The Paillier's Cryptosystem and Some Variants Revisited

Zhengjun Cao[1], Lihua Liu[2]
(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai University[1]
No. 99, Shangda Road, Shanghai, China
Department of Mathematics, Shanghai Maritime University[2]
No. 1550, Haigang Ave, Pudong New District, Shanghai, China
(Email: caozhj@shu.edu.cn; liulh@shmtu.edu.cn)
(Received Dec. 17, 2015; revised and accepted Mar. 6, 2016)

Abstract

At Eurocrypt'99, Paillier presented a public-key cryptosystem based on a novel computational problem. It has interested many researchers because of its additively homomorphic property. In this paper, we show that there is a big difference between the original Paillier's encryption and some variants. The Paillier's encryption can be naturally converted into a signature scheme but these variants miss the feature. In particular, we simplify the alternative decryption procedure of Bresson-Catalano-Pointcheval encryption scheme proposed at Asiacrypt'03. The new version is more applicable to cloud computing because of its double trapdoor decryption mechanism and its flexibility to be integrated into other cryptographic schemes. It captures a new feature that its two groups of secret keys can be distributed to different users so as to enhance the robustness of key management.

Keywords: Additively homomorphic encryption, double trapdoor decryption, Paillier's cryptosystem, robustness of key management

1 Introduction

Homomorphic encryption is a useful cryptographic primitive because it can translate an operation on ciphertexts into an operation on underlying plaintexts.

The property is very important for many applications, such as e-voting, threshold cryptosystems, watermarking and secret sharing schemes. For example, if an additively homomorphic encryption is used in an e-voting scheme, one can obtain an encryption of the sum of all ballots from their encryption. Consequently, it becomes possible that a single decryption will reveal the result of the election. That is, it is unnecessary to decrypt all ciphertexts one by one.

At Eurocrypt'99, Paillier [21] proposed a public-key cryptosystem based on a novel computational problem. It encrypts a message m by

$$E(m, r) = g^m r^n \mod n^2,$$

where $n = pq$ is an RSA modulus, g is a public parameter such that $n \mid \mathrm{ord}_{n^2}(g)$, and r is a random pad. The encryption function $E(m, r)$ has the additively homomorphic property, i.e.,

$$E(m_1, r_1)E(m_2, r_2) = E(m_1 + m_2, r_1 r_2).$$

More powerful, who knows the trapdoor of the encryption function can recover not only the message m but also the random pad r. This is another appreciated property for many applications. Due to this property, the Paillier's encryption scheme can be naturally transformed into a one-way trapdoor permutation and a digital signature scheme.

In 1984, Goldwasser and Micali [13] proposed the first probabilistic encryption scheme which was also homomorphic. It has been improved [19, 20]. In 1999, Paillier [21] presented a novel additively homomorphic encryption which was more powerful because it can recover the random pad r as well as the message m. At PKC'01, Damgård and Jurik [9] put forth a generalization of Paillier's encryption using computations modulo $n^i (i \geq 2)$ and taking a special base $g = n + 1$.

They [10] also investigated the applications of the generalization. The elliptic curve variant of Paillier's cryptosystem is due to Galbraith [11].

In 2001, Choi et al. [7] revisited the Paillier's encryption by taking a special base g such that $g^\lambda = 1 + n \mod n^2$, where $\lambda = \mathrm{lcm}(p-1, q-1)$. Shortly after that, Sakurai and Takagi [22] pointed out that the variant cannot resist a chosen ciphertext attack which can factor the modulus n by only one query to the decryption oracle.

At Eurocrypt'06, Schoenmakers and Tuyls [23] have considered the problem of converting a given Paillier's encryption of a value $x \in \mathbb{Z}_n$ into Paillier's encryption of the

bits of x. At Eurocrypt'13, Joye and Libert [15] obtained another generalization based on 2^k-th power residue problem. In 2013, Boneh et al. [1] considered the problem of private database queries using Paillier's homomorphic encryption. At Asiacrypt' 14, Catalano et al. [5] presented an instantiation of publicly verifiable delegation of computation on outsourced ciphertext which supports Paillier's encryption. In 2015, Castagnos and Laguillaumie [4] designed a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. Their scheme is somehow similar to the one of [2]. The Gentry's fully homomorphic encryption scheme [12] relies on hard problems related to lattices, which actually allows to evaluate any function on messages given their ciphertexts. But Paillier's cryptosystem based on the problem of factoring RSA integers is still more competitive for applications that need only to add ciphertexts. Recently, Hsien et al. have investigated the possible usage of homomorphic encryption in client-server scenario [6, 14, 16, 17, 18]. Note that a misapplication of a homomorphic encryption for numerical calculations can give rise to errors like the ones in [24] (see [3] for details).

In this paper, we revisit the Paillier's cryptosystem and reaffirm that the Paillier's encryption can be naturally converted into a signature scheme but some variants miss the feature. Our presentation of the cryptosystem and some variants is so plain and heuristic that it becomes possible to investigate the further applications of these schemes in different scenarios. In particular, we simplify the alternative decryption procedure of Bresson-Catalano-Pointcheval encryption scheme. Our new proposal is more applicable to cloud computing because of its double trapdoor decryption mechanism and its flexibility to be integrated into other cryptographic schemes.

It captures a new feature that its two groups of secret parameters can be allocated to different users so as to enhance the robustness of key management.

2 Paillier's Encryption Scheme

Let $n = pq$ be an RSA modulus and $\phi(n)$ be the Euler's totient function. Set $\lambda = \mathrm{lcm}(p-1, q-1)$. Hence, $|\mathbb{Z}_{n^2}^*| = \phi(n^2) = n\phi(n)$ and for any $w \in \mathbb{Z}_{n^2}^*$

$$w^{\lambda} = 1 \mod n, \quad w^{n\lambda} = 1 \mod n^2$$

which are due to Carmichael's theorem.

Definition 1. *A number z is said to be a n-th residue modulo n^2 if there exists a number $y \in \mathbb{Z}_{n^2}^*$ such that $z = y^n \bmod n^2$.*

The set of n-th residues is a multiplicative subgroup of $\mathbb{Z}_{n^2}^*$ of order $\phi(n)$. Each n-th residue has exactly n roots, among which exactly one is strictly smaller than n.

Let g be some element of $\mathbb{Z}_{n^2}^*$ and define the following integer-valued function

$$\mathcal{E}_g : \quad \mathbb{Z}_n \times \mathbb{Z}_n^* \longmapsto \mathbb{Z}_{n^2}^*$$

$$(x, y) \longmapsto g^x \cdot y^n \mod n^2.$$

Lemma 1. *If $n \mid ord_{n^2}(g)$, then $\mathcal{E}_g$ is bijective.*

Proof. Since the two groups $\mathbb{Z}_n \times \mathbb{Z}_n^*$ and $\mathbb{Z}_{n^2}^*$ have the same number of elements $n\phi(n)$, it suffices to prove that $\mathcal{E}_g$ is injective.

Suppose that $g^{x_1} y_1^n = g^{x_2} y_2^n \bmod n^2$, where $x_1, x_2 \in \mathbb{Z}_n, y_1, y_2 \in \mathbb{Z}_n^*$. It comes $g^{x_2 - x_1}(y_2/y_1)^n = 1 \bmod n^2$, which implies

$$\begin{aligned} g^{\lambda(x_2-x_1)}(y_2/y_1)^{\lambda n} &= g^{\lambda(x_2-x_1)} \\ &= 1 \mod n^2. \end{aligned}$$

Thus $\mathrm{ord}_{n^2}(g) \mid \lambda(x_2 - x_1)$.

Since $n \mid \mathrm{ord}_{n^2}(g)$, we have $n \mid \lambda(x_2 - x_1)$. In view of that $(n, \lambda) = 1$, we obtain $x_2 = x_1 \bmod n$. Since $x_1, x_2 \in \mathbb{Z}_n$, it comes $x_1 = x_2$. Thus, $(y_2/y_1)^n = 1 \bmod n^2$, which leads to the unique solution $y_2/y_1 = 1$ over $\mathbb{Z}_n^*$. This means $x_1 = x_2$ and $y_1 = y_2$. Therefore, $\mathcal{E}_g$ is bijective. □

By the above lemma, for a given $w \in \mathbb{Z}_{n^2}^*$, there exists a pair (x, y) such that $w = g^x y^n \bmod n^2$.

Problem 1. *Given an RSA modulus $n = pq$, $c, g \in \mathbb{Z}_{n^2}^*$, compute $x \in \mathbb{Z}_n^*$ such that*

$$g^x y^n = c \mod n^2,$$

where $n \mid ord_{n^2}(g)$ and y is some element of $\mathbb{Z}_{n^2}^*$.

Theorem 1. *If λ is known and $(\frac{g^{\lambda} - 1 \bmod n^2}{n}, n) = 1$, then one can solve Problem 1 by computing*

$$x = \left(\frac{c^{\lambda} - 1 \mod n^2}{n}\right)\left(\frac{g^{\lambda} - 1 \mod n^2}{n}\right)^{-1} \mod n.$$

Proof. By the definition of λ, we have

$$c^{\lambda} = 1 \mod n, g^{\lambda} = 1 \mod n.$$

Set

$$c^{\lambda} = an + 1 \mod n^2, \quad g^{\lambda} = bn + 1 \mod n^2,$$

i.e.,

$$a = \frac{c^{\lambda} - 1 \mod n^2}{n}, \quad b = \frac{g^{\lambda} - 1 \mod n^2}{n}.$$

Since $n \mid \mathrm{ord}_{n^2}(g)$, $\mathcal{E}_g$ is bijective. There exists a pair $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ such that $c = g^x y^n \bmod n^2$. Hence, $c^{\lambda} = (g^x y^n)^{\lambda} \bmod n^2$. Since $y^{n\lambda} = 1 \bmod n^2$, it comes $c^{\lambda} = (g^{\lambda})^x \bmod n^2$. Thus,

$$an + 1 = (bn + 1)^x = xbn + 1 \mod n^2$$

this is due to $n^2 \mid \binom{x}{i}(bn)^i, i \geq 2$. Therefore, $an = xbn \bmod n^2$. That means $a = xb \bmod n$. Since $(b, n) = 1$, it gives $x = ab^{-1} \bmod n$. □

Remark 1. *Paillier called the Problem 1 as Composite Residuosity Class Problem (see Definition 8 in [21]). In view of that the trapdoor λ plays a key role in computing the exponent x with respect to the base g, we would like to call the Problem 1 as Trapdoored Partial Discrete Logarithm Problem.*

Conjecture 1. *If the trapdoor λ is unknown, there exists no probabilistic polynomial time algorithm that solves Problem 1.*

Based on the above results, at Eurocrypt'99 Paillier proposed his cryptosystem. The cryptosystem includes a probabilistic encryption scheme, a one-way trapdoor permutation and a digital signature scheme. We now describe the encryption scheme as follows.

Table 1: Paillier's encryption scheme

Setup	Pick an RSA modulus $n = pq$. Set $\lambda = \text{lcm}(p-1, q-1)$. Select $g \in \mathbb{Z}^*_{n^2}$ such that $n \mid \text{ord}_{n^2}(g)$. Publish n, g and keep λ in secret.
Enc.	For $m \in \mathbb{Z}_n$, pick $r \in \mathbb{Z}_n$, compute the ciphertext $c = g^m r^n \bmod n^2$.
Dec.	$m = \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right) / \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right) \bmod n$

3 A Hybrid Computational Problem

We now consider another computational problem which is a hybrid of partial discrete logarithm problem and n-th residuosity problem.

Problem 2. *Given an RSA modulus $n = pq$, $c, g \in \mathbb{Z}^*_{n^2}$, compute $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}^*_n$ such that*

$$g^x y^n = c \mod n^2$$

where $n \mid ord_{n^2}(g)$.

Notice that the solvability of Problem 2 directly implies that of Problem 1. We shall prove that the inverse holds, too.

If the trapdoor λ is known, Paillier proposed a method to solve the hybrid computational problem. He pointed out that x, y can be computed by

$$\begin{aligned} x &= \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right)\left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n, \\ y &= (cg^{-x})^{1/n \bmod \lambda} \bmod n. \end{aligned}$$

The idea behind his method can be described as follows. By the existence of (x, y), it is easy to find that

$$\begin{aligned} & g^x y^n = c \mod n^2 \\ \Longrightarrow\ & g^x y^n = c \mod n \Longleftrightarrow y^n = cg^{-x} \mod n \\ \Longleftrightarrow\ & (y^n)^{1/n \bmod \lambda} = (cg^{-x})^{1/n \bmod \lambda} \mod n \\ \Longleftrightarrow\ & y = (cg^{-x})^{1/n \bmod \lambda} \mod n \end{aligned}$$

By the uniqueness of $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}^*_n$, we conclude that it is properly computed.

Theorem 2. *If λ is known and $(\frac{g^\lambda - 1 \bmod n^2}{n}, n) = 1$, then one can solve Problem 2 by computing*

$$\begin{aligned} x &= \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right)\left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n, \\ y &= (cg^{-x})^s \bmod n, \end{aligned}$$

where s is the integer with the least absolute value such that $\lambda \mid ns - 1$.

Proof. Since $(n, \lambda) = 1$, it is easy to compute the integer s with the least absolute value such that $\lambda \mid ns - 1$. By Theorem 1, we conclude that x is properly computed. By the existence of y and $y^n = cg^{-x} \bmod n^2$, we have

$$(cg^{-x})^\lambda = y^{n\lambda} = 1 \mod n^2$$

Now, suppose that $ns - 1 = \lambda\phi$ and $(cg^{-x})^s = \ell n + y \bmod n^2$ for some integers ϕ, ℓ. Hence, it comes

$$\begin{aligned} g^x \left((cg^{-x})^s - \ell n\right)^n &= g^x (cg^{-x})(cg^{-x})^{ns-1} = c(cg^{-x})^{\lambda\phi} \\ &= c((cg^{-x})^\lambda)^\phi = c \cdot 1^\phi = c \bmod n^2 \end{aligned}$$

This completes the proof. □

Note that the values s and $\left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n$ have no relation to the ciphertext c. They can be computed and stored previously.

Conjecture 2. *If λ is unknown, there exists no probabilistic polynomial time algorithm that solves Problem 2.*

4 The Paillier's One-way Trapdoor Permutation and The Digital Signature Scheme

In [21], Paillier has put forth a one-way trapdoor permutation and the digital signature scheme based on his computational method. We now relate them as follows.

5 Some Variants of Paillier's Encryption Scheme

5.1 Descriptons of Some Variants

In the same article [21], Paillier has pointed out that there was an efficient variant of his original encryption scheme.

Table 2: Paillier's signature scheme

Setup	See Table 1.
Sign	For a message m, compute $s_1 \leftarrow \rho\left(\frac{H(m)^{\lambda}-1 \bmod n^2}{n}\right) \bmod n.$ $s_2 \leftarrow ((H(m)g^{-s_1})^s \bmod n$ The signature is $(m; s_1, s_2)$.
Verify	$H(m) \stackrel{?}{=} g^{s_1} s_2^n \bmod n^2$

Table 3: Paillier's one-way trapdoor permutation

Setup	Set $n = pq$, $\lambda = \mathrm{lcm}(p-1, q-1)$. Select $g \in \mathbb{Z}_{n^2}^*$ such that $n \mid \mathrm{ord}_{n^2}(g)$. Compute $\rho = \left(\frac{g^{\lambda}-1 \bmod n^2}{n}\right)^{-1} \bmod n$, and s which is the integer with the least absolute value such that $\lambda \mid ns-1$. Publish n, g and keep λ, ρ, s in secret.
Enc.	Given $m \in \mathbb{Z}_{n^2}$, set $m = m_1 + nm_2$. The ciphertext is $c \leftarrow g^{m_1} m_2^n \bmod n^2$.
Dec.	$m_1 \leftarrow \rho\left(\frac{c^{\lambda}-1 \bmod n^2}{n}\right) \bmod n,$ $m_2 \leftarrow (cg^{-m_1})^s \bmod n.$ $m \leftarrow m_1 + nm_2.$

Shortly afterwards, other variants came out [2, 7, 8, 9]. We list some variants in Table 4.

Correctness of Variant 1. The variant takes $x = m, y = g^r$ in Problem 2. Since each n-th residue has exactly n roots, among which exactly one is strictly smaller than n, and $\mathrm{ord}_{n^2}(g) = \alpha n$, we have $g^{\alpha} = 1 \bmod n$. Otherwise, suppose $g^{\alpha} = sn + t \bmod n^2$ for some integers $0 \le s < n$ and $t\,(2 \le t < n)$. It leads to

$$1 = g^{\alpha n} = (sn+t)^n = t^n \mod n^2$$

which means $t = 1$. It is a contradiction. Thus, $g^{\alpha} = sn + 1 \bmod n^2$. By

$$\begin{aligned} c^{\alpha} &= (g^m (g^r)^n)^{\alpha} = (g^{\alpha})^m \\ &= (sn+1)^m = smn + 1 \mod n^2 \end{aligned}$$

we have

$$\frac{\frac{c^{\alpha}-1 \bmod n^2}{n}}{\frac{g^{\alpha}-1 \bmod n^2}{n}} = \frac{sm}{s} = m \mod n.$$

Correctness of Variant 2. The variant takes $g = 1 + n, x = m, y = r$ in Problem 2. It is easy to find that

$$\begin{aligned} \frac{c^{\kappa} - 1 \bmod n^2}{n} &= \frac{((1+n)^m r^n)^{\tau\lambda} - 1 \bmod n^2}{n} \\ &= \frac{(1+n)^{m\tau\lambda} - 1 \bmod n^2}{n} \\ &= \frac{nm\tau\lambda \bmod n^2}{n} = \frac{nm}{n} \\ &= m \end{aligned}$$

Correctness of Variant 3. The variant takes $x = m, y = r$ in Problem 2. It is easy to check that

$$\begin{aligned} \frac{c^{\lambda} - 1 \bmod n^2}{n} &= \frac{(g^m r^n)^{\lambda} - 1 \bmod n^2}{n} \\ &= \frac{(g^{\lambda})^m - 1 \bmod n^2}{n} \\ &= \frac{(1+n)^m - 1 \bmod n^2}{n} \\ &= m \end{aligned}$$

Correctness of Variant 4. It is easy to see that

$$\begin{aligned} & \frac{\frac{c}{(c^d \bmod n)^e} - 1 \bmod n^2}{n} \\ = & \frac{\frac{(1+n)^m r^e}{(((1+n)^m r^e)^d \bmod n)^e} - 1 \bmod n^2}{n} \\ = & \frac{\frac{(1+n)^m r^e}{r^e} - 1 \bmod n^2}{n} \\ = & m \end{aligned}$$

5.2 The Bresson-Catalano-Pointcheval Encryption Scheme Revisited

The Bresson-Catalano-Pointcheval encryption scheme has not directly specified that $n \mid \mathrm{ord}_{n^2}(g)$. But it is easy to find that such a picked g satisfies the condition with high probability. In view of that the condition is necessary to recover x in Problem 1 (see the proof of Theorem 1), we shall directly specify it in the Setup phase.

The random pad r is chosen by the sender and is blinded as

$$A = g^r \mod n^2, \quad B = h^r(1+mn) \mod n^2.$$

We have

$$A = g^r \cdot 1^n \mod n^2,$$

it here takes $x = r, y = 1$ in Problem 1. Thus one knowing the trapdoor λ can recover r using Paillier's computational method. Note that although B could be viewed as

$$B = (1+n)^m h^r \mod n^2.$$

It does not fall into the class of Problem 1. One cannot recover r from B whether the trapdoor is known or not.

After r is retrieved, one can recover $m = \frac{B/h^r - 1 \bmod n^2}{n}$ directly. Obviously, the original computational method incurs more cost.

Based on the observation, we now present a new revision of the scheme (see Table 5).

We stress that the new alternative decryption method does not invoke the secret parameter a, which means the secret parameters a, λ, ρ can be divided into two groups, $\{a\}$ and $\{\lambda, \rho\}$. The two groups of secret parameters can be allocated to different users so as to enhance the robustness of key management. The new version is more flexible to be integrated into other cryptographic schemes.

Table 4: Some variants of Paillier's encryption scheme

	$n = pq$ is an RSA modulus, $\lambda = \text{lcm}(p-1, q-1)$.
Variant 1 (Paillier)	$g \in \mathbb{Z}^*_{n^2}$, $\text{ord}_{n^2}(g) = \alpha n$. PK: n, g; SK: α.
	$m \in \mathbb{Z}_n$, $r \in \mathbb{Z}_n$, $c = g^{m+rn} \bmod n^2$.
	$m = \left(\frac{c^\alpha - 1 \bmod n^2}{n}\right) / \left(\frac{g^\alpha - 1 \bmod n^2}{n}\right) \bmod n$
Variant 2 (Damgård-Jurik)	$\kappa = \tau\lambda$, $\tau = \lambda^{-1} \bmod n$. PK: n; SK: κ.
	$m \in \mathbb{Z}_n$, $r \in \mathbb{Z}_n$, $c = (1+mn)r^n \bmod n^2$.
	$m = \frac{c^\kappa - 1 \bmod n^2}{n}$
Variant 3 (Choi-Choi-Won)	$g^\lambda = 1 + n \bmod n^2$. PK: n, g; SK: λ.
	$m \in \mathbb{Z}_n$, $r \in \mathbb{Z}_n$, $c = g^m r^n \bmod n^2$.
	$m = \frac{c^\lambda - 1 \bmod n^2}{n}$
Variant 4 (Catalano-Gennaro -Howgrave-Nguyen)	$e < n$, $d = e^{-1} \bmod \phi(n)$. PK: n, e; SK: d.
	$m \in \mathbb{Z}_n$, $r \in \mathbb{Z}_n$, $c = (1+mn)r^e \bmod n^2$.
	$m = \frac{\frac{c}{(c^d \bmod n)^e} - 1 \bmod n^2}{n}$

Table 5: The Bresson-Catalano-Pointcheval encryption scheme revisited

	The original	The revisited
Setup	$n = pq$, $\lambda = \text{lcm}(p-1, q-1)$. $\alpha \in \mathbb{Z}^*_{n^2}$, $a < n\lambda/2$, $g = \alpha^2 \bmod n^2, h = g^a \bmod n^2$. $\rho = \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n$. $\tau = \lambda^{-1} \bmod n$. PK: n, g, h; SK: a, λ, ρ, τ.	$n = pq$, $\lambda = \text{lcm}(p-1, q-1)$. $g \in \mathbb{Z}^*_{n^2}$, $n \mid \text{ord}_{n^2}(g)$. $a \in \mathbb{Z}^*_n$, $h = g^a \bmod n^2$. $\rho = \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n$. PK: n, g, h; SK: a, λ, ρ.
Enc.	For $m \in \mathbb{Z}_n$, pick $r \in \mathbb{Z}_n$, compute $A = g^r \bmod n^2$, $B = h^r(1+mn) \bmod n^2$. The ciphertext is $c = (A, B)$.	It is the same as the original.
Dec. 1	$m = \frac{B/A^a - 1 \bmod n^2}{n}$	It is the same as the original.
Dec. 2	$r = \rho\left(\frac{A^\lambda - 1 \bmod n^2}{n}\right) \bmod n$. $\gamma = ar \bmod n$. $m = \frac{\left(\frac{B}{g^\gamma}\right)^\lambda - 1 \bmod n^2}{n} \cdot \tau \bmod n$,	$r = \rho\left(\frac{A^\lambda - 1 \bmod n^2}{n}\right) \bmod n$. $m = \frac{B/h^r - 1 \bmod n^2}{n}$

Table 6: Comparisons of Paillier's encryption and some variants

The original	$c = g^m r^n \bmod n^2$. $n \mid \mathrm{ord}_{n^2}(g), x = m, y = r$. Verification w.r.t. (m, s_1, s_2): $H(m) \stackrel{?}{=} g^{s_1} s_2^n \bmod n^2$. **True**.
Variant 1	$c = g^m (g^r)^n = g^{m+rn} \bmod n^2$. $\mathrm{ord}_{n^2}(g) = \alpha n, x = m$, $y = g^r$ is a special random pad. Verification w.r.t. (m, s_1, s_2): $H(m) \stackrel{?}{=} g^{s_1+s_2 n} \bmod n^2$. **False**.
Variant 2	$c = (1+n)^m r^n = (1+mn) r^n \bmod n^2$. $g = 1+n, \mathrm{ord}_{n^2}(g) = n, x = m, y = r$ Verification w.r.t. (m, s_1, s_2): $H(m) \stackrel{?}{=} (1+s_1 n) s_2^n \bmod n^2$. **False**.
Variant 3	$c = g^m r^n \bmod n^2$. $g^\lambda = 1+n, x = m, y = r$ It can **not** resist a chosen ciphertext attack.
Variant 4	$c = (1+mn) r^e \bmod n^2$, $g = 1+n, ed = 1 \bmod \phi(n)$. Verification w.r.t. (m, s_1, s_2): $H(m) \stackrel{?}{=} (1+s_1 n) s_2^e \bmod n^2$. **False**.
Variant 5 (Bresson-Catalano -Pointcheval)	$(A, B) = (g^r \bmod n^2, (1+mn) h^r \bmod n^2)$ Verification w.r.t. (m, s_1, s_2): $H(m) \stackrel{?}{=} (1+s_1 n) h^{s_2} \bmod n^2$. **False**.

5.3 Comparisons

The Paillier's encryption scheme can be naturally converted into a signature scheme because it can retrieve the random pad r as well as the message m. This is due to that it only requires $n \mid \mathrm{ord}_{n^2}(g)$. But in the Variant 1, one cannot retrieve $r \in \mathbb{Z}_n^*$, instead $g^r \bmod n^2$. Though the Variant 3 is very similar to the original Paillier's encryption scheme, it is insecure against a chosen ciphertext attack [22]. The others, Variant 2, Variant 4 and Variant 5 cannot be converted into signature schemes. See Table 6 for details.

By the way, the claim that some variants are more efficient than the original Paillier's encryption scheme is somewhat misleading. Actually, in Paillier's encryption scheme the computation

$$\left(\frac{g^\lambda - 1 \bmod n^2}{n} \right)^{-1} \bmod n$$

has no relation to the ciphertext c. It can be computed and stored previously. The dominated computation in the decryption procedure is that

$$\frac{c^\lambda - 1 \bmod n^2}{n},$$

while the corresponding computation in Variant 4 is

$$m = \frac{\frac{c}{(c^d \bmod n)^e} - 1 \bmod n^2}{n},$$

and that in Variant 5 is

$$m = \frac{B/A^a - 1 \bmod n^2}{n}.$$

We find these decryptions require almost the same computational cost.

6 Conclusion

We revisit the Paillier's cryptosystem and present an efficient alternative decryption procedure for Bresson-Catalano-Pointcheval encryption scheme.

We reaffirm that the original Paillier's encryption scheme has a special property that it naturally implies a signature scheme, while those variants miss this feature.

We would like to stress that although a homomorphic encryption allows anyone to perform some computations on encrypted data, despite not having the secret decryption key, the computations are constrained to the underlying domain (finite fields or rings). A misapplication of a homomorphic encryption for numerical calculations can give rise to errors.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

References

[1] D. Boneh, C. Craigentry, S. Halevi, F. Wang, and D. Wu, "Private database queries using somewhat homomorphic encryption," in *Proceedings of Applied Cryptography and Network Security (ACNS'13)*, pp. 102–118, Banff, AB, Canada, June 2013.

[2] E. Bresson, D. Catalano, and D. Pointcheval, "A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications," in *Proceedings of Advances in Cryptology (ASIACRYPT'03)*, pp. 37–54, Banff, AB, Canada, Nov. 2003.

[3] Z. J. Cao and L. H. Liu, "Comment on 'harnessing the cloud for securely outsourcing large-scale systems of linear equations'," *IEEE Transactions on Parallel Distributed Systems*, vol. 27, pp. DOI 10.1109/TPDS.2016.2531669, 2016.

[4] G. Castagnos and F. Laguillaumie, "Linearly homomorphic encryption from ddh," in *Proceedings of the Cryptographer's Track at the RSA Conference (CT-RSA'15)*, pp. 487–505, San Francisco, CA, USA, 2015.

[5] D. Catalano, A. Marcedone, and O. Puglisi, "Authenticating computation on groups: New homomorphic primitives and applications," in *Proceedings of Advances in Cryptology (ASIACRYPT'14)*, pp. 193–212, Kaoshiung, Taiwan, Dec. 2014.

[6] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[7] D. Choi, S. Choi, and D. Won, "Improvement of probabilistic public key cryptosystem using discrete logarithm," in *Proceedings of Information Security and Cryptology (ICISC'01)*, pp. 72–80, Banff, AB, Canada, Dec. 2001.

[8] D. Choi, S. Choi, and D. Won, "Paillier's cryptosystem revisited," in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*, pp. 206–214, Philadelphia, Pennsylvania, USA, Nov. 2001.

[9] I. Damgård and J. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Proceedings of Public Key Cryptography (PKC'01)*, pp. 119–136, Cheju Island, Korea, Feb. 2001.

[10] I. Damgård, J. Jurik, and J. Nielsen, "A generalization of paillier's public-key system with applications to electronic voting," *International Journal of Information Security*, no. 9, pp. 371–385, 2010.

[11] D. Galbraith, "Elliptic curve paillier schemes," *Journal of Cryptology*, vol. 15, no. 2, pp. 129–138, 2002.

[12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09)*, pp. 169–178, Bethesda, MD, USA, May 2009.

[13] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Compter and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[14] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[15] M. Joye and B. Libert, "Efficient cryptosystems from 2k-th power residue symbols," in *Proceedings of Advances in Cryptology (EUROCRYPT'13)*, pp. 76–92, Athens, Greece, May 2013.

[16] C. C. Lee, M. S. Hwang, and S. F. Tzeng, "A new convertible authenticated encryption scheme based on the elgamal cryptosystem," *International Journal of Foundamation Computer Science*, vol. 20, no. 2, pp. 351–359, 2009.

[17] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[18] C.W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[19] D. Naccache and J. Stern, "A new public key cryptosystem based on higher residues," in *Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS'98)*, pp. 546–560, San Francisco, CA, USA, Nov. 1998.

[20] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Proceedings of Advances in Cryptology (EUROCRYPT'98)*, pp. 308–318, Espoo, Finland, May 1998.

[21] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of Advances in Cryptology (EUROCRYPT'99)*, pp. 223–238, Prague, Czech Republic, May 1999.

[22] K. Sakurai and T. Takagi, "On the security of a modified paillier public-key primitive," in *Proceedings of 7th Australian Conference on Information Security and Privacy (ACISP'02)*, pp. 436–448, Melbourne, Australia, July 2002.

[23] B. Schoenmakers and P. Tuyls, "Efficient binary conversion for paillier encrypted values," in *Proceedings of Advances in Cryptology (EUROCRYPT'06)*, pp. 522–537, St. Petersburg, Russia, May 2006.

[24] C. Wang, K. Ren, J. Wang, and Q. Wang, "Harnessing the cloud for securely outsourcing large-scale systems of linear equations," *IEEE Transaction on Parallel Distributed Systems*, vol. 24, no. 6, pp. 1172–1181, 2013.

Zhengjun Cao is an associate professor with the Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in

Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Lihua Liu is an associate professor with the Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.