数理解析研究所講究録
第 1691 巻 2010 年 36-43

新しい代数的性質を持つ公開鍵暗号
Public-Key Encryption with New Algebraic Properties

平野 貴人* 田中 圭介*

Abstract

We first consider a variant of the Schmidt-Samoa–Takagi encryption scheme without losing additively homomorphic properties. We show that this variant is secure in the sense of IND-CPA under the decisional composite residuosity assumption, and of OW-CPA under the assumption on the hardness of factoring $n = p^2q$. Second, we introduce new algebraic properties "affine" and "pre-image restriction", which are closely related to homomorphicity. Intuitively, "affine" is a tuple of functions which have a special homomorphic property, and "pre-image restriction" is a function which can restrict the receiver to having information on the encrypted message. Then, we propose an encryption scheme with primitive power roots of unity in $(\mathbb{Z}/n^{s+1})^\times$. We show that our scheme has, in addition to the additively homomorphic property, the above algebraic properties. In addition to the properties, we also show that the encryption scheme is secure in the sense of OW-CPA and IND-CPA under new number theoretic assumptions.

Keywords: Paillier's encryption scheme, factoring, homomorphism, power roots of unity.

1 Introduction

Background. Homomorphicity is a useful algebraic property in cryptography, and it has been well-studied. For groups $G$ and $H$, a function $f : G \to H$ is (group) homomorphism if for $g, g' \in G$, $f(g) \circ_H f(g') = f(g \circ_G g')$, where $\circ_G$ and $\circ_H$ are the group operations over $G$ and $H$, respectively. From a mathematical point of view, this property means that $f$ preserves the group structure of $G$. From a cryptographic point of view, we can obtain a meaningful ciphertext by combining several ciphertexts without knowing the corresponding hidden messages nor the secret key. This property is useful to many cryptographic applications such as electronic voting, electronic cash, and so on.

Let $G$ be a subgroup of an integer residue ring. We call $f$ a multiplicative homomorphism if $\circ_G$ is the multiplication "×" over the integer residue ring. There exist many encryption schemes with multiplicatively homomorphic properties, for example, the RSA encryption scheme [6], the ElGamal encryption scheme [3]. We call $f$ an additive homomorphism if $\circ_G$ is the addition "+" over the integer residue ring. There also exist many encryption schemes with additively homomorphic properties, for example, the Goldwasser-Micali encryption scheme [4], the Paillier encryption scheme [5]. In particular, the Paillier encryption scheme has interesting structure and many mathematical advantages. Many variants of his scheme have been proposed.

Our Contribution. In this paper, we consider a variant of the Schmidt-Samoa–Takagi encryption scheme [7] without losing additively homomorphic properties, described as $\mathcal{E}(r, m) = r^{n^s}(1 + n^t)^m \bmod n^{s+1}$, where $m \in \mathbb{Z}/(n^{s-t+1}/p)$ is a message and $r \in (\mathbb{Z}/n)^\times$ is a random number. We show that this variant is secure in the sense of IND-CPA under the decisional composite residuosity assumption, and of OW-CPA under the assumption on the hardness of factoring $n = p^2q$.

We formalize the notions of general homomorphic properties. Then, by extending our variant, we propose an encryption scheme with primitive power roots of unity in $(\mathbb{Z}/n^{s+1})^\times$. We show that this extended encryption scheme satisfies, in addition to the additively homomorphic property, our proposed notions of general homomorphic properties. We define a computational and a decisional problems which are the factoring problem and the decisional composite residuosity problem with power roots of unity as additional infor-

*Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8552, Japan. {hirano6, keisuke}@is.titech.ac.jp.
This research was supported in part by NTT Information Sharing Platform Laboratories and JSPS Global COE program "Computationism as Foundation for the Sciences".

mation, respectively. We also show that our extended encryption scheme is secure in the sense of OW-CPA under the assumption on the hardness of the computational problem, and of IND-CPA under the assumption on the hardness of the decisional problem. In order to show that our scheme works, we analyze several properties on primitive power roots of unity in $(\mathbb{Z}/n)^\times$, and give an algorithm which finds them efficiently.

Related Works. In 1999, Paillier proposed a public-key encryption scheme, which has the additively homomorphic property [5]. He showed that the encryption scheme is secure in the sense of IND-CPA under the decisional composite residuosity assumption. However, it is not known whether the one-wayness is reduced to the problem of factoring $n = pq$.

Damgård and Jurik proposed a variant of the Paillier encryption scheme where the ciphertext space $(\mathbb{Z}/n^2)^\times$ is extended to $(\mathbb{Z}/n^{s+1})^\times$ [1]. Thereby, it can efficiently handle messages of arbitrary length in their scheme, although the public key and the secret key are fixed. The security of their variant is similar to that of the Paillier encryption scheme and it is not known whether the one-wayness is reduced to the problem of factoring $n = pq$. Their scheme can be applied to threshold cryptosystem and zero-knowledge protocols. They constructed an electronic voting scheme by using these protocols and their threshold variant[2].

Schmidt-Samoa and Takagi proposed another variant which employs modulus $n = p^2q$ instead of $n = pq$ [7], where p and q are primes with same length. The Schmidt-Samoa–Takagi function f is as follows:

$$\begin{array}{cccc} f: & (\mathbb{Z}/n)^\times \times \mathbb{Z}/n & \longrightarrow & (\mathbb{Z}/n^2)^\times \\ & (r, m) & \longmapsto & r^n(1 + mn) \bmod n^2, \end{array}$$

where m is a message and r is a random number. Their scheme is secure in the sense of not only IND-CPA under the decisional composite residuosity assumption, but also OW-CPA under the assumption on the hardness of factoring $n = p^2q$. They constructed trapdoor hash families based on the problem of factoring $n = p^2q$, by applying the encryption scheme. These hash families suitable for on-line/off-line or chameleon signatures schemes.

Organization. The organization of this paper is as follows. In Section 2, we give some definitions. In Section 3, we propose a variant of the Schmidt-Samoa–Takagi encryption scheme. In Section 4, we describe new algebraic properties and a construction of primitive power roots of unity in $(\mathbb{Z}/n^{s+1})^\times$. Then, we extend our variant with primitive power roots of unity.

2 Preliminaries

We denote $\{0, 1, \ldots, n-1\}$ by $\mathbb{Z}/n$, and its reduced residue class group by $(\mathbb{Z}/n)^\times$, namely, $(\mathbb{Z}/n)^\times = \{x \in \mathbb{Z}/n \mid \gcd(x, n) = 1\}$. For $g \in (\mathbb{Z}/n)^\times$, $\mathrm{ord}_n\, g$ is defined as the smallest positive integer e such that $g^e \equiv 1 \pmod{n}$.

We denote the set of positive real numbers by $\mathbb{R}^+$. We say that a function $\varepsilon : \mathbb{N} \longrightarrow \mathbb{R}^+$ is negligible if and only if for every polynomial p, there exists $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$, $\varepsilon(k) < \frac{1}{p(k)}$.

We denote the probability distribution on a set X by $x \leftarrow X$ and the uniform distribution by $x \overset{u}{\leftarrow} X$.

We review the definitions of public-key encryption schemes, of the one-wayness against the chosen plaintext attack (OW-CPA), and of the indistinguishability against the chosen plaintext attack (IND-CPA).

Definition 1 *A public-key encryption scheme* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *consists of the following three algorithms:*

Key Generation $\mathcal{K}(1^k)$**:** *The key generation algorithm* $\mathcal{K}$ *is a randomized algorithm that takes a security parameter k and returns a pair* (pk, sk) *of keys, a public key and a matching secret key.*

Encryption $\mathcal{E}(pk, r, m)$**:** *The encryption algorithm* $\mathcal{E}$ *is a randomized algorithm that takes the public key pk, a randomness r, and a plaintext m and returns a ciphertext c.*

Decryption $\mathcal{D}(sk, c)$**:** *The decryption algorithm* $\mathcal{D}$ *is a deterministic algorithm that takes the secret key sk and a ciphertext c and returns the corresponding plaintext m or a special symbol* $\perp$ *to indicate that the ciphertext is invalid.*

Definition 2 *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a public-key encryption scheme and* $\mathcal{A}$ *an adversary. We define an advantage of* $\mathcal{A}$ *via* $\mathbf{Adv}^{\mathrm{ow-cpa}}_{\Pi,\mathcal{A}}(k) = \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k); c \leftarrow \mathcal{E}(pk, r, m) : \mathcal{A}(pk, c) = m]$. *We say that* Π *is secure in the sense of OW-CPA if* $\mathbf{Adv}^{ow-cpa}_{\Pi,\mathcal{A}}(k)$ *is negligible in k, for any probabilistic polynomial-time adversary* $\mathcal{A}$.

Definition 3 *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a public-key encryption scheme and* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *an adversary. We define the advantage of* $\mathcal{A}$ *via* $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\Pi,\mathcal{A}}(k) =$

$|2\Pr[(pk, sk) \leftarrow \mathcal{K}(1^k); m_0, m_1, state \leftarrow \mathcal{A}_1(pk); b \overset{u}{\leftarrow} \{0,1\}; c \leftarrow \mathcal{E}(pk, r, m_b) : \mathcal{A}_2(m_0, m_1, c, state) = b] - 1|$. *We say that $\Pi$ is secure in the sense of IND-CPA if $\mathbf{Adv}^{ind\text{-}cpa}_{\Pi,\mathcal{A}}(k)$ is negligible in k, for any probabilistic polynomial-time adversary $\mathcal{A}$.*

3 A Variant of the Schmidt-Samoa–Takagi Encryption Scheme

Paillier proposed the public-key encryption scheme with the additively homomorphic property which can be applied to many cryptographic applications [5]. Several variants of the Paillier encryption scheme have been studied. In this section, we review the Schmidt-Samoa–Takagi encryption scheme which is a variant of the Paillier encryption scheme [7]. Furthermore, we show that our variant is as secure as the Schmidt-Samoa–Takagi encryption scheme.

The Schmidt-Samoa-Takagi encryption scheme is secure in the sense of IND-CPA under the decisional composite residuosity assumption, and of OW-CPA under the assumption on the hardness of factoring $n = p^2q$. The decisional composite residuosity assumption is that there is no polynomial-time algorithm that solves the following "the decisional composite residuosity problem" with non-negligible advantage.

Definition 4 *Let $n$ be a randomly chosen k-bit p^2q modulus. For a probabilistic polynomial-time algorithm $\mathcal{A}$, we define the following probabilities: $P_{Random} = \Pr[x \leftarrow (\mathbb{Z}/n^2)^\times : \mathcal{A}(n, x) = 1]$ and $P_{Residue} = \Pr[x \leftarrow (\mathbb{Z}/n)^\times : \mathcal{A}(n, x^n \bmod n^2) = 1]$. Then, we denote an advantage of $\mathcal{A}$ by $\mathbf{Adv}^{\mathrm{DCR}}_{\mathcal{A}}(n) = |P_{Random} - P_{Residue}|$.*

In this paper, we use the above definition by replacing $(\mathbb{Z}/n^2)^\times$ and $x^n \bmod n^2$ with $(\mathbb{Z}/n^{s+1})^\times$ and $x^{n^s} \bmod n^{s+1}$, respectively.

3.1 Our Encryption Function

We consider a variant of the Schmidt-Samoa–Takagi encryption scheme via the idea of Damgård and Jurik [1]. Let $n = p^2q$, where $p$ and $q$ are primes with same length. In addition, we introduce new parameters $s, t \in \mathbb{N}$ such that $s \geq t$ to the Schmidt-Samoa–Takagi function. Then, we define a function $f$ as follows:

$$\begin{array}{rccc} f: & (\mathbb{Z}/n)^\times \times \mathbb{Z}/n^s & \longrightarrow & (\mathbb{Z}/n^{s+1})^\times \\ & (r, m) & \longmapsto & r^{n^s}(1 + n^t)^m \bmod n^{s+1}, \end{array}$$

where $m$ is a message and $r$ is a random number. We note that our function coincides with the Schmidt-Samoa–Takagi function if $s = t = 1$. Obviously, our function is additive homomorphism in $m$. We give properties of $f$, which can help us to compute $f^{-1}$.

Lemma 5 *Let $s, t \in \mathbb{N}$ such that $t \leq s < p, q$. Then,*

1. $1 + an^s \equiv (1 + n^t)^{an^{s-t}} \pmod{n^{s+1}}$ *for* $a \in (\mathbb{Z}/n^{s+1})^\times$.

2. $\mathrm{ord}_{n^{s+1}}(1 + n^t) = n^{s-t+1}$, *that is,* $\langle 1 + n^t \rangle \simeq \mathbb{Z}/n^{s-t+1}$.

Lemma 6 *For $x, y \in (\mathbb{Z}/n)^\times$ and $s \geq 1$,*

$$x^{n^s} \equiv y^{n^s} \pmod{n} \iff x \equiv y \pmod{pq}.$$

Corollary 7 $\{x \in (\mathbb{Z}/n)^\times \mid x \equiv y^{n^s} \pmod{n}, y \in (\mathbb{Z}/n)^\times\}$ *is a subgroup of $(\mathbb{Z}/n)^\times$, whose the order is* $(p-1)(q-1)$. *Especially, the subgroup is equivalent to $\{x^{n^s} \bmod n \mid x \in (\mathbb{Z}/pq)^\times\}$.*

By Lemma 5, 6 and Corollary 7, we have the following theorem and corollary.

Theorem 8 $f(r, m) = f(r + ipq, m - (r^{-1} \bmod n^s)in^{s-t}pq + jn^{s-t+1})$ *for $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, n^{t-1}\}$, that is, $f$ is an $(n^{t-1}p)$-to-1 function.*

Corollary 9 *1. The restriction $f_r = f|_{(\mathbb{Z}/pq)^\times \times \mathbb{Z}/n^{s-t+1}}$ on $r$ is 1-to-1. Then f_r holds the following equation : $f_r(r_1, m_1)f_r(r_2, m_2) = f_r(r_1r_2 \bmod pq, m_1 + m_2 + (r_{pq}^{-1} \bmod n^s)ln^{s-t}pq \bmod n^{s-t+1})$, where $r_{pq} = r_1r_2 \bmod pq$ and $l \in \{1, 2, \ldots, p\}$ such that $r_1r_2 = r_{pq} + lpq \bmod n$.*

2. *The restriction $f_m = f|_{(\mathbb{Z}/n)^\times \times \mathbb{Z}/(n^{s+t-1}/p)}$ on $m$ is 1-to-1. Then f_m holds the following equation : $f_m(r_1, m_1)f_m(r_2, m_2) = f_m(r_1r_2 - lpq \bmod n, m_1 + m_2 \bmod (n^{s-t+1}/p))$, where $m_{pq} = m_1 + m_2 \bmod (n^{s-t+1}/p)$ and $l \in \{1, 2, \ldots, p\}$ such that $m_1 + m_2 = m_{pq} - (r_{pq}^{-1} \bmod n^s)ln^{s-t}pq \bmod n^{s-t+1}$.*

3.2 Our Encryption Scheme

In this section, we give a variant of the Schmidt-Samoa–Takagi encryption scheme by using our function in the previous section.

Our encryption scheme is described as follows. Note that $s$ and $t$ are public system parameters and given to the key generation, the encryption, the decryption algorithms.

Key Generation: Given a security parameter k, choose randomly a modulus $n = p^2q$ of k bits, where p, q have same length with $t \leq s < p, q$. Compute $d \equiv n^{-s} \pmod{(p-1)(q-1)}$ and $l \in \mathbb{Z}$ such that $2^l < n^{s-t+1}/p < 2^{l+1}$. Then, the public key is $pk = (n, l)$ and the secret key is $sk = (p, q, d)$.

Encryption: To encrypt a message $m \in \{0, 1\}^l$, choose $r \in (\mathbb{Z}/n)^\times$ at random and compute $\mathcal{E}(r, m)$, where $\mathcal{E} = f_m$, that is,

$$\mathcal{E}(r, m) = r^{n^s}(1 + n^t)^m \bmod n^{s+1}.$$

Decryption: To decrypt a ciphertext c, compute $r = c^d \bmod pq$, and $y = c(r^{-1})^{n^s} \bmod n^{s+1}$. Then, by using Algorithm **XDJ** which is described below, we obtain a message $m \in \{0, 1\}^l$ by

$$\mathcal{D}(c) \;=\; \mathbf{XDJ}(s, t, n, y, 1) \bmod (n^{s-t+1}/p).$$

We describe the decryption algorithm of our variant in detail. First, we extract $r = c^d \bmod pq$ with the secret key where $c = r^{n^s}(1 + n^t)^m \bmod n^{s+1}$ is a ciphertext. Second, we set $y = c(r^{-1})^{n^s} \bmod n^{s+1} = (1 + n^t)^m \bmod n^{s+1}$. To decrypt a message $m \in \mathbb{Z}/(n^{s-t+1}/p)$ from y, we need to compute $x \in \mathbb{Z}/n^{s-t+1}$ such that $y = (1 + n^t)^x \bmod n^{s+1}$. We can find x efficiently via the idea by Damgård and Jurik [1], although it is hard to solve the discrete logarithm in general. We modify their idea as follows.

Now, we know $y = (1 + an^t)^m \bmod n^{s+1}$ and $a = 1$. Then, for $(1 + an^t)^x \bmod n^{s+1}$, we know the following equation:

$$\begin{aligned}(1 + an^t)^x &= 1 + \binom{x}{1}an^t + \binom{x}{2}a^2n^{2t} + \\ &\qquad \cdots + \binom{x}{\delta}a^\delta n^{t\delta} + n^{(\delta+1)t}(\cdots) \\ &\equiv 1 + \binom{x}{1}an^t + \binom{x}{2}a^2n^{2t} + \\ &\qquad \cdots + \binom{x}{\delta}a^\delta n^{\delta t} \pmod{n^{s+1}},\end{aligned}$$

where $\delta \in \mathbb{N}$ such that $\delta t < s+1 \leq (\delta+1)t$. In particular, $\delta = \lceil \frac{s}{t} \rceil - 1$.

In the first step, we compute $x_1 = x \bmod n^t$ as follows. By the above equation $y \equiv 1 + \binom{x_1}{1}an^t \equiv 1 + x_1an^t \pmod{n^{2t}}$, $x_1 = (a^{-1} \bmod n^{2t})\frac{(y \bmod n^{2t})-1}{n^t} \bmod n^t = (a^{-1} \bmod n^{2t})L_{n^t}(y \bmod n^{2t}) \bmod n^t$, where $L_{n^t}(x) = \frac{x-1}{n^t}$. In the second step, we compute $x_2 = x \bmod n^{2t}$ as follows. Since there exists $k \in \mathbb{Z}/n^t$ such that $x_2 = x_1 + kn^t$,

$$\begin{aligned} y &\equiv 1 + \binom{x_2}{1}an^t + \binom{x_2}{2}a^2n^{2t} \pmod{n^{3t}} \\ &\equiv 1 + x_2an^t + \binom{x_1 + kn^t}{2}a^2n^{2t} \pmod{n^{3t}} \\ &\equiv 1 + x_2an^t + \binom{x_1}{2}a^2n^{2t} \pmod{n^{3t}},\end{aligned}$$

therefore $x_2 = (a^{-1} \bmod n^{3t})\frac{(y \bmod n^{3t})-1}{n^t} - \binom{x_1}{2}an^t \bmod n^{2t} = (a^{-1} \bmod n^{3t})L_{n^t}(y \bmod n^{3t}) - \binom{x_1}{2}an^t \bmod n^{2t}$.

Generally, for $1 \leq i \leq \delta$, we use x_{i-1} to compute $x_i = x \bmod n^{it}$ as follows. There exists $k \in \mathbb{Z}/n^t$ such that $x_i = x_{i-1} + kn^{(i-1)t}$,

$$\begin{aligned} y &\equiv 1 + \binom{x_i}{1}an^t + \binom{x_i}{2}a^2n^{2t} + \\ &\qquad \cdots + \binom{x_i}{i}a^in^{it} \pmod{n^{(i+1)t}} \\ &\equiv 1 + x_ian^t + \binom{x_{i-1} + kn^{(i-1)t}}{2}a^2n^{2t} + \\ &\qquad \cdots + \binom{x_{i-1} + kn^{(i-1)t}}{i}a^in^{it} \pmod{n^{(i+1)t}} \\ &\equiv 1 + x_ian^t + \binom{x_{i-1}}{2}a^2n^{2t} + \\ &\qquad \cdots + \binom{x_{i-1}}{i}a^in^{it} \pmod{n^{(i+1)t}}.\end{aligned}$$

Therefore, we can compute x_i with the value $L_{n^t}(y \bmod n^{(i+1)t})$, since

$$\begin{aligned} x_i &= (a^{-1} \bmod n^{(i+1)t})\frac{(y \bmod n^{(i+1)t}) - 1}{n^t} \\ &\qquad - \binom{x_{i-1}}{2}an^t - \cdots - \binom{x_{i-1}}{i}a^{i-1}n^{(i-1)t} \bmod n^{it} \\ &= (a^{-1} \bmod n^{(i+1)t})L_{n^t}(y \bmod n^{(i+1)t}) \\ &\qquad - \sum_{j=2}^{i}\binom{x_{i-1}}{j}a^{j-1}n^{(j-1)t} \bmod n^{it}.\end{aligned}$$

This equation leads to Algorithm **XDJ**.

Algorithm 10 *Let $L_{n^t}(x) = \frac{x-1}{n^t}$. The following algorithm takes $y \in (\mathbb{Z}/n^{s+1})^\times$, $a \in (\mathbb{Z}/n^{s+1})^\times$, and $s, t \in \mathbb{N}$ such that $t \leq s$, and computes $x \in \mathbb{Z}/n^{s-t+1}$ such that*

$y = (1 + an^t)^x \bmod n^{s+1}$:

```
XDJ(s, t, n, y, a)
    $x := 0$
    $\delta := \lceil \frac{s}{t} \rceil - 1$
    for ($i := 1$ to $\delta$)
        $t_1 := (a^{-1} \bmod n^{(i+1)t})$
                $\times L_{n^t}(y \bmod n^{(i+1)t}) \bmod n^{it}$
        $t_2 := x$
        for ($j := 2$ to $i$)
            $x := x - 1$
            $t_2 := t_2 \times x \bmod n^{it}$
            $t_1 := t_1 - \frac{t_2 \times (an^t)^{j-1}}{j!} \bmod n^{it}$
        $x := t_1$
    return $x \bmod n^{s-t+1}$.
```

We can check whether $y$ is a valid form $(1 + an^t)^x$, since $(1 + an^t)^x - 1$ is divided by n^t. We note that Algorithm **XDJ** coincides with that by Damgård and Jurik when $t = a = 1$, and works for any $n \in \mathbf{N}$ if there exists $x$.

We give the following theorem on the security for our scheme.

Theorem 11 *For our scheme, the following securities hold.*

1. *Our scheme is secure in the sense of OW-CPA under the assumption on the hardness of factoring $n = p^2q$.*
2. *Our scheme is secure in the sense of IND-CPA under the decisional composite residuosity assumption by replacing $(\mathbf{Z}/n^2)^\times$ and $x^n \bmod n^2$ with $(\mathbf{Z}/n^{s+1})^\times$ and $x^{n^s} \bmod n^{s+1}$, respectively.*

4 Constructions Based on Primitive Power Roots of Unity

In this section, we first introduce new algebraic properties related to the homomorphic property. Second, we describe some facts on primitive power roots of unity, and apply them to our encryption function. Then, we propose an extended encryption scheme which has the above algebraic properties.

4.1 New Algebraic Properties

In this section, we formalize the notion of a general homomorphic property as follows: Let $f_1, f_2, \ldots, f_k, f$ be functions, and $*, g$ polynomial-time computable operations. For $m_1, m_2, \ldots, m_k$, we consider $f_1(m_1) * f_2(m_2) * \cdots * f_k(m_k) = f(g(m_1, m_2, \ldots, m_k))$. These functions do not always have common domain or common range. For example, a multiplicative homomorphism can be expressed by $f_1 = f_2 = \cdots = f_k = f$ and $g(a_1, a_2, \ldots, a_k) = a_1 \times a_2 \times \cdots \times a_k$. With this formalization, we consider two properties. A tuple $(\{f_1, f_2, \ldots, f_k\}, f)$ of functions is called "affine with $x_1, x_2, \ldots, x_k$" if $f_1(m_1) * f_2(m_2) * \cdots * f_k(m_k) = f(x_1m_1 + x_2m_2 + \cdots + x_km_k)$, that is, $g(m_1, m_2, \ldots, m_k) = x_1m_1 + x_2m_2 + \cdots + x_km_k$. An additive homomorphism can be considered as the special case. A tuple of $(\{f_1, f_2, \ldots, f_k\}, f)$ of functions is called "pre-image restriction with modulo $n$" if $m = m_1 = m_2 = \cdots = m_k$ and $f_1(m) * f_2(m) * \cdots * f_k(m) = f(m \bmod n)$, that is, $g(m, m, \ldots, m) = m \bmod n$.

Definition 12 *A tuple $(\{f_1, f_2, \ldots, f_k\}, f)$ of functions has the property of affine with $x_1, x_2, \ldots, x_k$ if for $m_1, m_2, \ldots, m_k$, $f_1(m_1) * f_2(m_2) * \cdots * f_k(m_k) = f(x_1m_1 + x_2m_2 + \cdots + x_km_k)$.*

Definition 13 *A tuple of functions $(\{f_1, f_2, \ldots, f_k\}, f)$ has the property of pre-image restriction with modulo $n$ if for $m$, $f_1(m) * f_2(m) * \cdots * f_k(m) = f(m \bmod n)$.*

4.2 Our Extended Encryption Function

In order to extend our function $f$ in Section 3.1, we introduce primitive power roots of unity in $(\mathbf{Z}/n^{s+1})^\times$ to $f$.

At first, we give the definition of primitive power roots of unity in the integer residue ring.

Definition 14 *Let $n$ and $\ell$ be positive integers. $w_\ell \in (\mathbf{Z}/n)^\times$ is a primitive $\ell$-th root of 1 in $(\mathbf{Z}/n)^\times$ if $\mathrm{ord}_n\, w_\ell = \ell$.*

In order to show existence conditions and constructions of primitive power roots of unity, we give some facts on primitive power roots of unity in $(\mathbf{Z}/n^{s+1})^\times$ (See [8, Section 6.5]).

Lemma 15 *For $\ell \in \mathbf{N}$, let $p$ be an odd prime such that $\ell \mid p - 1$. Then, there exist $\varphi(\ell)$ primitive $\ell$-th roots of 1 in $(\mathbf{Z}/p)^\times$, where $\varphi$ is the Euler phi-function, and we* *can compute them efficiently if we know prime factors of $p - 1$. In particular, for a generator g of $(\mathbb{Z}/p)^\times$, $g^{(p-1)/\ell} \bmod p$ is a primitive ℓ-th root of 1 in $(\mathbb{Z}/p)^\times$.*

Now, we use primitive ℓ-th roots of 1 in $(\mathbb{Z}/p)^\times$ to those in $(\mathbb{Z}/n^{s+1})^\times$ by employing the Chinese Remainder Theorem, where $n = p^2q$ and $s \in \mathbb{N}$ such that $s < p, q$. We give the following important lemma (see e.g. [8, Section 6.5]).

Lemma 16 *Let p and q be distinct odd primes, and e and e' positive integers.*

1. *$(\mathbb{Z}/p^e)^\times$ is a cyclic group. In particular, $|(\mathbb{Z}/p^e)^\times| = p^{e-1}(p-1)$.*
2. *For a group $(\mathbb{Z}/p^eq^{e'})^\times$, $\max_{g\in(\mathbb{Z}/p^eq^{e'})^\times}\{\mathrm{ord}_{p^eq^{e'}}\, g\} = \mathrm{lcm}(|(\mathbb{Z}/p^e)^\times|, |(\mathbb{Z}/q^{e'})^\times|) = \mathrm{lcm}(p^{e-1}(p-1), q^{e'-1}(q-1))$.*

We can efficiently compute a generator g of $(\mathbb{Z}/p^{2s+2})^\times$ using the Hensel lifting due to Lemma 16 if we know prime factors of $p - 1$. Similarly, we can compute a generator h of $(\mathbb{Z}/q^{s+1})^\times$ efficiently. From g and h, we can find an element $w \in (\mathbb{Z}/n^{s+1})^\times$ such that $\mathrm{ord}_{n^{s+1}}\, w = \mathrm{lcm}(p^{2s+1}(p-1), q^s(q-1))$, by using the Chinese Remainder Theorem. Now, let $p-1 = \ell p'$, $q-1 = \ell q'$, and $\gcd(p-1, q-1) = \ell$, where $p', q' \in \mathbb{N}$. Let $w_\ell = w^{(\mathrm{ord}_{n^{s+1}}\, w)/\ell} \bmod n^{s+1}$. Then, w_ℓ is a primitive ℓ-th root of 1 in $(\mathbb{Z}/n^{s+1})^\times$ since $\mathrm{ord}_{n^{s+1}}\, w = p^{2s+1}q^sp'q'\ell$. Thus, we can compute a primitive ℓ-th root of 1 efficiently.

Let W_ℓ be the set of ℓ-th roots of 1 in $(\mathbb{Z}/n^{s+1})^\times$. The set of w_ℓ constructed by the above computation of primitive ℓ-th roots of 1 in $(\mathbb{Z}/n^{s+1})^\times$ is a subset of W_ℓ. We define this subset as S_ℓ. In other words,

$$S_\ell = \{w_\ell \in W_\ell \mid \mathrm{ord}_{p^{2s+2}}\, w_\ell = \mathrm{ord}_{q^{s+1}}\, w_\ell = \ell\}.$$

Remark 17 *If $\gcd(\ell, (p-1)(q-1)) = 1$, we see that there exists no primitive ℓ-th root of 1: In the RSA encryption scheme [6], the encryption function $f(X) = X^e \bmod n$, where the exponent e is relatively prime to $\varphi(n) = (p-1)(q-1)$, is a permutation on $(\mathbb{Z}/n)^\times$. So is on $(\mathbb{Z}/p)^\times$ and $(\mathbb{Z}/q)^\times$ by the Chinese Remainder Theorem. Hence, for all $x \in (\mathbb{Z}/n)^\times$, there exists only one e-th root, that is, the e-th root of 1 is 1 in $(\mathbb{Z}/n)^\times$.*

Factoring-based cryptographic schemes are often instantiated by choosing n to be the product of two strong primes (we note that $p \in \mathbb{N}$ is a strong prime if p is prime and $p = 2p' + 1$, where p' is also prime). It is well-known that strong primes have resistance against factoring attacks which depend on the structure of primes. Such attacks include the $p - 1$ method and the elliptic curve method. However, since ℓ is limited to 2 or p' for a strong prime p, there are only g_2, $g_{p'}$ in $(\mathbb{Z}/p)^\times$ as primitive ℓ-th roots of 1. We consider to use the following primes with many power roots of unity in $(\mathbb{Z}/p)^\times$, called "semi ℓ-smooth primes".

Definition 18 *For $\ell \in 2\mathbb{N}$, a prime $p \in \mathbb{N}$ is semi ℓ-smooth if $p = \ell p' + 1$, where p' is prime such that $p' > \ell$.*

In our extended encryption function and scheme, we require that ℓ is constant and much smaller than p', in order to resist against factoring attacks mentioned above. We do not know whether the number of the primes above is infinite. However, we assume that there exist infinite number of semi ℓ-smooth primes for any $\ell \in \mathbb{N}$. Henceforth in this paper, we assume that p and q are semi ℓ-smooth prime.

For $i \in \{1, 2, \ldots, \ell\}$, we define an extended encryption function f_i with a primitive ℓ-th root of 1 in $(\mathbb{Z}/n^{s+1})^\times$ as follows:

$$\begin{array}{rccc} f_i: & (\mathbb{Z}/n)^\times \times \mathbb{Z}/n^s & \longrightarrow & (\mathbb{Z}/n^{s+1})^\times \\ & (r, m) & \longmapsto & r^{n^s}(1 - w_\ell^i n)^m \bmod n^{s+1}, \end{array}$$

where m is a message, r is a random number, and w_ℓ is a primitive ℓ-th root of 1 in $(\mathbb{Z}/n^{s+1})^\times$. We note that our extended encryption function is similar to the Schmidt-Samoa–Takagi function if $s = 1$ and $i = \ell$, since $w_\ell^\ell \equiv 1 \pmod{n^{s+1}}$. In addition, the extended encryption function is considered as $t = 1$. Obviously, our function is additive homomorphism in m. We give the following property on f_i.

Corollary 19 *Let $s \in \mathbb{N}$ and $a \in (\mathbb{Z}/n^{s+1})^\times$. Then, $\mathrm{ord}_{n^{s+1}}\,(1 + an) = n^s$, that is, $\langle 1 + an\rangle \simeq \mathbb{Z}/n^s$.*

We see that $\mathrm{ord}_{n^{s+1}}\,(1 - w_\ell^i n) = n^s$ since w_ℓ^i is relatively prime to n for any i. Therefore, for any i, we obtain the properties similar to Theorem 8 and Corollary 9.

Theorem 20 *For any $i \in \{1, 2, \ldots, \ell\}$,*

1. *$f_i(r, m) = f_i(r + jpq, m - (r^{-1} \bmod n^s)jpqn^{s-1})$ for $j \in \{1, 2, \ldots, p\}$, that is, f_i is a p-to-1 function.*
2. *The restriction $f_{i,r} = f_i|_{(\mathbb{Z}/pq)^\times \times \mathbb{Z}/n^s}$ on r is 1-to-1. Then $f_{i,r}$ holds the following equation:*

$f_{i,r}(r_1, m_1) f_{i,r}(r_2, m_2) = f_{i,r}(r_1 r_2 \bmod pq, m_1 + m_2 + (r_{pq}^{-1} \bmod n^s) lpq \bmod n^s)$, *where* $r_{pq} = r_1 r_2 \bmod pq$ *and* $l \in \{1, 2, \ldots, p\}$ *such that* $r_1 r_2 = r_{pq} + lpq \bmod n$.

3. *The restriction* $f_{i,m} = f_i|_{(\mathbf{Z}/n)^\times \times \mathbf{Z}/(n^s/p)}$ *on* m *is* 1-*to*-1. *Then* $f_{i,m}$ *holds the following equation:* $f_{i,m}(r_1, m_1) f_{i,m}(r_2, m_2) = f_{i,m}(r_1 r_2 - lpq \bmod n, m_1 + m_2 \bmod (n^s/p))$, *where* $m_{pq} = m_1 + m_2 \bmod (n^s/p)$ *and* $l \in \{1, 2, \ldots, p\}$ *such that* $m_1 + m_2 = m_{pq} - (r_{pq}^{-1} \bmod n^s) lpq \bmod n^{s-t+1}$.

4.3 Our Extended Encryption Scheme

We propose a concrete scheme based on our extended encryption function f_i. We describe our extended encryption scheme as follows. Note that s and ℓ are public system parameters and given to the key generation, the encryption, the decryption algorithms.

Key Generation: Given a security parameter k, choose randomly a modulus $n = p^2 q$ of k bits, where p, q are semi ℓ-smooth prime such that $p \mid q - 1$ and $q \mid p - 1$ with the same length, and $\ell \leq s < p, q$. Compute $d \equiv n^{-s} \pmod{(p-1)(q-1)}$, $l \in \mathbf{Z}$ such that $2^l < n^s/p < 2^{l+1}$ and a primitive ℓ-th root $w_\ell \in S_\ell$ of 1 in $(\mathbf{Z}/n^{s+1})^\times$. Then, the public key is $pk = (n, l, w_\ell)$ and the secret key is $sk = (p, q, d)$.

Encryption: To encrypt a message $m \in \{0, 1\}^l$, choose $i \in \{1, 2, \ldots, \ell\}$ and randomly $r_i \in (\mathbf{Z}/n)^\times$, and compute $\mathcal{E}_i(r_i, m)$, where $\mathcal{E}_i = f_{i,m}$, that is,

$$c_i = \mathcal{E}_i(r_i, m) = r_i^{n^s}(1 - w_\ell^i n)^m \bmod n^{s+1}.$$

Then, the ciphertext is (c_i, i).

Decryption: To decrypt c_i, compute $r = c_i^d \bmod pq$ and $y = c_i (r^{-1})^{n^s} \bmod n^{s+1}$. Then, by using Algorithm **XDJ**, we obtain a message $m \in \{0, 1\}^l$ by

$$\mathcal{D}((c_i, i)) = \mathbf{XDJ}(s, 1, n, y, -w_\ell^i) \bmod (n^s/p).$$

Obviously, $\mathcal{E}_i$ has the additively homomorphic property, for any i.

Now, we show the security proofs of OW-CPA and IND-CPA. However, it might be hard to compute w_ℓ from n with no information on p or q. That is, we cannot prove in a similar fashion of the proof for Theorem 11.

Here, we consider the following computational problem, denoted by the factoring problem with power roots, which is not harder than the standard factoring problem.

Definition 21 *Let* n *be a randomly chosen* k*-bit* $p^2 q$ *modulus, where* p *and* q *are semi* ℓ*-smooth prime. For a probabilistic polynomial-time algorithm* $\mathcal{A}$, *we denote an advantage of* $\mathcal{A}$ *by*

$$\Pr[w_\ell \leftarrow S_\ell : \mathcal{A}(n, w_\ell, \ell) = p],$$

where S_ℓ *is described in Section 4.2.*

In addition to the computational problem, we can also consider a decisional problem, that is, the decisional composite residuosity problem with additional information of w_ℓ, denoted by the decisional composite residuosity problem with power roots. Then, in a similar fashion of Theorem 11, we can show the security properties on OW-CPA and IND-CPA.

Theorem 22 *For any* $i \in \{1, 2, \ldots, \ell\}$, *the following securities hold.*

1. *Our extended encryption scheme is secure in the sense of OW-CPA under the assumption on the hardness of factoring* $n = p^2 q$ *with* w_ℓ.
2. *Our extended encryption scheme is secure in the sense of IND-CPA under the assumption on the hardness of the decisional composite residuosity problem with* w_ℓ, *by replacing* $(\mathbf{Z}/n^2)^\times$ *and* $x^n \bmod n^2$ *with* $(\mathbf{Z}/n^{s+1})^\times$ *and* $x^{n^s} \bmod n^{s+1}$, *respectively.*

In addition to the security proofs, our extended encryption scheme satisfies the algebraic properties "affine" and "pre-image restriction". Let $F_t(r, m) = r^{n^s}(1 - n^t)^m \bmod n^{s+1}$, which is the same as the encryption function described at Section 3.1.

Theorem 23 *For the functions* $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_\ell$, *the following properties hold:*

1. *For all* $i, j, k \in \{1, 2, \ldots, \ell\}$, *there exist* $x_{i,k}$ *and* $x_{i,j}$ *such that* $(\{\mathcal{E}_i, \mathcal{E}_j\}, \mathcal{E}_k)$ *is an affine tuple with* $x_{i,k}$ *and* $x_{j,k}$ *on* m, *that is, for all* $r_i, r_j \in (\mathbb{Z}/n)^\times$ *and* $m_i, m_j \in \mathbb{Z}/(n^s/p)$, $\mathcal{E}_i(r_i, m_i)\mathcal{E}_j(r_j, m_j) = \mathcal{E}_k(r_i r_j, x_{i,k} m_i + x_{j,k} m_j)$, *where* $x_{a,b} \in \mathbf{Z}/n^s$ *such that* $1 - w_\ell^a n \equiv (1 - w_\ell^b n)^{x_{a,b}} \pmod{n^{s+1}}$. *In particular, we can compute* $x_{i,k}$ *and* $x_{j,k}$, *efficiently.*
2. *For all* $t \in \mathbb{N}$ *such that* $t \mid \ell$, $(\{\mathcal{E}_\delta, \mathcal{E}_{2\delta}, \ldots, \mathcal{E}_{t\delta}\}, F_t)$ *is a pre-image restriction modulo* n^{s-t+1} *tuple on* m, *where* $\delta = \ell/t$, *that is, for all* $r_\delta, r_{2\delta}, \ldots, r_{t\delta} \in (\mathbf{Z}/n)^\times$ *and*

$m \in \mathbb{Z}/n^s$, $\mathcal{E}_\delta(r_\delta, m)\mathcal{E}_{2\delta}(r_{2\delta}, m)\cdots\mathcal{E}_{t\delta}(r_{t\delta}, m) = F_t(r_\delta r_{2\delta}\cdots r_{t\delta}, m \bmod n^{s-t+1})$. *In particular,* $\mathcal{E}_\delta(r_\delta, m)\ \mathcal{E}_{2\delta}(r_{2\delta}, m)\cdots\mathcal{E}_{t\delta}(r_{t\delta}, m) = F_t(r_\delta r_{2\delta}\cdots r_{t\delta}, m)$.

Note that we can also construct a scheme based on the Damgård–Jurik encryption scheme [1] instead of the Schmidt-Samoa–Takagi scheme, although we do not know whether the one-wayness is reduced to the problem of factoring $n = pq$.

References

[1] I. Damgård and M. Jurik. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. *PKC 2001, LNCS*, 1992:119–136, 2001.

[2] I. Damgård and M. Jurik. A Length-Flexible Threshold Cryptosystem with Applications. *ACISP 2003, LNCS*, 2727:350–364, 2003.

[3] T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on information Theory*, 31(4):469–472, 1985.

[4] S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and Systems Sciences*, 28(2):270–299, 1984.

[5] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *EUROCRYPT'99, LNCS*, 1592:223–238, 1999.

[6] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[7] K. Schmidt-Samoa and T. Takagi. Paillier's Cryptosystem Modulo p^2q and Its Applications to Trapdoor Commitment Schemes. *Mycrypt 2005, LNCS*, 3715:296–313, 2005.

[8] V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge Unversity Press, 2005.