Advancements in Distributed RSA Key Generation: Enhanced Biprimality Tests

ChihYun Chuang[1], IHung Hsu[1], and TingFang Lee[2]

[1] AMIS, Taipei, Taiwan
{chihyun,glen}@maicoin.com
[2] Division of Biostatistics, NYU Langone Health
Ting-Fang.Lee@nyulangone.org

Abstract. RSA is widely used in modern cryptographic practice, with certain RSA-based protocols relying on the secrecy of p and q. A common approach is to use secure multiparty computation to address the privacy concerns of p and q. Specifically constrained to distributed RSA modulus generation protocols, the biprimality test for Blum integers $N = pq$, where $p \equiv q \equiv 3 \pmod 4$ are two primes, proposed by Boneh and Franklin (2001) is the most commonly used. Over the past 20 years, the worst-case acceptance rate of this test has been consistently assumed to be 1/2 under the condition $\gcd(pq, p + q - 1) = 1$. This paper demonstrates that the acceptance probability for the Boneh-Franklin test is at most 1/4, rather than 1/2, except in the specific case where $p = q = 3$. Notably, 1/4 is shown to be the tightest upper bound. This result substantially improves the practical effectiveness of the Boneh-Franklin test: achieving the same level of soundness for the RSA modulus now requires only half the iterations previously considered necessary. Furthermore, we propose a generalized biprimality test based on the Lucas sequence. In the worst case, the acceptance rate of the proposed test is at most $1/4 + 1.25/(p_{\min} - 3)$, where $p_{\min}$ is the smallest prime factors of N. To validate our approach, we implemented the variant Miller-Rabin test, the Boneh-Franklin test, and our proposed test, performing pairwise comparisons of their effectiveness. Simulations indicate that the proposed test is generally more efficient than the Boneh-Franklin test in detecting cases where N is not an RSA modulus. Additionally, this test is applicable to generating RSA moduli for arbitrary odd primes p, q. A corresponding protocol is developed for this test, validated for resilience against semi-honest adversaries, and shown to be applicable to most known distributed RSA modulus generation protocols. After thoroughly analyzing and comparing well-known protocols for Blum integers, including Burkhardt et al.'s protocol (CCS 2023), and the Boneh-Franklin protocol, our protocol is competitive for generating distributed RSA moduli.

1 Introduction

The RSA cryptosystem [35] is one of the pioneering and widely used public key cryptosystems. In classical scenarios, two large distinct primes, p and q, are initially generated as secret keys, and the public key, $N = pq$, is derived as the

product of these two distinct primes. However, this method may introduce a vulnerability due to a single point of attack. To mitigate this concern, multi-party computation (MPC) becomes crucial, allowing participants to collectively compute a function using inputs from all parties while preserving the confidentiality of each party's input. This feature is essential for various cryptographic protocols and primitives, including threshold homomorphic encryption [22, 25], time-lock puzzles [1, 30, 36], accumulators [4, 7, 28], and verifiable delay functions [6, 15, 20, 26, 33, 38].

The goal is that, provided with n parties, of which any $t < n$ can potentially be compromised by an adversary, we seek a secure protocol that generates a random and valid **RSA modulus** $N = pq$, where p and q are two distinct primes of a specified size. The objective is to ensure that the adversary gains no knowledge except for N from the protocol while maintaining the privacy of p and q. The concept of such a protocol consists of two parts: **(a) Prime Candidate Sieving**: participants generate a potential RSA modulus N that does not divide by a prime less than a predetermined integer B; and **(b) Biprimality test**: the candidate N is repeatedly tested by a biprimality test. If N is rejected by the biprimality test, then the process starts over.

The current fastest approach for part (a) fundamentally involves generating candidates N using the Chinese Remainder Theorem (CRT) [13,37] such that N is coprime to all small primes. For part (b), two primality tests, **Miller-Rabin (primality) test** (cf. [12, Section 3.2]) and **Boneh-Franklin's (biprimality) tests** (cf, Theorem 1), were commonly employed.

Currently, both methods are specifically restricted to the scenario where $p \equiv q \equiv 3 \pmod 4$. In the worst case, the Miller-Rabin test may accept a composite with a probability of $1/4$ [11,34]. Regarding Boneh-Franklin test, in their original findings [8], they proved that the acceptance with a probability in the worst scenes is at most $1/2$. In addition, based on the average estimation results [16,17], Miller-Rabin can achieve soundness error no greater than 2^{-67} with only two executions, when the public key $N = pq$ is 2048-bit. The similar results for the Boneh-Franklin test are still an open question to date [14, 17]. Therefore, to reach the same soundness error, the Boneh-Franklin test requires 67 checks, significantly increasing the verification cost. In the paper by Burkhardt et al. [12], owing to the superior discriminative power of variant Miller-Rabin test[3], it demonstrates enhanced efficiency, although the expense of running a single MPC version of the variant Miller-Rabin test exceeds that of the Boneh-Franklin test.

However, in practical applications, we observe two key obstacles when applying Burkhardt et al.'s approach using the Miller-Rabin test. First, they assume that p and q are of equal length (cf. [12, Input assumptions]). Second, the averaged results of Miller-Rabin test rely on the assumption that p and q are selected from a uniform distribution. However, all known algorithms for distributed RSA modulus generation [8, 13, 14, 17, 21, 37] do not produce p and q from a uniform distribution, which is a distribution of a sum of uniform variables actually. As a

[3] The variant Miller-Rabin test they used is a special case of the original Miller-Rabin test. See Subsection 5.1

result, directly applying the average results of the Miller-Rabin test in practical scenarios remains constrained and requires further investigation.

For current distributed RSA-moduli protocols, extensive research has focused on Prime Candidate Sieving, but research on biprimality tests remains limited. In this paper, we focus on the following questions.

Which of the Boneh-Franklin or Miller-Rabin tests offers greater advantages for determining RSA moduli? Are there more efficient or general alternatives to biprimality tests?

1.1 Our contribution

Our paper aims to develop an optimal biprimality test that improves efficiency and relaxes existing limitations. The first finding is that, in the worst-case scenario, the probability of the commonly used Boneh-Franklin test accepting a non-RSA modulus is $1/4$ instead of $1/2$, thereby refining the previously established upper bound. The reasoning behind this result is outlined in the Technical Overview subsection. Furthermore, we identify the necessary and sufficient conditions for the types of p and q that result in the worst acceptance rate (cf. Corollary 1). Notably, there exist infinitely many pairs of p and q that produce this worst-case scenario.

Secondly, a novel Lucas (biprimality) test is proposed to improve the efficiency in detecting cases where N is not an RSA modulus. Inspired by classical Lucas primality tests, we naturally consider, for an integer D with $\gcd(N, 2D) = 1$,

$$\mathcal{Z}(D,N) := \left\{ (P,Q) \;\middle|\; \begin{array}{l} P^2 - 4Q = D \pmod N, \\ \gcd(Q,N) = 1, 0 \le P, Q < N \end{array} \right\},$$

and

$$\mathrm{LPBP}(D,N,e_4) := \left\{ (P,Q) \;\middle|\; \begin{array}{l} 0 \le P, Q < N, P^2 - 4Q = D \pmod N, \\ \gcd(Q,N) = 1, (\alpha\beta^{-1})^{e_4} = \pm 1 \pmod{N\mathcal{O}_D} \end{array} \right\}.$$

Here α, β are the two distinct roots of the quadratic polynomial $x^2 - Px + Q$, the ring of integer $\mathcal{O}_D$ of the quadratic field extension $\mathbb{Q}(\sqrt{D})$, and $e_4 := (p + [\frac{-1}{p}])(q + [\frac{-1}{q}])/4$. In particular, if $p \equiv q \equiv 3 \pmod 4$, $e_4 = (p-1)(q-1)/4$ is introduced by Boneh-Franklin. Our findings indicate that $|\mathrm{LPBP}(D,N,e_4)| < |\mathcal{Z}(D,N)|$, when N is an RSA modulus. Therefore, $\mathcal{Z}(D,N)$ cannot serve as the set considered in the biprimality test. Fortunately, the set $\mathrm{LPBP}(D,N,e_4)$ and the set $\mathcal{Z}^{+1}(D,N) := \mathcal{Z}(D,N) \cap \{(P,Q) \mid \left[\frac{Q}{N}\right] = 1\}$ exhibit features similar to those considered in the Boneh-Franklin test (cf. Theorem 1 and 2). This enables us to use the proposed Lucas test to determine whether N is an RSA modulus. From this point forward, we will refer to the proposed Lucas test as the Lucas test for convenience.

Our study indicate that the Lucas test is more efficient than the Boneh-Franklin test. Firstly, in the protocol for $p \equiv q \equiv 3 \pmod 4$, the complexity of

both tests is nearly identical (cf. Table 3). Next, both tests consider a set G and its subset H, satisfying the condition that if N is an RSA modulus, then $|G| = |H|$, and otherwise $|H| < |G|$. Let $N = pq = \prod_i p_i^{r_i}$. According to the counting formula of non-perfect-square N (cf. Theorem 1, Proposition 1), the sizes of $|G|$ in the Lucas test and the Boneh test are nearly identical when p_i are sufficiently large for all i. However, for $|H|$, the Boneh-Franklin test (resp. Lucas test) results in a count $2\prod_i \gcd(e_4, p_i - 1)$ (resp. $\prod_i \big(\gcd(e_4, p_i - 1) - 1\big) + \prod_i \gcd(e_4, p_i - 1)$). This observation shows that in most cases, it is likely to find a p_i such that $\gcd(e_4, p_i - 1) = 1$. Consequently, the size of $|H|$ in the Boneh-Franklin test is twice that of the Lucas test. As a result, the Lucas test often achieves nearly twice the probability of detecting that N is not an RSA modulus when randomly selecting elements from G, and p_i sufficiently large for all i.

Practically, ensuring that N has no small prime factors p_i is straightforward via trial division, a necessary step in any efficient distributed RSA modulus generation protocol. Additionally, Table 2 indirectly suggests that when p and q are randomly selected from a specific distribution, performing the same number of biprimality tests makes it highly likely that the Lucas test will achieve a better security level compared to the variant Miller-Rabin test (cf. [16]).

The improvement involves of proposed Lucas biprimality test relaxing the restrictions imposed by current distributed RSA protocols, which require the primes p and q to satisfy $p \equiv q \equiv 3 \pmod 4$. In practical cryptography, the assumption that $p \equiv q \equiv 3 \pmod 4$ is common. To the best of our knowledge, only the work by Boudabra et al. [9], which proposes a variant of KMOV cryptosystems [18, 29] for signature and encryption, requires the condition $p \equiv q \equiv 1 \pmod 4$. Consequently, this aspect of our research leans more toward theoretical completeness compared to other protocols.

Compared to the Boneh-Franklin's protocol, our proposed protocol requires sampling an integer D to satisfy a special condition $\left[\frac{-D}{N}\right] = 1$, and $\left[\frac{-D}{p}\right] = -1$. Specifically, when considering $p \equiv q \equiv 3 \pmod 4$, D can be directly chosen as 1 (i.e. no additional leakage, as in the case of the Boneh-Franklin protocol). However, in the other cases, although we can find an integer D such that $\left[\frac{-D}{N}\right] = 1$ without leaking information about p and q, the probability that $\left[\frac{-D}{p}\right] = -1$ is only $\frac{1}{2}$ because $p \pmod D$ is almost uniformly distributed in $\mathbb{Z}_D$. The failed D might leak some information about p and q (i.e., for a given D, the Jacobi symbols of the secret p and q can be learned). Nonetheless, since we only need to select one D that satisfies the required condition and p, q have large bit-lengths, the leaked information is nearly negligible.

We summarize the comparison of the three tests in Table 1. The proposed protocol for cases where $p \equiv q \equiv 3 \pmod 4$ is highly competitive when compared to both the Boneh-Franklin test and the variant Miller-Rabin test. For other scenarios, our proposed test is advised for generating RSA moduli. In addition, a performance assessment was conducted using real experimental data, comparing the Boneh-Franklin test with our proposed tests on a standard laptop, as detailed in Subsection 5.3. We have implemented and rigorously validated the proposed

Table 1: Ranking Features of Three Tests: A Comparative Overview

Method	Boneh-Franklin	Variant Miller-Rabin	Proposed test
The worst case excluding special conditions	$1/2 \to 1/4$	$1/4$	$1/4 + 1.25/(p_{\min} - 3)$
Exceptional	$p = q = 3$	$p, q \leq 9$	$p_{\min} < 11$
Extra assumption	$\gcd(pq, e_4) = 1$	equal-length[1]	$\gcd(pq, e_4) = 1$
Detecting of non-RSA moduli	*3*	*2*	*1*
MPC Protocol efficiency	*1*	*3*	*1*
Local computation efficiency	*1*	*3*	*2*
Leakage	*No*	*No*	Blum:*No*; Non-Blum: *Negligible.*
RSA Moduli Type	Blum	Blum	Arbitrary

The numbers in the table represent rankings. **The worst case excluding special conditions** is derived from Theorem 1, 2, and Lemma 5. **Exceptional** means that the exclusion of the worst-case scenario. **Extra assumption** means the additional conditions required by each test. The ranking for **Detecting of non-RSA moduli** comes from the Table 2. The ranking for **MPC protocol efficiency** comes from the Subsection 5.2. Finally, the ranking for **Local computation efficiency** is based on the comparison of local computations in Subsection 5.2, and Protocol 4, 5, and 6.
The Blum moduli in the **RSA Moduli Type** require the condition $p \equiv q \equiv 3 \pmod 4$. $p_{\min}$ is the smallest prime factor of $N = pq$.
[1] The condition of equal-length for primes p, q implies that $\gcd(pq, e_4) = \gcd(pq, p + q - 1) = 1$.

test through empirical analysis, benchmarking it against competing methods. The corresponding codes can be found here[4].

1.2 Technical Overview

First, let us explain why the worst-case acceptance rate can be improved. In the original Boneh-Franklin's proof, the condition $\gcd\big(pq, (p-1)(q-1)\big) = 1$ was not assumed. However, this omission allowed for the existence of non-RSA moduli N, (i.e. $p = p_1^{d_1}, q = p_2^{d_2}$, $d_1 > 0$, and $q \equiv 1 \pmod{p_1^{d_1 - 1}}$, where p_1, p_2 are distinct primes) which would still pass the test. To address this issue, the assumption $\gcd\big(pq, (p-1)(q-1)\big) = 1$ was introduced to exclude these pathological cases[5]. However, in the original proof (i.e. they proved $\mathrm{BF}(N, e_4) \subsetneq G(N)$), the condition $\gcd\big(pq, (p-1)(q-1)\big) = 1$ was not easy to apply directly. Here

$$\mathrm{BF}(N, e_4) := \left\{ g \in \mathbb{Z}_N^\times \mid g^{e_4} \equiv \pm 1 \pmod N \right\} \subset G(N) := \left\{ g \in \mathbb{Z}_N^\times \;\middle|\; \left[\frac{g}{N}\right] = 1 \right\},$$

and $\left[\frac{\cdot}{\cdot}\right]$ is the Jacobi symbol.

[4] https://github.com/lukakusilk/Three-biprimality-test-comparison/blob/main/README.md

[5] Another method involves multiple verifications of an exponential operation in $\big(\mathbb{Z}_N[x]/(x^2+1)\big)^\times / \mathbb{Z}_N^\times$.

To effectively leverage the conditions $\gcd\big(pq, (p-1)(q-1)\big) = 1$, we adopted an alternative approach based on two key insights. This enabled us to derive an accurate counting formula for $\mathrm{BF}(N, e_4)$ successfully.

- The oddness of e_4 (i.e. $p \equiv q \equiv 3 \pmod 4$) gives that the mapping $g \mapsto -g$ being bijective allows us

$$\left|\{g \in \mathbb{Z}_N^\times \mid g^{e_4} \equiv \pm 1 \pmod N\}\right| = 2\left|\{g \in \mathbb{Z}_N^\times \mid g^{e_4} \equiv 1 \pmod N\}\right|.$$

- By applying CRT (Chinese Remainder Theorem), we convert the counting problems of $\{g \in \mathbb{Z}_N^\times \mid g^{e_4} \equiv 1 \pmod N\}$, into the finite product of $\mathrm{BF}(p_i^{r_i}, e_4) \subset (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$. Moreover, the number of e_4-roots of 1 in a cyclic group (i.e. $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$) can be easily derived (cf. Lemma 1).

When N is not square-free, analyzing the the quotient $|\mathrm{BF}(N, e_4)|/|G(N)|$ is relatively straightforward. However, when N is square-free, a more careful analysis is required to understand how the ratio changes. In the worst-case scenarios, such as $N = p_1p_2p_3$ and $N = p_1p_2p_3p_4$, we found that the worst-case acceptance rate is $1/4$ instead of $1/2$. For example, consider the case $p = p_1$ and $q = p_2p_3$. We can assume that $p_1 \equiv p_2 \equiv 3 \pmod 4$, and $p_3 \equiv 1 \pmod 4$, and $p_i - 1 = 2^{k_i}d_i$, where d_i is odd for all $1 \le i \le 3$, and $k_1 = k_2 = 1$, $k_3 \ge 2$. Then Lemma 3 gives us

$$\frac{|\mathrm{BF}(N, e_4)|}{|G(N)|} = \frac{2\prod_{i=1}^3 \gcd(e_4, d_i)}{2^{-1}\prod_{i=1}^3 (p_i - 1)} \le \frac{4d_1d_2d_3}{2^{k_1+k_2+k_3}d_1d_2d_3} \le \frac{1}{4}.$$

In conclusion, the main difference between this approach and the original proof is that the original method only demonstrated that $\mathrm{BF}(N, e_4)$ is a subgroup of $G(N)$, without providing any insight into the relative size. In contrast, our method accurately computes their exact counts. The same proof of the strategy can also be applied to the proposed Lucas test, which is more complex in proving $\mathrm{LPBP}(D, N, e_4) \subset \mathcal{Z}^{+1}(D, N)$, as well as counting the two sets.

In the proposed Lucas test, one of the key points is proving that, regardless of the form of p, q the set $\mathrm{LPBP}(D, N, e_4)$ is always a subset $\mathcal{Z}^{+1}(D, N)$ for any odd integers N and an integer D with $[\frac{-D}{N}] = 1$, and $[\frac{-D}{p}] = -1$. In the original Boneh-Franklin paper, this was straightforward because $p \equiv q \equiv 3 \pmod 4$, and e_4 is odd. This allowed the result $\mathrm{BF}(N, e_4) \subset G(N)$ to be easily derived from the following observation:

$$\left[\frac{g}{N}\right]^{e_4} = \left[\frac{g^{e_4}}{N}\right] = \left[\frac{\pm 1}{N}\right] = 1.$$

However, in our case, $\alpha\beta^{-1}$ does not belong to $\mathbb{Z}_N$, so this trick must be applied with caution. Recall that α, β are the two distinct roots of the quadratic polynomial $x^2 - Px + Q$. In our study (cf. Proposition 2), we found that when $\left(\alpha\beta^{-1}\right)^{e_4} \equiv \pm 1 \pmod{N\mathcal{O}_D}$, β^{2e_4} will belong to $\mathbb{Z}_N$. We can then express $(\alpha\beta)^{e_4}$ as $\left(\alpha\beta^{-1}\right)^{e_4} \cdot \beta^{2e_4}$, where all three elements belong to $\mathbb{Z}_N$, and apply the same method to complete the proof.

In terms of security proof, to successfully simulate the transcript of proposed Lucas protocol, we must carefully construct a method to generate a uniform distribution over $L = \{P \in \mathbb{Z}_N \mid [\frac{P^2-D}{N}] = 1\}$. In the scenario considered by Boneh-Franklin, they use $a^2(-1)^b$ to simulate g, where $a \in \mathbb{Z}_N^\times$. They utilize $b = 0$ or 1 to control $(a^2(-1)^b)^{e_4}$. However, in our case, due to the more complex situation (i.e., not just $p \equiv q \equiv 3 \pmod 4$), we change the selection range of a to $\left(\frac{v+w\sqrt{D}}{v-w\sqrt{D}}\right)$ with $v^2 - w^2 D \in \mathbb{Z}_N^\times$ for all $v, w \in \mathbb{Z}_N$. Furthermore, we prove that this construction can produce the desired uniform distribution of the set L (cf. Proposition 5).

Overall, the proposed protocol for the Lucas test closely resembles the Boneh-Franklin protocol, with the key distinction being that, for cases where $p \not\equiv 3 \pmod 4$ or $q \not\equiv 3 \pmod 4$, it is essential to select a D that satisfies the condition $[\frac{-D}{N}] = 1$, and $[\frac{-D}{p}] = -1$. In the next step, participants use their respective secrets concerning p and q to jointly compute $(\alpha\beta^{-1})^{e_4}$. Next, for the GCD test, we verify $\gcd(N, e_4) = \gcd\big(N, p[\frac{-1}{q}] + q[\frac{-1}{p}] + [\frac{-1}{N}]\big) = 1$. The parties $\mathcal{P}_i$ then jointly generate a random number r, which is used in an MPC multiplication to compute $r\big(p[\frac{-1}{q}] + q[\frac{-1}{p}] + [\frac{-1}{N}]\big)$. We also need to compute the value of $[\frac{-D}{p}]$. As proposed in [24], although not proven in detail, this can be done by first jointly generating s, then jointly computing and publishing $s^2 p \pmod D$ thus obtaining $[\frac{p}{D}]$. This can be computed using the basic rules of the Legendre symbol (cf. π_{Leg}).

1.3 Related work

Boneh and Franklin [8] first proposed the distributed RSA moduli generation. They provided an efficient distributed RSA moduli test protocol which can test if $N = pq$ is an RSA modulus without needing to know information about p and q and is secure in semi-honest adversary model against an honest majority. They prove their test has the property that it always accepts when N is an RSA modulus, and otherwise accepts with probability at most $1/2$. In their paper, they offered two types of biprimality test. Excluding identical verification steps, one involves multiple checks for $\gcd(pq, (p-1)(q-1)) = 1$, while the other involves multiple verifications of an exponential operation in $\big(\mathbb{Z}_N[x]/(x^2+1)\big)^\times/\mathbb{Z}_N^\times$. The current mainstream approach mostly involves checking the version where $\gcd(pq, p+q-1) = 1$. Algesheimer et al. [2] proposed a distributed Miller–Rabin test that achieves semi-honest security against a dishonest majority. Following that, there are several related papers [12, 17] that utilize the Miller-Rabin test to design biprimality tests. Regarding the estimation of the average error in primality tests, Damgård et al. [16] obtained an upper bound for the Miller-Rabin case. Einsele et al. [19] provided an upper bound for the case of Lucas strong primes. For articles addressing the optimization of RSA moduli candidates and proposing a more secure security model, Burkhardt et al.'s paper [12] underwent a comprehensive review.

2 Preliminaries

Basic notations. Let $\mathbf{P}$ be the set of all primes, $\mathbb{N}$ be the nature numbers, and $\mathbb{Z}$ be the ring of integers. For a finite set S, $|S|$ means the cardinality of S. Let $\mathbb{Z}_N$ be the additive group of order N, and $\mathbb{Z}_N^\times$ be the multiplicative group in $\mathbb{Z}_N$. Moreover, $|\mathbb{Z}_N^\times| = \phi(N)$, where ϕ is the Euler's totient function. For an interval $\mathcal{I}$, we set $\mathbf{P}(\mathcal{I}) := \{p \in \mathbf{P} \mid p \in \mathcal{I}\}$. The greatest common divisor of two positive integers x and $y \in \mathbb{N}$ is denoted by $\gcd(x, y)$. Let $[\![a]\!]_m$(resp. $[\![a]\!]_\mathbb{Z}$) be the secure additive sharing of value a in the integer domain $\mathbb{Z}_m$ (resp. $\mathbb{Z}$). That is each of the participants, $\{\mathcal{P}_i\}_{i=1}^n$, has their own secret $\mathfrak{a}_i \in \mathbb{Z}_m$(resp. $\mathfrak{a}_i \in \mathbb{Z}$) such that $\sum_{i=1}^n \mathfrak{a}_i \equiv a \pmod m$ (resp. $\sum_{i=1}^n \mathfrak{a}_i = a$).

For ease of reference, we present some symbols that have already appeared elsewhere. Given two odd positive integers p, q and a positive integer n, set $e_4(= e_4(p, q)) := \frac{1}{4}\big(p + \left[\frac{-1}{p}\right]\big)\big(q + \left[\frac{-1}{q}\right]\big)$. Here $\left[\frac{\cdot}{\cdot}\right]$ is the Jacobi symbol. For odd integers p, q, we set

$$\mathrm{MR}(p) := \{g \in \mathbb{Z}_p^\times \mid g^{(p-1)/2} \equiv \pm 1 \pmod p\},$$

$$\mathrm{BF}(N, e_4) := \left\{g \in \mathbb{Z}_N^\times \mid g^{e_4} \equiv \pm 1 \pmod N\right\}, G(N) := \left\{g \in \mathbb{Z}_N^\times \;\middle|\; \left[\frac{g}{N}\right] = 1\right\},$$

$$\mathcal{Z}^\epsilon(D, N) := \left\{(P, Q) \;\middle|\; \begin{array}{l} P^2 - 4Q = D \pmod N, \left[\frac{Q}{N}\right] = \epsilon, \\ \gcd(Q, N) = 1, 0 \le P, Q < N \end{array}\right\}, \text{ for } \epsilon \in \{\pm 1\},$$

$\mathcal{Z}(D, N) = \cup_{\epsilon \in \{\pm 1\}} \mathcal{Z}^\epsilon(D, N)$, and

$$\mathrm{LPBP}(D, N, e_4) := \left\{(P, Q) \;\middle|\; \begin{array}{l} 0 \le P, Q < N, P^2 - 4Q = D \pmod N, \\ \gcd(Q, N) = 1, (\alpha\beta^{-1})^{e_4} = \pm 1 \pmod N \end{array}\right\}.$$

If $p \equiv q \equiv 3 \pmod 4$, the set $\mathrm{BF}(N, e_4)$ (resp. $\mathrm{LPBP}(D, N, e_4)$) is a subgroup (resp. subset) of $G(N)$ (resp. $\mathcal{Z}^{+1}(D, N)$) (cf. Proposition 2).

Given that $p \equiv q \equiv 3 \pmod 4$ and a perfect square D, we are interested in studying the following two quantities: $\beta_{\mathrm{Lucas}}(D, N, e_4) := \frac{|\mathrm{LPBP}(D,N,e_4)|}{|\mathcal{Z}^{+1}(D,N)|}$, and $\beta_{\mathrm{BF}}(N, e_4) := \frac{|\mathrm{BF}(N,e_4)|}{|G(N)|}$, where two quantities are used to evaluate the proportion of randomly selected elements in the set of denominators that pass the test when $N = pq$ is not an RSA modulus. These values always belong to the range $[0, 1]$, and the smaller the value, the easier it is to determine that p and q are not an RSA modulus. In fact, Proposition 1 and Proposition 2 implies that $\beta_{\mathrm{Lucas}}(D, N, e_4)$ is independent of the chosen of perfect squares D, if $p \equiv q \equiv 3 \pmod 4$. For simplicity, when we write $\beta_{\mathrm{Lucas}}(N, e_4) = \beta_{\mathrm{Lucas}}(1, N, e_4)$.

2.1 Two Mathematical Results

Lemma 1. [3, Lemma 2.1] *Let G be a cyclic group and d an integer. There are exactly* $\gcd(d, |G|)$ *dth-root of* 1 *in G.*

Lemma 2 (Hensel's Lemma). [32, Theorem 2.23 or 2.24] *Let $f(x)$ be a polynomial with integer coefficients. If p is a prime number and a is an integer such that $f(a) \equiv 0 \pmod{p^j}$, and $f'(a) \not\equiv 0 \pmod{p}$ then, there exists an integer $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

2.2 Lucas Pseudo-primes

We recall Lucas sequence and some results [3]. Let P and Q be integers and $D := P^2 - 4Q$. The Lucas sequence (U_k, V_k) that is associated with the parameters P, Q are defined as, for $k \geq 0$,

$$\begin{cases} U_{k+2} = PU_{k+1} - QU_k; \\ V_{k+2} = PV_{k+1} - QV_k, \end{cases} \quad \text{with} \quad \begin{cases} U_0 = 0, U_1 = 1; \\ V_0 = 2, V_1 = P. \end{cases}$$

It is well known that $U_{p-\left[\frac{D}{p}\right]} \equiv 0 \pmod{p}$ for any prime $p \nmid 2QD$. For the Lucas sequence [3, Section 3], (U_k, V_k) associated with P, Q and $P^2 - 4Q \neq 0$, we have the general formula: for all $k \in \mathbb{N}$,

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},\ V_k = \alpha^k + \beta^k,$$

where α, β are two distinct roots of the polynomial $x^2 - Px + Q$. Let $\mathcal{O}_D$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$, and $\tau := \alpha\beta^{-1}$. If $N \nmid 2QD$, then we have, for $k \in \mathbb{N}$,

$$N \mid U_k \text{ if and only if } \tau^k \equiv 1 \pmod{N\mathcal{O}_D}. \tag{1}$$

Given an element $u + v\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, the norm map is given by $\mathbf{N}(u + v\sqrt{D}) = u^2 - v^2 D \in \mathbb{Q}$. When $x \in \mathcal{O}_D$, the norm $\mathbf{N}(x) \in \mathbb{Z}$. Consider the multiplicative group of norm 1 elements denoted by $\widehat{(\mathcal{O}_D/N)}$ in a free $\mathbb{Z}/N\mathbb{Z}$-algebra of rank 2. This group is the image of the set

$$\{x \in \mathcal{O}_D \mid \mathbf{N}(x) \equiv 1 \pmod{N}\}$$

by the canonical map $\mathcal{O}_D \to \mathcal{O}_D/N$.

2.3 The Security Model

Our focus is on static semi-honest adversaries. "Static" implies that the adversary is limited to selecting a set of parties to corrupt before the protocol execution starts and is not allowed to change this set afterward. Semi-honest adversaries participate in the protocol honestly but attempt to glean as much information as possible from the messages received from other parties. Here, we adopt the definition provided in [36, Definition 7.5.1], as follows.

Let $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$ be an $n-$ary functionality, where $f_i(x_1, \ldots, x_n)$ denotes the i-th element of $f(x_1, \ldots, x_n)$. For $I = \{i_1, \ldots i_t\} \subset \{1, \ldots, n\}$, we let

$f_I(x_1,\ldots,x_n)$ denote the subsequence $f_{i_1}(x_1,\ldots,x_n),\ldots,f_{i_t}(x_1,\ldots,x_n)$. Let Π be an n-party protocol for computing f. The view of the $i-$th party during an execution of Π on $\boldsymbol{x}=(x_1,\ldots,x_n)$, denoted $\mathrm{VIEW}_i^{\Pi}(\boldsymbol{x})$, is $(x_i,r_i,m_{i_1},\ldots,m_{i_\ell})$, where r_i represents the outcome of the $i-$th party's internal coin tosses, and m_{i_j} represents the $j-$th message it has received. For $I=\{i_1,\ldots,i_t\}$, we let $\mathrm{VIEW}_I^{\Pi}(\boldsymbol{x}) := (I,\mathrm{VIEW}_{i_1}^{\Pi}(\boldsymbol{x}),\ldots,\ \mathrm{VIEW}_{i_t}^{\Pi}(\boldsymbol{x}))$.

Definition 1. *We say that Π privately computes f if there exists a probabilistic polynomial-time algorithm, denoted S, such that for every $I\subseteq\{1,\ldots,n\}$, it holds that*

$$\begin{aligned}&\{(S(I,(x_{i_1},\ldots,x_{i_t}),f_I(\boldsymbol{x})),f(\boldsymbol{x}))\}_{\boldsymbol{x}\in(\{0,1\}^*)^n}\\ \overset{\mathrm{c}}{\equiv}&\{(\ \mathrm{VIEW}_I^{\Pi}(\boldsymbol{x}),\ \mathrm{OUTPUT}^{\Pi}(\boldsymbol{x}))\}_{\boldsymbol{x}\in(\{0,1\}^*)^n}.\end{aligned}$$

Here $\mathrm{OUTPUT}^{\Pi}(\boldsymbol{x})$ denotes the output sequence of all parties during the execution represented in $\mathrm{VIEW}_I^{\Pi}(\boldsymbol{x})$, and $\overset{\mathrm{c}}{\equiv}$ is computationally indistinguishable of two distribution ensembles.

3 Refine Boneh-Franklin Biprimality Testing

We show that in the worst-case scenario, the value 1/4 is the tightest upper bound of the Boneh-Franklin test, and provide the sufficient and necessary conditions for the worst-case scenario of p and q. The counting formula of $\mathrm{BF}(N,e_4)$ is given as below.

Lemma 3. *Let $p\equiv q\equiv 3 \pmod 4$, and $\gcd\left(pq,e_4\right)=1$. Assume that $N=\prod_{i=1}^{s}p_i^{r_i}$, where p_i is prime for all i, then we have*

$$|\mathrm{BF}(N,e_4)| = 2\cdot\prod_{i=1}^{s}\gcd(e_4,d_i).$$

Here $p_i-1=2^{k_i}d_i$ with $2\nmid d_i$ for all $1\le i\le s$.

Proof. Since e_4 is odd, we have

$$|\{g\in\mathbb{Z}_N^{\times}\mid g^{e_4}\equiv 1 \pmod N\}| = |\{g\in\mathbb{Z}_N^{\times}\mid g^{e_4}\equiv -1 \pmod N\}|$$

by the bijective map $g\mapsto -g$, which implies that

$$|\mathrm{BF}(N,e_4)| = 2\cdot|\{g\in\mathbb{Z}_N^{\times}\mid g^{e_4}\equiv 1 \pmod N\}|.$$

According to CRT, we reduce the problem to count the cardinality of e_4-th roots of 1 in $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^{\times}$ which are cyclic groups for all i [27, Theorem 3, Chapter 4], since N is odd. Combining this fact, $\gcd(pq,e_4)=1$, and Lemma 1, one has the number of e_4-th roots of 1 in the group $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^{\times}$ is

$$\gcd(e_4,p_i^{r_i-1}(p_i-1)) = \gcd(e_4,d_i).$$

The above discussion implies the desired result.

Before diving into the proof of the main theorem, we recall that if $p \equiv q \equiv 3 \pmod 4$ and $N = pq$, then $\mathrm{BF}(N, e_4)$ is a subgroup of $G(N)$.

Theorem 1 (Boneh-Franklin biprimality test). *Let $p \equiv q \equiv 3 \pmod 4$, and $\gcd\left(pq, e_4\right) = 1$, where $e_4 = (p-1)(q-1)/4$. Assume that $N := pq$. If p, q are both distinct primes, then we have $\mathrm{BF}(N, e_4) = G(N)$. For the other cases, we have $|\mathrm{BF}(N, e_4)| \leq |G(N)|/4$, except for the case $p = q = 3$.*

Proof. Recall that $p_i - 1 = 2^{k_i} d_i$ with odd d_i for all i as the same notations in the Lemma 3. At first, consider the case p, q are distinct primes, which implies $e_4 = d_1 d_2$ and $k_1 = k_2 = 1$. Note that if N is not perfect square, then $|G(N)| = \phi(N)/2$; Otherwise, $|G(N)| = \phi(N)$. The proof of this case is completed by the following equality:

$$|\mathrm{BF}(N, e_4)| = 2\gcd(e_4, d_1) \cdot \gcd(e_4, d_2) = 2d_1 d_2 = \phi(N)/2.$$

Now, assume that the number of prime factors of N is greater than 2. Consider the case perfect square N. Lemma (3) implies that

$$\begin{aligned}\beta_{\mathrm{BF}}(N, e_4) =& \frac{|\mathrm{BF}(N, e_4)|}{|G(N)|} = \frac{2\prod_{i=1}^{s} \gcd(e_4, d_i)}{\prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1)} \leq \frac{2\prod_{i=1}^{s} d_i}{\prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1)} \\ =& \frac{2\prod_{i=1}^{s} 2^{-k_i}}{\prod_{i=1}^{s} p_i^{r_i - 1}} < 2^{1-1} \cdot 5^{-1} = \frac{1}{5},\end{aligned}$$

except for the case $p = q = 3$.

Consider the case N is non square-free (i.e. there exists i such that $r_i \geq 2$) and non-perfect-square. The condition non-perfect-square means that $s \geq 2$. If not, $s = 1$, then $N = p_1^{r_1}$. Since $p \equiv q \equiv 3 \pmod 4$, which implies that $N \equiv 1 \pmod 4$ and $p_1 \equiv 3 \pmod 4$, and r_1 is even, which gives a contradiction. Now, one has

$$\beta_{\mathrm{BF}}(N, e_4) = \frac{4\prod_{i=1}^{s} \gcd(e_4, d_i)}{\prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1)} \leq 2^{-k_1 - \ldots - k_s + 2} \left(\prod_{i=1}^{s} p_i^{r_i - 1}\right)^{-1}.$$

If there exists $p_i \geq 5$ with $r_i \geq 2$ then

$$\beta_{\mathrm{BF}}(N, e_4) \leq 2^{2-1-1} \cdot 5^{-1} = 1/5.$$

Additionally, if $s \geq 3$, then

$$\beta_{\mathrm{BF}}(N, e_4) \leq 2^{2-1-1-1} \cdot 3^{-1} = 1/6.$$

Therefore, we only consider the case $N = 3^{r_1} \prod_{i=2}^{s} p_i$ with $r_1 = 2$ due to

$$\beta_{\mathrm{BF}}(N, e_4) \leq 2^{2-1-1} \cdot 3^{-2} = 1/9 \text{ as } r_1 \geq 3.$$

As for the case $s = 2$, then $p_2 \equiv 1 \pmod 4$ since $N \equiv 1 \pmod 4$. This case also implies that

$$\beta_{\mathrm{BF}}(N, e_4) \leq 2^{2-1-2} \cdot 3^{-1} = 1/6.$$

In conclusion, when N is non-square-free with $s \geq 2$, $\beta_{\mathrm{BF}}(N, e_4) \leq 1/6$. When N is square-free, we consider the case $s = 3$. Because $p \equiv q \equiv 3 \pmod 4$, two elements of the set $\{p_1, p_2, p_3\}$ are 3 module 4 and one of it is 1 module 4, which gives the bound

$$\beta_{\mathrm{BF}}(N, e_4) \leq 2^{-k_1-\ldots-k_s+2} = 2^{2-1-1-2} = 1/4.$$

For all $s \geq 4$, we have $\beta_{\mathrm{BF}}(N, e_4) \leq 2^{-k_1-\ldots-k_s+2} \leq 2^{-2}$, since $k_i \geq 1$ for all i.

Based on the proof of Theorem 1, we can establish the following sufficient and necessary conditions for the worst-case scenario to occur.

Corollary 1. *Assume that the assumption of Theorem 1 holds.* $|\mathrm{BF}(N, e_4)| = |G(N)|/4$ *if and only if one of the two situations occurred without considering the symmetry of* p *and* q*. 1).* $s = 3$, $\gcd(e_4, d_i) = d_i$, $p = p_1p_2$, *and* $q = p_3$, *where* $p_1 \equiv 5 \pmod 8$, *and* $p_2 \equiv p_3 \equiv 3 \pmod 4$*; 2).* $s = 4$, $\gcd(e_4, d_i) = d_i$, $p = p_1p_2p_3$, *and* $q = p_4$, *where* $p_i \equiv 3 \pmod 4$ *for all* $1 \leq i \leq s$.

The bound in the result of Theorem 1 is tight. Taking $p_1 = 3, p_2 = 5$, and $p_3 \equiv 23 \pmod{420}$, Dirichlet Theorem[6] says that there are infinitely many $N = (p)q = (p_1p_2)p_3$ such that $|\mathrm{BF}(N, e_4)| = |G(N)|/4$, since $\gcd(N, e_4) = \gcd(15q, 7(q-1)) = 1$ and $\gcd(420, 23) = 1$.

4 The Lucas Biprimality Test

In this section, we introduce another test for identifying RSA moduli for odd integers p, q with $\gcd\left(pq, (p + [\frac{-1}{p}])(q + [\frac{-1}{q}])\right) = 1$, and subsequently provide a distributed protocol that is resilient to semi-honest adversaries.

4.1 A Lucas Biprimality Testing

The proof of the Lucas biprimality testing is similar to the proof process in the Boneh-Franklin test. First, we derive the formulas for the number of elements in $\mathrm{LPBP}(D, N, e_4)$ and $\mathcal{Z}^{+1}(D, N)$. Next, we also analyze the upper bound of their quotient (i.e., the acceptance rate) in the worst-case scenario. To begin, we examine the special case where $N = p^r$.

Lemma 4. *Let* p *be an odd prime, and* D *be an element of* $\mathbb{Z}_p^\times$*, then for* $\epsilon \in \{\pm 1\}$,

$$|\mathcal{Z}^{\epsilon}(D, p^r)| = \begin{cases} \left(\frac{1+\epsilon}{2}\right) p^{r-1} \left(p - \left[\frac{D}{p}\right] - 1\right), & \text{if } 2 \mid r; \\ p^{r-1} \left[\frac{(p - \left[\frac{D}{p}\right] - 1) - \epsilon}{2}\right], & \text{if } 2 \nmid r. \end{cases}$$

[6] If $\gcd(a, n) = 1$, then there exists infinite prime x with $x \equiv a \pmod n$ [31, Corollary 13.8].

Proof. In the case where $2 \mid r$, the condition $\left[\frac{Q}{p^r}\right] = 1$ always holds. Therefore, $|\mathcal{Z}^{+1}(D, p^r)| = |\mathcal{Z}(D, p^r)|$. In the special case $r = 1$, it is sufficient to consider the cardinality of the set $\{P \in \mathbb{Z}_p | P^2 = D + 4Q, 0 < Q < p\}$. Note that the equation $x^2 = D$ has two (resp. zero) solutions in $\mathbb{Z}_p$ if $\left[\frac{D}{p}\right] = 1$(resp. $\left[\frac{D}{p}\right] = -1$), there are $\frac{p-1}{2} - \frac{1+\left[\frac{D}{p}\right]}{2}$ values of Q such that $x^2 = D + 4Q$ has two distinct solutions. Additionally, there is one value of Q (specifically $Q = \frac{-D}{4}$) for which $x^2 = D + 4Q$ has a single solution. Thus, the total number of solutions is given by $(\frac{p-1}{2} - \frac{1+\left[\frac{D}{p}\right]}{2}) \cdot 2 + 1 = p - \left[\frac{D}{p}\right] - 1$. For $r > 1$, the desired result can be obtained using Hensel's lemma (cf. Lemma 2). The detail proof can be found in Proposition 4.

As for the case $2 \nmid r$, we first consider the case $r = 1$ and $\epsilon = 1$. Then we can assume that $Q = Q'^2$. It implies that $\mathcal{Z}^{+1}(D, p)$, which is equal to

$$\left\{ (P, Q') \;\middle|\; \begin{array}{l} (P/2)^2 = (Q')^2 + D/4 \pmod p, \gcd(Q', p) = 1, \\ 0 \le P < p, 1 \le Q' \le (p-1)/2. \end{array} \right\}.$$

Now, for counting the above set, we study the following sum

$$\sum_{i=1}^{(p-1)/2} \left[\frac{i^2 + D/4}{p}\right] = \frac{-1 - \left[\frac{D}{p}\right]}{2} \text{ (by Lemma 7)},$$

which gives us the relation

$$|S^{-1}| = |S^{+1}| + \frac{1 + \left[\frac{D}{p}\right]}{2}, \tag{2}$$

where $S^{\epsilon} = \left\{ 1 \le i \le (p-1)/2 \mid \left[\frac{i^2 + D/4}{p}\right] = \epsilon, i^2 \not\equiv -D/4 \pmod p \right\}$ (i.e. if there exists i such that $i^2 \equiv -D/4 \pmod p$, then $\left[\frac{i^2 + D/4}{p}\right] = 0$).

Note that $|S^{+1}| + |S^{-1}|$ depends on whether exist i such that $i^2 \equiv -\frac{D}{4} \pmod p$. Specifically,

$$|S^{+1}| + |S^{-1}| = \frac{p-1}{2} - \frac{1 + \left[\frac{-D}{p}\right]}{2}. \tag{3}$$

Moreover, for each $i \in S^{+1}$, we can find two distinct solutions for $(x/2)^2 \equiv i^2 + D/4 \pmod p$. If $\left[\frac{-(D/4)}{p}\right] = \left[\frac{-D}{p}\right] = 1$, then an additional solution can be found (i.e. $(0, \frac{-D}{4}) \in \mathcal{Z}^{+1}(D, p)$). Therefore,

$$|\mathcal{Z}^{+1}(D, p)| = 2 \cdot |S^{+1}| + \frac{1 + \left[\frac{-D}{p}\right]}{2}. \tag{4}$$

Combining (2), (3), and (4) gives that

$$\left|\mathcal{Z}^{+1}(D,p)\right| = \frac{p - \left[\frac{D}{p}\right] - 2}{2}.$$

Furthermore, combining Proposition 4, one has

$$\left|\mathcal{Z}^{-1}(D,p)\right| = |\mathcal{Z}(D,p)| - \left|\mathcal{Z}^{+1}(D,p)\right| = p - \left[\frac{D}{p}\right] - 1 - \left(\frac{p - \left[\frac{D}{p}\right] - 2}{2}\right) = \frac{p - \left[\frac{D}{p}\right]}{2}.$$

The proof is complete by Hensel's Lemma for the general case $r \geq 2$ (cf. Lemma 6)..

The counting formula of general N is given as below.

Proposition 1. *Let D be an integer and $N := \prod_{i=1}^{s} p_i^{r_i}$ be a positive integer with $\gcd(N, 2D) = 1$. Write $S = S_0 \cup S_1$, where $S_j := \{i \mid r_i \equiv j \pmod 2, 1 \leq i \leq s\}$. Then, one has, if N is not a perfect square in $\mathbb{Z}$,*

$$|\mathcal{Z}^{+1}(D,N)| = \left[\frac{\prod_{i\in S} p_i^{r_i-1}}{2}\right]\left[\prod_{i\in S_0}\left(p_i - \left[\frac{D}{p_i}\right] - 1\right)\right] \cdot \left[\prod_{i\in S_1}\left(p_i - \left[\frac{D}{p_i}\right] - 1\right) + (-1)^{|S_1|}\right].$$

Otherwise, if N is a perfect square,

$$|\mathcal{Z}^{+1}(D,N)| = \prod_{i\in S} p_i^{r_i-1}\left(p_i - \left[\frac{D}{p_i}\right] - 1\right).$$

Proof. If N is a perfect square, we obtain the desired result from Lemma 4 and CRT. If N is not a square, from CRT we have

$$|\mathcal{Z}^{+1}(D,N)| = \left[\prod_{i\in S_0} |\mathcal{Z}^{+1}(D,p_i^{r_i})|\right]\left[\sum_{\epsilon_1\cdot\ldots\cdot\epsilon_{|S_1|}=1}\prod_{i\in S_1}|\mathcal{Z}^{\epsilon_i}(D,p_i^{r_i})|\right].$$

Using Lemma 4 and CRT, we only need to prove

$$\sum_{\epsilon_1\cdot\ldots\cdot\epsilon_{|S_1|}=1}\prod_{i\in S_1}|\mathcal{Z}^{\epsilon_i}(D,p_i^{r_i})| = \left[\prod_{i\in S_1} p_i^{r_i-1}\right]\left[\prod_{i\in S_1}\left(p_i - \left[\frac{D}{p_i}\right] - 1\right) + (-1)^{|S_1|}\right] \Big/ 2.$$

This proof can be concluded through mathematical induction on the cardinality of $|S_1|$. When $|S_1| = 1$, it follows that ϵ must equal 1, leading to the desired

result. Assuming that $|S_1| = k$, the equality is satisfied. Let $A_i = p_i - \left[\frac{D}{p_i}\right] - 1$. Then, when $|S_1| = k+1$, applying $|\mathcal{Z}^{-1}(D,N)| = |\mathcal{Z}(D,N)| - |\mathcal{Z}^{+1}(D,N)|$, and Proposition 4, we have

$$\begin{aligned}
&\sum_{\epsilon_1\cdot\ldots\cdot\epsilon_{k+1}=1}\prod_{i\in S_1}|\mathcal{Z}^{\epsilon_i}(D,p_i^{r_i})| \\
=&|\mathcal{Z}^{-1}(D,p_{k+1}^{r_{k+1}})|\cdot\sum_{\epsilon_1\cdot\ldots\cdot\epsilon_k=-1}\prod_{i=1}^{k}|\mathcal{Z}^{\epsilon_i}(D,p_i^{r_i})| + |\mathcal{Z}^{+1}(D,p_{k+1}^{r_{k+1}})|\cdot\sum_{\epsilon_1\cdot\ldots\cdot\epsilon_k=1}\prod_{i=1}^{k}|\mathcal{Z}^{\epsilon_i}(D,p_i^{r_i})| \\
=&\frac{\left[\prod_{i=1}^{k+1}p_i^{r_i-1}\right]\left[A_{k+1}+1\right]\left[2\prod_{i=1}^{k}A_i-\left(\prod_{i=1}^{k}A_i+(-1)^k\right)\right]}{4} \\
&+\frac{\left[\prod_{i=1}^{k+1}p_i^{r_i-1}\right]\left[A_{k+1}-1\right]\left[\prod_{i=1}^{k}A_i+(-1)^k\right]}{4} \\
=&\left[\prod_{i\in S_1}p_i^{r_i-1}\right]\left[\prod_{i\in S_1}A_i+(-1)^{|S_1|}\right]\Big/2=\left[\prod_{i\in S_1}p_i^{r_i-1}\right]\left[\prod_{i\in S_1}\left(p_i-\left[\frac{D}{p_i}\right]-1\right)+(-1)^{|S_1|}\right]\Big/2.
\end{aligned}$$

Next, we study the cardinality of the set LPBP and prove that it is a subset of $\mathcal{Z}^{+1}$.

Proposition 2. *Let p,q be positive odd integers, $N = pq = \prod_{i=1}^{s}p_i^{r_i}$, and D be an integer in $\mathbb{Z}$ with $\gcd(2D,N) = 1$, and $\left[\frac{-D}{p}\right] = \left[\frac{-D}{q}\right] = -1$. Then we have the set $\mathrm{LPBP}(D,N,e_4)$ is a subset of $\mathcal{Z}^{+1}(D,N)$. Furthermore assuming $\gcd(N,e_4) = 1$, its cardinality is given by*

$$|\mathrm{LPBP}(D,N,e_4)| = \prod_{i=1}^{s}\big(\gcd(e_4,d_i)-1\big) + \prod_{i=1}^{s}\gcd(e_4,d_i).$$

Here $p_i - \left[\frac{D}{p_i}\right] = 2^{k_i}d_i$ with $2\nmid d_i$ for all $1\le i\le s$.

Proof. For sake of proving $\mathrm{LPBP}(D,N,e_4)\subseteq\mathcal{Z}^{+1}(D,N)$, we need to prove that taking any pair $(P,Q)\in\mathrm{LPBP}(D,N,e_4)$ then one has $(\alpha\beta^{-1})^{e_4}\equiv\pm1 \pmod{N\mathcal{O}_D}$, where α,β are two distinct roots of the polynomial x^2-Px+Q, which implies that $\left[\frac{Q}{N}\right] = 1$. Note that $(\alpha\beta^{-1})^{e_4}\equiv\pm1 \pmod{N\mathcal{O}_D}$ can be viewed as an element in $\mathbb{Z}_N^{\times}$, and $Q=\alpha\beta\in\mathbb{Z}_N^{\times}$ imply that $\beta^{2e_4}\in\mathbb{Z}_N^{\times}$. Because e_4 is odd, we have

$$\left[\frac{Q}{N}\right] = \left[\frac{Q}{N}\right]^{e_4} = \left[\frac{(\alpha\beta)^{e_4}}{N}\right] = \left[\frac{\beta^{2e_4}}{N}\right]\left[\frac{(\alpha\beta^{-1})^{e_4}}{N}\right].$$

Recall that $(\alpha\beta^{-1})^{e_4}\equiv\pm1 \pmod N$, then $\alpha^{e_4} = \pm\beta^{e_4}$, which implies that $(P+\sqrt{D})^{e_4} = \pm(P-\sqrt{D})^{e_4} \pmod{N\mathcal{O}_D}$. Now, consider the case $(P+\sqrt{D})^{e_4} = -(P-\sqrt{D})^{e_4} \pmod{N\mathcal{O}_D}$. Write $(P+\sqrt{D})^{e_4} = A + B\sqrt{D} \pmod{N\mathcal{O}_D}$, where $A = \sum_{\substack{i=0:\\ 2\nmid i}}^{e_4}\binom{e_4}{i}P^iD^{(e_4-i)/2}$ and $B = \sum_{\substack{i=0:\\ 2\mid i}}^{e_4}\binom{e_4}{i}P^iD^{(e_4-1-i)/2}$. Then $-(P-$

$\sqrt{D})^{e_4} = -A + B\sqrt{D} \pmod{N\mathcal{O}_D}$. Therefore, the equality $A + B\sqrt{D} \equiv -A + B\sqrt{D} \pmod{N\mathcal{O}_D}$ gives us $A \equiv 0 \pmod{N\mathcal{O}_D}$, since N is odd. Now, we have

$$\beta^{e_4} = \left(\frac{P + \sqrt{D}}{2}\right)^{e_4} \equiv \frac{B(\sqrt{D})}{2^{e_4}} \pmod{N\mathcal{O}_D},$$

which implies that $\beta^{2e_4} \equiv 2^{-2e_4}B^2D \pmod{N}$. In conclusion, when $(\alpha\beta^{-1})^{e_4} \equiv -1 \pmod{N\mathcal{O}_D}$, we have

$$\left[\frac{Q}{N}\right] = \left[\frac{\beta^{2e_4}}{N}\right]\left[\frac{(\alpha\beta^{-1})^{e_4}}{N}\right] = \left[\frac{D}{N}\right]\left[\frac{-1}{N}\right] = \left[\frac{D}{p}\right]\left[\frac{D}{q}\right]\left[\frac{-1}{p}\right]\left[\frac{-1}{q}\right] = 1.$$

Similarly, when $\alpha^{e_4} = \beta^{e_4}$, we have $\beta^{e_4} \equiv 2^{-e_4}A \pmod{N}$, which gives us

$$\left[\frac{Q}{N}\right] = \left[\frac{\beta^{2e_4}}{N}\right]\left[\frac{(\alpha\beta^{-1})^{e_4}}{N}\right] = \left[\frac{2^{-2e_4}A^2}{N}\right]\left[\frac{1}{N}\right] = 1.$$

The proof of the cardinality of $\mathrm{LPBP}(D, N, e_4)$ can be found in [3, Section 1.4].

Finally, the acceptance rate, β_{Lucas}, in this test is estimated as follows.

Theorem 2. *Let p, q be odd integers, $\gcd\left(pq, e_4\right) = 1$. Set $N = pq$. Assume that D is an integer in $\mathbb{Z}$ with $\gcd(2D, N) = 1$, and $\left[\frac{-D}{p}\right] = \left[\frac{-D}{q}\right] = -1$. If p, q are both distinct primes, then we have $\mathrm{LPBP}(D, N, e_4) = \mathcal{Z}^{+1}(D, N)$. For the remainder cases, set $p_{\min}$ be the minimal prime factor of N. Assume $p_{\min} \geq 11$, then we have*

$$\beta_{\mathrm{Lucas}}(D, N, e_4) = \frac{|\mathrm{LPBP}(D, N, e_4)|}{|\mathcal{Z}^{+1}(D, N)|} < \frac{1}{4} + \frac{1.25}{p_{\min} - 3}.$$

Proof. Consider the case p, q are distinct primes. Set $p_1 = p$ and $p_2 = q$. Recall that $p_i - \left[\frac{D}{p_i}\right] = 2d_i$ for all i. Thus, one has $e_4 = \frac{(p - \left[\frac{D}{p}\right])(q - \left[\frac{D}{q}\right])}{4} = d_1 d_2$. Now, we only need to prove that $|\mathcal{Z}^{+1}(D, N)| = |\mathrm{LPBP}(D, N, e_4)|$, because Proposition 2 says that $\mathrm{LPBP}(D, N, e_4)$ is a subset of $\mathcal{Z}^{+1}(D, N)$. The proof can be completed by the following equality:

$$\begin{aligned}|\mathrm{LPBP}(D, N, e_4)| =& \left(\gcd(e_4, d_1) - 1\right) \cdot \left(\gcd(e_4, d_2) - 1\right) + \gcd(e_4, d_1) \cdot \gcd(e_4, d_2) \\ =& (d_1 - 1)(d_2 - 1) + d_1 d_2 = \frac{(2d_1 - 1)(2d_2 - 1) + 1}{2} = |\mathcal{Z}^{+1}(D, N)|.\end{aligned}$$

Consider the case perfect square N. Proposition 1, and Proposition 2 imply that, for all $p_i \geq 7$,

$$\begin{aligned}\beta_{\mathrm{Lucas}}(D, N, e_4) &\leq \left(\frac{2}{\prod_{i=1}^{s} p_i^{r_i - 1}}\right)\left(\frac{\prod_{i=1}^{s} 2^{-k_i}(p_i - 1)}{\prod_{i=1}^{s}(p_i - 2)}\right) \\ &\leq \left(\frac{2}{\prod_{i=1}^{s} p_i^{r_i - 1}}\right)\left(\prod_{i=1}^{s}\left(\frac{1}{2} + \frac{1}{2(p_i - 2)}\right)\right) \leq \left(\frac{2}{7}\right)\left(\frac{1}{2} + \frac{1}{10}\right) = \frac{6}{35}.\end{aligned}$$

Note that

$$\prod_{i\in S_0}\left(p_i-\left[\frac{D}{p_i}\right]-1\right)\left(\prod_{i\in S_1}\left(p_i-\left[\frac{D}{p_i}\right]-1\right)+(-1)^{|S_1|}\right)\geq\prod_{i\in S_0}(p_i-2)\left(\prod_{i\in S_1}(p_i-2)-1\right).$$

Similarly for the case non-square-free (i.e. there exists an i such that $r_i\geq 2$) and non-perfect-square N (i.e. $|S_1|\geq 1$), Proposition 1, and Proposition 2 say that, for all $p_i\geq 11$,

$$\begin{aligned}\beta_{\text{Lucas}}(D,N,e_4)&\leq\left(\frac{4}{\prod_{i=1}^{s}p_i^{r_i-1}}\right)\left(\frac{\prod_{i=1}^{s}2^{-k_i}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)-\prod_{i\in S_0}(p_i-2)}\right)\\&\leq\left(\frac{4}{\prod_{i=1}^{s}p_i^{r_i-1}}\right)\left(\frac{\prod_{i=1}^{s}\left(\frac{1}{2}+\frac{1}{2(p_i-2)}\right)}{1-\left(\prod_{i\in S_1}(p_i-2)\right)^{-1}}\right)\leq\left(\frac{4}{11}\right)\left(\frac{\frac{1}{2}+\frac{1}{18}}{1-9^{-1}}\right)=\frac{5}{22}.\end{aligned}$$

When N is square-free. Consider the case $s=3$. Then there exists one of $\{p_1,p_2,p_3\}$ is $4\mid p_i-\left[\frac{D}{p_i}\right]$. If not, for all $1\leq i\leq 3$, $p_i-\left[\frac{D}{p_i}\right]=2d_i$ with odd d_i hold, which is equivalent to $p_i\equiv-\left[\frac{D}{p_i}\right]\pmod 4$. Since $s=3$, we can assume without loss of generality that $p=p_1$ and $q=p_2p_3$. For such q and the assumption $\left[\frac{-D}{q}\right]=-1$, we have

$$q\equiv\left[\frac{D}{p_2p_3}\right]\equiv\left[\frac{D}{q}\right]=-\left[\frac{-1}{q}\right]\pmod 4=\begin{cases}1,\ \text{if } q\equiv 3\pmod 4;\\3,\ \text{if } q\equiv 1\pmod 4.\end{cases}$$

It gives a contradiction. Therefore, applying Lemma 8, we obtain that

$$\beta_{\text{Lucas}}(D,N,e_4)<\frac{1}{4}\left(\frac{\prod_{i=1}^{3}(p_i-1)}{\prod_{i=1}^{3}(p_i-2)-1}\right)<\frac{1}{4}\left(\frac{(p_{\min}-1)^3}{(p_{\min}-2)^3-1}\right).$$

Similarly, as $s=4$, we have

$$\beta_{\text{Lucas}}(D,N,e_4)<\frac{1}{4}\left(\frac{(p_{\min}-1)^4}{(p_{\min}-2)^4-1}\right).$$

When $s\geq 5$, applying the following fact

$$\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)-1}<\left(\frac{\prod_{i=1}^{4}(p_i-1)}{\prod_{i=1}^{4}(p_i-2)-1}\right)\left(\frac{\prod_{i=5}^{s}(p_i-1)}{\prod_{i=5}^{s}(p_i-2)-1}\right),$$

and Lemma 9 with $j=5$, we arrive that, for $s\geq 5$,

$$\beta_{\text{Lucas}}(D,N,e_4)\leq 2^{2-k_1-\ldots-k_s}\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)-1}<\frac{1}{4}\left(\frac{(p_{\min}-1)^4}{(p_{\min}-2)^4-1}\right).$$

Lastly, we have

$$\begin{aligned}&\frac{1}{4}\left(\frac{(p_{\min}-1)^4}{(p_{\min}-2)^4-1}\right)=\frac{1}{4}+\frac{1}{4}\left(\frac{(p_{\min}-1)^4-(p_{\min}-2)^4+1}{(p_{\min}-2)^4-1}\right)\\=&\frac{1}{4}+\frac{1}{4}\left(\frac{4}{(p_{\min}-2)-1}+\frac{2}{(p_{\min}-2)^2+1}\right)<\frac{1}{4}+\frac{1.25}{p_{\min}-3}.\end{aligned}$$

The condition $\left[\frac{-D}{p}\right] = -1$ cannot be satisfied when p is a square integer. However, the probability of selecting square integers is quite low, and in such cases, $N = pq$ would not be RSA moduli.

4.2 The Proposed Protocol

We propose a protocol based on Theorem 2 and provide its security proof under the semi-honest adversary model. First, we consider the following functionality and then propose its realization $\pi_{\text{Lucas}}(n, \kappa)$.

Functionality 1 $\mathcal{F}_{\text{Biprime}}(n)$

Inputs: Each party $\mathcal{P}_i$ has a public number $N = pq$, $p \pmod 4, q \pmod 4$, shares $[p]_{\mathbb{Z}}$ and $[q]_{\mathbb{Z}}$, where each share satisfies $\mathfrak{p}_1 \equiv p \pmod 4$, $\mathfrak{q}_1 \equiv q \pmod 4$, and $\mathfrak{p}_i \equiv \mathfrak{q}_i \equiv 0 \pmod 4$ for all $2 \leq i \leq n$.

Outputs:
If $p \equiv q \equiv 3 \pmod 4$:

- If $p \neq q$ are both primes and $\gcd(N, e_4) = 1$, then each party receives $(1, \phi)$.
- Otherwise, each party receives $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.

Else:

- If $p \neq q$ are both primes and $\gcd(N, e_4) = 1$, then each party receives $\left(1, \left\{ \left[\frac{D_k}{p}\right] \right\}_{D_k \in S_{\min}}\right)$, where

$$S_{\min} := \left\{ D_k \in \mathbf{P}([3, D_{\min}]) \middle| \left[\frac{-D_k}{N}\right] = 1 \right\},$$

  and $D_{\min}$ is the minimal odd prime such that $\left[\frac{-D_{\min}}{p}\right] = -1$ and $\left[\frac{-D_{\min}}{N}\right] = 1$.
- Otherwise, each party receives $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.

In order to design a protocol to securely compute $\mathcal{F}_{\text{Biprime}}$, we need functionality $\mathcal{F}_{\text{Leg}}$ to compute the quadratic symbol $\left[\frac{-D}{p}\right]$.

Functionality 2 $\mathcal{F}_{\text{Leg}}(n)$

Inputs: Each party $\mathcal{P}_i$ has a share $[p]_{\mathbb{Z}}$, $p \pmod 4$, and a prime D with $\gcd(D, p) = 1$.

Outputs: Each party $\mathcal{P}_i$ receives the value $\left[\frac{-D}{p}\right]$.

Lucas biptimality test π_{Lucas} protocol consists of two parts: verifying that $\gcd(e_4, N) = 1$, and performing the exponential test from Theorem 2. The probability of N being an RSA modulus increases with the number of successful exponential tests.

Protocol 1 Lucas Biprimality Test $\pi_{\text{Lucas}}(n, \kappa)$

Inputs: Each party $\mathcal{P}_i$ has $p \pmod 4$, $q \pmod 4$, N and $[p]_{\mathbb{Z}}, [q]_{\mathbb{Z}}$, where each share satisfies $\mathfrak{p}_1 \equiv p \pmod 4$, $\mathfrak{q}_1 \equiv q \pmod 4$, and $\mathfrak{p}_i \equiv \mathfrak{q}_i \equiv 0 \pmod 4$ for all $2 \leq i \leq n$.

Outputs: $\left(1, \left\{\left[\frac{D_k}{p}\right]\right\}_{D_k \in S_{\min}}\right)$ or $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.

Select an appropriate positive integer D:

1. If $p \equiv q \equiv 3 \pmod 4$, parties set $D = 1$, $S_{\min} := \phi$, and go to the step 5.
2. Else, parties find the minimal k such that $\left[\frac{-D_k}{N}\right] = 1$, where $D_1 = 3, D_2 = 5, D_3 = 7, \ldots$ is the odd prime number sequence.
3. The party $\mathcal{P}_i$ sends $([p]_{\mathbb{Z}}, p \pmod 4, D_k)$ to $\mathcal{F}_{\text{Leg}}$ to obtain $\left[\frac{D_k}{p}\right]$ and adds D_k to $S_{\min}$.
4. If $\left[\frac{-D_k}{p}\right] = -1$ then parties set $D = D_k$. Else parties find next k such that $\left[\frac{-D_k}{N}\right] = 1$ and restart from step 3.

Exponential verification: For $1 \leq j \leq \kappa$:

5. Parties agree on a random $P_j \in \mathbb{Z}_N$ and let $Q_j := (P_j^2 - D)/4$. If $\gcd(N, Q_j) \neq 1$, then broadcast $\mathfrak{p}_i, \mathfrak{q}_i$ and output $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.
6. If $\left[\frac{Q_j}{N}\right] \neq 1$, then restart from the previous step.
7. The party $\mathcal{P}_1$ sets $y_{1,j} := (\alpha_j \beta_j^{-1})^{(N + \mathfrak{p}_1\left[\frac{-1}{q}\right] + \mathfrak{q}_1\left[\frac{-1}{p}\right] + \left[\frac{-1}{N}\right])/4} \in \mathbb{Z}_N^\times$ and the other parties set $y_{i,j} := (\alpha_j \beta_j^{-1})^{(\mathfrak{p}_i\left[\frac{-1}{q}\right] + \mathfrak{q}_i\left[\frac{-1}{p}\right])/4} \in \mathbb{Z}_N^\times$ for all $2 \leq i \leq n$, where α_j and β_j are two roots of the polynomial $x^2 - P_j x + Q_j$. Party $\mathcal{P}_i$ sends $y_{i,j}$ to $\mathcal{F}_{\text{Shuffle}}$ and then obtain u_j.
8. All parties check $u_j \equiv \pm 1 \pmod{N\mathcal{O}_D}$. If the check fails then they broadcast $\mathfrak{p}_i, \mathfrak{q}_i$ and return $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.

GCD Test

9. Each party randomly generates shares $[r]_N$. They send $([r]_N, (p[\frac{-1}{q}] + q[\frac{-1}{p}] + [\frac{-1}{N}]))$ to $\mathcal{F}_{\text{ModMul}}$ to obtain $[z]_N$.
10. Each party broadcasts his share $\mathfrak{z}_i$ of $[z]_N$, then they check if $\gcd(N, z) = 1$. If the check fails they broadcast $\mathfrak{p}_i, \mathfrak{q}_i$ and return $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$.

If all verification pass, then output $\left(1, \left\{\left[\frac{D_k}{p}\right]\right\}_{D_k \in S_{\min}}\right)$.

A security proof of π_{Lucas} under the semi-honest adversary model is provided below.

Theorem 3. *Let p and q be odd integers, $N = pq$, and D be an integer with $\left[\frac{-D}{p}\right] = \left[\frac{-D}{q}\right] = -1$, and $\gcd(D, N) = 1$. The inputs to $\mathcal{P}_i$ are given as*

$$(N, [p]_{\mathbb{Z}}, [q]_{\mathbb{Z}}),$$

where each share satisfies $\mathfrak{p}_1 \equiv p \pmod 4$, $\mathfrak{q}_1 \equiv q \pmod 4$, and $\mathfrak{p}_i \equiv \mathfrak{q}_i \equiv 0 \pmod 4$ for all $2 \leq i \leq n$. If $p_{min} \geq 11$, then the Protocol π_{Lucas} securely computes the functionality $\mathcal{F}_{\text{Biprime}}$ in the $\mathcal{F}_{\text{Shuffle}}$, $\mathcal{F}_{\text{ModMul}}$-hybrid model and in the presence of a static semi-honest adversary corrupting up to $n-1$ parties.

Proof. **Correctness**. Assuming $p > q$ are both primes(i.e. the case $p < q$ is similar) with $\gcd(N, e_4) = 1$, we show that such p and q do not output $(0, \{p_i, q_i\}_{i=1}^n)$ with overwhelming probability. Note that for any $1 \leq j \leq \kappa$,

$$\begin{aligned}
&\mathbb{P}[\gcd(Q_j, N) = 1] \\
=&\mathbb{P}[(P_j^2 - D)/4 \in \mathbb{Z}_N^\times] \geq 1 - \frac{N - \phi(N)}{\phi(N)/4} \geq 1 - \frac{4(p+q-1)}{\phi(N)} \geq 1 - 4\frac{2p-1}{q^2-1} \\
\geq& 1 - \frac{16p}{q^2} \geq 1 - 2^{-\log_2 q + |\log_2 p - \log_2 q| + 4}, \qquad (5)
\end{aligned}$$

which implies that such p, q will pass all tests in step 5 with overwhelming probability(cf. Remark 1). For the check of step 8, by Theorem 2, we have $u_j = (\alpha\beta^{-1})^{e_4} \equiv \pm 1 \pmod{N\mathcal{O}_D}$ for all $1 \leq j \leq \kappa$. Using the similar argument as in (5), we may assume $r \in \mathbb{Z}_N^\times$ which implies

$$\gcd(N, z) = \gcd(N, e_4) = 1.$$

The output of π_{Lucas} is $\left(1, \left\{\left[\frac{D_i}{p}\right]\right\}_{D_i \in S_{\min}}\right)$. In the case where $\gcd(N, e_4) \neq 1$, we have $\gcd(N, z) > 1$, and both π_{Lucas} and $\mathcal{F}_{\text{Biprime}}$ output $(0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n)$. When p and q are not distinct primes but $\gcd(N, e_4) = 1$, the probability of exponential test pass is not greater than $\frac{1}{4} + \frac{1.25}{p_{\min} - 3}$, according to Theorem 2. Hence the probability of π_{Lucas} outputting $\left(1, \left\{\left[\frac{D_i}{p}\right]\right\}_{D_i \in S_{\min}}\right)$ is bounded by $(\frac{1}{4} + \frac{1.25}{p_{\min} - 3})^\kappa$.

Privacy. Let $\mathcal{P}^*$ be the set of corrupt parties. We show that a simulator $\mathcal{S}$ can be constructed to simulate the transcript of π_{Lucas}. If the input of $\mathcal{S}$ is

$$(\mathcal{P}^*, N, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i \in \mathcal{P}^*}, 0, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i=1}^n),$$

then $\mathcal{S}$ only needs to follow the honest parties' strategy to simulate the view of the protocol. Therefore, we consider the case $\mathcal{S}$ is given the input

$$\left(\mathcal{P}^*, N, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i\in\mathcal{P}^*}, 1, \left\{ \left[\frac{D_i}{p}\right] \right\}_{D_i\in S_{\min}}\right).$$

1: For all $1 \le j \le \kappa$, $\mathcal{S}$ randomly samples $v_j, w_j \in \mathbb{Z}_N$ with $\gcd(v_j^2 - w_j^2 D, N) = 1$, $b_j \in \{0,1\}$, and sets $a_j = \frac{v_j + w_j\sqrt{D}}{v_j - w_j\sqrt{D}}$, $P'_j \in \mathbb{Z}_N$ such that the two roots of polynomial $x^2 - P'_j x + Q'_j$ are $\beta'_j := \frac{\sqrt{D}}{a_j^2 \cdot (-1)^{b_j} - 1}$ and $\alpha'_j := \beta'_j + \sqrt{D}$.
2: The simulator $\mathcal{S}$ randomly generates $z' \in \mathbb{Z}_N^\times$, and it's additive shares $[z']_N$.
3: The adversary $\mathcal{S}$ outputs

$$\left(\mathcal{P}^*,\ N, \{\mathfrak{p}_i, \mathfrak{q}_i\}_{i\in\mathcal{P}^*}, \{P'_j, (-1)^{b_j}\}_{i=1}^{\kappa}, [z']_N, \{z'_i\}_{i=1}^{n}\right).$$

First, we argue that $P'_j \in \mathbb{Z}_N$ with overwhelming probability. Note that

$$\begin{aligned} P'_j =& \alpha'_j + \beta'_j \\ =& \frac{2\sqrt{D}(v_j - w_j\sqrt{D})^2}{(v_j + w_j\sqrt{D})^2 \cdot (-1)^{b_j} - (v_j - w_j\sqrt{D})^2} + \sqrt{D} \\ =& \left(\frac{v_j^2 + w_j^2 D}{2 v_j w_j}\right)^{1-2b_j} D^{b_j} \in \mathbb{Z}_N. \end{aligned}$$

Secondly, we show that the distribution of $(P'_j, (-1)^{b_j})$ generated by the simulator is indistinguishable from the distribution of the real-world transcript $(P_j, u_j) = (P_j, (\alpha_j \beta_j^{-1})^{e_4})$. Note that $(\alpha'_j \beta_j'^{-1})^{e_4} = ((\beta'_j + \sqrt{D})\beta_j'^{-1})^{e_4} = (a_j^2 (-1)^{b_j})^{e_4}$. Due to the symmetry between p and q, we only need to consider proving

$$(a_j^2)^{e_4} \equiv 1 \pmod{p\mathcal{O}_D}.$$

Since p, q are odd primes and e_4 is odd, we have

1. If $\left[\frac{D}{p}\right] = -1$, we have

$$\left(\frac{v_j + w_j\sqrt{D}}{v_j - w_j\sqrt{D}}\right)^{2e_4} \equiv \left(\mathbf{N}\left(\frac{v_j + w_j\sqrt{D}}{v_j - w_j\sqrt{D}}\right)\right)^{(q + [\frac{-1}{q}])/2} \equiv 1 \pmod{p\mathcal{O}_D}.$$

2. If $\left[\frac{D}{p}\right] = 1$ (i.e. $\sqrt{D} \in \mathbb{Z}_p^\times$), Euler theorem says that

$$\left(\frac{v_j + w_j\sqrt{D}}{v_j - w_j\sqrt{D}}\right)^{(p + [\frac{-1}{p}])(q + [\frac{-1}{q}])/2} \equiv 1 \pmod{p}.$$

Therefore, $(\alpha'_j \beta_j'^{-1})^{e_4} \equiv (-1)^{b_j} \pmod{N\mathcal{O}_D}$ by CRT. Note that the distribution of P'_j produced by the simulator $\mathcal{S}$ at the step 1. Proposition 5 says that the distributions of P_j and P'_j are identical. Lastly, $\gcd(N, e_4) = 1$ implies that

$(p[\frac{-1}{q}] + q[\frac{-1}{p}] + [\frac{-1}{N}]) \in \mathbb{Z}_N^\times$, and $z \equiv r(p[\frac{-1}{q}] + q[\frac{-1}{p}] + [\frac{-1}{N}]) \pmod N$ is uniformly distributed in $\mathbb{Z}_N$. The statistical distance between the distributions of z and z' is

$$\frac{1}{2}\left(\sum_{x\in\phi(N)}\left(\frac{1}{\phi(N)}-\frac{1}{N}\right)+\sum_{x\in N\setminus\phi(N)}\frac{1}{N}\right)=\frac{N-\phi(N)}{N},$$

which is negligible using a similar argument as in (5). We conclude that the joint distribution of the outputs generated by $\mathcal{S}$ and $\mathcal{F}_{\text{Biprime}}$, and of the view and output of an execution π_{Lucas} are indistinguishable.

Remark 1. In the practical scenario (e.g. [13]), distributed RSA moduli protocols generate $p=\sum_{i=1}^{n}\mathfrak{p}_i$ and $q=\sum_{i=1}^{n}\mathfrak{q}_i$, where $\mathfrak{p}_i$ and $\mathfrak{q}_i$ are uniformly sampled from $[0, 2^{\ell-\log_2 n}]$, with ℓ being the security parameter. This implies $\max\{p,q\}$ is at most ℓ-bits and

$$\mathbb{P}[\min\{p,q\} \text{ is larger than } (\ell-\log_2 n-80)\text{-bits }] \geq 1-2^{-80n}.$$

Therefore, $|\log_2 p-\log_2 q| \leq 80+\log_2 n$ (i.e. $2^{-\log_2 q+|\log_2 p-\log_2 q|+4}$ is negligible) with overwhelming probability.

For completeness, we provide π_{Leg} which is a protocol that securely realizes Functionality $\mathcal{F}_{\text{Leg}}$. A similar protocol for computing the Legendre symbol was proposed in [24] but was not proven in detail.

Protocol 2 Legendre symbol $\pi_{\text{Leg}}(n)$

Inputs: Each party $\mathcal{P}_i$ has $[p]_{\mathbb{Z}}$, $p \pmod 4$, and a prime D with $\gcd(D,p)=1$.

Outputs: $\left[\frac{-D}{p}\right]$.

1. Each party randomly sample $\mathfrak{s}_i \in \mathbb{Z}_D$ sends $(\mathfrak{s}_i, \mathfrak{s}_i, D)$ to $\mathcal{F}_{\text{ModMul}}$ to obtain $[s^2]_D$.
2. Each party sends $([s^2]_D, \mathfrak{p}_i \pmod D, D)$ to $\mathcal{F}_{\text{ModMul}}$ to obtain $[s^2p]_D$.
3. Each party opens $[s^2p]_D$. If $\gcd(s^2p, D) \neq 1$, then restarts to the step 1. Otherwise, output $\begin{cases} -\left[\frac{s^2p}{D}\right], & \text{if } p\equiv 3 \pmod 4 \text{ and } D\equiv 1 \pmod 4; \\ \left[\frac{s^2p}{D}\right], & \text{otherwise.} \end{cases}$

Proposition 3. *Protocol π_{Leg} securely computes the functionality $\mathcal{F}_{\text{Leg}}$ in $\mathcal{F}_{\text{ModMul}}$-hybrid model in the presence of a static semi-honest adversary corrupting up to $n-1$ parties.*

Proof. We construct the simulator $\mathcal{S}$ to simulate the transcript of π_{Leg}. Suppose $\mathcal{S}$ is given input

$$\left(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4, D, \left[\frac{-D}{p}\right]\right).$$

1: $\mathcal{S}$ uniformly samples $s \in \mathbb{Z}_D^\times$ and $\mathfrak{s}_i \in \mathbb{Z}_D$ for $i \in \{1, \ldots, n\}$ such that $\sum_{i=1}^n \mathfrak{s}_i \equiv s \pmod{D}$.
2: $\mathcal{S}$ uniformly samples $\mathfrak{s}'_i \in \mathbb{Z}_D$ for $i \in \{1, \ldots, n\}$ such that $\sum_{i=1}^n \mathfrak{s}'_i \equiv s^2 \pmod{D}$.
3: $\mathcal{S}$ uniformly samples $r \in \mathbb{Z}_D^\times$ such that

$$\left[\frac{r}{D}\right] = \begin{cases} -\left[\frac{-D}{p}\right], & \text{if } p \equiv 3 \pmod 4 \text{ and } D \equiv 1 \pmod 4; \\ \left[\frac{-D}{p}\right], & \text{otherwise.} \end{cases}$$

4: $\mathcal{S}$ uniformly samples $\mathfrak{r}_i \in \mathbb{Z}_D$ for $i \in \{1, \ldots, n\}$ such that $\sum_{i=1}^n \mathfrak{r}_i \equiv r \pmod{D}$.
5: $\mathcal{S}$ outputs

$$(\{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D, \{\mathfrak{s}_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{s}'_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{r}_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{r}_i\}_{i\in\{1,\ldots,n\}\setminus\mathcal{P}^*})$$

Because $\mathcal{F}_{\text{Leg}}$ is a deterministic function, we only need to prove

$$\left\{\mathcal{S}\Big(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D, \left[\frac{-D}{p}\right]\Big)\right\} \stackrel{c}{\equiv} \{\text{view}_{\mathcal{P}^*}^{\pi_{\text{Leg}}}(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D)\}$$

for any $\mathcal{P}^* \subseteq \{1, \ldots, n\}, |\mathcal{P}^*| \leq n-1, \{\mathfrak{p}_i\}_{i=1}^n$ and prime D. In the beginning, fixed any $\{\mathfrak{p}_i\}_{i=1}^n$ and D, we claim that the output of

$$\mathcal{S}\left(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D, \left[\frac{-D}{p}\right]\right)$$

and the view

$$\text{view}_{\mathcal{P}^*}^{\pi_{\text{Leg}}}(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D)$$

are identical. Observe that

$$\begin{aligned}\left[\frac{p}{D}\right] &= \left[\frac{D}{p}\right] \cdot (-1)^{\frac{p-1}{2}\frac{D-1}{2}} = \left[\frac{-D}{p}\right] \cdot \left[\frac{-1}{p}\right] \cdot (-1)^{\frac{p-1}{2}\frac{D-1}{2}} \\ &= \left[\frac{-D}{p}\right] \cdot (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{D-1}{2}}\end{aligned}$$

implies that $\left[\frac{p}{D}\right] = \left[\frac{r}{D}\right]$. The facts that D is a prime, and s is uniformly randomly chosen from $\mathbb{Z}_D^\times$, which gives us the identical distribution between $\{s^2 p \mid s \in \mathbb{Z}_D^\times\}$ with $\left\{r \in \mathbb{Z}_D^\times \mid \left[\frac{r}{D}\right] = (-1)^{\frac{(p-1)(D-3)}{4}} \left[\frac{-D}{p}\right]\right\}$. Due to $|\mathcal{P}^*| < n$, $\mathfrak{s}_i, \mathfrak{s}'_i$ in the $\text{view}_{\mathcal{P}^*}^{\pi_{\text{Leg}}}(\mathcal{P}^*, N, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D)$ and

$$\mathcal{S}\left(\mathcal{P}^*, N, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4), D, \left[\frac{-D}{p}\right]\right)$$

are both independently and uniformly distributed in $\mathbb{Z}_D$. We conclude that for any $\mathcal{P}^* \subseteq \{1,\ldots,n\}, |\mathcal{P}^*| \leq n-1, \{\mathfrak{p}_i\}_{i=1}^n$, and prime D

$$\begin{aligned}
&\left\{\mathcal{S}\left(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4, D, \left[\frac{-D}{p}\right]\right)\right\}\\
\equiv&(\{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4, D, \{\mathfrak{s}_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{s}'_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{r}_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{r}_i\}_{i\in\{1,\ldots,n\}\setminus\mathcal{P}^*})\\
\equiv&(\{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4, D, \{\mathfrak{s}_i\}_{i\in\mathcal{P}^*}, \{\mathfrak{s}'_i\}_{i\in\mathcal{P}^*}, \{s^2\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, \{s^2\mathfrak{p}_i\}_{i\in\{1,\ldots,n\}\setminus\mathcal{P}^*})\\
\equiv&\{\mathrm{view}_{\mathcal{P}^*}^{\pi_{\mathrm{Leg}}}(\mathcal{P}^*, \{\mathfrak{p}_i\}_{i\in\mathcal{P}^*}, p \pmod 4, D)\}.
\end{aligned}$$

5 Implementation, Benchmarks, and Evaluation

In this section, we first experimentally evaluate the effectiveness of the Boneh-Franklin, the Miller-Rabin test, and the proposed test. In subsection 5.2, we compare the widely used protocols based on the variant Miller-Rabin test by Burkhardt et al. [12, FIGURE 6.1], the Boneh-Franklin test [21], and the proposed protocol. In subsection 5.3, we implement both the Boneh-Franklin test and our protocol independently and present runtime data from executions performed on a laptop.

5.1 Comparing the effectives of Three Tests

We begin by recalling the variant Miller-Rabin test [12] and determine which of the three tests, Boneh-Franklin, the variant Miller-Rabin test or our proposed Lucas test, is more effective at identifying when N is not an RSA modulus. Consider $N = pq$ with $p \equiv q \equiv 3 \pmod 4$ and $f \in \{p, q\}$. The algorithm of the variant Miller-Rabin test is as follows:

1. Uniformly sample an element $v \in \mathbb{Z}_N^\times$ [7] (i.e. in [12], v is chosen in $\mathbb{Z}_N$).
2. Compute $\gamma = v^{\frac{f-1}{2}} \pmod N$.
3. If $\gamma \equiv \pm 1 \pmod f$, then output **probably prime**. Otherwise output **composite**.

The biprimality test proposed in [12, 17] applies the variant Miller-Rabin test separately to $f \in \{p, q\}$. Therefore, for any $N = pq$ with $p \equiv q \equiv 3 \pmod 4$ and $\gcd(N, e_4) = 1$ the probability that N passes the process is (cf. Lemma 5)

$$\beta_{\mathrm{MR}}(p) := \frac{|\mathrm{MR}(p)|}{\phi(p)} = 2\left(\prod_{p_i|p} \frac{\gcd(d_i, \frac{p-1}{2})}{p_i^{r_i-1}(p_i-1)}\right).$$

In particular, when $p = q$ is prime, such an RSA modulus candidate p, q will always pass this algorithm's test with 100% certainty. Therefore, we recommend

[7] We narrow the selection range of v from $\mathbb{Z}_N$ to $\mathbb{Z}_N^\times$ because an element $v \in \mathbb{Z}_N \setminus \mathbb{Z}_N^\times$ will let the test output composite even when f is prime.

Table 2: Pairwise comparison charts among the three tests.

Method	$\beta = \frac{\beta_{\mathrm{BF}}(N,e_4)}{\beta_{\mathrm{MR}}(p)\beta_{\mathrm{MR}}(q)}$	$\beta = \frac{\beta_{\mathrm{BF}}(N,e_4)}{\beta_{\mathrm{Lucas}}(N,e_4)}$	$\beta = \frac{\beta_{\mathrm{Lucas}}(N,e_4)}{\beta_{\mathrm{MR}}(p)\beta_{\mathrm{MR}}(q)}$
$\beta < 1$	0.08%	$< 0.01\%$	54.26%
$\beta = 1$	54.18%	0%	0%
$\beta > 1$	45.74%	$> 99.99\%$	45.74%

Count how many non-RSA moduli $N = pq$ with $p \equiv q \equiv 3 \pmod 4$, $\gcd(N, e_4) = 1$, and $\gcd(pq, p') = 1$ for all primes $p' \leq 541$ satisfy $\beta > 1$, $\beta = 1$ or $\beta < 1$, which run over all $3 \leq p < q \leq 1440003$.

incorporating a check to verify whether N is a perfect square to exclude this case. Notably, the papers [12,17] do not include this check.

We simplify the formula comparing any two of these tests and analyze the resulting ratios under three different scenarios. Let $\mathbf{1}_{\mathbb{P}}(\cdot)$ be the indicator function of positive integers (i.e. $\mathbf{1}_{\mathbb{P}}(0) = 0$).

– **Variant Miller-Rabin VS Boneh-Franklin Test:**

$$\frac{\beta_{\mathrm{BF}}(N,e_4)}{\beta_{\mathrm{MR}}(p)\beta_{\mathrm{MR}}(q)} = \left(\frac{1}{\mathbf{1}_{\mathbb{P}}(\sqrt{N})+1}\right)\left(\prod_{\substack{p_i|p\\ p_i\nmid q}}\frac{\gcd(e_4,d_i)}{\gcd(d_i,\frac{p-1}{2})}\right)\left(\prod_{\substack{p_i|q\\ p_i\nmid p}}\frac{\gcd(e_4,d_i)}{\gcd(d_i,\frac{q-1}{2})}\right)$$
$$\cdot\left(\prod_{p_i|\gcd(p,q)}\frac{(p_i-1)\gcd(e_4,d_i)}{p_i\gcd(d_i,\frac{p-1}{2})\gcd\left(d_i,\frac{q-1}{2}\right)}\right).$$

– **Lucas Test VS Boneh-Franklin Test**

$$\frac{\beta_{\mathrm{Lucas}}(N,e_4)}{\beta_{\mathrm{BF}}(N,e_4)} = \left[\frac{\prod_{i=1}^{s}(\gcd(e_4,d_i)-1)+\prod_{i=1}^{s}\gcd(e_4,d_i)}{2\prod_{i=1}^{s}\gcd(e_4,d_i)}\right]$$
$$\cdot\left[\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i\in S_0}(p_i-2)\left(\prod_{i\in S_1}(p_i-2)+\mathbf{1}_{\mathbb{P}}(|S_1|)(-1)^{|S_1|}\right)}\right].$$

– **Lucas Test VS Variant Miller-Rabin Test**

$$\frac{\beta_{\mathrm{Lucas}}(N,e_4)}{\beta_{\mathrm{MR}}(p)\beta_{\mathrm{MR}}(q)} = \left[\frac{\prod_{i=1}^{s}(\gcd(e_4,d_i)-1)+\prod_{i=1}^{s}\gcd(e_4,d_i)}{2\prod_{p_i|p}\gcd(\frac{p-1}{2},d_i)\prod_{p_i|q}\gcd(\frac{q-1}{2},d_i)}\right]$$
$$\cdot\left[\frac{\left(\prod_{i=1}^{s}(p_i-1)\right)\left(\prod_{p_i|\gcd(p,q)}(1-p_i^{-1})\right)}{\prod_{i\in S_0}(p_i-2)\left(\prod_{i\in S_1}(p_i-2)+\mathbf{1}_{\mathbb{P}}(|S_1|)(-1)^{|S_1|}\right)}\right].$$

Table 2 demonstrates that, among the three tests, the ability to identify non-RSA moduli shows a slight advantage for the Lucas test over the variant Miller-Rabin test, and a significant advantage for the Lucas test over the Boneh-Franklin test.

Table 3: Computation Procedures for Three Tests

Method	Boneh-Franklin	Variant Miller-Rabin	Proposed test
Basis selection (local)	$g \leftarrow \mathbb{Z}_N, \left[\frac{g}{N}\right] = 1$	$v \leftarrow \mathbb{Z}_N$	$P \leftarrow \mathbb{Z}_N, \left[\frac{P^2-1}{N}\right] = 1$
Exponential calculation (local)	$\mathcal{P}_1 : g^{(N-(\mathfrak{p}_i+\mathfrak{q}_i)+1)/4}$ $\mathcal{P}_i : g^{(-\mathfrak{p}_i-\mathfrak{q}_i)/4}$	$\mathcal{P}_1 : v^{(\mathfrak{f}_i-1)/2}$ $\mathcal{P}_i : v^{\mathfrak{f}_i/2}$	$\mathcal{P}_1 : (\alpha\beta^{-1})^{(N-(\mathfrak{p}_i+\mathfrak{q}_i)+1)/4}$ $\mathcal{P}_i : (\alpha\beta^{-1})^{(-\mathfrak{p}_i-\mathfrak{q}_i)/4}$
Other computations (MPC)	$g^{e_4} \leftarrow$Shuffle $[r] \leftarrow$RandomSample $[r \cdot (p+q-1)] \leftarrow$Mult	Mul-to-Add $\left[v^{(f-1)/2}\right] \leftarrow$ Divisible $[y_{+1}], [y_{-1}] \leftarrow$ $[y_{+1} \cdot y_{-1}] \leftarrow$Mult	$(\alpha\beta^{-1})^{e_4} \leftarrow$ Shuffle $[r] \leftarrow$RandomSample $[r \cdot (p+q-1)] \leftarrow$Mult

All computations of the Variant Miller-Rabin test need to be executed twice, for $f \in \{p, q\}$. **Basis selection** refers to the conditions of the basis for exponential calculations. We consider the semi-honest model; hence, the basis is determined by $\mathcal{P}_1$. In **Exponential calculation**, $\mathcal{P}_i$ represents $\mathcal{P}_2, \ldots \mathcal{P}_n$, and α, β are the two roots of the polynomial $x^2 + Px + (P^2-1)/4$. In **Other computations**, the Shuffle protocol outputs the product of shares. Mul-to-Add refers to the conversion of multiplicative shares to additive shares. RandomSample outputs a random element from a specified set. The output of Divisible $y_{\pm 1}$ indicates whether $v^{(f\pm 1)/2} \equiv 0 \pmod f$. Mult denotes the MPC multiplication between additive shares.

5.2 Comparison of Computational Cost for Three Tests

Burkhardt et al. [12] demonstrated that their protocol exhibits superior efficiency compared to the Boneh-Franklin test presented by Frederiksen et al. [21] at the same security level. In their comparisons between the Boneh-Franklin and Miller-Rabin tests, the Boneh-Franklin test required more iterations to achieve equivalent soundness due to its original acceptance rate of $1/2$ in the worst case. To evaluate the effectiveness of the three protocols, including the Lucas test, we adopt the terminology introduced in Burkhardt et al.'s paper (cf. Subsection 6.5) and summarize it in Table 3. It is evident that in terms of overall computational efficiency, the Boneh-Franklin test is the most optimal. However, the Lucas test type is not far behind, with the difference mainly arising from local computations. Given the current computational power, the gap between the two is nearly negligible.

5.3 Implementation

Our experiment is mainly composed of three parts (cf. Section 6.5):

1. **Generate an RSA modulus candidate**: Utilizing the CRT-Sampling protocol [13, Protocol 4.4] generates N, $\mathfrak{p}_i$, $\mathfrak{q}_i$, and $\{\mathfrak{p}_i \pmod 4, \mathfrak{q}_i \pmod 4\}_{i=1}^n$ satisfying $p = \sum_i \mathfrak{p}_i \equiv 3 \pmod 4$ and $q = \sum_i \mathfrak{q}_i \equiv 3 \pmod 4$. Meanwhile, set a parameter B to check that no prime smaller than B dividing $N = pq$. In our case, $B = 62017$. For $N = 2048$ (resp. 3072) bits, passing this check implies approximately a 0.0767% (resp. 0.0341%) probability that both p

and q are prime. This is based on DeBruijn's formula [10]: for a k bit integer p,

$$\Pr(p \in \mathbf{P} | \text{ trial division up to } B) \sim 2.57 \cdot \ln B \cdot k^{-1}.$$

Like most experiments, our MPC multiplication with secret-sharing is proposed by Gennaro et al. [23, Figure 2], assuming an honest majority.

2. **A biprimality test**: We continue checking the exponential conditions required by both biprimality tests until the soundness error is reduced to 2^{-80}.
3. **Verify** $\gcd\big(pq, (p + \left[\frac{-1}{p}\right])(q + \left[\frac{-1}{p}\right])\big) = 1$: Sample an $r \in \mathbb{Z}_N^\times$, calculate $z = r\big(p\left[\frac{-1}{q}\right] + q\left[\frac{-1}{p}\right] + \left[\frac{-1}{N}\right]\big)$, and check $\gcd(pq, z) = 1$. If the check failure, then return to step 1.

The scheme is implemented by the Golang programming language and its provided "math/big" library. In order to achieve a probability of accepting a non-RSA modulus at least 2^{-80}, we set 40 iteration for the two biprimality tests. The experiments were conducted with N set to 2048 bits and 3072 bits, and involved $2, 3$, to 4 parties. All programs were executed in a single-threaded manner on an Apple M2 with 16GB LPDDR5 RAM in the 13-inch (2022) MacBook Pro. The running times are presented in Table 4.

Table 4: The mean ± standard deviation of execution time (in seconds) for our methods and the competing method.

		Proposed test	Boheh-Franklin
$N = 2048$	$n = 2$	18.84 ± 18.50	20.47 ± 19.64
	$n = 3$	33.01 ± 35.36	43.46 ± 42.68
	$n = 4$	59.67 ± 60.12	64.16 ± 61.07
$N = 3072$	$n = 2$	117.59 ± 119.24	109.66 ± 119.97
	$n = 3$	174.59 ± 200.88	169.81 ± 161.44
	$n = 4$	232.81 ± 249.38	274.67 ± 273.64

In our experiments, both the Lucas test and the Boneh-Franklin test demonstrated distinct advantages in average execution time. We observed that when N is not an RSA modulus, both tests effectively identified this in a single run. Thus, performance variations are likely due to the probability of generating an RSA modulus during the selection of p and q, rather than significant differences between the tests themselves.

Regarding computational complexity within the MPC protocol (cf. Subsection 5.2), the Lucas test and Boneh-Franklin test are comparable, both outperforming the variant Miller-Rabin test. Importantly, the most efficient Prime Candidate Sampling methods [13, 37] cannot be directly applied to Burkhardt et al.'s approach, as they cannot guarantee equal length for p and q. Specifically, Chen et al. [13] restrict $\mathfrak{p}_i$ and $\mathfrak{q}_i$ to the interval $[0, 2^{\ell - \log_2 n}]$, while Guilhem et

al. [37] use $[2^{\ell-1}, 2^{\ell-1+80}]$, where ℓ is the security parameter related to the bit lengths of p and q. Thus, in generating p and q, the variant Miller-Rabin test incurs additional time overhead compared to the Boneh-Franklin test and Lucas test.

At the same time, exhaustive experiments Table 2 indicate that, "on average," the Lucas test achieves the best average soundness error. In other words, if the Miller-Rabin test requires only two iterations to reach a certain error rate, then our proposed test should require no more than two iterations.

In conclusion, assuming the local computation overhead difference between the Boneh-Franklin test and the Lucas test is negligible, the proposed Lucas test is highly competitive.

References

1. Abadi, A., Ristea, D., Murdoch, S.J.: Delegated time-lock puzzle. arXiv preprint arXiv:2308.01280 (2023) 1
2. Algesheimer, J., Camenisch, J., Shoup, V.: Efficient computation modulo a shared secret with application to the generation of shared safe - prime products. In: Yung, M. (ed.) Advances in Cryptology — CRYPTO 2002. pp. 417 – 432. Springer Berlin Heidelberg, Berlin, Heidelberg (2002) 1.3
3. Arnault, F.: The rabin-monier theorem for lucas pseudoprimes. Math. Comput. **66**, 869–881 (04 1997). https://doi.org/10.1090/S0025-5718-97-00836-3 1, 2.2, 4.1, 6.2
4. Benaloh, J., de Mare, M., Accumulators, O.W.: A decentralized alternative to digital signatures. In: Advances in Cryptology-Proceedings of Eurocrypt. vol. 93 (1994) 1
5. Benaloh, J.: Secret sharing homomorphisms: keeping shares of a secret secret. In: Proceedings on Advances in cryptology—CRYPTO '86. vol. LNCS 263, pp. 251–260 (01 1987) 6.4
6. Boneh, D., Bonneau, J., Bünz, B., Fisch, B.: Verifiable delay functions. In: Annual international cryptology conference. pp. 757–788. Springer (2018) 1
7. Boneh, D., Bünz, B., Fisch, B.: Batching techniques for accumulators with applications to iops and stateless blockchains. In: Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I 39. pp. 561–586. Springer (2019) 1
8. Boneh, D., Franklin, M.: Efficient generation of shared rsa keys. Journal of the ACM **48** (12 2001). https://doi.org/10.1145/502090.502094 1, 1.3, 6.5, 6.5
9. Boudabra, M., Nitaj, A.: A new rsa variant based on elliptic curves. Cryptography (2023). https://doi.org/10.3390/cryptography7030037 1.1
10. Bruijn, de, N.: On the number of uncancelled elements in the sieve of eratosthenes. Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A: Mathematical Sciences **53**(5-6), 803–812 (1950) 5.3
11. Buhler, J., Stevenhagen, P.: Algorithmic number theory. Lattices, number fields, curves and cryptography. Reprint of the 2008 hardback ed. Cambridge University Press (01 2011) 1
12. Burkhardt, J., Damgård, I., Frederiksen, T., Ghosh, S., Orlandi, C.: Improved distributed rsa key generation using the miller-rabin test. CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security

pp. 2501–2515 (2023). https://doi.org/10.1145/3576915.3623163 1, 1.3, 5, 5.1, 5.2, 6.5, 6.5, 6.5, 5
13. Chen, M., Doerner, J., Kondi, Y., Lee, E., Rosefield, S., Shelat, A., Cohen, R.: Multiparty generation of an rsa modulus. Journal of Cryptology **35** (04 2022). https://doi.org/10.1007/s00145-021-09395-y 1, 1, 5.3, 5.3
14. Chen, M., Hazay, C., Ishai, Y., Kashnikov, Y., Micciancio, D., Riviere, T., Shelat, A., Venkitasubramaniam, M., Wang, R.: Diogenes: Lightweight scalable rsa modulus generation with a dishonest majority. In: 2021 IEEE Symposium on Security and Privacy (SP). pp. 590–607. IEEE (2021) 1
15. Chvojka, P.: Private coin verifiable delay function. Cryptology ePrint Archive (2023) 1
16. Damgård, I., Landrock, P., Pomerance, C.: Average case error estimates for the strong probable prime test. Mathematics of Computation - Math. Comput. **61**, 177–177 (09 1993). https://doi.org/10.2307/2152945 1, 1.1, 1.3
17. Damgård, I., Mikkelsen, G.: Efficient, robust and constant-round distributed rsa key generation. In: Theory of Cryptography. pp. 183–200. Springer Berlin Heidelberg (02 2010). https://doi.org/10.1007/978-3-642-11799-2_12 1, 1.3, 5.1
18. Demytko, N.: A new elliptic curve based analogue of rsa. In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 40–49. Springer (1993). https://doi.org/10.1007/3-540-48285-7_4 1.1
19. Einsele, S., Paterson, K.: Average case error estimates of the strong lucas test. Designs, Codes and Cryptography pp. 1–38 (01 2024). https://doi.org/10.1007/s10623-023-01347-w 1.3
20. Ephraim, N., Freitag, C., Komargodski, I., Pass, R.: Continuous verifiable delay functions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 125–154. Springer (2020) 1
21. Frederiksen, T., Lindell, Y., Osheter, V., Pinkas, B.: Fast Distributed RSA Key Generation for Semi-honest and Malicious Adversaries: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part II, pp. 331–361. Springer International Publishing (07 2018). https://doi.org/10.1007/978-3-319-96881-0_12 1, 5, 5.2, 5
22. Friedman, O., Marmor, A., Mutzari, D., Scaly, Y.C., Spiizer, Y., Yanai, A.: Tiresias: Large scale, maliciously secure threshold paillier. Cryptology ePrint Archive (2023) 1
23. Gennaro, R., Rabin, M.: Simplified vss and fast-track multiparty computations with applications to threshold cryptography. Proc. of 17th PODC (06 1998). https://doi.org/10.1145/277697.277716 5.3
24. Grassi, L., Rechberger, C., Rotaru, D., Scholl, P., Smart, N.: Mpc-friendly symmetric key primitives. In: CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 430–443 (10 2016). https://doi.org/10.1145/2976749.2978332 1.2, 4.2
25. Hazay, C., Mikkelsen, G.L., Rabin, T., Toft, T., Nicolosi, A.A.: Efficient rsa key generation and threshold paillier in the two-party setting. Journal of Cryptology **32**, 265–323 (2019) 1
26. Hoffmann, C., Hubáček, P., Kamath, C., Krňák, T.: (verifiable) delay functions from lucas sequences. Cryptology ePrint Archive (2023) 1
27. Ireland, K., Rosen, M.I.: A classical introduction to modern number theory, vol. 84. Springer Science & Business Media (01 1990) 3

28. Khedr, W.I., Khater, H.M., Mohamed, E.R.: Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage. IEEE Access **7**, 65635–65651 (2019) 1
29. Koyama, K., Maurer, U., Okamoto, T., Vanstone, S.A.: New public-key schemes based on elliptic curves over the ring zn. In: Annual International Cryptology Conference (1991), `https://api.semanticscholar.org/CorpusID:911427` 1.1
30. Malavolta, G., Thyagarajan, S.A.K.: Homomorphic time-lock puzzles and applications. In: Annual International Cryptology Conference. pp. 620–649. Springer (2019) 1
31. Montgomery, H.L., Vaughan, R.C.: Multiplicative Number Theory I: Classical Theory. Cambridge Studies in Advanced Mathematics, Cambridge University Press (2006). https://doi.org/10.1017/CBO9780511618314 6
32. Niven, I., Zuckerman, H.S., Montgomery, H.L.: An introduction to the theory of numbers. Wiley, New York, fifth edition. edn. (1991) 2, 6.2
33. Pietrzak, K.: Simple verifiable delay functions. In: 10th innovations in theoretical computer science conference (itcs 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2018) 1
34. Rabin, M.: Probabilistic algorithm for testing primality. Journal of Number Theory **12**, 128–138 (02 1980). https://doi.org/10.1016/0022-314X(80)90084-0 1
35. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **26**, 96–99 (01 1983). https://doi.org/10.1145/359340.359342 1
36. Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. 1996 Technical Report (1996) 1
37. Delpech de Saint Guilhem, C., Makri, E., Rotaru, D., Tanguy, T.: The return of eratosthenes: Secure generation of rsa moduli using distributed sieving. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. pp. 594–609 (2021) 1, 5.3
38. Wesolowski, B.: Efficient verifiable delay functions. In: Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38. pp. 379–407. Springer (2019) 1

Appendix 6 Appendix

We detail the number of elements in the set related to $\mathrm{MR}(p)$ for the Miller-Rabin test when $p \equiv 3 \pmod 4$ in Subsection 6.1. Subsection 6.2 includes missing proofs related to the Lucas test. Subsection 6.3 examines the distribution consistency required in Theorem 3, while Subsection 6.4 covers missing protocols utilized within the main protocol. For ease of comparison, we summarize the three RSA modulus protocols in Subsection 6.5.

6.1 Variant Miller-Rabin Test

For completeness, we provide the formula for the number of variants of the Miller-Rabin test, which proof is similar to Theorem 1.

Lemma 5. *Let* $p = \prod_{i=1}^{s} p_i^{r_i} \equiv 3 \pmod 4$. *Then*

$$|\mathrm{MR}(p)| = 2\prod_{i}^{s} \gcd\left((p-1)/2, d_i\right).$$

Proof. Since $(p-1)/2$ is odd, we have

$$|\{g \in \mathbb{Z}_p^\times \mid g^{(p-1)/2} \equiv 1 \pmod p\}| = |\{g \in \mathbb{Z}_p^\times \mid g^{(p-1)/2} \equiv -1 \pmod p\}|$$

and

$$|\mathrm{MR}(p)| = 2 \cdot |\{g \in \mathbb{Z}_p^\times \mid g^{(p-1)/2} \equiv 1 \pmod p\}|.$$

Similar to Lemma 3, we consider the problem of counting the cardinality of $\frac{(p-1)}{2}$-th roots of 1 in $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ using CRT. Combining the fact $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ is cyclic, $\gcd(p, (p-1)/2) = 1$, and Lemma 1, one has the number of $\frac{(p-1)}{2}$-th roots of 1 in the group $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ is

$$\gcd((p-1)/2, p_i^{r_i-1}(p_i-1)) = \gcd((p-1)/2, d_i).$$

The above discussion implies the desired result.

6.2 Missing Proofs of Section 4

When D is not a square, the result have already been provided in [3, Section 5]. Here, we extend this result to general integers D.

Proposition 4. *Let* D *be an integer and* $N := \prod_{i=1}^{s} p_i^{r_i}$ *be a positive integer with* $\gcd(N, 2D) = 1$. *Then we have* $|\mathcal{Z}(D, N)| = \prod_{i=1}^{s} p_i^{r_i-1}\left(p_i - \left[\frac{D}{p_i}\right] - 1\right)$.

Proof. Similarly, applying CRT, we only consider the case $\mathcal{Z}(D, p^r)$. When $r = 1$, in the beginning proof of Lemma 4 gives us $|\mathcal{Z}(D, p)| = p_i - \left[\frac{D}{p_i}\right] - 1$. When $r \geq 2$, we first the case where $Q \equiv -D/4 \pmod{p}$, and need to compute the cardinality of the set

$$\left\{ (P, Q) \;\middle|\; \begin{array}{l} P^2 \equiv 0 \pmod{p}, \\ \gcd(Q, p^r) = 1, 0 \leq P, Q < p^r \end{array} \right\}. \tag{6}$$

The number of solution (P, Q) is p^{r-1}, which form is $(P, Q) = \big(tp, ((tp)^2 - D)/4\big)$, where $t \in \mathbb{Z}_{p^{r-1}}$.

For the case $Q \not\equiv -D/4 \pmod{p}$, we consider $Q = a + tp$, where $t \in \mathbb{Z}_{p^{r-1}}$ and

$$a \in \mathcal{T} := \left\{ Q \not\equiv -D/4 \in \mathbb{Z}_p^\times \;\middle|\; x^2 \equiv D + 4Q \mod p \text{ is solvable} \right\}.$$

For each $Q \in \mathbb{Z}_{p^r}$ with $Q \not\equiv -D/4 \pmod{p}$, if $f_Q(x) := x^2 - 4Q - D \equiv 0 \pmod{p}$ has m solutions in $\mathbb{Z}_p$, and $f'_Q(a) \not\equiv 0 \pmod{p}$ for all $a \in \mathcal{T}$. Therefore, by Lemma 2, $f_Q(x) \equiv 0 \pmod{p^r}$ also has m solutions in $\mathbb{Z}_{p^r}$. Since $t \in \mathbb{Z}_{p^{r-1}}$ is arbitrary, then the number of solutions for this case is $p^{r-1}(|\mathcal{Z}(D, p)| - 1)$. Therefore, the total number of solutions is $p^{r-1}(|\mathcal{Z}(D, p)| - 1) + p^r = p^{r-1}(|\mathcal{Z}(D, p)|)$.

This part completes the proof of the Lemma 4.

Lemma 6. *Let p be an odd prime, and D be an element of $\mathbb{Z}_p^\times$. Then we have, for any $r \geq 1$ and $\epsilon \in \{\pm 1\}$,*

$$|\mathcal{Z}^\epsilon(D, p^r)| = p^{r-1} \cdot |\mathcal{Z}^\epsilon(D, p)|.$$

Proof. When $r = 1$, the desired result have been proved in the proof of Lemma 4. Here, we only consider the case $2 \nmid r$, because $\mathcal{Z}^{+1}(D, N) = \mathcal{Z}(D, N)$ as $2 \mid r$, which result can be obtain by Proposition 4. Assume $\epsilon = 1$, since we have $|\mathcal{Z}(D, p^r)| = p^{r-1} \cdot |\mathcal{Z}(D, p)|$ by Proposition 4 and $|\mathcal{Z}^{-1}(D, p^r)| = |\mathcal{Z}^(D, p^r)| - |\mathcal{Z}^{+1}(D, p^r)|$. When $\left[\frac{-D/4}{p}\right] = 1$ holds, one has $\big(tp, ((tp)^2 - D)/4\big) \in \mathcal{Z}^{+1}(D, p^r)$ for $t \in \mathbb{Z}_{p^{r-1}}$, which implies that the cardinality of the set (6) is p^{r-1}. Using the same trick as in the Proposition 4, express Q as $a + tb$, where $t \in \mathbb{Z}_{p^{r-1}}$, and

$$a \in \left\{ Q \not\equiv -D/4 \in \mathbb{Z}_p^\times \;\middle|\; x^2 \equiv D + 4Q \mod p \text{ is solvable }, \left[\frac{Q}{p}\right] = 1 \right\}.$$

Notice that $\left[\frac{Q}{p^r}\right] = \left[\frac{Q}{p}\right] = 1$, since r is odd. Therefore, For each $Q \in \mathbb{Z}_{p^r}$, if $x^2 \equiv D + 4Q \mod p$ and $\left[\frac{Q}{p}\right] = 1$ has m solutions, then $x^2 \equiv D + 4Q \mod p^r$ and $\left[\frac{Q}{p^r}\right] = 1$ also has m solutions by Lemma 2. Since $t \in \mathbb{Z}_{p^{r-1}}$ is arbitrary, then the number of solutions of $\mathcal{Z}^{+1}(D, p^r)$ is $p^{r-1}\big(|\mathcal{Z}^{+1}(D, p)| - 1\big)$. For the case where $\left[\frac{-D/4}{p}\right] = -1$, there are no $(P, Q) \in \mathcal{Z}^{+1}(D, p^r)$ with $Q \equiv -D/4 \pmod{p}$. Consequently, the number of solutions of $|\mathcal{Z}^{+1}(D, p^r)|$ is given by $p^{r-1}|\mathcal{Z}^{+1}(D, p)|$ following the same reasoning as above.

Some lemmas are used in Theorem 4.

Lemma 7. *Let p be an odd prime and $D \not\equiv 0 \pmod{p}$. Then*

$$\sum_{i=1}^{(p-1)/2} \left\lceil \frac{i^2+D}{p} \right\rceil = \frac{-1-\left\lceil \frac{D}{p} \right\rceil}{2}.$$

Proof. First, we prove that

$$\sum_{i=1}^{p} \left\lceil \frac{i^2+D}{p} \right\rceil = -1.$$

According to Euler's criterion (cf. [32, Theorem 3.1]), the above considering sum can be written as

$$\sum_{i=1}^{p} (i^2+D)^{\frac{p-1}{2}}.$$

Since $\mathbb{Z}_p^\times$ is a cyclic group, there exists a generator g, which induces that

$$\sum_{i=1}^{p-1} i^k \pmod{p} = \sum_{i=0}^{p-2} g^{ik} \pmod{p} = \begin{cases} 0, \text{ if } p-1 \nmid k; \\ -1, \text{ if } p-1 \mid k. \end{cases}$$

Therefore, applying this fact and expending $(i^2+D)^{\frac{p-1}{2}}$, one has

$$\sum_{i=1}^{p} \left\lceil \frac{i^2+D}{p} \right\rceil \equiv \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell} D^\ell \sum_{i=1}^{p} i^{p-1-2\ell} \equiv D^{(p-1)/2} \sum_{i=1}^{p} 1 + \sum_{i=1}^{p} i^{p-1} \equiv -1 \pmod{p}.$$

Notice that

$$\left| \sum_{i=1}^{p} \left\lceil \frac{i^2+D}{p} \right\rceil \right| \leq p,$$

which implies that $\sum_{i=1}^{p} \left\lceil \frac{i^2+D}{p} \right\rceil = -1$ or $p-1$. However, if $\sum_{i=1}^{p} \left\lceil \frac{i^2+D}{p} \right\rceil = p-1$, then we must have $p-1$ terms equal to 1 and exactly 1 term $a^2+D \equiv 0 \pmod{p}$ with $a \equiv -a \pmod{p}$, which implies that $a \equiv 0 \pmod{p}$, since p is odd. Therefore, one has $D \equiv 0 \pmod{p}$, which gives us a contradiction.

The proof is completed by the above fact and the following observation.

$$2\sum_{i=1}^{\frac{p-1}{2}} \left\lceil \frac{i^2+D}{p} \right\rceil = \sum_{i=1}^{p-1} \left\lceil \frac{i^2+D}{p} \right\rceil = -1 - \left\lceil \frac{D}{p} \right\rceil.$$

Lemma 8. *Let $p_i > 3$ be distinct primes and $s \geq 1$. Then*

$$\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)-1} \leq \frac{(p_{\min}-1)^s}{(p_{\min}-2)^s-1}.$$

Here $p_{\min} := \min\limits_{1 \leq i \leq s} \{p_i\}$.

Proof. Observe that

$$\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)-1}=\left(\frac{\prod_{i=1}^{s}(p_i-1)}{\prod_{i=1}^{s}(p_i-2)}\right)\left(\frac{\prod_{i=1}^{s}(p_i-2)}{\prod_{i=1}^{s}(p_i-2)-1}\right).$$

Since $(p_i-1)/(p_i-2)$ is a decreasing function for p_i, we have

$$\prod_{i=1}^{s}\left(\frac{p_i-1}{p_i-2}\right)\leq\frac{(p_{\min}-1)^s}{(p_{\min}-2)^s}.$$

The proof is completed by the facts that $x/(x-1)$ is decreasing and $\prod_{i=1}^{s}(p_i-2)\geq(p_{\min}-2)^s$.

Lemma 9. *Let $p_i>5$ be distinct primes and $s\geq 1$. Then for any $1\leq j\leq s$,*

$$\prod_{i=j}^{s}(p_i-1)<\prod_{i=j}^{s}2(p_i-2)-2^{s-j+1}.$$

Proof. For all $p_i\geq 5$, we have

$$\prod_{i=j}^{s}(p_i-1)+2^{s-j+1}\leq\prod_{i=j}^{s}\big((p_i-1)+2\big)=\prod_{i=j}^{s}(p_i+1)\leq\prod_{i=j}^{s}2(p_i-2).$$

6.3 The Identical Distributions of P_j and P'_j in Theorem 3

In this subsection, for an integer m, if $\sqrt{D}\in\mathbb{Z}_m^{\times}$, then $\pmod m$ refers to the module $m\mathbb{Z}$; otherwise, if $\sqrt{D}\notin\mathbb{Z}_m^{\times}$, $\pmod m$ refers to the module $m\mathcal{O}_D$. To investigate the distribution of P_j and P'_j, we will examine the relationship between $S_{\text{real}(m,b)}$ and $S_{\text{ideal}(m,b)}$ given an odd integer m and $b\in\{0,1\}$. Here

$$S_{\text{real}(m,b)}:=\left\{P\in\mathbb{Z}_m\;\middle|\;\left[\frac{(P^2-D)/4}{m}\right]=(-1)^b\right\},\text{ and}$$

$$S_{\text{ideal}(m,b)}:=\left\{\frac{2\sqrt{D}}{a^2(-1)^b-1}+\sqrt{D}\;\middle|\;a=\frac{v+w\sqrt{D}}{v-w\sqrt{D}},v,w\in\mathbb{Z}_m,v^2-w^2D\in\mathbb{Z}_m^{\times},\ a^2(-1)^b\not\equiv 1\pmod m\right\}.$$

Then we have

Lemma 10. *If p is an odd prime, and D is an integer with $\left[\frac{-D}{p}\right]=-1$, then we have $S_{\text{real}(p,b)}=S_{\text{ideal}(p,b)}$ for $b\in\{0,1\}$.*

Proof. For any $P' \in S_{\text{ideal}(p,b)}$, we have

$$\begin{aligned}(P'^2 - D)/4 &= \left(\left(\frac{\sqrt{D}}{a^2(-1)^b - 1}\right)\left(\frac{\sqrt{D}}{a^2(-1)^b - 1} + \sqrt{D}\right)\right) \\ &= D\left[\frac{(v^2 - w^2D)^2(-1)^b}{\left((v + w\sqrt{D})^2(-1)^b - (v - w\sqrt{D})^2\right)^2}\right]\end{aligned}$$

Therefore,

$$\left[\frac{(P'^2 - D)/4}{p}\right] = \begin{cases} \left[\frac{1/(v^2w^2)}{p}\right] = 1 & \text{, if b = 0;} \\ \left[\frac{-D/(v^2+w^2D)^2}{p}\right] = -1 & \text{, if b = 1.} \end{cases}$$

We derive $\left[\frac{(P'^2-D)/4}{p}\right] = (-1)^b$ and $S_{\text{real}(p,b)} \supseteq S_{\text{ideal}(p,b)}$. On the other hand, let P be an element in $S_{\text{real}(p,b)}$. We assume that there exists a belonging the set

$$\left\{\frac{v + w\sqrt{D}}{v - w\sqrt{D}}\middle| \, v, w \in \mathbb{Z}_p, v^2 - w^2D \in \mathbb{Z}_{p^\times}, (v+w\sqrt{D})^2 \equiv (-1)^b(v-w\sqrt{D})^2 \pmod p\right\}$$

such that $a^2(-1)^b = \frac{P+\sqrt{D}}{P-\sqrt{D}} \not\equiv 1 \pmod p$. Then we have

$$P \equiv \frac{2\sqrt{D}}{\frac{P+\sqrt{D}}{P-\sqrt{D}} - 1} + \sqrt{D} \equiv \frac{2\sqrt{D}}{a^2(-1)^b - 1} + \sqrt{D} \pmod p,$$

which implies $S_{\text{real(p,b)}} \subseteq S_{\text{ideal(p,b)}}$. To prove the assumption, we split it into two cases.

Case1: $\left[\frac{D}{p}\right] = 1$ (i.e. $\sqrt{D} \in \mathbb{Z}_p^\times$).

Since the condition in Lemma gives $\left[\frac{-D}{p}\right] = -1$, we have $\left[\frac{-1}{p}\right] = -1$. Then one has

$$\begin{aligned}&\left[\frac{(-1)^b \cdot (P + \sqrt{D})/(P - \sqrt{D})}{p}\right] = \left[\frac{(-1)^b \cdot (P + \sqrt{D})^2/(P^2 - D)}{p}\right] \\ &= \left[\frac{(-1)^b(P^2 - D)}{p}\right] = \left[\frac{(-1)^b}{p}\right](-1)^b = 1.\end{aligned}$$

There exists $t \in \mathbb{Z}_p^\times$ such that $t^2 \equiv (-1)^b \frac{P+\sqrt{D}}{P-\sqrt{D}} \pmod p$. Assume $t \not\equiv 1 \pmod p$, we take $(v, w) = (\frac{t+1}{t-1}\sqrt{D}, 1)$ and then $a^2 \equiv \left(\frac{v+w\sqrt{D}}{v-w\sqrt{D}}\right)^2 \equiv (-1)^b \frac{P+\sqrt{D}}{P-\sqrt{D}} \pmod p$. If $t = 1$, we set $(v, w) = (1, 0)$, then $a^2 = 1$.

Case2: $\left[\frac{D}{p}\right] = -1$.

If $b = 0$ (resp. $b = 1$), then we take $(v, w) = (\frac{P+\sqrt{4(P^2-D)}}{2}, 1) \in \mathbb{Z}_p \times \mathbb{Z}_p$ (resp.

$(v, w) = (\frac{D+\sqrt{D(D-P^2)}}{P}, 1) \in \mathbb{Z}_p \times \mathbb{Z}_p)$. Racall that $a = \frac{v+w\sqrt{D}}{v-w\sqrt{D}}$. Then, one has $a^2 \equiv (-1)^b \frac{P+\sqrt{D}}{P-\sqrt{D}} \pmod{p}$.

Assume p is an odd prime and $D \in \mathbb{Z}_p^\times$. Let

$$G := \left\{ (a, b) \;\middle|\; a, b \in \mathbb{Z}_p, a^2 - b^2 D \in \mathbb{Z}_p^\times \right\}.$$

Given $g_1 = (a_1, b_1), g_2 = (a_2, b_2) \in G$, define $g_1 * g_2 = (a_1 a_2 + b_1 b_2 D, a_1 b_2 + b_1 a_2)$. Then G is a group with the identity $(1, 0)$, and its inverse of $g = (a, b)$ is $\big(a/(a^2 - b^2 D), -b/(a^2 - b^2 D)\big)$. Let

$$H := \left\{ \frac{a + b\sqrt{D}}{a - b\sqrt{D}} \in \mathbb{Z}_p(\sqrt{D}) \;\middle|\; a, b \in \mathbb{Z}_p, a^2 - b^2 D \in \mathbb{Z}_p^\times \right\},$$

which is also a group under the field multiplication. Here $\mathbb{Z}_p(\sqrt{D})$ is the fractional field of the ring $\{a + b\sqrt{D} \mid a, b \in \mathbb{Z}_p\}$. The inverse of any $h = \frac{a+b\sqrt{D}}{a-b\sqrt{D}} \in H$ is $\frac{a-b\sqrt{D}}{a+b\sqrt{D}}$, and the identity is 1.

Lemma 11. *Let p be an odd prime, and $D \in \mathbb{Z}_p^\times$. Consider a group homomorphism $f : G \to H$ defined by*

$$g = (a, b) \in G \mapsto \left(\frac{a + b\sqrt{D}}{a - b\sqrt{D}} \right)^2 \in H.$$

Then the set of $f(g)$ forms a subgroup of H, and $|\ker(f)| = 2p - 2$.

Proof. It is a subgroup can be verified directly using the definition. We omit this step. The map f is a group homomorphism, which can be verified by showing that for any $(a_1, b_1), (a_2, b_2) \in G$:

$$f(a_1, b_1) f(a_2, b_2) = \frac{a_1 a_2 + b_1 b_2 D + (a_1 b_2 + a_2 b_1)\sqrt{D}}{a_1 a_2 + b_1 b_2 D - (a_1 b_2 + a_2 b_1)\sqrt{D}} = f((a_1, b_1) * (a_2, b_2)).$$

Let $g = (a, b) \in G$ with $f(g) = 1$. Then $\left(\frac{a+b\sqrt{D}}{a-b\sqrt{D}}\right)^2 = 1$, which implies that $ab\sqrt{D} = 0$. Therefore $a = 0$ or $b = 0$. If $a = 0$ and $b \in \mathbb{Z}_p^\times$, then $f(g) = 1$. Similarly, if $b = 0$, then $a \in \mathbb{Z}_p^\times$, then $f(g) = 1$. In conclusion, the cardinality of kernel of f is $2p - 2$.

Proposition 5. *If $N = pq$ is an odd RSA modulus, and D is an integer with $\left[\frac{-D}{p}\right] = \left[\frac{-D}{q}\right] = -1$, then we have $S_{\text{real}(N,0)} = S_{\text{ideal}(N,0)} \cup S_{\text{ideal}(N,1)}$. Furthermore, uniformly sampling $u, v \in \mathbb{Z}_N$, $b \in \{0, 1\}$ with $u^2 - v^2 D \in \mathbb{Z}_N^\times$ and $a^2(-1)^b \not\equiv 1 \pmod{N}$ is equivalent to randomly selecting from the set $S_{\text{real}(N,0)}$.*

Proof. According to the CRT, we have

$$S_{\text{real}(N,0)} = \left(S_{\text{real}(p,0)} \times S_{\text{real}(q,0)}\right) \cup \left(S_{\text{real}(p,1)} \times S_{\text{real}(q,1)}\right).$$

Similarly, one has

$$S_{\text{ideal}(N,0)} = S_{\text{ideal}(p,0)} \times S_{\text{ideal}(q,0)}, \text{ and } S_{\text{ideal}(N,1)} = S_{\text{ideal}(p,1)} \times S_{\text{ideal}(q,1)}.$$

Thus, according to Lemma 10, there exists a bijective map from $S_{\text{ideal}(N,0)} \cup S_{\text{ideal}(N,1)}$ to $S_{\text{real}(N,0)}$.

Notice that to ensure $S_{\text{ideal}(N,b)}$ is well-defined, we need to assume $a^2(-1)^b \not\equiv 1 \pmod{N}$. Specifically, for any odd prime p satisfying $\left[\frac{-D}{p}\right] = -1$, then this condition is equivalent to $a^2 \equiv 1 \mod p$ and $b = 0$, which is also equivalent to $u = 0, w \in \mathbb{Z}_p^\times$ or $u \in \mathbb{Z}_p^\times, v = 0$. Let $T_N := \{(u,w) : u^2 - w^2 D \in \mathbb{Z}_N^\times\}$. Lemma 11 says that there is a surjective map f from T_p to the set $S_{\text{ideal}(p,b)}$ for any $b \in \{0,1\}$ such that $|f^{-1}(x)| = 2p-2$ for all $x \in S_{\text{ideal}(p,b)}$. This map induces a bijective map

$$T_p - \{u,v \mid uv = 0, (u,v) \neq (0,0)\} \times T_p \to S_{\text{ideal}(p,0)} \times S_{\text{ideal}(p,1)}.$$

In fact, the set $\{u,v \mid uv = 0, (u,v) \neq (0,0)\}$ is $f^{-1}(1)$.

Lastly, the CRT says that $T_N = T_p \times T_q$. Therefore, there exists a map g such that $|g^{-1}(x)| = (2p-2)(2q-2)$ for all $x \in S_{\text{ideal}(N,0)} \cup S_{\text{ideal}(N,1)}$. The proof is complete.

6.4 Missing Functionalities and Protocols

The functionality describes that each party $\mathcal{P}_i$ has two shares, $\mathfrak{x}_i$ and $\mathfrak{y}_i$, the functionality outputs $\mathfrak{z}_i$ where $[z]_N = [xy]_N$ and assigns to $\mathcal{P}_i$.

Functionality 3 Modular Multiplication $\mathcal{F}_{\text{ModMul}}(n)$

Inputs: Each party $\mathcal{P}_i$ has shares $[x]_N$, $[y]_N$ and N.

Outputs: Each party has shares of $[z]_N = [x \cdot y]_N$, with uniformly random $\mathfrak{z}_i \in \mathbb{Z}_N$ for all $1 \leq i \leq n$.

The functionality below is to ensure that participants can learn $\prod_i y_i$ without revealing their own y_i.

Functionality 4 $\mathcal{F}_{\text{Shuffle}}(n)$

Inputs: Each party $\mathcal{P}_i$ has y_i in a finite group G.

Outputs: Each party $\mathcal{P}_i$ receives $y := \prod_{i=1}^{n} y_i \in G$.

In the following protocol [5], each party splits their own input y_i into $n-1$ partitions and randomly send one share to other parties to avoid revealing their own input y_i. Every party will calculate the product of all obtained shares $\prod_i z_i$ and publish it. Eventually, we have $\prod_{i=1}^{n} z_i = \prod_{i=1}^{n} y_i$.

Protocol 3 Shuffle $\pi_{\text{Shuffle}}(n)$

Inputs: Each party $\mathcal{P}_i$ has $y_i \in (\mathcal{O}_D/N)^{\times}$.

Outputs: $\prod_{i=1}^{n} y_i \in (\mathcal{O}_D/N)^{\times}$.

1. Each party $\mathcal{P}_i$ randomly chooses $x_{i,j} \in (\mathcal{O}_D/N)^{\times}$ for all $1 \leq j \leq n$ such that $\prod_{j=1}^{n} x_{i,j} = 1$ (i.e. randomly chooses $x_{i,j}$ for $1 \leq j \leq n-1$ and $x_{i,n}^{-1} := \prod_{j=1}^{n-1} x_{i,j}$). Set $y_{i,1} := x_{i,1} \cdot y_i$ and $y_{i,j} := x_{i,j}$ for all $2 \leq j \leq n$. Send $y_{i,j}$ to the party $\mathcal{P}_j$ for all $1 \leq j \neq i \leq n$.
2. Each party $\mathcal{P}_i$ computes $z_i := \prod_{j=1}^{n} y_{j,i}$. Broadcast z_i to the other party $\mathcal{P}_j$.
3. Outputs $z := \prod_{i=1}^{n} z_i$.

6.5 Three RSA Moduli Protocols

In this section, we rewrite the Lucas test using macros from [12] to facilitate comparison with the Boneh-Franklin test [8] and Burkhardt's et al.'s [12] protocols. Here, we always assum $p \equiv q \equiv 3 \pmod 4$. Finally, we note that an RSA modulus refers to N, which is the product of two distinct prime numbers. In contrast, a biprime refers to N being the product of any two prime numbers.

Protocol 4 Lucas Biprimality test type (n)

Inputs: Each party $\mathcal{P}_i$ has odd integers $[p]_{\mathbb{Z}}$, $[q]_{\mathbb{Z}}$, $D = 1$, and N.

Outputs:

1. Party $\mathcal{P}_1$ randomly chooses $0 \leq P < N$ such that $Q = (P^2 - D)/4$ and $\left[\frac{Q}{N}\right] = 1$. Send this P to the other parties.
2. Party $\mathcal{P}_1$ computes $v_1 := g^{(N-\mathfrak{p}_1-\mathfrak{q}_1+1)/4} \pmod N$, where $g := \frac{P-\sqrt{D}}{P+\sqrt{D}}$. The other parties compute $v_i := g^{-(\mathfrak{p}_i+\mathfrak{q}_i)/4} \pmod N$. Parties broadcast v_i to compute $v := \prod_{i=1}^{n} v_i \pmod N$. They then check if

$$v = \prod_{i=1}^{n} v_i \equiv 1 \pmod N.$$

If the test fails, return **Non-RSA Modulus**.

3. Parties verify $\gcd(N, e) = 1$ as follows:
   3.1 obtain $[r]_N \leftarrow \texttt{RandomSample}(\mathbb{Z}_N)$.
   3.2 compute $[p]_N \leftarrow \texttt{Int-to-mod}(\mathbb{Z}_N, [p]_{\mathbb{Z}})$ and $[q]_N \leftarrow \texttt{Int-to-mod}(\mathbb{Z}_N, [q]_{\mathbb{Z}})$.
   3.3 call $[b]_N \leftarrow \texttt{Mult}(\mathbb{Z}_N, [r]_N, [p]_N + [q]_N - 1)$.
   3.4 obtain $b \leftarrow \texttt{OpenAll}(\mathbb{Z}_N, [b]_N)$. If $b \neq 1$ then output **Non-RSA Modulus**. Otherwise, output **RSA Modulus**.

Below is Boneh-Franklin protocol [8], as cited from the version in [12, FIGURE 7.1].

Protocol 5 Boneh-Franklin biprimality protocol(n)

Inputs: Each party has $[p]_{\mathbb{Z}}$, $[q]_{\mathbb{Z}}$ and N.

Outputs:

1. Party $\mathcal{P}_1$ randomly chooses $g \in \mathbb{Z}_N^{\times}$ and $\left[\frac{g}{N}\right] = 1$. Send this g to the other parties.
2. Party $\mathcal{P}_1$ computes $v_1 := g^{(N - \mathfrak{p}_1 - \mathfrak{q}_1 + 1)/4} \pmod N$. The other parties compute $v_i := g^{-(\mathfrak{p}_i + \mathfrak{q}_i)/4} \pmod N$. Parties broadcast v_i to compute $v := \prod_{i=1}^{n} v_i \pmod N$. They then check if

$$v = \prod_{i=1}^{n} v_i \equiv \pm 1 \pmod N.$$

   If the test fails, return **Non-RSA Modulus**.
3. Parties verify $\gcd(N, e) = 1$ as follows:
   3.1 obtain $[r]_N \leftarrow \texttt{RandomSample}(\mathbb{Z}_N)$.
   3.2 compute $[p]_N \leftarrow \texttt{Int-to-mod}(\mathbb{Z}_N, [p]_{\mathbb{Z}})$ and $[q]_N \leftarrow \texttt{Int-to-mod}(\mathbb{Z}_N, [q]_{\mathbb{Z}})$.
   3.3 call $[b]_N \leftarrow \texttt{Mult}(\mathbb{Z}_N, [r]_N, [p]_N + [q]_N - 1)$.
   3.4 obtain $b \leftarrow \texttt{OpenAll}(\mathbb{Z}_N, [b]_N)$. If $b \neq 1$ then output **Non-RSA Modulus**. Otherwise, output **RSA Modulus**.

Herein lies Burkhardt's protocol. For further details, please consult [12].

Protocol 6 Miller-Rabin biprimality protocol$(\kappa_{\mathrm{lenP}}, s, n)$

Inputs: Each party has $[p]_{\mathbb{Z}}$, $[q]_{\mathbb{Z}}$, P, Q and N. Here P and Q are primes satisfying $n^2 2^{2\kappa_P} < nP < Q$.

Outputs:

1. Let $G = \emptyset$, for $f \in \{p, q\}$:
   1.1 $\mathcal{P}_n$ uniformly samples $v \in \mathbb{Z}_N$ and broadcasts v.

1.2 Compute $<\gamma>_N$ as follows: Party $\mathcal{P}_1$ sets $\gamma_1 := v^{\frac{f_1-1}{2}} \pmod N$. For $2 \leq i \leq n$, $\mathcal{P}_i$ sets $\gamma_i := v^{\frac{f_i}{2}} \pmod N$.
1.3 Obtain $[\gamma]_N \leftarrow \texttt{Mul-to-Add}(\mathbb{Z}_N, <\gamma>_N)$.
1.4 Compute $[\gamma+1]_N$ and $[\gamma-1]_N$.
1.5 For $\delta \in \{\gamma+1, \gamma-1\}$, compute

$$[y_\delta]_Q \leftarrow \texttt{Divisible}(\kappa_{\mathrm{lenP}}, s, \mathbb{Z}_P, \mathbb{Z}_Q, [\delta]_N, [f]_{\mathbb{Z}}).$$

1.6 Compute $[y]_Q \leftarrow \texttt{Mult}(\mathbb{Z}_Q, [y_{\gamma+1}]_Q, [y_{\gamma-1}]_Q)$.
1.7 Reveal $y \leftarrow \texttt{OpenAll}(\mathbb{Z}_Q, [y]_Q)$.
1.8 If $y = 0$, set $G = G \cup \{f\}$.
2. If $G = \{p, q\}$ output **Biprime**, otherwise output **Non-Biprime**.

The number of macros used in each test are summarized below.

Table 5: The number of macros in biprimality tests.

	# `Random-sample`	♯ `Int-to-mod`	♯ `Mult`	♯ `OpenAll`	♯ `Mult-to-add`
Boneh-Franklin [21]	1	2	1	1	0
Millier-Rabin [12]	≥ 2	4	≥ 6	≥ 4	2
Type-(I)	1	2	1	1	0

In addition to the aforementioned, Burkhardt's protocol includes other macros such as **Invert** and **Larger-domain**.