem 1. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then,*

$$|QR_p(a + QR_p)| = \frac{|\mathbb{Z}_p^* \setminus SQRT_p(a,-a)|}{4}.$$

We have now all the necessary elements to calculate the cardinals of the sets $Y(a + X)$, with $X, Y \in \{QR_p, QNR_p\}$. For the sake of simplicity we introduce the following notation.

Notation 21 *Let $p > 2$ be a prime and $a \in \mathbb{Z}$ such that p does not divide a. We denote by $\tau^1_{p,a}$, $\bar{\tau}^1_{p,a}$, $\tau^3_{p,a}$, and $\bar{\tau}^3_{p,a}$ the following symbols:*

$$\tau^i_{p,a} = \begin{cases} 1, & \textit{if } (p)_4 = i \textit{ and } (a)_p \in QR_p \\ 0, & \textit{otherwise} \end{cases}$$

and

$$\bar{\tau}^i_{p,a} = \begin{cases} 1, & \textit{if } (p)_4 = i \textit{ and } (a)_p \in QNR_p \\ 0, & \textit{otherwise,} \end{cases}$$

where $i = 1, 3$.

These symbols have useful properties such as:

1. *$\tau^1_{p,a} = \tau^1_{p,-a}$, $\bar{\tau}^1_{p,a} = \bar{\tau}^1_{p,-a}$, and $\tau^3_{p,a} = \bar{\tau}^3_{p,-a}$ (when $(p)_4 = 1$, $(a)_p$ is a quadratic residue modulo p if and only if $(-a)_p$ is a quadratic residue modulo p);*
2. *Exactly one of these symbols is one, the others being zero (there are exactly two possibilities for $(p)_4$ and exactly two possibilities for $(a)_p$ with respect to its quadratic residuosity; therefore, there are exactly four combinations and exactly one of them holds for a given p and a);*

3. The product of two or more symbols, all of them for the same integers p and a, is zero (this follows immediately from the second property).

Corollary 3. *Let $p > 2$ be a prime, $k = p \operatorname{div} 4$, and $a \in \mathbb{Z}_p^*$. Then,*

$$|QR_p(a + QR_p)| = k - \tau^1_{p,a}.$$

Proof. According to Theorem 1, everything comes down to the computation of $|\mathbb{Z}_p^* \setminus SQRT_p(a, -a)|$. Four cases are in order.

Case 1: $p = 4k + 1$ for some integer k, and $a \in QR_p$. Then $|SQRT_p(a, -a)| = 4$ because $(-a)_p \in QR_p$. As a result, $|\mathbb{Z}_p^* \setminus SQRT_p(a, -a)| = 4k - 4$.

Case 2: $p = 4k+1$ for some integer k, and $a \in QNR_p$. Then $|SQRT_p(a, -a)| = 0$ because $(-a)_p \in QNR_p$. As a result, $|\mathbb{Z}_p^* \setminus SQRT_p(a, -a)| = 4k$.

Case 3: $p = 4k + 3$ for some integer k, and $a \in QR_p$. Then $|SQRT_p(a, -a)| = 2$ because $(-a)_p \in QNR_p$. As a result, $|\mathbb{Z}_p^* \setminus SQRT_p(a, -a)| = 4k$.

Case 4: $p = 4k+3$ for some integer k, and $a \in QNR_p$. Then $|SQRT_p(a, -a)| = 2$ because $(-a)_p \in QR_p$. As a result, $|\mathbb{Z}_p^* \setminus SQRT_p(a, -a)| = 4k$.

All these cases lead to the statement in the corollary.

Corollary 4. *Let $p > 2$ be a prime, $k = p \operatorname{div} 4$, and $a \in \mathbb{Z}_p^*$. Then,*

$$|QNR_p(a + QR_p)| = k + \tau^3_{p,a}.$$

Proof. The set $(a + QR_p)^*$ is partitioned into quadratic residues and quadratic non-residues modulo p. Therefore,

$$|QNR_p(a + QR_p)| = |(a + QR_p)^*| - |QR_p(a + QR_p)|.$$

We will accomplish this computation on cases.

Case 1: $p = 4k + 1$ for some integer k, and $a \in QR_p$. Then, $(-a)_p \in QR_p$ and, therefore, $|(a+QR_p)^*| = 2k-1$ (by Proposition 2) and $|QR_p(a+QR_p)| = k-1$ (by Corollary 3). As a result, $|QNR_p(a + QR_p)| = k$.

Case 2: $p = 4k + 1$ for some integer k, and $a \in QNR_p$. Then, $(-a)_p \in QNR_p$ and, therefore, $|(a + QR_p)^*| = 2k$ (by Proposition 2) and $|QR_p(a + QR_p)| = k$ (by Corollary 3). As a result, $|QNR_p(a + QR_p)| = k$.

Case 3: $p = 4k+3$ for some integer k, and $a \in QR_p$. Then, $(-a)_p \in QNR_p$ and, therefore, $|(a + QR_p)^*| = 2k + 1$ (by Proposition 2) and $|QR_p(a + QR_p)| = k$ (by Corollary 3). As a result, $|QNR_p(a + QR_p)| = k + 1$.

Case 4: $p = 4k + 3$ for some integer k, and $a \in QNR_p$. Then, $(-a)_p \in QR_p$ and, therefore, $|(a + QR_p)^*| = 2k$ (by Proposition 2) and $|QR_p(a + QR_p)| = k$ (by Corollary 3). As a result, $|QNR_p(a + QR_p)| = k$.

Corollary 5. *Let $p > 2$ be a prime, $k = p \operatorname{div} 4$, and $a \in \mathbb{Z}_p^*$. Then,*

$$|QR_p(a + QNR_p)| = k + \bar{\tau}_{p,a}^3$$

and

$$|QNR_p(a + QNR_p)| = k - \bar{\tau}_{p,a}^1.$$

Proof. The set $\mathbb{Z}_p^*$ is partitioned into QR_p and QNR_p. Therefore, $a + \mathbb{Z}_p^*$ is a disjoint set union

$$a + \mathbb{Z}_p^* = (a + QR_p) \cup (a + QNR_p)$$

This leads to the set partitions

$$QR_p(a + \mathbb{Z}_p^*) = QR_p(a + QR_p) \cup QR_p(a + QNR_p)$$

and

$$QNR_p(a + \mathbb{Z}_p^*) = QNR_p(a + QR_p) \cup QNR_p(a + QNR_p).$$

As a conclusion,

$$|QR_p(a + QNR_p)| = |QR_p(a + \mathbb{Z}_p^*)| - |QR_p(a + QR_p)|$$

and

$$|QNR_p(a + QNR_p)| = |QNR_p(a + \mathbb{Z}_p^*)| - |QNR_p(a + QR_p)|$$

Now, the corollary follows from Corollaries 2 to 4.

Similar to Corollary 1 one can prove the following result.

Corollary 6. *Let $p > 2$ be a prime and $a, b \in \mathbb{Z}_p^*$.*

1. *If a and b are of the same quadratic residuosity, then*
   (a) $|QR_p(a + QR_p)| = |QR_p(b + QR_p)|$,
   (b) $|QNR_p(a + QR_p)| = |QNR_p(b + QR_p)|$,
   (c) $|QR_p(a + QNR_p)| = |QR_p(b + QNR_p)|$, *and*
   (d) $|QNR_p(a + QNR_p)| = |QNR_p(b + QNR_p)|$;
2. *If a and b are of opposite quadratic residuosities, then*
   (a) $|QR_p(a + QNR_p)| = |QNR_p(b + QR_p)|$ *and*
   (b) $|QNR_p(a + QNR_p)| = |QR_p(b + QR_p)|$.

We close this sub-section with a result which establishes an interesting bijection between $(a + QR_p)^*$ and $(b + QNR_p)^*$. This bijection can be used to obtain alternative proofs for some of the results already obtained in this sub-section.

Lemma 3. *Let $p > 2$ be a prime and $a, b \in \mathbb{Z}_p^*$ of opposite quadratic residuosities. Then, there exists a bijective map*

$$f : (a + QR_p)^* \to (b + QNR_p)^*$$

such that f maps $QR_p(a + QR_p)$ onto $QNR_p(b + QNR_p)$ and $QNR_p(a + QR_p)$ onto $QR_p(b + QNR_p)$. Moreover, such a bijection can be found in $\mathcal{O}((\log p)^2)$ time complexity.

Proof. Corollary 1 shows that $|(a+QR_p)^*| = |(b+QNR_p)^*|$ and, therefore, there exists a bijection from $(a+QR_p)^*$ to $(b+QNR_p)^*$. Such a bijection can be easily found if we compute the unique solution $e \in \mathbb{Z}_p^*$ to the linear congruence $ax \equiv_p b$ in the non-determinate x. Once we have found the solution e, we consider the function

$$f : (a + QR_p)^* \to (b + QNR_p)^*$$

given by $f(x) = (e \cdot x)_p$, for any $x \in (a + QR_p)^*$.

By taking into account that e must be a quadratic non-residue (a and b are of opposite quadratic residuosities) and $QNR_p = \{(e \cdot \alpha)_p \mid \alpha \in QR_p\}$, we easily obtain that f is well-defined and bijective.

Let us show now that f maps $QR_p(a+QR_p)$ onto $QNR_p(b+QNR_p)$. Indeed,

- Given $x = (a+\alpha)_p \in QR_p(a+QR_p)$, where $\alpha \in QR_p$, we have that $(e \cdot x)_p \in QNR_p$ and

  $$(e \cdot x)_p = ((e \cdot a)_p + (e \cdot \alpha)_p)_p = (b + (e \cdot \alpha)_p)_p \in b + QNR_p.$$

  This shows that $f(x)$ is a quadratic non-residue in $b + QNR_p$;
- For any quadratic non-residue $y = (b + \beta)_p \in b + QNR_p$, the integer $x = (a + \alpha)_p$, where $e \cdot \alpha = \beta$, satisfies $f(x) = y$; moreover, $y = (e \cdot x)_p$ which shows that x is a quadratic residue modulo p (because both y and e are quadratic non-residues modulo p).

As a conclusion, f maps $QR_p(a + QR_p)$ onto $QNR_p(b + QNR_p)$.

In a similar way it is shown that f maps $QNR_p(a + QR_p)$ onto $QR_p(b + QNR_p)$. Moreover, to obtain f we only need to compute e, and this can be done in $\mathcal{O}((\log p)^2)$ time complexity [25].

2.2 Composite moduli

We are now extending the results in the previous sub-section to the case of RSA moduli $n = pq$, where p and q are distinct odd primes[4]. First of all, we recall a well-known result, tailored for RSA moduli, that can be found in almost any standard book on number theory, such as [19] (this result can also be regarded as a special case of CRT, as presented in Section 1).

[4] One may notice that the results developed in this section can easily be extended to moduli that are product of more than two distinct odd primes.

Theorem 2 **([19]).** *Let $n = pq$ be an RSA modulus. Then, the function $f : \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$ given by*

$$f(x) = ((x)_p, (x)_q),$$

for any $x \in Z_n$, is bijective and maps $\mathbb{Z}_n^*$ onto $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

One of the main applications of the bijection f in Theorem 2 is to show that Euler's totient function ϕ is multiplicative. The bijection f has other applications as well, and some of them will be discussed by us below.

Theorem 3. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $(a + \mathbb{Z}_n^*)^*$ onto $((a)_p + \mathbb{Z}_p^*)^* \times ((a)_q + \mathbb{Z}_q^*)^*$;*
2. *f maps $(a + QR_n)^*$ onto $((a)_p + QR_p)^* \times ((a)_q + QR_q)^*$;*
3. *f maps $(a + J_n^+ \setminus QR_n)^*$ onto $((a)_p + QNR_p)^* \times ((a)_q + QNR_q)^*$;*
4. *f maps $(a + J_n^{\pm})^*$ onto $((a)_p + QR_p)^* \times ((a)_q + QNR_q)^*$;*
5. *f maps $(a + J_n^{\mp})^*$ onto $((a)_p + QNR_p)^* \times ((a)_q + QR_q)^*$.*

Proof. We will only prove (3) (the other properties follow a similar proof line).

Let $x \in (a + J_n^+ \setminus QR_n)^*$. Then, $x \in \mathbb{Z}_n^*$ and $x = (a + \alpha)_n$, for some $\alpha \in J_n^+ \setminus QR_n$. Therefore, $(x)_p \in \mathbb{Z}_p^*$, $(x)_q \in \mathbb{Z}_q^*$, $(x)_p = ((a)_p + (\alpha)_p)_p$, and $(x)_q = ((a)_q + (\alpha)_q)_q$. As

$$1 = J_n(\alpha) = J_p((\alpha)_p) \cdot J_q((\alpha)_q)$$

and $\alpha \notin QR_n$, it follows that

$$((\alpha)_p, (\alpha)_q) \in QNR_p \times QNR_q.$$

Therefore,

$$f(x) \in ((a)_p + QNR_p)^* \times ((a)_q + QNR_q)^*.$$

To show that f is onto, we consider $(y, z) \in ((a)_p + QNR_p)^* \times ((a)_q + QNR_q)^*$. Therefore, $y \in \mathbb{Z}_p^*$, $z \in \mathbb{Z}_q^*$, $y = ((a)_p + \beta)_p$, and $z = ((a)_q + \gamma)_q$, for some $\beta \in QNR_p$ and $\gamma \in QNR_q$. Starting with β and γ, CRT gives rise to a unique $\alpha \in \mathbb{Z}_n^*$ such that $(\alpha)_p = \beta$ and $(\alpha)_q = \gamma$. Then,

$$J_n(\alpha) = J_p(\alpha) \cdot J_q(\alpha) = J_p(\beta) \cdot J_q(\gamma) = (-1)(-1) = 1,$$

which shows that $\alpha \in J_n^+$. Moreover, $\alpha \notin QR_n$ because $(\alpha)_p \notin QR_p$ and $(\alpha)_q \notin QR_q$.

Consider now $x = (a + \alpha)_n$. Clearly, $x \in a + J_n^+ \setminus QR_n$. Moreover, $x \in (a + J_n^+ \setminus QR_n)^*$ because $(x)_p = y \in \mathbb{Z}_p^*$ and $(x)_q = z \in \mathbb{Z}_q^*$. Therefore, f is onto.

Several consequences of Theorem 3 are in order.

Corollary 7. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then,*

1. $|(a+\mathbb{Z}_n^*)^*| = (p-2)(q-2)$.
2. $|(a+QR_n)^*| = \frac{(p-2-J_p(-a))(q-2-J_q(-a))}{4}$.
3. $|(a+J_n^+ \setminus QR_n)^*| = \frac{(p-2+J_p(-a))(q-2+J_q(-a))}{4}$.
4. $|(a+J_n^\pm)^*| = \frac{(p-2-J_p(-a))(q-2+J_q(-a))}{4}$.
5. $|(a+J_n^\mp)^*| = \frac{(p-2+J_p(-a))(q-2-J_q(-a))}{4}$.
6. $|(a+J_n^+)^*| = \frac{(p-2)(q-2)+J_p(-a)J_q(-a)}{2}$.
7. $|(a+J_n^-)^*| = \frac{(p-2)(q-2)-J_p(-a)J_q(-a)}{2}$.
8. $|(a+QNR_n)^*| = \frac{3(p-2)(q-2)+J_p(-a)(q-2)+J_q(-a)(p-2)-J_p(-a)J_q(-a)}{4}$.

Proof. (1) follows from Theorem 3(1) and Proposition 1, (2) from Theorem 3(2) and Proposition 2, (3) from Theorem 3(3) and Proposition 2, (4) from Theorem 3(4) and Proposition 2, and (5) from Theorem 3(5) and Proposition 2.

(6) is based on the disjoint set union

$$(a+J_n^+)^* = (a+QR_n)^* \cup (a+J_n^+ \setminus QR_n)^*$$

together with (2) and (3), while (7) is based on

$$(a+J_n^-)^* = (a+J_n^\pm)^* \cup (a+J_n^\mp)^*,$$

(4), and (5). The last property follows, for instance, from (7) and (3).

We present now other properties of the function f in Theorem 2, necessary to partition the set $(a+\mathbb{Z}_n^*)^*$ in the same way $\mathbb{Z}_n^*$ is partitioned by Jacobi symbols.

Theorem 4. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $QR_n(a+\mathbb{Z}_n^*)$ onto $QR_p((a)_p+\mathbb{Z}_p^*) \times QR_q((a)_q+\mathbb{Z}_q^*)$;*
2. *f maps $(J_n^+ \setminus QR_n)(a+\mathbb{Z}_n^*)$ onto $QNR_p((a)_p+\mathbb{Z}_p^*) \times QNR_q((a)_q+\mathbb{Z}_q^*)$;*
3. *f maps $J_n^\pm(a+\mathbb{Z}_n^*)$ onto $QR_p((a)_p+\mathbb{Z}_p^*) \times QNR_q((a)_q+\mathbb{Z}_q^*)$;*
4. *f maps $J_n^\mp(a+\mathbb{Z}_n^*)$ onto $QNR_p((a)_p+\mathbb{Z}_p^*) \times QR_q((a)_q+\mathbb{Z}_q^*)$.*

Proof. It is similar to the proof of Theorem 3.

Corollary 8. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then,*

1. $|QR_n(a+\mathbb{Z}_n^*)| = \frac{(p-2-J_p(a))(q-2-J_q(a))}{4}$.
2. $|(J_n^+ \setminus QR_n)(a+\mathbb{Z}_n^*)| = \frac{(p-2+J_p(a))(q-2+J_q(a))}{4}$.
3. $|J_n^\pm(a+\mathbb{Z}_n^*)| = \frac{(p-2-J_p(a))(q-2+J_q(a))}{4}$.

4. $|J_n^{\mp}(a+\mathbb{Z}_n^*)| = \frac{(p-2+J_p(a))(q-2-J_q(a))}{4}$.
5. $|J_n^{+}(a+\mathbb{Z}_n^*)| = \frac{(p-2)(q-2)+J_p(a)J_q(a)}{2}$.
6. $|J_n^{-}(a+\mathbb{Z}_n^*)| = \frac{(p-2)(q-2)-J_p(a)J_q(a)}{2}$.
7. $|QNR_n(a+\mathbb{Z}_n^*)| = \frac{3(p-2)(q-2)+J_p(a)(q-2)+J_q(a)(p-2)-J_p(a)J_q(a)}{4}$.

Proof. For (1)-(4) we use Theorem 4(1)-(4), respectively, and Corollary 2. The properties (5)-(7) are immediate consequences of (1)-(4).

We use now the function f in Theorem 2 to partition the set $a + QR_n$.

Theorem 5. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $QR_n(a + QR_n)$ onto $QR_p((a)_p + QR_p) \times QR_q((a)_q + QR_q)$;*
2. *f maps $(J_n^+ \setminus QR_n)(a+QR_n)$ onto $QNR_p((a)_p+QR_p)\times QNR_q((a)_q+QR_q)$;*
3. *f maps $J_n^{\pm}(a + QR_n)$ onto $QR_p((a)_p + QR_p) \times QNR_q((a)_q + QR_q)$;*
4. *f maps $J_n^{\mp}(a + QR_n)$ onto $QNR_p((a)_p + QR_p) \times QR_q((a)_q + QR_q)$.*

Proof. It is similar to the proof of Theorem 3.

Corollary 9. *Let $n = pq$ be an RSA modulus, $k_1 = p \operatorname{div} 4$, $k_2 = q \operatorname{div} 4$, and $a \in \mathbb{Z}_n^*$. Then,*

1. $|QR_n(a + QR_n)| = (k_1 - \tau_{p,a}^1)(k_2 - \tau_{q,a}^1)$.
2. $|(J_n^+ \setminus QR_n)(a + QR_n)| = (k_1 + \tau_{p,a}^3)(k_2 + \tau_{q,a}^3)$.
3. $|J_n^{\pm}(a + QR_n)| = (k_1 - \tau_{p,a}^1)(k_2 + \tau_{q,a}^3)$.
4. $|J_n^{\mp}(a + QR_n)| = (k_1 + \tau_{p,a}^3)(k_2 - \tau_{q,a}^1)$.
5. $|J_n^{+}(a+QR_n)| = 2k_1k_2 + k_1(\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1\tau_{q,a}^1 + \tau_{p,a}^3\tau_{q,a}^3$.
6. $|J_n^{-}(a+QR_n)| = 2k_1k_2 + k_1(\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1\tau_{q,a}^3 - \tau_{p,a}^3\tau_{q,a}^1$.
7. $|QNR_n(a + QR_n)| = 3k_1k_2 + k_1(2\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(2\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1\tau_{q,a}^3 - \tau_{p,a}^3\tau_{q,a}^1 + \tau_{p,a}^3\tau_{q,a}^3$.

Proof. For (1)-(4) we use Theorem 5(1)-(4), respectively, and Corollaries 3 and 4. The properties (5)-(7) are immediate consequences of (1)-(4).

The following theorem shows how to partition $a + J_n^+ \setminus QR_n$.

Theorem 6. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $QR_n(a+J_n^+ \setminus QR_n)$ onto $QR_p((a)_p+QNR_p)\times QR_q((a)_q+QNR_q)$;*

2. *f maps $(J_n^+\setminus QR_n)(a+J_n^+\setminus QR_n)$ onto $QNR_p((a)_p+QNR_p)\times QNR_q((a)_q+QNR_q)$;*
3. *f maps $J_n^\pm(a+J_n^+\setminus QR_n)$ onto $QR_p((a)_p+QNR_p)\times QNR_q((a)_q+QNR_q)$;*
4. *f maps $J_n^\mp(a+J_n\setminus QR_n)$ onto $QNR_p((a)_p+QNR_p)\times QR_q((a)_q+QNR_q)$.*

Proof. It is similar to the proof of Theorem 3.

Corollary 10. *Let $n=pq$ be an RSA modulus, $k_1=p \text{ div } 4$, $k_2=q \text{ div } 4$, and $a\in\mathbb{Z}_n^*$. Then,*

1. $|QR_n(a+J_n^+\setminus QR_n)|=(k_1+\bar{\tau}_{p,a}^3)(k_2+\bar{\tau}_{q,a}^3)$.
2. $|(J_n^+\setminus QR_n)(a+J_n^+\setminus QR_n)|=(k_1-\bar{\tau}_{p,a}^1)(k_2-\bar{\tau}_{q,a}^1)$.
3. $|J_n^\pm(a+J_n^+\setminus QR_n)|=(k_1+\bar{\tau}_{p,a}^3)(k_2-\bar{\tau}_{q,a}^1)$.
4. $|J_n^\mp(a+J_n^+\setminus QR_n)|=(k_1-\bar{\tau}_{p,a}^1)(k_2+\bar{\tau}_{q,a}^3)$.
5. $|J_n^+(a+J_n^+\setminus QR_n)|=2k_1k_2+k_1(\bar{\tau}_{q,a}^3-\bar{\tau}_{q,a}^1)+k_2(\bar{\tau}_{p,a}^3-\bar{\tau}_{p,a}^1)+\bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^3+\bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^1$.
6. $|J_n^-(a+J_n^+\setminus QR_n)|=2k_1k_2+k_1(\bar{\tau}_{q,a}^3-\bar{\tau}_{q,a}^1)+k_2(\bar{\tau}_{p,a}^3-\bar{\tau}_{p,a}^1)-\bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^1-\bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^3$.
7. $|QNR_n(a+J_n^+\setminus QR_n)|=3k_1k_2+k_1(\bar{\tau}_{q,a}^3-2\bar{\tau}_{q,a}^1)+k_2(\bar{\tau}_{p,a}^3-2\bar{\tau}_{p,a}^1)-\bar{\tau}_{p,a}^3\bar{\tau}_{q,a}^1-\bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^3+\bar{\tau}_{p,a}^1\bar{\tau}_{q,a}^1$.

Proof. For (1)-(4) we use Theorem 6(1)-(4), respectively, and Corollary 5. The properties (5)-(7) are immediate consequences of (1)-(4).

For the partitioning of the set $a+J_n^\pm$ we have the following result.

Theorem 7. *Let $n=pq$ be an RSA modulus and $a\in\mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $QR_n(a+J_n^\pm)$ onto $QR_p((a)_p+QR_p)\times QR_q((a)_q+QNR_q)$;*
2. *f maps $(J_n^+\setminus QR_n)(a+J_n^\pm)$ onto $QNR_p((a)_p+QR_p)\times QNR_q((a)_q+QNR_q)$;*
3. *f maps $J_n^\pm(a+J_n^\pm)$ onto $QR_p((a)_p+QR_p)\times QNR_q((a)_q+QNR_q)$;*
4. *f maps $J_n^\mp(a+J_n^\pm)$ onto $QNR_p((a)_p+QR_p)\times QR_q((a)_q+QNR_q)$.*

Proof. It is similar to the proof of Theorem 3.

Corollary 11. *Let $n=pq$ be an RSA modulus, $k_1=p \text{ div } 4$, $k_2=q \text{ div } 4$, and $a\in\mathbb{Z}_n^*$. Then,*

1. $|QR_n(a+J_n^\pm)|=(k_1-\tau_{p,a}^1)(k_2+\bar{\tau}_{q,a}^3)$.
2. $|(J_n^+\setminus QR_n)(a+J_n^\pm)|=(k_1+\tau_{p,a}^3)(k_2-\bar{\tau}_{q,a}^1)$.
3. $|J_n^\pm(a+J_n^\pm)|=(k_1-\tau_{p,a}^1)(k_2-\bar{\tau}_{q,a}^1)$.
4. $|J_n^\mp(a+J_n^\pm)|=(k_1+\tau_{p,a}^3)(k_2+\bar{\tau}_{q,a}^3)$.

5. $|J_n^+(a+J_n^\pm)| = 2k_1k_2 + k_1(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + k_2(\tau_{p,a}^3 - \tau_{p,a}^1) - \tau_{p,a}^1\bar{\tau}_{q,a}^3 - \tau_{p,a}^3\bar{\tau}_{q,a}^1$.
6. $|J_n^-(a+J_n^\pm)| = 2k_1k_2 + k_1(\bar{\tau}_{q,a}^3 - \bar{\tau}_{q,a}^1) + k_2(\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1\bar{\tau}_{q,a}^1 + \tau_{p,a}^3\bar{\tau}_{q,a}^3$.
7. $|QNR_n(a+J_n^\pm)| = 3k_1k_2 + k_1(\bar{\tau}_{q,a}^3 - 2\bar{\tau}_{q,a}^1) + k_2(2\tau_{p,a}^3 - \tau_{p,a}^1) + \tau_{p,a}^1\bar{\tau}_{q,a}^1 + \tau_{p,a}^3\bar{\tau}_{q,a}^3 - \tau_{p,a}^3\bar{\tau}_{q,a}^1$.

Proof. For (1)-(4) we use Theorem 7(1)-(4), respectively, and Corollaries 3 to 5. The properties (5)-(7) are immediate consequences of (1)-(4).

The last application of Theorem 1 we discuss in this subsection is with respect to the set $a + J_n^\mp$.

Theorem 8. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 has the following properties:*

1. *f maps $QR_n(a+J_n^\mp)$ onto $QR_p((a)_p + QNR_p) \times QR_q((a)_q + QR_q)$;*
2. *f maps $(J_n^+ \setminus QR_n)(a+J_n^\mp)$ onto $QNR_p((a)_p+QNR_p) \times QNR_q((a)_q+QR_q)$;*
3. *f maps $J_n^\pm(a+J_n^\mp)$ onto $QR_p((a)_p + QNR_p) \times QNR_q((a)_q + QR_q)$;*
4. *f maps $J_n^\mp(a+J_n^\mp)$ onto $QNR_p((a)_p + QNR_p) \times QR_q((a)_q + QR_q)$.*

Proof. It is similar to the proof of Theorem 3.

Corollary 12. *Let $n = pq$ be an RSA modulus, $k_1 = p \operatorname{div} 4$, $k_2 = q \operatorname{div} 4$, and $a \in \mathbb{Z}_n^*$. Then,*

1. $|QR_n(a+J_n^\mp)| = (k_1 + \bar{\tau}_{p,a}^3)(k_2 - \tau_{q,a}^1)$.
2. $|(J_n^+ \setminus QR_n)(a+J_n^\mp)| = (k_1 - \bar{\tau}_{p,a}^1)(k_2 + \tau_{q,a}^3)$.
3. $|J_n^\pm(a+J_n^\mp)| = (k_1 + \bar{\tau}_{p,a}^3)(k_2 + \tau_{q,a}^3)$.
4. $|J_n^\mp(a+J_n^\mp)| = (k_1 - \bar{\tau}_{p,a}^1)(k_2 - \tau_{q,a}^1)$.
5. $|J_n^+(a+J_n^\mp)| = 2k_1k_2 + k_1(\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) - \bar{\tau}_{p,a}^3\tau_{q,a}^1 - \bar{\tau}_{p,a}^1\tau_{q,a}^3$.
6. $|J_n^-(a+J_n^\mp)| = 2k_1k_2 + k_1(\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(\bar{\tau}_{p,a}^3 - \bar{\tau}_{p,a}^1) + \bar{\tau}_{p,a}^3\tau_{q,a}^3 + \bar{\tau}_{p,a}^1\tau_{q,a}^1$.
7. $|QNR_n(a+J_n^\mp)| = 3k_1k_2 + k_1(2\tau_{q,a}^3 - \tau_{q,a}^1) + k_2(\bar{\tau}_{p,a}^3 - 2\bar{\tau}_{p,a}^1) + \bar{\tau}_{p,a}^3\tau_{q,a}^3 + \bar{\tau}_{p,a}^1\tau_{q,a}^1 - \bar{\tau}_{p,a}^1\tau_{q,a}^3$.

Proof. For (1)-(4) we use Theorem 8(1)-(4), respectively, and Corollaries 3 to 5. The properties (5)-(7) are immediate consequences of (1)-(4).

We have thus provided formulas for all cardinalities of the sets in Figure 1.

2.3 Probability distributions on $a + \mathbb{Z}_n^*$

The results developed in the previous sub-sections allow us to calculate various probability distributions on subsets $(a+X)^*$, where X is $\mathbb{Z}_n^*$, QR_n, $J_n^+ \setminus QR_n$, $J_n^{\pm}$, $J_n^{\mp}$, J_n^+, J_n^-, or QNR_n. We will give below a few examples. The notation

$$P(x \in Y \,:\, x \leftarrow (a+X)^*)$$

stands for the probability that x is in Y when it is uniformly at random sampled from $(a+X)^*$, where Y is a subset of $(a+X)^*$ as those in the previous sub-sections. Using our notation, this probability can be calculated by

$$P(x \in Y \,:\, x \leftarrow (a+X)^*) = \frac{|Y(a+X)|}{|(a+X)^*|} = \frac{|(a+X)^* \cap Y|}{|(a+X)^*|}.$$

We will provide below just a few examples of calculating such probabilities.

Corollary 13. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the following hold:*

1. $P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{4}, & \text{if } a \in J_n^+ \setminus QR_n, \\ \frac{1}{4} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right), & \text{otherwise.} \end{cases}$
2. $P\left(x \in J_n^+ \setminus QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{4}, & \text{if } a \in J_n^+ \setminus QR_n, \\ \frac{1}{4} + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right), & \text{otherwise.} \end{cases}$
3. $P\left(x \in J_n^{\pm} \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{4}, & \text{if } a \in J_n^+ \setminus QR_n, \\ \frac{1}{4} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right), & \text{otherwise.} \end{cases}$
4. $P\left(x \in J_n^{\mp} \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{4}, & \text{if } a \in J_n^+ \setminus QR_n, \\ \frac{1}{4} + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right), & \text{otherwise.} \end{cases}$
5. $P\left(x \in J_n^+ \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{2}, & \text{if } a \in QNR_n, \\ \frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right), & \text{otherwise.} \end{cases}$
6. $P\left(x \in J_n^- \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{2}, & \text{if } a \in QNR_n, \\ \frac{1}{2} - \mathcal{O}\left(\frac{1}{n}\right), & \text{otherwise.} \end{cases}$
7. $P\left(x \in QNR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{3}{4}, & \text{if } a \in J_n^+ \setminus QR_n, \\ \frac{3}{4} + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right), & \text{otherwise.} \end{cases}$

Proof. We will only prove (1) as an example; the other properties follow a similar proof line.

First, recall that by Corollaries 7 and 9 we have

$$\begin{aligned} P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) &= \frac{|QR_n(a+QR_n)|}{|(a+QR_n)^*|} \\ &= \frac{4(k_1-\tau^1_{p,a})(k_2-\tau^1_{q,a})}{(p-2-J_p(-a))(q-2-J_q(-a))}, \end{aligned}$$

where $k_1 = p \operatorname{div} 4$ and $k_2 = q \operatorname{div} 4$. What we have now to do is to consider several cases with respect to p, q, and a.

Case 1: $a \in J_n^+ \backslash QR_n$. Then, regardless of $(p)_4$ and $(q)_4$ we have $p-2-J_p(-a) = 4k_1$, $q-2-J_q(-a) = 4k_2$, and $\tau^1_{p,a} = 0 = \tau^1_{q,a}$. Therefore,

$$P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \frac{1}{4}.$$

Case 2: $a \in J_n^{\mp}$. Then, regardless of $(p)_4$ we have $p-2-J_p(-a) = 4k_1$ and $\tau^1_{p,a} = 0$. A simple computation on the two possible values of $(q)_4$ leads to

$$P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \begin{cases} \frac{1}{4}\left(1-\frac{1}{2k_2-1}\right), & \text{if } (q)_4 = 1 \\ \frac{1}{4}\left(1-\frac{1}{2k_2+1}\right), & \text{if } (q)_4 = 3 \end{cases}$$

Case 3: $a \in J_n^{\pm}$. This case is similar to the previous one (simply switch k_2 with k_1 and q with p).

Case 4: $a \in QR_n$. Then, we obtain

$$P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \\ \begin{cases} \frac{1}{4}\left(1-\frac{2k_1+2k_2-3}{(2k_1-1)(2k_2-1)}\right), & \text{if } (p)_4 = 1 = (q)_4 \\ \frac{1}{4}\left(1-\frac{2k_1+2k_2-1}{(2k_1-1)(2k_2+1)}\right), & \text{if } (p)_4 = 1 \text{ and } (q)_4 = 3 \\ \frac{1}{4}\left(1-\frac{2k_1+2k_2-1}{(2k_1+1)(2k_2-1)}\right), & \text{if } (p)_4 = 3 \text{ and } (q)_4 = 1 \\ \frac{1}{4}\left(1-\frac{2k_1+2k_2+1}{(2k_1+1)(2k_2+1)}\right), & \text{if } (p)_4 = 3 = (q)_4 \end{cases}$$

From these cases one can easily infer the result in (1).

Remark 2. The probability in Corollary 13(1) is paired with that in Corollary 13(2). The pairing means that when

$$P\left(x \in QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \frac{1}{4} - \frac{c}{\sqrt{n}}$$

then

$$P\left(x \in J_n \setminus QR_n \,:\, x \leftarrow (a+QR_n)^*\right) = \frac{1}{4} + \frac{c}{\sqrt{n}},$$

for some constant $c > 0$ (to see it, one has to do a similar calculation for Corollary 13(2) as we did for Corollary 13(1)). The same happens with the probabilities in Corollary 13(3)(4), Corollary 13(5)(6), and Corollary 13(1)(7).

3 Applications

We believe that the results developed in the previous section have important applications to quadratic residuosity-based cryptography. We will illustrate some of these applications in the next sub-sections.

3.1 Cocks' IBE Scheme and Galbraith's Test

Identity-based cryptography was proposed in 1984 by Adi Shamir [24] who formulated its basic principles and provided an identity-based signature scheme. In 2000, Sakai, Ohgishi and Kasahara [23] have proposed an identity-based key agreement scheme, and one year later, Cocks [8] and Boneh and Franklin [5] have proposed the first *identity-based encryption* (IBE) schemes. Cocks' scheme is based on quadratic residues, while Boneh and Franklin's scheme is based on bilinear maps. Since then, some other IBE schemes based on quadratic residues have been proposed [6,16,1,7,11,12,17], although some of them are not secure (see [26] for details).

An IBE scheme consists of four PPT algorithms: *Setup*, $KeyGen$, *Encrypt*, and *Decrypt*. The first one takes as input a security parameter and outputs the system's public parameters together with a master key. The $KeyGen$ algorithm takes as input an identity ID together with the public parameters and the master key and outputs a private key associated to ID. The *Encrypt* algorithm, starting with a message m, an identity ID, and the public parameters, encrypts m into some ciphertext c (the encryption key is ID or some binary string derived from ID). The last algorithm decrypts c into m by using the private key associated to ID.

A standard scenario on using IBE is as follows. Whenever Alice wants to send a message m to Bob, she encrypts m by using Bob's identity $ID(B)$. In order to decrypt the message received from Alice, Bob asks the key generator $KeyGen$ to deliver him the private key associated to $ID(B)$ (if he does not already have it).

Cocks' IBE scheme [8]

Setup(λ) **:** Generate $(p,q) \leftarrow RSAgen(\lambda)$ and compute $n = pq$. Generate uniformly at random $e \in J_n^+ \setminus QR_n$ and output the public parameters $PP = (n, e, h)$, where h is a cryptographic hash function that maps identities into J_n^+. The master key is the factorization (p,q) of n;

$KeyGen(p,q,ID)$ **:** Let $a = h(ID)$. Set $a' = a$, if $a \in QR_n$, and $a' = ea$, otherwise. Uniformly at random choose a square root r of a' and output it as the private key;

Encrypt(PP, ID, m) **:** Let $a = h(ID)$. To encrypt a bit $m \in \{-1, 1\}$, choose uniformly at random $t_1, t_2 \in \mathbb{Z}_n^*$ such that $J_n(t_1) = J_n(t_2) = m$. Compute $c_1 = t_1 + at_1^{-1} \bmod n$ and $c_2 = t_2 + eat_2^{-1} \bmod n$ and output the ciphertext (c_1, c_2);

Decrypt$((c_1, c_2), r)$ **:** Set $c = c_1$ if $r^2 \equiv a \bmod n$, or $c = c_2$, otherwise. Then, output $m = J_n(c + 2r)$.

For a given $m \in \{-1, 1\}$, the generation of an integer $t \in \mathbb{Z}_n^*$ with $J_n(t) = m$ can be done by repetition because the probability of success for a random choice of t is $1/2$ (for RSA moduli, $|J_n^+| = |J_n^-|$ [25]).

The correctness of Cocks' IBE scheme can be obtained as follows. Assume t is chosen such that $J_n(t) = m$, $x \in QR_n$, r is a square root of x, and $c = t + xt^{-1} \bmod n$. Then,

$$c + 2r \equiv_n t(1 + 2rt^{-1} + (rt^{-1})^2) \equiv_n t(1 + rt^{-1})^2$$

which shows that $J_n(c + 2r) = J_n(t) = m$. In Cocks' IBE scheme, either a or ea is a quadratic residue modulo n. The decryptor decides this by means of the private key r.

It was shown in [8,14,17] that Cocks' IBE scheme is IND-ID-CPA secure in the random oracle model under the QR assumption for *RSAgen* (the random oracle model assumes that the output of a cryptographic hash function behaves as the output of random function [2]).

According to [4], Galbraith developed a test to show that Cocks' IBE scheme is not anonymous in the following sense. Given two random public keys (identities) $a, b \in J_n^+$, one may distinguish with overwhelming probability whether a ciphertext c is encrypted under the public key a or under the public key b. *Galbraith's test* (abbreviated GT), was briefly described in [4,1], but some claims were not rigorously proved. Using the results developed in the previous sections, we can complete GT description in [4,1] by rigorous arguments. First of all, let us introduce the following sets of integers:

$$\begin{aligned} C_n(a) &= \{(t + at^{-1})_n \mid t \in \mathbb{Z}_n^*\} \\ C_n^*(a) &= C_n(a) \cap \mathbb{Z}_n^* \\ G_n(a) &= \{c \in \mathbb{Z}_n^* \mid J_n(c^2 - 4a) = 1\} \end{aligned}$$

where $n > 2$ and $a \in \mathbb{Z}_n^*$.

When n is an RSA modulus and $a \in J_n^+$, the set $C_n(a)$ corresponds to the set of encryptions in Cocks' IBE scheme, and $G_n(a)$ corresponds to the set of all integers in $\mathbb{Z}_n^*$ that "pass" GT [4,1].

We develop now some counting results, similar to the ones in Section 2, for $C_n(a)$, $C_n^*(a)$, and $G_n(a)$. We begin with the case of prime moduli.

Theorem 9. *Let $p > 2$ be a prime and $a, c \in \mathbb{Z}_p^*$. Then,*

1. *$0 \in C_p(a)$ if and only if $-a \in QR_p$;*
2. *$c \in C_p(a)$ if and only if $c^2 - 4a \equiv_p 0$ or $(c^2 - 4a)_p \in QR_p$.*

Proof. For (1) we have:

$$\begin{aligned} 0 \in C_p(a) &\Leftrightarrow t + at^{-1} \equiv_p 0, \text{ for some } t \in \mathbb{Z}_p^* \\ &\Leftrightarrow a + t^2 \equiv_p 0, \text{ for some } t \in \mathbb{Z}_p^* \\ &\Leftrightarrow -a \equiv_p t^2, \text{ for some } t \in \mathbb{Z}_p^* \\ &\Leftrightarrow -a \in QR_p. \end{aligned}$$

In order to prove (2) remark that $c \in C_p(a)$ if and only if the quadratic congruence

$$t^2 - ct + a \equiv_p 0 \tag{3.1}$$

has solutions in $\mathbb{Z}_p^*$. Moreover, (3.1) has integer solutions if and only if its discriminant $\Delta = (c^2 - 4a)_p$ is 0 or a quadratic residue modulo p. It remains to prove that, in any of these two cases, (3.1) has solutions in $\mathbb{Z}_p^*$.

If $\Delta = 0$, then $a \equiv_p (c/2)^2$. The congruence (3.1) has exactly one solution in $\mathbb{Z}_p$, namely $t = (c/2)_p$. Moreover, $t \in \mathbb{Z}_p^*$ because $c \in \mathbb{Z}_p^*$.

If $\Delta \in QR_p$, then the congruence (3.1) has two solutions in $\mathbb{Z}_p$, namely $((c+r)/2)_p$ and $((c-r)/2)_p$, where r and $(-r)_p$ are the two square roots of Δ in $\mathbb{Z}_p$. If we assume now that $((c+r)/2) \equiv_p 0$ or $((c-r)/2) \equiv_p 0$, then $(c+r)(c-r) \equiv_p 0$ and, therefore, $c^2 - r^2 \equiv_p 0$. This leads to a contradiction because $c^2 - r^2 \equiv_p 4a$ and $a \in \mathbb{Z}_p^*$. Therefore, $((c+r)/2)_p$ and $((c-r)/2)_p$ are in $\mathbb{Z}_p^*$.

Corollary 14. *Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then, $C_p^*(a)$ can be written as a disjoint set union $C_p^*(a) = C_p^0(a) \cup C_p^1(a)$, where*

- *$C_p^0(a) = \{c \in \mathbb{Z}_p^* \mid J_p(c^2 - 4a) = 0\}$ and*
- *$C_p^1(a) = \{c \in \mathbb{Z}_p^* \mid J_p(c^2 - 4a) = 1\}$.*

Proof. This is in fact a new way to express the statement in Theorem 9(2).

Corollary 15. *Let $p > 2$ be a prime, $k = p \text{ div } 4$, and $a \in \mathbb{Z}_p^*$. Then,*

1. *$|C_p^0(a)| = 2(\tau_{p,a}^1 + \tau_{p,a}^3)$;*
2. *$|C_p^1(a)| = 2|QR_p(a + QRp)| = 2(k - \tau_{p,a}^1)$;*
3. *$|C_p^*(a)| = 2(k + \tau_{p,a}^3)$;*
4. *$|C_p(a)| = 2(k + \tau_{p,a}^3) + \tau_{p,a}^1 + \bar{\tau}_{p,a}^3$;*

Proof. We count the integers in $C_p(a)$ with the help of Theorem 9 as follows:

(a) If $a \in QR_p$ and r and $(-r)_p$ are the square roots modulo p of a, then $(2r)_p$ and $(-2r)_p$ are the only (incongruent modulo p) integers in $C_p^0(a)$;
(b) Each quadratic residue $u = (-4a + c^2)_p \in (-4a + QR_p)$ gives rise to two (incongruent modulo p) integers in $C_p^1(a)$, namely c and $(-c)_p$;
(c) The integers obtained as above are pairwise incongruent modulo p;
(d) $0 \in C_p(a)$ if and only if $-a \in QR_p$.

Therefore, the item (a) gives rise to $|C_p^0(a)| = 2(\tau_{p,a}^1 + \tau_{p,a}^3)$. The items (b) and (c) lead to

$$|C_p^1(a)| = 2|QR_p(-4a + QR_p)| = 2(k - \tau_{p,-a}^1) = 2(k - \tau_{p,a}^1) = 2|QR_p(a + QR_p)|$$

(we have used Corollary 3, the fact that a and $4a$ have the same quadratic residuosity, and $\tau_{p,a}^1 = \tau_{p,-a}^1$). From these, (3) follows immediately. To obtain (4) we count the integer 0 as well, by means of (d).

Theorem 10. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, the bijection f in Theorem 2 maps the set $C_n(a)$ onto $C_p((a)_p) \times C_q((a)_q)$ and the set $C_n^*(a)$ onto $C_p^*((a)_p) \times C_q^*((a)_q)$.*

Proof. We will only prove the theorem for the case of the set $C_n^*(a)$ (the other case is similar to this). Given $c = (t + at^{-1})_n \in C_n^*(a)$, $f(c) = ((c)_p, (c)_q)$. We may write $(c)_p = ((t)_p + (a)_p(t)_p^{-1})_p$ and $(c)_q = ((t)_q + (a)_q(t)_q^{-1})_q$. Then, clearly, $((c)_p, (c)_q) \in C_p^*((a)_p) \times C_q^*((a)_q)$.

Conversely, given $c_1 = (t_1 + (a)_p t_1^{-1})_p \in C_p^*((a)_p)$ and $c_2 = (t_2 + (a)_q t_2^{-1})_q \in C_q^*((a)_q)$, one may compute by means of CRT an unique $t \in \mathbb{Z}_n^*$ such that $t \equiv_p t_1$ and $t \equiv_q t_2$. Then, it is straightforward to check that $c = (t + at^{-1})_n \in C_n^*(a)$ and $f(c) = (c_1, c_2)$.

Given an RSA modulus $n = pq$, $a \in \mathbb{Z}_n^*$, and $e_1, e_2 \in \{-1, 0, 1\}$, define

$$C_n^{e_1,e_2} = \{c \in \mathbb{Z}_n^* \mid J_p(c^2 - 4a) = e_1,\ J_q(c^2 - 4a) = e_2\}.$$

Now, we are ready to prove the following results regarding $|C_n(a)|$, $|C_n^*(a)|$, and $|G_n(a)|$.

Corollary 16. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then, $C_n^*(a)$ can be written as a disjoint set union $C_n^*(a) = C_n^{0,0}(a) \cup C_n^{0,1}(a) \cup C_n^{1,0}(a) \cup C_n^{1,1}(a)$.*

Proof. It follows directly from Theorem 10 and Corollary 14.

Corollary 17. *Let $n = pq$ be an RSA modulus, $k_1 = p \operatorname{div} 4$, $k_2 = q \operatorname{div} 4$, and $a \in \mathbb{Z}_n^*$. Then,*

1. $|C_n^{0,0}(a)| = 4(\tau_{p,a}^1 + \tau_{p,a}^3)(\tau_{q,a}^1 + \tau_{q,a}^3)$;
2. $|C_n^{0,1}(a)| = 4(\tau_{p,a}^1 + \tau_{p,a}^3)(k_2 - \tau_{q,a}^1)$;
3. $|C_n^{1,0}(a)| = 4(\tau_{q,a}^1 + \tau_{q,a}^3)(k_1 - \tau_{p,a}^1)$;
4. $|C_n^{1,1}(a)| = 4|QR_n(a + QR_n)| = 4(k_1 - \tau_{p,a}^1)(k_2 - \tau_{q,a}^1)$;
5. $|C_n^*(a)| = 4(k_1 + \tau_{p,a}^3)(k_2 + \tau_{q,a}^3)$;
6. $|C_n(a)| = (2(k_1 + \tau_{p,a}^3) + \tau_{p,a}^1 + \bar{\tau}_{p,a}^3)(2(k_2 + \tau_{q,a}^3) + \tau_{q,a}^1 + \bar{\tau}_{q,a}^3)$.

Proof. It follows directly from Theorem 10 and Corollary 15.

Theorem 11. *Let $n = pq$ be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then,*

1. $G_n(a) = C_n^{1,1}(a) \cup C_n^{-1,-1}(a)$.
2. $|G_n(a)| = 4|QR_n(a + J_n^+)|$.

Proof. (1) follows from the definitions of $G_n(a)$ and $C_n^{1,1}(a)$. For (2) we remark first that

$$G_n(a) = \{c \in \mathbb{Z}_n^* \mid (c^2)_n \in 4a + J_n^+\}.$$

Then, observe that each $u \in QR_n$ has exactly four square roots in $\mathbb{Z}_n^*$. Moreover, distinct quadratic residues modulo n have distinct square roots in $\mathbb{Z}_n^*$. Then, (2) follows from $|QR_n(4a + J_n^+)| = |QR_n(a + J_n^+)|$.

Theorem 11 provides a very good image on the relationship between $C_n^*(a)$ and $G_n(a)$; this is pictorially represented in Figure 2. There is one more remark we would like to make. Given $c \in \mathbb{Z}_n^*$, there exists $a \in J_n^+$ such that $c \in C_n^*(a)$. Indeed, such an a can be obtained as described in Algorithm 1.

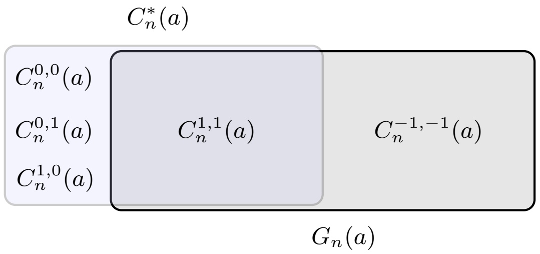

Fig. 2. The sets C_n^* and $G_n(a)$

Algorithm 1. Computing a.

```
Input: RSA modulus $n = pq$ and $c \in \mathbb{Z}_n^*$.
Output: An integer $a \in J_n^+$ such that $c \in C_n^*(a)$.
while $c^2 - s_1 \notin QR_p$ do
    $s_1 \xleftarrow{\$} QR_p$
end
$a_1 \leftarrow ((c^2 - s_1)/4)_p$
while $c^2 - s_2 \notin QR_q$ do
    $s_2 \xleftarrow{\$} QR_q$
end
$a_2 \leftarrow ((c^2 - s_2)/4)_q$
Use CRT to compute $a$ such that $a \equiv_p a_1$ and $a \equiv_q a_2$ return $a$
```

The probability of generating s_1 as in the first step of Algorithm 1 is negligible close to 1/2 because

$$c^2 - QR_p = \begin{cases} c^2 + QR_p, & \text{if } (p)_4 = 1 \\ c^2 + QNR_p, & \text{if } (p)_4 = 3 \end{cases}$$

and thus almost half of the integers in $c^2 - QR_p$ are quadratic residues modulo p (by Corollaries 3 and 5). Similarly, the probability of generating s_2 as in the third step of Algorithm 1 is negligible close to 1/2. The integer a computed in the fifth step of Algorithm 1 is a quadratic residue modulo n because a_1 and a_2 are quadratic residues modulo p and q, respectively.

To show that $c \in C_n^*(a)$ it is sufficient to remark that $c^2 - 4a$ is a quadratic residue modulo n because, according to our construction, $c^2 - 4a \equiv_p s_1$, $c^2 - 4a \equiv_q s_2$, and both s_1 and s_2 are quadratic residues modulo p and q, respectively.

We are now in a position to present Galbraith's test. Assume that an identity $a \in J_n^+$ is given and we would like to decide whether an integer $c \in \mathbb{Z}_n^*$ was encrypted under a. Directly from Corollary 17 it follows that $c \notin C_n(a)$ if $J_n(c^2 - 4a) = -1$. On the other side, if $J_n(c^2 - 4a) = 1$, then the probability that $c \in C_n^*(a)$ is

$$P(c \in C_n^*(a) \,:\, c \leftarrow G_n(a)) = \frac{|C_n^{1,1}(a)|}{|G_n(a)|} = \frac{4|QR_n(a + QR_n)|}{4|QR_n(a + J_n^+)|} = \frac{1}{2} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

(the property $|QR_n(a + J_n^+)| = |QR_n(a + QR_n)| + |QR_n(a + J_n^+ \setminus QR_n)|$ has been used, together with Corollaries 9 and 10).

Algorithm 2 presents Galbraith's test. As we have already discussed, the probability that Algorithm 2 outputs 1 is negligible close to 1/2. One may also remark that it outputs 0 even for $c \in C_n^{0,0} \cup C_n^{0,1} \cup C_n^{1,0} \subseteq C_n^*(a)$. However, the probability that Cocks' IBE scheme outputs such ciphertexts is $\mathcal{O}(1/\sqrt{n})$ (according to Corollary 17), which is negligible.

Algorithm 2. Galbraith's Test.

```
Input: RSA modulus $n$, $a \in J_n^+$, and $c \in \mathbb{Z}_n^*$.
Output: 1, if $c \in C_n^*(a)$ with probability negligible close to 1/2, and 0,
        otherwise.
if $J_n(c^2 - 4a) = 1$ then
    return 1
end
else
    return 0
end
```

When using Cocks' IBE scheme, the ciphertext consists of a sequence of encrypted bits under the same identity. Therefore, Galbraith's test applied to each encrypted bit in the sequence determines whether the ciphertext is encrypted under a given identity or not with overwhelming probability.

3.2 Statistical indistinguishability

We will illustrate in this sub-section the utility of the results developed in our paper to prove statistical indistinguishability.

As argued in the previous sub-section, Cocks' IBE scheme is not anonymous. In [1], several results have been developed in order to obtain an anonymous variant of Cocks' IBE scheme. In order to prove security of their schemes, the authors of [1] have first established a series of computational indistinguishability results, denoted Lemma 2.1, Lemma 2.2, and Lemma 2.3 (these results are also used in [7,17]). The first indistinguishability result in [1] (Lemma 2.1) states that, given n an RSA modulus and $a \in J_n^+$, the distribution

$$X_n = \{J_n(x) \mid x \leftarrow (a + QR_n)^*\}$$

is computationally indistinguishable from the uniform distribution U on $\{-1, 1\}$, under the QR assumption for $RSAgen$. The third result in [1] (Lemma 2.3) states that, given n an RSA modulus and $a \in J_n^+$, the distribution

$$Y_n = \{J_n(x) \mid x \leftarrow (-4a + QR_n)^*\}$$

is computationally indistinguishable from the uniform distribution U on $\{-1, 1\}$, under the QR assumption for $RSAgen$. Both proofs of Lemma 2.1 and 2.3 in [1] are directly based on the IND-ID-CPA security of Cocks' IBE scheme.

Using the results developed in Section 2 we can prove stronger results for the two distributions above.

Theorem 12. *Let n be an RSA modulus and $a \in J_n^+$. Then, the distributions*

$$X_n = \{J_n(x) \mid x \leftarrow (a + QR_n)^*\}$$

and

$$Y_n = \{J_n(x) \mid x \leftarrow (-a + QR_n)^*\}$$

are each of them statistically indistinguishable from the uniform distribution U on $\{-1, 1\}$.

Proof. We will prove the theorem only for the case of X_n (the other case follows a similar proof line). Therefore, we show that the statistical distance $\Delta(X_n, U)$ between X_n and U is negligible, where

$$\Delta(X_n, U) = \frac{1}{2}\left(\sum_{b \in \{-1,1\}} \mid P(X_n = b) - P(U = b) \mid\right).$$

In order to compute $P(X_n = b)$ we make use of Corollary 13. Thus, taking into account that $P(a \in QR_n) = P(a \in J_n^+ \setminus QR_n) = 1/2$ because $a \in J_n^+$, we obtain

$$\begin{aligned}P(X_n = 1) =& P(x \in J_n^+ \ : \ x \leftarrow (a + QR_n)^*)\\ =& P(x \in J_n^+ \ : \ x \leftarrow (a + QR_n)^* \mid a \in QR_n) \cdot P(a \in QR_n) +\\ & P(x \in J_n^+ \ : \ x \leftarrow (a + QR_n)^* \mid a \in J_n^+ \setminus QR_n) \cdot P(a \in J_n^+ \setminus QR_n)\\ =& \left(\frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right)\right) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right).\end{aligned}$$

In a similar way one can obtain

$$P(X_n = -1) = \frac{1}{2} - \mathcal{O}\left(\frac{1}{n}\right).$$

Now, the statistical distance $\Delta(X_n, U)$ becomes

$$\Delta(X_n, U) = \frac{1}{2}\left(\left|\frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right) - \frac{1}{2}\right| + \left|\frac{1}{2} - \mathcal{O}\left(\frac{1}{n}\right) - \frac{1}{2}\right|\right) = \mathcal{O}\left(\frac{1}{n}\right).$$

Since n is exponentially large in the security parameter λ, the statistical distance is negligible.

It is well-known that the statistical indistinguishability implies the computational indistinguishability [13]. Therefore, the results mentioned above, namely Lemma 2.1 and Lemma 2.3 in [1], simply follow from Theorem 12. Moreover, our result does not make use of the QR assumption for $RSAgen$, nor of the security of Cocks' IBE scheme.

Lemma 2.2 in [1] states that the distributions

$$D_0(\lambda) = \{(a, c, n) \mid n \leftarrow RSAgen(\lambda),\ a \leftarrow J_n^+,\ c \leftarrow C_n^*(a)\}$$

and

$$D_1(\lambda) = \{(a, c, n) \mid n \leftarrow RSAgen(\lambda),\ a \leftarrow J_n^+,\ c \leftarrow G_n(a) \setminus C_n^*(a)\}$$

are computationally indistinguishable under the QR assumption for $RSAgen$. Moreover, the proof of this result in [1] uses the IND-ID-CPA security of Cocks' IBE scheme (because it uses Lemma 2.1). However, this is not necessary if one uses Theorem 12 instead of Lemma 2.1 (see [1] for the proof of Lemma 2.2).

We would like to emphasize that a and n are "variable" in the distributions $D_0(\lambda)$ and $D_1(\lambda)$, while they are fixed in the distributions in Theorem 12. The variability of a is very important to prove that $D_0(\lambda)$ and $D_1(\lambda)$ are computationally indistinguishable under the QR assumption. This property allows, given $r \in J_n^+$, to find c and a such that $(c^2 - 4a)_n = r$. If a is fixed, finding c with the above property would have required the extraction of a square root of $(4a + r)_n$ modulo n without knowing the factorization of n (for details, the reader is referred to [1]).

Lemma 2.2 in [1] also implies that the distributions

$$D_{0,n,a} = \{c \mid c \leftarrow C_n^*(a)\}$$

and

$$D_{1,n,a} = \{c \mid c \leftarrow G_n(a) \setminus C_n^*(a)\},$$

where n is an RSA modulus and $a \in J_n^+$, are computationally indistinguishable under the QR assumption.

4 Conclusion

The theory of quadratic residues modulo composite integers plays a very important role in cryptography. In this paper we have focused on the distribution of quadratic residues and non-residues in sets of the form $a+X = \{(a+x) \bmod n \mid x \in X\}$, where n is a prime or the product of two primes $n = pq$, and X is a subset of $\mathbb{Z}_n^*$ whose elements have some given Jacobi pattern. The results we have obtained (Section 2) allowed us to perform a deeper and a more rigorous analysis of some distributions related to Cocks' IBE scheme and Galbraith's test (Section 3.1). Moreover, we were also able to prove (Section 3.2) that some probability distributions related to Cocks' IBE scheme are statistically indistinguishable from the uniform distribution on $\{-1, 1\}$ (previous results have shown that the corresponding distributions are computationally indistinguishable under the QR assumption).

The two applications discussed in Section 3 of the paper were possible because the formulas developed in Section 2 are exact and not approximate. Because of this, we expect our results to have many other applications to cryptography.

The results developed in Section 2 refer only to sequences of length two. A natural question is whether they can be extended to sequences of length three or more, such as

$$QR_n(a_2 + QNR_n(a_1 + J_n^{\pm}))$$

or

$$J_n^{\pm}(a_3 + QR_n(a_2 + QNR_n(a_1 + J_n^{\pm}))).$$

This question does not have a straightforward answer because we are looking for exact formulas and the increment for our sets is arbitrary (a_1, a_2, a_3, etc.).

References

1. Ateniese, G., Gasti, P.: Universally anonymous IBE based on the quadratic residuosity assumption. In: CT-RSA 2009. Lecture Notes in Computer Science, vol. 5473, pp. 32–47. Springer (2009)
2. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: CCS 1993. pp. 62–73. ACM (1993)
3. Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo-random number generator. SIAM J. Comput. **15**(2), 364–383 (May 1986). https://doi.org/10.1137/0215025, http://dx.doi.org/10.1137/0215025

4. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027, pp. 506–522. Springer (2004)
5. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 213–229. Springer (2001)
6. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: FOCS 2007. pp. 647–657. IEEE Computer Society (2007)
7. Clear, M., Tewari, H., McGoldrick, C.: Anonymous IBE from quadratic residuosity with improved performance. In: AFRICACRYPT 2014. Lecture Notes in Computer Science, vol. 8469, pp. 377–397. Springer (2014)
8. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: IMACC 2001. Lecture Notes in Computer Science, vol. 2260, pp. 360–363. Springer (2001)
9. Davenport, H.: On the distribution of quadratic residues (mod p). Journal of the London Mathematical Society **s1-6**(1), 49–54 (1931)
10. Davenport, H.: On the distribution of quadratic residues (mod p). Journal of the London Mathematical Society **s1-8**(1), 46–52 (1933)
11. Elashry, I., Mu, Y., Susilo, W.: Jhanwar-Barua's identity-based encryption revisited. In: NSS 2014, Lecture Notes in Computer Science, vol. 8792, pp. 271–284. Springer (2014)
12. Elashry, I., Mu, Y., Susilo, W.: An efficient variant of Boneh-Gentry-Hamburg's identity-based encryption without pairing. In: WISA 2014, Lecture Notes in Computer Science, vol. 8909, pp. 257–268. Springer (2015)
13. Goldreich, O.: Foundations of cryptography: Volume 1, Basic tools. Cambridge University Press (2007)
14. Goldwasser, S.: Cocks' IBE scheme. Bilinear maps. MIT Lecture Notes: "6876: Advanced Cryptography" (2004)
15. Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information. In: STOC 1982. pp. 365–377. ACM (1982)
16. Jhanwar, M.P., Barua, R.: A variant of Boneh-Gentry-Hamburg's pairing-free identity based encryption scheme. In: INSCRYPT 2008. Lecture Notes in Computer Science, vol. 5487, pp. 314–331. Springer (2009)
17. Joye, M.: Identity-based cryptosystems and quadratic residuosity. In: PKC 2016. Lecture Notes in Computer Science, vol. 9614, pp. 225–254. Springer (2016)
18. Justus, B.: The distribution of quadratic residues and non-residues in the Goldwasser-Micali type of cryptosystem. Journal of Mathematical Cryptology **8**(8), 115–140 (2014)
19. Nathanson, M.B.: Elementary methods in number theory. Graduate Texts in Mathematics, Springer (2000)
20. Peralta, R.: On the distribution of quadratic residues and nonresidues modulo a prime number. Mathematics of Computation **58**(197), 433–440 (1992)
21. Perron, O.: Bemerkungen über die verteilung der quadratischen reste. Mathematische Zeitschrift **56**(2), 122–130 (1952)
22. Rabin, M.O.: Digitalized signatures and public-key functions as intractable as factorization. Tech. rep., MIT (1979)
23. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairings. In: SCIS 2000 (2000)
24. Shamir, A.: Identity-based cryptosystems and signature schemes. In: CRYPTO 1984. Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer (1985)

25. Shoup, V.: A computational introduction to number theory and algebra. Cambridge University Press (2008)
26. Ţiplea, F.L., Iftene, S., Teşeleanu, G., Nica, A.M.: Security of identity-based encryption schemes from quadratic residues. In: SECITC 2016. Lecture Notes in Computer Science, vol. 10006, pp. 63–77. Springer (2016)