ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

A Variant of the Schmidt-Takagi Encryption Scheme

Takato Hirano, Koichiro Wada, and Keisuke Tanaka

February 2008, C–252

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

A Variant of the Schmidt-Takagi Encryption Scheme

Takato Hirano, Koichiro Wada, and Keisuke Tanaka

Dept. of Mathematical and Computing Sciences
Tokyo Institute of Technology
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{hirano6, wada4, keisuke}@is.titech.ac.jp

February 28, 2008

Abstract

Schmidt and Takagi proposed a variant of the Paillier encryption scheme which employs modulus $n = p^2q$ [16]. Their scheme has a good property that the one-wayness is under the factoring assumption, and has an additively homomorphic property. Their scheme can be applied to trapdoor commitment and on-line/off-line signature.
In this paper, we propose a new variant of the Schmidt-Takagi encryption scheme described as $\mathcal{E}_t(r, m) = r^{n^s}(1 + mn^t) \bmod n^{s+1}$, where n, s, t are the public key, m a message, and r a random number. Our scheme has the one-wayness under the chosen plaintext attack based on the factoring problem, and the indistinguishability under the chosen plaintext attack based on the desicional composite residuosity problem.
Our scheme implies the Schmidt-Takagi encryption scheme when $s = t = 1$. Compared with the Damgård-Jurik encryption scheme, although the modulus of our schemes employs $n = p^2q$ (their scheme employs $n = pq$), the encryption and decryption speed of our scheme is faster than that of their scheme.
Furthermore, we get that $\mathcal{E}_t$ is additively homomorphic in m if $t \geq \lceil (s+1)/2 \rceil$. In addition, by adding a parameter t we have some properties closely related to homomorphic, which can be applied to cryptographic applications [9].

Keywords: Paillier encryption scheme, additively homomorphic, provable security.

1 Introduction

Fundamental requirements for a secure public-key encryption scheme are the one-wayness and the indistinguishability against the chosen plaintext attack (IND-CPA). It is important that the securities it is reduced to well-studied problems such as the factoring problem and the discrete logarithm problem.

In 1999, Paillier proposed a public-key encryption scheme, which is IND-CPA based on the decisional composite residuosity problem [12]. It is not known whether the one-wayness is equivalent to the factoring assumption[1]. The encryption scheme $\mathcal{E}$ has an additively homomorphic property: $\mathcal{E}(r_1, m_1)\mathcal{E}(r_2, m_2) = \mathcal{E}(r_1 r_2, m_1 + m_2)$ where r_1, r_2 are random numbers and m_1, m_2 are messages, and has many cryptographic applications.

Damgård and Jurik proposed its variant which can be applied to threshold cryptosystems and electronic votings [6]. The security is similar to that of Paillier's encryption scheme.

Schmidt and Takagi proposed another variant which employs modulus $n = p^2q$ [16]. Their scheme has a good property that the one-wayness is under the factoring assumption, and can be applied to trapdoor commitment and on-line/off-line signature.

[1] For its bit security, see [2]

Other variants of the Paillier encryption scheme have been studied, for example, based on the factoring assumption [15, 8, 10], IND-CCA [13, 5], threshold [6, 7], RSA-type [3, 4, 14], double trapdoor decryption [1] and so on.

In this paper, we propose a new variant of the Schmidt-Takagi encryption scheme described as $\mathcal{E}(m,r) = r^{n^s}(1+mn) \bmod n^{s+1}$, where n, s are the public key, m a message, and r a random number. Our scheme has the one-wayness under the chosen plaintext attack based on the factoring problem, and the indistinguishability under the chosen plaintext attack based on the decisional composite residuosity problem.

However, unlike several Paillier-based schemes [12, 6, 16], our scheme does not have additively homomorphic. In order to solve this situation, by adding a parameter $t \in \mathbb{N}$ we modify our encryption function as follows: $\mathcal{E}'(r,m) = r^{n^s}(1+mn^t) \bmod n^{s+1}$, where n, s, t are the public key, m a message, and r a random number. Then, we obtain that $\mathcal{E}'$ has additively homomorphic in m if $t \geq \lceil (s+1)/2 \rceil$. In addition, by adding a parameter t we have some properties closely related to homomorphic, which can be applied to cryptographic applications [9].

Our scheme implies the Schmidt-Takagi encryption scheme when $s = 1$ or $s = t = 1$. Compared with the Damgård-Jurik encryption scheme, although the modulus of our schemes employs $n = p^2q$ (their scheme employs $n = pq$), the encryption and decryption speed of our scheme is faster than that of their scheme.

This paper organized as follows: In Section 2, we briefly recall the Schmidt-Takagi encryption scheme. In Section 3, we propose a variant of the Schmidt-Takagi encryption scheme, and show its securities, that is, the one-wayness and the indistinguishability against chosen plaintext attack. In Section 4, we propose a variant of our scheme, then show that the encryption scheme is additively homomorphic. In Section 5, we conclude and provide some open problems.

2 Preliminaries

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

Now, we briefly recall the Schmidt-Takagi's encryption scheme whose the one-wayness is reduced to the factoring assumption [16].

Let n be the product of p square and q, where p and q are large primes such that $|p| = |q|$ (that is $n = p^2q$)[2]. The encryption function $\mathcal{E}$ is the following function:

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

The function satisfies that $\mathcal{E}(r,m) = \mathcal{E}(r+ipq, m-r^{-1}ipq)$ for $i \in \mathbb{Z}$, which means that $\mathcal{E}$ is p-to-1. Then we obtain the following properties:

- The restriction $\mathcal{E}_r = \mathcal{E}|_{(\mathbb{Z}/pq)^\times \times \mathbb{Z}/n}$ is 1-to-1. Then it has a group homomorphic with respect to the group operation $\circ_r : (r_1, m_1) \circ_r (r_2, m_2) = (r_1 r_2 \bmod pq, m_1 + m_2 + l r_{pq}^{-1} pq \bmod n)$, where r_{pq} is $r_1 r_2 \bmod pq$ and l is a integer between 0 and p such that $r_1 r_2 = r_{pq} + lpq \bmod n$.
- The restriction $\mathcal{E}_m = \mathcal{E}|_{(\mathbb{Z}/n)^\times \times \mathbb{Z}/pq}$ is 1-to-1. Then it has a group homomorphic with respect to the group operation $\circ_m : (r_1, m_1) \circ_m (r_2, m_2) = (r_1 r_2 - lpq \bmod n, m_1 + m_2 \bmod pq)$, where m_{pq} is $m_1 + m_2 \bmod pq$ and l is a integer between 0 and p such that $m_1 + m_2 = m_{pq} - l r_{pq}^{-1} pq \bmod n$.

As mentioned above, we see that $\mathcal{E}_r$ is multiplicatively homomorphic in r, and $\mathcal{E}_m$ additively homomorphic in m.

[2]The first approach to the form $n = p^2q$ in encryption schemes appeared in [11].

3 Our Encryption Scheme

We propose a variant of the Schmidt-Takagi encryption scheme, replacing computations modulo n^2 with computations modulo n^{s+1} for $s > 1$ and plaintext space $\mathbb{Z}/n$ with $\mathbb{Z}/n^s$, where $n = p^2q$. Before introducing our public-key encryption scheme, we prove several mathematical foundations by techniques of Schmidt and Takagi.

Definition 1. *We define* $Residue_n[n^s]$ *by* $\{x \in (\mathbb{Z}/n)^\times \mid x \equiv y^{n^s} \pmod{n}, y \in (\mathbb{Z}/n)^\times\}$.

Then we prove the following theorem:

Theorem 2. *For* $x, y \in (\mathbb{Z}/n)^\times$ *and* $s \geq 1$,

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

Proof. ("⇒") Since there exists a integer k such that $x^{n^s} = y^{n^s} + kp^2q$, it holds that $x^{n^s} \equiv y^{n^s} \pmod{pq}$. Therefore, we obtain $x \equiv y \pmod{pq}$ because $\phi(pq) = (p-1)(q-1)$ and $\gcd(n^s, (p-1)(q-1)) = 1$.

("⇐") There exists a integer k such that $y = x+kpq$. Hence $y^{n^s} = (x+kpq)^{n^s} = \sum_{i=0}^{n^s} \binom{n^s}{i} x^{n^s-i}kpq^i = x^{n^s} + n(x^{n^s-1}kpq + \cdots) \equiv x^{n^s} \pmod{n}$. □

Corollary 3. $Residue_n[n^s]$ *is a subgroup of* $(\mathbb{Z}/n)^\times$*, whose the order is* $(p-1)(q-1)$*. Especially,* $Residue_n[n^s] = \{x^{n^s} \bmod n \mid x \in (\mathbb{Z}/pq)^\times\}$

We now show the following properties which are closed to the Schmidt-Takagi's encryption function [16]:

Theorem 4. *Let* f *be the following function:*

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

Then,

- $f(r, m) = f(r + ipq, m - n^{s-1}r^{-1}ipq)$ *for* $i \in \mathbb{Z}$*, that is p-to-*1.
- *The restrictions* $f_r = f|_{(\mathbb{Z}/pq)^\times \times \mathbb{Z}/n^s}$ *and* $f_m = f|_{(\mathbb{Z}/n)^\times \times \mathbb{Z}/(n^s/p)}$ *are* 1*-to-*1.

Proof.

$$\begin{aligned} f(r + ipq, m) &\equiv (r + ipq)^{n^s}(1 + mn) \pmod{n^{s+1}} \\ &\equiv (r^{n^s} + n^s r^{n^s-1} ipq + n^{s+1}(\cdots))(1 + mn) \\ &\equiv (r^{n^s} + n^s r^{n^s-1} ipq)(1 + mn) \\ &\equiv r^{n^s}(1 + n^s r^{-1} ipq)(1 + mn) \\ &\equiv r^{n^s}(1 + mn + n^s r^{-1} ipq) \\ &\equiv r^{n^s}(1 + (m + n^{s-1}r^{-1}ipq)n) \\ &\equiv f(r, m + n^{s-1}r^{-1}ipq). \end{aligned}$$

Hence, we see that $f(r, m) = f(r + ipq, m - n^{s-1}r^{-1}ipq)$. Furthermore, as above, it follows that f_r and f_m are 1-to-1. □

We now introduce a public-key encryption scheme based on the Schmidt-Takagi's one. This scheme has the one-wayness under the factoring assumption and IND-CPA under the decisional composite residuosity assumption which is similar to Schmidt-Takagi's one. Our scheme, however, also has a weakness against active attacks, that is, the chosen ciphertext attack. In addition, unlike several Paillier-based schemes [12, 6, 16], our encryption function is not additively homomorphic in m. In Section 4, we will propose a variant of our scheme which has additively homomorphism properties.

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

Encryption: To encrypt a message $m \in \mathbb{Z}/n^s$, choose a random number $r \in \{0,1\}^l$, and then compute

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

Decryption: Given a ciphertext c, first compute $r = c^d \bmod pq$. Clearly, if $c = \mathcal{E}_{pk}(r, m)$, we get

$$\mathcal{D}_{sk}(c) = L_n(c(r^{n^s})^{-1} \bmod n^{s+1}) \bmod n^s,$$

where $L_n(x) = \frac{x-1}{n}$.

3.1 Efficiency

Our scheme implies the Schmidt-Takagi encryption scheme when $s = 1$. Compared with the Damgård-Jurik encryption scheme, although the modulus of our schemes employs $n = p^2q$ (their scheme employs $n = pq$), the encryption and decryption speed of our scheme is faster than that of their scheme. Since there are twice computations of large modular exponentiation in encryption phase of their scheme, and once computation of large modular exponentiation and many computations[3] of binomial coefficients in decryption phase. On the other hand, there is once computations of large modular in encryption phase, and so in the decryption phase. Since we can regard our encryption scheme as a variant of the RSA-Paillier based scheme, the encryption and decryption speeds are faster than original Paillier-based schemes.

3.2 Security

Theorem 5. *Our Scheme has the one-wayness under the factoring p^2q assumption.*

Proof. We assume that there exists an adversary $\mathcal{A}$ that on input a random ciphertext $c = r^{n^s}(1 + mn) \bmod n^{s+1}$, output $m \in \mathbb{Z}/n^s$ with non-negligible advantage ϵ. Then we will construct a probabilistic polynomial time algorithm $\mathcal{B}$ by using this adversary $\mathcal{A}$.

$\mathcal{B}$ chooses $r' \in (\mathbb{Z}/n)^\times$ and $m' \in \mathbb{Z}/n^s$. Then with probability $1 - 1/p$, obtains $r' > pq$. $\mathcal{B}$ computes $c' = r'^{n^s}(1 + m'n) \bmod n^{s+1}$, and runs $\mathcal{A}$ on c'. Since $\mathcal{E}(r + ipq, m) = \mathcal{E}(r, m + n^{s-1}r^{-1}ipq)$, $\mathcal{A}(c')$ outputs $\bar{m} = m' + n^{s-1}\bar{r}^{-1}ipq \bmod n^{s+1}$ with probability ϵ, where $\bar{r} = r' \bmod pq$. From $m' - \bar{m} = n^{s-1}\bar{r}^{-1}ipq$ (i.e. $\frac{m'-\bar{m}}{n^{s-1}} = \bar{r}^{-1}ipq$), $\bar{r} \in (\mathbb{Z}/pq)^\times$ and $0 \le i < p$, we obtain $\gcd(\frac{m'-\bar{m}}{n^{s-1}}, n^s) = pq$. Hence, $\mathcal{B}$ can factor $n = p^2q$ with probability $(1 - 1/p)\epsilon$. □

In order to show that our scheme is IND-CPA, we now introduce an assumption as well as that of Schmidt-Takagi's scheme [16].

Definition 6. *(The Desicional Composite Residuosity Problem) Let n be a randomly chosen k-bit p^2q modulus. For every probabilistic polynomial time algorithm $\mathcal{A}$, define the following probabilities:*

$$P_{Random} = \Pr[x \leftarrow (\mathbb{Z}/n^{s+1})^\times : \mathcal{A}(x) = 1]$$

and

$$P_{Residue} = \Pr[x \leftarrow (\mathbb{Z}/n)^\times : \mathcal{A}(x^{n^s} \bmod n^{s+1}) = 1].$$

Then, we denote the advantage of $\mathcal{A}$ by

$$\mathbf{Adv}(\mathcal{A}) = |P_{Random} - P_{Residue}|.$$

[3] approximately, $O(s^2)$.

	c_0	$\dots$	$c_{t'-t-1}$	$c_{t'-t}$	$\dots$	c_{s-t+1}	c_{s-t+2}	$\dots$
m_1	a_0	$\dots$	$a_{t'-t-1}$	$a_{t'-t}$	$\dots$	a_{s-t+1}	0	$\dots$
m_2	0	$\dots$	0	b_0	$\dots$	$b_{s-t'+1}$	0	$\dots$
$m_1 + m_2 n^{t'-t}$	a_0	$\dots$	$a_{s-t'-1}$	$a_{t'-t} + b_0$	$\dots$	$a_{s-t+1} + b_{s-t'+1}$	0	$\dots$

Table 1: The value $m_1 + m_2 n^{t'-t} = c_0 + c_1 n + \cdots + c_s n^s$.

Theorem 7. *Our scheme is IND-CPA if and only if the decisional composite residuosity problem is intractable.*

Proof. ("⇒") We will construct a probabilistic polynomial time algorithm $\mathcal{D}$ such that breaks Assumption 7 by using the adversary $\mathcal{A}$ against IND-CPA with the advantage $\mathbf{Adv}(\mathcal{A}) = \epsilon$. Let x be an instance of the decisional composite residuosity problem. $\mathcal{A}$ first chooses randomly two messages $m_0, m_1 \in (\mathbb{Z}/n^{s+1})^\times$. Next $\mathcal{D}$ chooses a random bit $b \in \{0,1\}$, computes $c = x(1+m_b n) \bmod n^{s+1}$, and runs $\mathcal{A}$ on (c, m_0, m_1). If x is an n-th residue, then c is a valid ciphertext, otherwise c is a random element of $(\mathbb{Z}/n^{s+1})^\times$. Therefore, let $\mathcal{D}$ outputs 1 if $\mathcal{A}(c, m_0, m_1) = b$, or 0 otherwise. Hence, we can obtain $\mathbf{Adv}(\mathcal{D}) = \epsilon/2$.

("⇐") Next, we will construct a probabilistic polynomial time algorithm $\mathcal{A}$ such that breaks IND-CPA by using the adversary $\mathcal{D}$ against the decisional composite residuosity problem with the advantage $\mathbf{Adv}(\mathcal{D}) = \epsilon$. $\mathcal{A}$ first chooses randomly two messages $m_0, m_1 \in (\mathbb{Z}/n^{s+1})^\times$, and sends them to the challenger. Next, the challenger chooses a random number $r \in (\mathbb{Z}/pq)^\times$ and random bit $b \in \{0,1\}$, then he computes $c = r^{n^s}(1 + m_b n)$. Given a challenge $c \in (\mathbb{Z}/n^{s+1})^\times$, $\mathcal{A}$ computes[4] the multiplicative inverse $(1 + m_b n)^{-1}$ in $(\mathbb{Z}/n^{s+1})^\times$ and $c' = c(1 + mb_n)^{-1} \bmod n^{s+1}$, and runs $\mathcal{D}$ on c'. If c is a ciphertext of m_b, then c' is an n-th residue, or a random element of $(\mathbb{Z}/n^{s+1})^\times$ otherwise. Therefore, let $\mathcal{A}$ outputs b if $\mathcal{D}(c') = 1$, or $1 - b$ otherwise. Then we can obtain $\mathbf{Adv}(\mathcal{A}) = \epsilon/2$ by applying the discussion above. □

Remark 8. *We recall that, in our encryption scheme, the randomness space is $(\mathbb{Z}/pq)^\times$ and the plaintext space $\mathbb{Z}/n^s$. As the same way, we can prove the same security, replacing the randomness space $(\mathbb{Z}/pq)^\times$ with $(\mathbb{Z}/n)^\times$ and the plaintext space $\mathbb{Z}/n^s$ with $\mathbb{Z}/(n^s/p)$ $(n^s/p = p^{2s-1}q^s)$.*

4 Homomorphic Properties

Additively homomorphic is important to many cryptographic applications. Unlike several variants of the Paillier encryption scheme [12, 6, 16], our encryption function $\mathcal{E}$ is multiplicatively

[4]Note that we can compute the multiplicative inverse of $1 + m_b n$ in $(\mathbb{Z}/n^{s+1})^\times$ due to $\gcd(1 + m_b n, n^s) = 1$. In addition, this inverse forms $1 + (\cdots)n$, which is a candidate for ciphertexts.

homomorphic in $r \in (\mathbb{Z}/pq)^\times$ but not additively homomorphic in $m \in \mathbb{Z}/n^s$ since

$$\begin{aligned}
\mathcal{E}(r_1, m_1)\mathcal{E}(r_2, m_2) &\equiv r_1^{n^s}(1 + m_1 n) r_2^{n^s}(1 + m_2 n) \\
&\qquad\qquad\qquad\qquad (\mathrm{mod}\ n^{s+1}) \\
&\equiv (r_1 r_2)^{n^s}(1 + m_1 n)(1 + m_2 n) \\
&\equiv (r_{pq} + ipq)^{n^s}(1 + m_1 n)(1 + m_2 n) \\
&\equiv (r_{pq}^{n^s} + n^s r_{pq}^{n^s - 1} ipq) \\
&\quad (1 + (m_1 + m_2)n + m_1 m_2 n^2) \\
&\equiv r_{pq}^{n^s}(1 + n^s r_{pq}^{-1} ipq) \\
&\quad (1 + (m_1 + m_2 + m_1 m_2 n)n) \\
&\equiv r_{pq}^{n^s}(1 + (m_1 + m_2 + \\
&\quad m_1 m_2 n + n^{s-1} r_{pq}^{-1} ipq)n) \\
&\equiv \mathcal{E}(r_{pq}, m_1 + m_2 + \\
&\qquad m_1 m_2 n + n^{s-1} r_{pq}^{-1} ipq),
\end{aligned}$$

where $r_{pq} = r_1 r_2 \bmod pq$ and $0 \leq i < p$. The restricted function [5] $\mathcal{E}_m = \mathcal{E}|_{(\mathbb{Z}/n)^\times \times \mathbb{Z}/(n^s/p)}$ is not additively homomorphic even though Schmidt-Takagi's encryption function f_m is so (see Section 2). Clearly,

$$\mathcal{E}_m(r_1, m_1)\mathcal{E}_m(r_2, m_2) \equiv \mathcal{E}_m(r_1 r_2, m_1 + m_2 + m_1 m_2 n).$$

The reason that our encryption function is not homomorphic in m follows from $n^2 \not\equiv 0$ (in fact, in every additively homomorphic variants of Paillier's encryption scheme it holds $n^2 \equiv 0$, because every moduli are n^2).

4.1 A Variant of Our Scheme and Homomorphic Property

Now, we add a parameter $t \in \mathbb{N}$ to the public-key in order to solve the situation above. Then, we modify our encryption function as follows:

$$\begin{array}{rcl}
\mathcal{E}_t : (\mathbb{Z}/n)^\times \times \mathbb{Z}/(n^{s-t+1}/p) & \longrightarrow & (\mathbb{Z}/n^{s+1})^\times \\
(r, m) & \longmapsto & r^{n^s}(1 + mn^t),
\end{array}$$

where n, s, t are the public key, m a message, and r a random number. Then, we have that $\mathcal{E}_1$ is equivalent to the previous encryption function $\mathcal{E}_m$. We note that the plaintext space decreases with increasing the parameter t. Nevertheless, we get some interesting properties by using the parameter t.

Remark 9. *Our scheme replaced the encryption function $\mathcal{E}$ with $\mathcal{E}_t$ also has the same security, that is, the one-wayness is equivalent to the factoring assumption, and IND-CPA. This proof follows from Theorem 5 and Theorem 8.*

First, we show that the encryption scheme $\mathcal{E}_t$ is additively homomorphic in m when t is at least $(s+1)/2$.

Theorem 10. *The encryption function $\mathcal{E}_t$ is homomorphic in m if $t \geq \lceil (s+1)/2 \rceil$.*

Proof. First, for any t such that $1 \leq \forall t \leq s$, it follows that for $i \in \mathbb{Z}$,

$$\mathcal{E}_t(r, m) = \mathcal{E}_t(r + ipq, m - n^{s-t} r^{-1} ipq)$$

[5] From Remark 9, we know that the scheme with $\mathcal{E}_m$ has the same security of previous one.

	n	**Plaintext**	**Randomness**	**Ciphertext**	**One-Wayness**	**IND-CPA**
[12]	pq	$\mathbb{Z}/n$	$(\mathbb{Z}/n)^\times$	$(\mathbb{Z}/n^2)^\times$	-	DCRA
[6]	pq	$\mathbb{Z}/n^s$	$(\mathbb{Z}/n)^\times$	$(\mathbb{Z}/n^{s+1})^\times$	-	DCRA
[16]	p^2q	$\mathbb{Z}/pq$	$(\mathbb{Z}/n)^\times$	$(\mathbb{Z}/n^2)^\times$	Factoring p^2q	DCRA
Ours 1	p^2q	$\mathbb{Z}/n^s$	$(\mathbb{Z}/pq)^\times$	$(\mathbb{Z}/n^{s+1})^\times$	Factoring p^2q	DCRA
Ours 2	p^2q	$\mathbb{Z}/(n^{s-t+1}/p)$	$(\mathbb{Z}/n)^\times$	$(\mathbb{Z}/n^{s+1})^\times$	Factoring p^2q	DCRA

Table 2: Comparison between our schemes and other variants.

(according to Theorem 4). From $n^{2t} \equiv 0 \pmod{n^{s+1}}$ if $2t \geq s+1$, we obtain

$$\mathcal{E}_t(r_1, m_1)\mathcal{E}_t(r_2, m_2) = \mathcal{E}_t(r_1 r_2, m_1 + m_2).$$

Let m' be $m_1 + m_2 \bmod n^{s-t+1}/p$. For r_1, r_2, there exists $0 \leq i < p$ such that $m_1 + m_2 \equiv m' + in^{s-t}r_{pq}^{-1}pq \bmod n^{s-t+1}/p$, where $r_{pq} = r_1 r_2 \bmod pq$. As above, we see

$$\begin{aligned}\mathcal{E}_t(r_1 r_2, m_1 + m_2) &= \mathcal{E}_t(r_1 r_2 + ipq, m_1 + m_2 - \\ &\qquad in^{s-t}r_{pq}^{-1}pq) \\ &= \mathcal{E}_t(r_n, m'),\end{aligned}$$

where $r_n = r_1 r_2 + ipq \bmod n$. Hence, the encryption function $\mathcal{E}_t$ is homomorphic in m. □

Next, we consider two parameters t, t' such that $t + t' \geq \lceil (s+1)/2 \rceil$ and $t' \geq t$. We consider two encryption functions $\mathcal{E}_t$ and $\mathcal{E}_{t'}$. Then,

$$\begin{aligned}\mathcal{E}_t(r_1, m_1)\mathcal{E}_{t'}(r_2, m_2) &\equiv r_1^{n^s}(1 + m_1 n^t) r_2^{n^s}(1 + m_2 n^{t'}) \\ &\qquad \pmod{n^{s+1}} \\ &\equiv (r_1 r_2)^{n^s}(1 + m_1 n^t)(1 + m_2 n^{t'}) \\ &\equiv (r_1 r_2)^{n^s}(1 + m_1 n^t + \\ &\qquad m_2 n^{t'} + m_1 m_2 n^{t+t'}) \\ &\equiv (r_1 r_2)^{n^s}(1 + (m_1 + m_2 n^{t'-t})n^t) \\ &\equiv \mathcal{E}_t(r_1 r_2, m_1 + m_2 n^{t'-t}).\end{aligned}$$

We obtain $m = m_1 + m_2 n^{t'-t} \in \mathbb{Z}/(n^{s-t-1}/p)$ when decrypt the above equation. This means that if we represent m_1 and m_2 as n-adic numbers, denoted by $m_1 = a_0 + a_1 n + \cdots + a_s n^s$ and $m_2 = b_0 + b_1 n + \cdots + b_s n^s$ (where, $a_i b_j \in \mathbb{Z}/n$)[6], then there appear terms which have a homomorphic property (see Table 1). That is, the terms from n^0 until $n^{t'-t-1}$ are unchanged, but after $n^{t'-t}$ are affected by a homomorphic property.

Furthermore, we obtain another homomorphic property as follows: we fix $s = 3$ for simplicity. Since $(s+1)/2 = 2$, $\mathcal{E}_2$ is additively homomorphic, but $\mathcal{E}_1$ is not. Now, we denote how to transform $\mathcal{E}_1$ into $\mathcal{E}_2$ (that is, we give $\mathcal{E}_1$ some properties such as additively homomorphic), by decomposing given messages.

First, for a message m, we decompose m into (m_1, m_2) as follows: Then, we take $m_1 = m$ and $m_2 = -m$. The reason is due to

$$1 - x^2 = (1 + x)(1 - x).$$

As above, for random numbers r_1, r_2, we see that:

$$(r_1 r_2)^{n^3}(1 - m^2 n) = r_1^{n^3}(1 + m_1 n)\ r_2^{n^3}(1 - m_1 n).$$

[6] the plaintext size depends on $\mathcal{E}_t$ from $s - t' + 1 \leq s - t + 1$.

That is, $\mathcal{E}_2(r_1r_2, m^2) = \mathcal{E}_1(r_1, m_1)\mathcal{E}_1(r_2, m_2)$. Hence, for messages m and m', we can make a ciphertext of $m^2 + m'^2$ from m's decomposition (m_1, m_2), m''s decomposition (m'_1, m'_2), and $\mathcal{E}_1$.

Remark 11. *We see that using the homomorphic property above the receiver obtains* $\sum_i m_i^2$. *Actually, by considering the factorization of cyclotomic polynomials* $x^l - 1$ $(l > 2)$, *we can extend* $\sum_i m_i^2$ *to* $\sum_i m_i^l$. *In fact,* $x^2 - 1$ *is a cyclotomic polynomial with degree 2. Furthermore, we can also deal with* $\sum_i m_i$ *by applying the ciphertext of* $m = 1$ *(see [9]).*

5 Discussion

We have seen variants of the Schmidt-Takagi encryption scheme. Now, we discuss comparison between our schemes and other variants. In particular, we refer to Damård-Jurik's and Schmidt-Takagi's scheme.

Damgård and Jurik proposed a threshold cryptosystems based on their encryption scheme. They showed that their threshold scheme can be applied to electronic votings. Now, we modify our schemes into threshold schemes by their techniques. However, the authorities need the information on p in share decryption phase. The reason for the situation above follows that the modulus of our encryption schemes employs $n = p^2q$, but not $n = pq$. Therefore, we cannot construct threshold cryptosystems, directly.

Schmidt and Takagi proposed two trapdoor commitment schemes based on the factoring problem, by using their encryption scheme. In fact, our scheme implies their scheme when $s = 1$, and inherits many properties from their scheme. Therefore, our scheme can be applied to trapdoor commitment schemes. Furthermore, we can reduced them to the factor assumption.

6 Conclusions

We have seen variants of the Schmidt-Takagi encryption scheme: One is $\mathcal{E}(m, r) = r^{n^s}(1+mn) \bmod n^{s+1}$, where n, s are the public key, m a message, and r a random number, and another is $\mathcal{E}_t(m, r) = r^{n^s}(1 + mn^t) \bmod n^{s+1}$, where n, s, t are the public key, m a message, and r a random number.

Our schemes have the one-wayness against the chosen plaintext attack based on the factoring problem, and the indistinguishability against the chosen plaintext attack based on the decisional composite residuosity problem.

Table 2 is for comparison between our schemes and other variants of the Paillier encryption scheme.

$\mathcal{E}_t$ has some homomorphic properties which can be applied to cryptographic applications. It remains to analyze the advantage of such homomorphic properties as open problems.

References

[1] Bresson, E., Catalano, D., and Pointcheval, D. A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications. *Advances in Cryptology-ASIACRYPT 2003, Lecture Notes in Computer Science 2894* (2003), 37–54.

[2] Catalano, D., Gennaro, R., and Howgrave-Graham, N. Paillier's Trapdoor Function Hides up to $O(n)$ Bits. *Journal of Cryptology 15*, 4 (2002), 251–269.

[3] Catalano, D., Gennaro, R., Howgrave-Graham, N., and Nguyen, P. Q. Paillier's Cryptosystem Revisited. *Proceedings of the 8th ACM conference on Computer and Communications Security* (2001), 206–214.

[4] Catalano, D., Nguyen, P. Q., and Stern, J. The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm. *Advances in Cryptology-ASIACRYPT 2002, Lecture Notes in Computer Science 2501* (2002), 299–310.

[5] Cramer, R., and Shoup, V. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. *Advances in Cryptology-EUROCRYPT 2002, Lecture Notes in Computer Science 2332* (2002), 45–64.

[6] Damgård, I., and Jurik, M. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. *PKC 2001, Lecture Notes in Computer Science 1992* (2001), 119–136.

[7] Fouque, P. A., and Pointcheval, D. Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks. *Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science 2248* (2001), 351–368.

[8] Galindo, D., Martin, S., Morillo, P., and Villar, J. L. A practical public key cryptosystem from Paillier and Rabin schemes. *PKC 2003, Lecture Notes in Computer Science 2567* (2003), 279–291.

[9] Hirano, T., Wada, K., and Tanaka, K. Simple Decomposition of Ciphertexts. *SCIS* (2008). to appear.

[10] Kurosawa, K., and Takagi, T. Some RSA-Based Encryption Schemes with Tight Security Reduction. *Advances in Cryptology-ASIACRYPT 2003, Lecture Notes in Computer Science 2894* (2003), 19–36.

[11] Okamoto, T., and Uchiyama, S. A New Public-Key Cryptosystem as Secure as Factoring. *Advances in cryptology-EUROCRYPT'98, Lecture Notes in Computer Science 1403* (1998), 308–318.

[12] Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *Advances in Cryptology-EUROCRYPT'99, Lecture Notes in Computer Science 1592* (1999), 223–238.

[13] Paillier, P., and Pointcheval, D. Efficient Public-Key Cryptosystems Provably Secure against Active Adversaries. *Advances in Cryptology-ASIACRYPT'99, Lecture Notes in Computer Science 1716* (1999), 165–179.

[14] Sakurai, K., and Takagi, T. New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive. *PKC 2002, Lecture Notes in Computer Science 2274* (2002), 1–16.

[15] Sakurai, K., and Takagi, T. On the Security of a Modified Paillier Public-Key Primitive. *ACISP 2002, Lecture Notes in Computer Science 2384* (2002), 436–448.

[16] Schmidt-Samoa, K., and Takagi, T. Paillier's Cryptosystem Modulo p^2q and Its Applications to Trapdoor Commitment Schemes. *Mycrypt 2005, Lecture Notes in Computer Science 3715* (2005), 296–313.