Message Expansion of Homomorphic Encryption Using Product Pairing

Soo Kyung Eom, Hyang-Sook Lee, and Seongan Lim

The Boneh, Goh, and Nissim (BGN) cryptosytem is the first homomorphic encryption scheme that allows additions and multiplications of plaintexts on encrypted data. BGN-type cryptosystems permit very small plaintext sizes. The best-known approach for the expansion of a message size by *t* times is one that requires *t* implementations of an initial scheme; however, such an approach becomes impractical when *t* is large. In this paper, we present a method of message expansion of BGN-type homomorphic encryption using composite product pairing, which is practical for relatively large *t*. In addition, we prove that the indistinguishability under chosen plaintext attack security of our construction relies on the decisional Diffie–Hellman assumption for all subgroups of prime order of the underlying composite pairing group.

Keywords: BGN cryptosystem, pairing, product pairing, homomorphic encryption, decisional Diffie–Hellman problem.

Manuscript received July 8, 2015; revised Sept. 15, 2015; accepted Sept. 25, 2015.

This work was supported by the basic science Research Program of Korean Government (Grant number 2012R1A2A1A03006706, Grant number 2013R1A1A2206063268), Priority Research Centers Program of the Ministry of Education of Korea (Grant number 2009-0093827), and Brain Korea 21 plus Mathematical Science Team for Global Women Leaders.

Soo Kyung Eom (esk9030@gmail.com) and Hyang-Sook Lee (hsl@ewha.ac.kr) are with the Department of Mathematics, Ewha Womans University, Seoul, Rep. of Korea.

Seongan Lim (corresponding author, seongannym@ewha.ac.kr) is with the Institute of Mathematical Sciences, Ewha Womans University, Seoul, Rep. of Korea.

I. Introduction

Developing an efficient homomorphic encryption scheme is a hot issue in cryptography due to its versatility in providing security in cloud services. Currently, many homomorphic encryption schemes are constructed from lattices. However, a lattice-based homomorphic encryption scheme requires parameters of very large size, which makes such schemes impractical in the near future. On the other hand, pairing-based cryptography is now considered as practical for use with many platforms.

The Boneh, Goh, and Nissim (BGN) cryptosystem is additively homomorphic, but it allows multiplication over ciphertext only once. Such a restriction on a homomorphic evaluation might have limited applications. However, many statistics of numerical data can be expressed as quadratic polynomials and the BGN cryptosystem can be used to evaluate such statistics homomorphically over ciphertexts. The BGN cryptosystem can be used to construct an efficient secure auction protocol. Despite its invaluable contribution as an efficient (+, ×)-homomorphic encryption, the original BGN cryptosystem has, in practice, suffered from two challenging issues: message sizes are required to be very small and it uses larger elliptic curve groups.

The BGN cryptosystem uses a pairing $e: G \times G \to G_T$ with $|G| = |G_T| = N = PQ$ [1]. Here, the cyclic group G is a subgroup of an elliptic curve group over a finite field. It is proven that the security of the BGN cryptosystem is based on the subgroup decision problem for G_P in G, which is as hard as factoring N [2]. Currently, at the year 2015, it is recommended that N be at least 2,048 [3], [4]. This requires that group G in the BGN cryptosystem be larger compared to that of many known elliptic curve–based cryptosystems.

Freeman presented how to convert a BGN cryptosystem of composite pairing to a (+, ×)-homomorphic encryption using a product of prime pairings [5]. Therefore, Freeman contributed to reducing the size of the parameters of the original BGN cryptosystem. However, the message size of the Freeman conversion is the same as that of the original BGN cryptosystem. The best-known method of expanding the message size by t times while preserving the (+, ×)-homomorphic feature requires t implementations of an initial scheme using the Chinese remainder theorem (CRT) directly. However, this method becomes impractical when t is large.

In this paper, we present how to expand the message size of the BGN cryptosystem while maintaining efficient parameter sizes. Our idea is to use Freeman's product pairing with a bilinear group — of composite order n. In our scheme, all prime factors of n are public, and we use the prime factors to expand the message size. This distinguishes our scheme from many other schemes that use pairing groups of composite order, for such schemes assume that prime factors are private, not public [6], [7].

By using a bilinear group of composite order $n = p_1 p_2 \cdots p_t$ with known prime factors p_i, we expand the bit size of a message by t times. We also prove that the indistinguishability under chosen plaintext attack (IND-CPA) security of our construction relies on the decisional Diffie–Hellman (DDH) assumption on the subgroups of order p_i of the underlying composite pairing group, for all $i = 1, \ldots, t$.

The rest of the paper is organized as follows. In Section II, we review the BGN cryptosystem and product pairing with projections. We also present a naive message expansion of a (+, ×)-homomorphic cryptosystem using the CRT. In Section III, we describe how to construct a product of composite pairing. In Section IV, we present our scheme with security proof. We also suggest how to select parameters and compare it with the naive approach of [5]. In Section V, we conclude our paper.

II. Preliminaries

1. BGN Cryptosystem

The original BGN cryptosystem uses a symmetric pairing; however, we present a scheme based on an asymmetric pairing by considering recently announced security issues related to symmetric pairing. The BGN cryptosystem uses a pairing $e: G_1 \times G_2 \to G_T$ with $|G_1| = |G_2| = |G_T| = N = PQ$ and $G_j = \langle g_j \rangle$, where N is difficult to factor. The BGN cryptosystem consists of the following five algorithms:

1) KeyGen: for security parameter λ, output

$$\mathrm{pk} = \begin{pmatrix} N, e: G_1 \times G_2 \to G_T, \\ g_1, g_2, h_1 = g_1^P, h_2 = g_2^P \end{pmatrix},$$

$$\mathrm{sk} = Q$$

2) Enc: for a message $m \in [0, 2^\alpha]$, output $\mathbf{c} = (g_1^m h_1^r, g_2^m h_2^{r'})$ for randomly chosen $r, r' \in Z_N^*$

3) Eval$_\times$: for ciphertexts $\mathbf{c}_1 = (c_{11}, c_{12}), \mathbf{c}_2 = (c_{21}, c_{22}) \in G_1 \times G_2$, compute $c_\times = e(c_{11}, c_{22})$

4) Eval$_+$: for ciphertexts $c_1, c_2 \in G_1 \times G_2 \cup G_T$, compute

$$c_+ = \begin{cases} \mathbf{c}_1 \cdot \mathbf{c}_2 & \text{if } \mathbf{c}_1, \mathbf{c}_2 \in G_1 \times G_2, \\ c_1 \cdot c_2 & \text{if } c_1, c_2 \in G_T, \\ c_1 \cdot e(g_1, c_{22}) & \text{if } c_1 \in G_T, \mathbf{c}_2 \in G_1 \times G_2, \\ e(g_1, c_{12}) \cdot c_2 & \text{if } \mathbf{c}_1 \in G_1 \times G_2, c_2 \in G_T. \end{cases}$$

5) Dec: for a ciphertext $\mathbf{c} \in G_1 \times G_2 \cup G_T$, compute

$$m = \begin{cases} \log_{g_1^Q} c_{11}^Q & \text{if } \mathbf{c} = (c_{11}, c_{12}) \in G_1 \times G_2, \\ \log_{e(g_1, g_2)^Q} c^Q & \text{if } \mathbf{c} \in G_T. \end{cases}$$

We note that α, the size of plaintext, should be chosen to be as small as possible such that a decryption can still be efficiently computed.

2. Product Pairing with Projections

We begin with a product pairing introduced by Freeman [5] for the BGN cryptosystem.

Definition 1. For a pairing $\hat{e}: G_1 \times G_2 \to G_T$, we define the product pairing $e: G_1^2 \times G_2^2 \to G_T^4$ by

$$e\big((g_{11}, g_{12}), (g_{21}, g_{22})\big) = \big(\hat{e}(g_{11}, g_{21}), \hat{e}(g_{11}, g_{22}), \hat{e}(g_{12}, g_{21}), \hat{e}(g_{12}, g_{22})\big).$$

To define the BGN cryptosystem over the product pairing, the following notations are used. Assume that $|G_1| = |G_2| = |G_T| = n$. We note that Freeman only considers n to be a prime number in the product pairing; whereas, we consider a composite number n in the following.

For $x_{ij}, y_{ij}, z_{ij} \in Z_n$, $u, v \in G_i$, and $\alpha, \beta, \gamma, \nu \in G_T$, we denote

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}, \quad \mathbf{Y} = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix}, \quad \mathbf{Z} = \begin{bmatrix} z_{ij} \end{bmatrix}_{1 \le i, j \le 4}.$$

We also denote

$$\mathbf{X} \otimes \mathbf{Y} = \begin{bmatrix} x_{11}y_{11} & x_{11}y_{12} & x_{12}y_{11} & x_{12}y_{12} \\ x_{11}y_{21} & x_{11}y_{22} & x_{12}y_{21} & x_{12}y_{22} \\ x_{21}y_{11} & x_{21}y_{12} & x_{22}y_{11} & x_{22}y_{12} \\ x_{21}y_{21} & x_{21}y_{22} & x_{22}y_{21} & x_{22}y_{22} \end{bmatrix},$$

$$(u, v)^X = (u^{x_{11}} v^{x_{21}}, u^{x_{12}} v^{x_{22}}),$$

and

$$(\alpha,\beta,\gamma,\nu)^{\mathbf{Z}}=(\alpha^{z_{11}}\beta^{z_{21}}\gamma^{z_{31}}\nu^{z_{41}},\ \alpha^{z_{12}}\beta^{z_{22}}\gamma^{z_{32}}\nu^{z_{42}},\ \alpha^{z_{13}}\beta^{z_{23}}\gamma^{z_{33}}\nu^{z_{43}},\ \alpha^{z_{14}}\beta^{z_{24}}\gamma^{z_{34}}\nu^{z_{44}}).$$

For a randomly chosen $(a_j,b_j)\in Z_n^*\times Z_n^*$, we consider the subgroups $H_1=\left\langle\left(g_1^{a_1},g_1^{b_1}\right)\right\rangle\subset G_1^2$ and $H_2=\left\langle\left(g_2^{a_2},g_2^{b_2}\right)\right\rangle\subset G_2^2$, as well as matrices

$$\mathbf{A}=\begin{bmatrix}-b_1 & -b_1\\ a_1 & a_1\end{bmatrix},\quad \mathbf{B}=\begin{bmatrix}-b_2 & -b_2\\ a_2 & a_2\end{bmatrix}.$$

We also define projections $\pi_j:G_j^2\to G_j^2$ for j = 1, 2, and $\pi_T:G_T^4\to G_T^4$ as follows: $\pi_1\left((g_{11},\,g_{12})\right)=(g_{11},g_{12})^{\mathbf{A}}=(g_{11}^{-b_1}g_{12}^{a_1},g_{11}^{-b_1}g_{12}^{a_1})$, $\pi_2\left((g_{21},g_{22})\right)=(g_{21},g_{22})^{\mathbf{B}}=(g_{21}^{-b_2}g_{22}^{a_2},g_{21}^{-b_2}g_{22}^{a_2})$, and $\pi_T(\gamma_1,\gamma_2,\gamma_3,\gamma_4)=(\gamma_1,\gamma_2,\gamma_3,\gamma_4)^{\mathbf{A}\otimes\mathbf{B}}$.

With these projections, we see that (1) below holds.

For all $g_{11},g_{12}\in G_1$ and $g_{21},g_{22}\in G_2$,

$$e\left(\pi_1(g_{11},g_{12}),\pi_2(g_{21},g_{22})\right)=\pi_T\left(e\left((g_{11},g_{12}),(g_{21},g_{22})\right)\right).\tag{1}$$

The reason is as follows. First, we have

$$\begin{aligned}&e\left(\pi_1(g_{11},g_{12}),\pi_2(g_{21},g_{22})\right)\\&=e\left((g_{11}^{-b_1}g_{12}^{a_1},g_{11}^{-b_1}g_{12}^{a_1}),(g_{21}^{-b_2}g_{22}^{a_2},g_{21}^{-b_2}g_{22}^{a_2})\right)\\&=(\gamma,\gamma,\gamma,\gamma),\end{aligned}$$

where

$$\begin{aligned}\gamma&=\hat{e}\left(g_{11}^{-b_1}g_{12}^{a_1},g_{21}^{-b_2}g_{22}^{a_2}\right)\\&=\frac{\hat{e}(g_{11},g_{21})^{b_1b_2}\,\hat{e}(g_{12},g_{22})^{a_1a_2}}{\hat{e}(g_{11},g_{22})^{a_2b_1}\,\hat{e}(g_{12},g_{21})^{a_1b_2}}.\end{aligned}$$

We also have,

$$\begin{aligned}&\pi_T\left(e\left((g_{11},g_{12}),(g_{21},g_{22})\right)\right)\\&=\pi_T\left(\hat{e}(g_{11},g_{21}),\hat{e}(g_{11},g_{22}),\hat{e}(g_{12},g_{21}),\hat{e}(g_{12},g_{22})\right)\\&=\left(\hat{e}(g_{11},g_{21}),\hat{e}(g_{11},g_{22}),\hat{e}(g_{12},g_{21}),\hat{e}(g_{12},g_{22})\right)^{\mathbf{A}\otimes\mathbf{B}}\\&=\left(\tilde{\gamma},\tilde{\gamma},\tilde{\gamma},\tilde{\gamma}\right),\end{aligned}$$

where

$$\tilde{\gamma}=\frac{\hat{e}(g_{11},g_{21})^{b_1b_2}\,\hat{e}(g_{12},g_{22})^{a_1a_2}}{\hat{e}(g_{11},g_{22})^{a_2b_1}\,\hat{e}(g_{12},g_{21})^{a_1b_2}}=\gamma.$$

Therefore, (1) holds. We also have, for i = 1, 2,

$$\begin{aligned}\pi_i\left(\left(g_i^{a_i},g_i^{b_i}\right)\right)&=\left(g_i^{-a_ib_i+a_ib_i},g_i^{-a_ib_i+a_ib_i}\right)\\&=\left(1_{G_i},1_{G_i}\right),\end{aligned}$$

or equivalently, we have $H_i\subset\ker(\pi_i)$.

Combining with (1), we see that

$$H_1\times G_2^2\cup G_1^2\times H_2\subset\ker(\pi_T).$$

We also define the canonical projections as follows:

$$\mathrm{proj}_1:G_1^2\times G_2^2\to G_1^2\ \text{ by }\ \mathrm{proj}_1(\mathbf{u}_1,\mathbf{u}_2)=\mathbf{u}_1,$$

$$\mathrm{proj}_2:G_1^2\times G_2^2\to G_2^2\ \text{ by }\ \mathrm{proj}_2(\mathbf{u}_1,\mathbf{u}_2)=\mathbf{u}_2.$$

Freeman pointed out that the subgroup decision assumption for a subgroup H_i of G_i^2 is equivalent to the DDH assumption on G_i when $|G_i|$ is prime. Freeman converted the BGN cryptosystem to a scheme using a product of prime pairings with projection. Freeman's conversion of the BGN to a product pairing is exactly the case t = 1 in our construction, which will be described later. The size of the plaintext of Freeman's conversion of the BGN cryptosystem is the same as that of the original BGN cryptosystem. A simple approach of expanding the message size by t times is to perform t implementations of the basic scheme and combine them with the CRT.

3. CRT

Throughout this paper, we use two public tuples of prime numbers, (q_1, … , q_t) and (p_1, … , p_t), where the q_i's are to be used to encode plaintexts and p_i's to encrypt the resulting encoded plaintexts.

For $N=q_1q_2\cdots q_t\ (q_i\neq q_j)$, the CRT provides a ring isomorphism, $\mathrm{mod}_{q_1,\ldots,q_t}:Z_N\to Z_{q_1}\times\cdots\times Z_{q_t}$, defined by $\mathrm{mod}_{q_1,\ldots,q_t}(x)=(x \bmod q_1,\ldots,x \bmod q_t)$. We see that the inverse of $\mathrm{mod}_{q_1,\ldots,q_t}$ is $\mathrm{CRT}_{(q_1,\ldots,q_t)}$.

Remark. A naive message expansion of a (+, ×)-homomorphic cryptosystem using CRT can be described as follows. Suppose we have a (+, ×)-homomorphic encryption scheme with message space $M=Z_Q$ and ciphertext space C.

Set $N=q_1q_2\cdots q_t\ (q_i\neq q_j)$, where the q_i's are primes such that $q_i\leq Q$. The encryption process can then be defined as follows:

For any $m\in Z_N$, we encode $\tilde{m}=\mathrm{mod}_{q_1,\ldots,q_t}(m)=(m_1,\ldots,m_t)$, $m_i\leq Q$, and then encrypt each m_i using the encryption scheme. Then, we obtain a ciphertext $c_i\in C$ and set the ciphertext **c** of m as $\mathbf{c}=(c_1,\ldots,c_t)\in C^t$.

The decryption process is as follows. For a given ciphertext, $\mathbf{c}=(c_1,\ldots,c_t)\in C^t$, decrypt each c_i and obtain $m_i\in Z_{q_i}$. Then, we compute $m=\mathrm{CRT}_{(q_1,\ldots,q_t)}(m_1,\ldots,m_t)$.

Because the CRT is a ring isomorphism, the resulting encryption scheme is (+, ×) homomorphic. Therefore, one can expand the message size of the encryption by t times. However, we see that a ciphertext expansion of the same ratio is inevitable in this approach. Therefore, if t is large, then it becomes impractical.

III. Composite Product Pairing

1. Pairings of Composite Order

Boneh and others [8] constructed ordinary curves with composite-order bilinear groups using the Cocks–Pinch method. As a result, one can construct a pairing $\hat{e}: G_1 \times G_2 \to G_T$ of composite order n with $|G_1| = |G_2| = |G_T| = n$, where G_1 is a cyclic subgroup of $E(F_q)$, an elliptic curve group over the finite field F_q, G_2 is a cyclic subgroup of $E(F_{q^k})$, an elliptic curve group over the finite field F_{q^k}, and G_T is a cyclic subgroup of $F_{q^k}^*$.

Because G_T is a subgroup of $F_{q^k}^*$, we see that n divides $q^k - 1 = |F_{q^k}^*|$. By the Pohlig–Hellman algorithm [9], it is necessary to choose q^k such that $(q^k - 1)/n$ has a large enough prime factor to resist discrete logarithm problem solving for G_T as a subgroup of $F_{q^k}^*$. Currently, it is recommended to have a prime factor of 2,048 bits. We also note that G_1 is a subgroup of $E(F_q)$, which implies that n divides $|E(F_q)|$. Note that, we have

$$\hat{e}(P_1, P_2) = f_{n,P_1}(P_2)^{\frac{q^k - 1}{n}},$$

where $f_{n,P_1}(*)$ is a rational map, which is usually computed by using the Miller algorithm.

A bilinear map is parameterized by $(q, n, \mathrm{tr}, k, D)$, where $\mathrm{tr} = q + 1 - |E(F_q)|$ is the trace of the elliptic curve, k is the embedding degree, and D is the discriminant.

Koblitz [10] found that an ordinary curve of embedding degree $k > 2$ with composite-order group could leak the factorization of the group order. As in many cryptographic schemes using composite pairings, if the prime factors of a group order are to be kept secret for its security, then an ordinary curve of embedding degree $k > 2$ should not be used. However, in our scheme, we use a composite pairing where all the prime factors are public. Therefore, we can use a higher embedding degree. The security requirement related to prime factors in our scheme is the DDH assumption on the cyclic group of each of the prime factors.

Currently, it is recommended that the prime factor p should be of 224 bits to guarantee the DDH assumption on the cyclic groups of order p until the year 2030 [3], [4].

We present examples of bilinear groups of composite order $n = p_1 p_2 p_3$ for distinct primes p_1, p_2, p_3 of small sizes using the Cocks–Pinch method. In our experiment, we use MAGMA. In the following examples, we choose a generator, g_2, from the elliptic curve over the base field since $E(F_q)$ is also a subgroup of $E(F_{q^k})$, which yields $g_T = e(g_1, g_2) \in F_q^*$. Next, we should set generators g_2, g_T with the property of non-degeneracy in the pairing evaluation. In general, curves with small ratio of $\log_2 n$ and $\log_2 q$ are desirable to speed up the arithmetic on the elliptic curves [9]. On the other hand though, at times, a larger ratio of $\log_2 n$ and $\log_2 q$ is acceptable for the sake of a fast pairing computation. Not many results are known for the generation of pairing-friendly elliptic curves for pairings that are of composite order and public prime factors [11]. This necessitates further work on generating pairing-friendly elliptic curves for pairings that are of composite order.

The following are example parameters $(q, n, \mathrm{tr}, k, D)$, of composite order pairing $\hat{e}: G_1 \times G_2 \to G_T$ with $|G_1| = |G_2| = |G_T| = n$.

Example 1. We provide an example of pairing $\hat{e}: G_1 \times G_2 \to G_T$ with $n = p_1 p_2 p_3$, $k = 1$, $D = 1$. We generate an elliptic curve over F_q, defined by $y^2 = x^3 + x$. We choose the cyclic groups $G_1 = \langle g_1 \rangle, G_2 = \langle g_2 \rangle$, and $G_T = \langle g_T \rangle$ as shown in Table 1.

Owing to the embedding degree ($k = 1$) in Example 1, the cyclic subgroups, G_i's, are two distinct subgroups of elliptic curves over the field F_q, and G_T is a cyclic subgroup of the multiplicative group F_q^*.

Example 2. We provide an example of a pairing, $\hat{e}: G_1 \times G_2 \to G_T$ with $n = p_1 p_2 p_3$, $k = 2$, $D = 1$. We generate an elliptic curve over F_q, defined by $y^2 = x^3 + x$. And we choose the cyclic groups $G_1 = \langle g_1 \rangle, G_2 = \langle g_2 \rangle$, and $G_T = \langle g_T \rangle$ as follows (see Table 2).

Because we consider the embedding degree $k = 2$ in this

Table 1. Parameters for Example 1.

	Values
tr	2
q	20549628775099879807802880798391242427507615994080782349521479948676141703719433 83, where $\log_2 q = 309$
Curves	$y^2 = x^3 + x$
$n = p_1 p_2 p_3$	3777641531202213662745286501136101531862152453, where $\log_2 n = 151$ with $\log_2 p_1 = 49$, $\log_2 p_2 = 50$, $\log_2 p_3 = 52$
g_1	(1540744634019546811640085066756787302312959849291276890690273568303293163055573582533279 64255: 23855145529495738741518234077923477655414037898769430856790056427212045710879853124845348 6858)
g_2	(1282733480099721371687324949832027341047277751562377469778305621408877866761332660985780 396938: 47797129551823110014230211875234125922336012548918666243602854503712415815990875789576168 2282)
g_T	19831455731741492965248123919886560541826641958968279139978407648885078896824085120849005 32019

Table 2. Parameters for Example 2.

	Values
tr	68256080518212369350138789467224298131905786
q	30749904011561444574057403920274727714775476919227093461657663739765170552500441017013148355381436666436781011365806729621477153721685743195925134076623082343866173121436 93, where $\log_2 q = 569$
Curves	$y^2 = x^3 + x$
$n = p_1 p_2 p_3$	34128040259106184675069394733612149065952893, where $\log_2 n = 145$ with $\log_2 p_1 = 50$, $\log_2 p_2 = 50$, $\log_2 p_3 = 45$
g_1	(23428622896351232103710031347237864468795865442293900850390825585726287554452915639188585983670558362312047383252646205470739296611406002654842556271384541498182430654186 2: 148892934331759104177995282728057240102269153402693158310571017649771947221967482265261768100346989138939281410091014487687320477405191530831432171801020313667918903017122 4)
g_2	(13485165939113975683527902212637269985582702755970220561177692125691461077378287034076661113690103992734885268198272558091030751631185518877496477959727369384777753746705 49: 112015831065313068391618245656854609898687500582459086089173059007187048857205409755582930401957718034558679867814590035051411665712800355988783017491997721111792155922944 8)
g_T	984817615074110364047095501784422463070126933162713943914881346165187447211386559702179594487590125665450808309131574638128061640148088646045217425572785442113677430069227

Table 3. Parameters for Example 3.

	Values
tr	52955814630012836916177515923214573423313806 2
q	94304227576927869732324529284116169487436818416751871410538689907368095278146641320729533382991760455233504182207491399143320692957473505069417190392390826372714536820454365 1194561, where $\log_2 q = 598$
Curves	$y^2 = x^3 + 2x$
$n = p_1 p_2 p_3$	566234142875821840780288412704986392583220713, where $\log_2 n = 151$ with $\log_2 p_1 = 50$, $\log_2 p_2 = 51$, $\log_2 p_3 = 50$
g_1	(81548062600040187575403827416750854007349741343136341005476320970822261186966492832468175944856145097506376599058855300281182547908272403378253116621755351058990424305578418745882 6: 401651204535170985287741440897419801958272435870013778389443083056917764854606427110441201960997806737652925849407018199779835174094261831415431466883958957569494786789243486885425)
g_2	(52319751706087867127198336786266810960958341884407003568694522492357013672277660922331394702803533732353434662700091517991915385941058452904509990194782348249532290504626022489694 2: 260570329107605390794080892421196594471140273461760588121577364564786295034005793802859289551577530607288747904475821942996205124330951003761887178412668793557405297661442873788686)
g_T	882586683663552083670275758545909413371735242577186838871004859284660746426395362342279791567302271280790968320552268531347845648562937883445181531931978190549253954893690857759496

example, G_2 is a cyclic subgroup of $E(F_{q^2})$ and G_T is a cyclic subgroup of the multiplicative group $F_{q^2}^*$. For simplicity, we present the case $G_2 \subset E(F_q) \subset E(F_{q^2})$, and $G_T \subset F_q^* \subset F_{q^2}^*$. In [12], Scott presents an efficient setup for some choice of curves with $k = 2$ and implementations.

Example 3. We provide an example of a pairing, $\hat{e}: G_1 \times G_2 \to G_T$ with $n = p_1p_2p_3$, $k = 4$, $D = 1$. We consider an elliptic curve over F_q, defined by $y^2 = x^3 + 2x$. In addition, we choose the cyclic groups $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, and $G_T = \langle g_T \rangle$ as shown in Table 3.

Because we consider the embedding degree $k = 4$ in this example, G_2 is a cyclic subgroup of $E(F_{q^4})$ and G_T is a cyclic subgroup of the multiplicative group $F_{q^4}^*$. For simplicity, we present the case $G_2 \subset E(F_q) \subset E(F_{q^4})$, and $G_T \subset F_q^* \subset F_{q^4}^*$.

For a given pairing, $\hat{e}: G_1 \times G_2 \to G_T$, of composite order, we can define the product pairing $e: G_1^2 \times G_2^2 \to G_T^4$ as in Definition 1 with the projections $\pi_i : G_i^2 \to G_i^2$ for $i = 1, 2$ and $\pi_T : G_T^4 \to G_T^4$, where (1) holds.

2. DDH Problem (DDHP) on Cyclic Groups of Composite Order

In our paper, we consider a bilinear group G of composite order, where the DDHP is infeasible on G. There are known results on the hardness of the discrete logarithm problem on a cyclic group of composite order in terms of the subgroups of prime orders [9]. However, we cannot find any results on the DDHP on a cyclic group of composite order. In this paper, we present how to assure the hardness of the DDHP on a cyclic group of composite order.

The DDHP on a cyclic group G is the problem of deciding if $z = g^{ab}$ for a given random triple $(g, g^a, g^b, z) \in G^4$. For our purposes, we define the DDHP on the product of cyclic groups of prime order.

The DDHP for the group $G_{p_1} \times \cdots \times G_{p_t}$ is the problem to decide whether $z_i = u_i^{a_i b_i}$, for all i and for a randomly given tuple $((u_1, u_2, \ldots, u_t);\ u_1^{a_1}, \ldots, u_t^{a_t},\ u_1^{b_1}, \ldots, u_t^{b_t};\ z_1, \ldots, z_t)$.

Now, we prove the following theorem on the equivalences of the hardness of the DDHP for the groups G and $G_{p_1} \times \cdots \times G_{p_t}$.

Theorem 1. The DDHP for a cyclic group G with $|G| = n = p_1 \cdots p_t$ is equivalently hard to the DDHP for a product group $G_{p_1} \times \cdots \times G_{p_t}$, where $G_{p_i} = \langle u_i \rangle$ with $u_i = g^{n/p_i}$.

Proof. It is enough to show that any DDHP instance for G can be converted to a DDHP instance for $G_{p_1} \times \cdots \times G_{p_t}$, which gives the correct answer to the original instance of the DDHP in G, and vice versa. Suppose that the DDHP instance $(g, g^a, g^b, z) \in G^4$ is given. We compute an instance of DDHP for the group $G_{p_1} \times \cdots \times G_{p_t}$ as follows:

$$T = \left((u_1, \ldots, u_t); (u_1^{a_1}, \ldots, u_t^{a_t}), (u_1^{b_1}, \ldots u_t^{b_t}); (z_1, \ldots, z_t)\right),$$

where $u_i = g^{n/p_i}$, $u_i^{a_i} = (g^a)^{n/p_i}$, $u_i^{b_i} = (g^b)^{n/p_i}$, and $z_i = z^{n/p_i}$. It is clear to see that T is a DDH tuple for $G_{p_1} \times \cdots \times G_{p_t}$ if and only if (g, g^a, g^b, z) is a DDH tuple for G. Therefore, the solution of a DDHP for the instance T is the solution of the DDHP instance (g, g^a, g^b, z) in G.

Now, we suppose that an instance S of the DDHP for the group $G_{p_1} \times \cdots \times G_{p_t}$ is given as

$$S = \left((u_1, \ldots, u_t);\ u_1^{a_1}, \ldots, u_t^{a_t},\ u_1^{b_1}, \ldots, u_t^{b_t};\ z_1, \ldots, z_t\right).$$

We compute an instance (g, v, w, z) of the DDHP for group G as follows:

$$\begin{cases} g = u_1 u_2 \cdots u_t, \\ v = u_1^{a_1} u_2^{a_2} \cdots u_t^{a_t}, \\ w = u_1^{b_1} u_2^{b_2} \cdots u_t^{b_t}, \\ z = z_1 z_2 \cdots z_t. \end{cases}$$

Now, we show that (g, v, w, z) is a DDH tuple in G if and only if S is a DDH tuple in $G_{p_1} \times \cdots \times G_{p_t}$. Because the order of u_i, z_i's is p_i, we see that

$$\begin{cases} g^{\frac{n}{p_i}} = u_i^{\frac{n}{p_i}}, \\ v^{\frac{n}{p_i}} = u_i^{\frac{a_i n}{p_i}}, \\ w^{\frac{n}{p_i}} = u_i^{\frac{b_i n}{p_i}}, \\ z^{\frac{n}{p_i}} = z_i^{\frac{n}{p_i}}, \end{cases} \quad \text{or equivalently} \quad \begin{cases} \left(g^{\frac{n}{p_i}}\right)^{\zeta_i} = u_i, \\ \left(v^{\frac{n}{p_i}}\right)^{\zeta_i} = u_i^{a_i}, \\ \left(w^{\frac{n}{p_i}}\right)^{\zeta_i} = u_i^{b_i}, \\ \left(z^{\frac{n}{p_i}}\right)^{\zeta_i} = z_i. \end{cases}$$

Here, we use the fact that there are $s_i, \zeta_i \in Z$ such that $s_i p_i + \zeta_i \cdot \dfrac{n}{p_i} = 1$ from $\gcd\left(p_i, \dfrac{n}{p_i}\right) = 1$.

Therefore, we see that if (g, v, w, z) is a DDH tuple in G, then $(u_i, u_i^{a_i}, u_i^{b_i}, z_i)$ is a DDH tuple in G_{p_i} for all $i = 1, \ldots, t$; that is, S is a DDH tuple in $G_{p_1} \times \cdots \times G_{p_t}$. Conversely, if S is a DDH tuple in $G_{p_1} \times \cdots \times G_{p_t}$, then $(g^{n/p_i}, v^{n/p_i}, w^{n/p_i}, z^{n/p_i})$ is a DDH tuple in G_{p_i} for all i, which implies that (g, v, w, z) is a DDH tuple in G.

Therefore, the solution of the DDHP for the instance (g, v, w, z) in G is the solution of the DDHP instance S in $G_{p_1} \times \cdots \times G_{p_t}$. ■

By Theorem 1, we see that the DDHP in the cyclic group G with $|G| = n = p_1 \cdots p_t$ is hard if and only if the DDHP is hard in the cyclic subgroup of G of order p_i, for all $i = 1, \ldots, t$. Therefore, one has to choose p_i's as large as the order of the cyclic group where the DDH assumption holds to assure the hardness of the DDHP in G. Currently, by taking the size of p_i's to be as large as 224 bits, we can assume that the DDHP in G is hard.

IV. Our Construction

1. Proposed Scheme

We now present our message expansion of the BGN cryptosystem by using a product of composite pairing. We present how to expand the message size by up to t times. In our construction, we set the message space as Z_N, where $N = q_1 \cdots q_t$; the q_i's are small distinct primes, where the discrete logarithm problem with an exponent less than q_i is easily solvable. Note the factor q_i is of the same size as the message size of the original BGN as well as Freeman's construction. Therefore, our construction expands the plaintext size by up to t times compared to the original schemes.

KeyGen: for a given security parameter, proceed with the following:

1) Generate a bilinear map $\hat{e}: G_1 \times G_2 \to G_T$ of a composite order $|G_j| = |G_T| = n = p_1 \cdots p_t$, where $G_j = \langle g_j \rangle$ for $j = 1$, 2 and $p_1, \ldots, p_t$ are distinct primes of λ bits. And construct the composite product pairing $e: G_1^2 \times G_2^2 \to G_T^4$ as in Definition 1.

2) Generate $\mathbf{g}_j \in G_j^2$ at random.

3) Generate $(a_1, b_1), (a_2, b_2) \in Z_n^* \times Z_n^*$ at random and set

$$\mathbf{h}_1 = \left(g_1^{a_1}, g_1^{b_1}\right), \quad \mathbf{h}_2 = \left(g_2^{a_2}, g_2^{b_2}\right),$$

$$\mathbf{A}=\begin{bmatrix}-b_1 & -b_1\\ a_1 & a_1\end{bmatrix},\quad \mathbf{B}=\begin{bmatrix}-b_2 & -b_2\\ a_2 & a_2\end{bmatrix}.$$

We denote $H_i=\langle \mathbf{h}_i\rangle \subset G_i^2$.

4) Set

$$\begin{cases}\pi_1(u_1,v_1)=(u_1,v_1)^{\mathbf{A}},\\ \pi_2(u_2,v_2)=(u_2,v_2)^{\mathbf{B}},\\ \pi_T(\gamma_1,\gamma_2,\gamma_3,\gamma_4)=(\gamma_1,\gamma_2,\gamma_3,\gamma_4)^{\mathbf{A}\otimes\mathbf{B}}.\end{cases}$$

5) Set the message space Z_N, where $N=q_1\ \ldots\ q_t$ and q_i's are small distinct primes, as described above.

6) Output

$$\text{pk}=\left(N,(p_i)_{1\le i\le t},\mathbf{g}_1,\mathbf{g}_2,\mathbf{h}_1,\mathbf{h}_2,e:G_1^2\times G_2^2\to G_T^4\right),$$
$$\text{sk}=(\pi_1,\pi_2,\pi_t).$$

Enc: for a message $m\in Z_N$,

a) for the prime factors q_i of N, compute $\text{mod}_{q_1,\ldots,q_t}(m)=(m_1,\ldots,m_t)\in Z_{q_1}\times\cdots\times Z_{q_t}$.

b) compute the ciphertext, for $n=p_1\cdots p_t$, and randomly choose $r,r'\in Z_n^*$.

$$\mathbf{c}=\left((\mathbf{g}_1)^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}(\mathbf{h}_1)^r,(\mathbf{g}_2)^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}(\mathbf{h}_2)^{r'}\right).$$

Eval$_\times$: for ciphertexts $\mathbf{c}_1,\mathbf{c}_2\in G_1^2\times G_2^2$, compute

$$\mathbf{c}_\times=e\left(\text{proj}_1(\mathbf{c}_1),\text{proj}_2(\mathbf{c}_2)\right)\in G_T^4.$$

Eval$_+$: for ciphertexts $\mathbf{c}_1$, $\mathbf{c}_2$, compute

$$\mathbf{c}_+=\begin{cases}\mathbf{c}_1\cdot\mathbf{c}_2 & \text{Case (i)},\\ \mathbf{c}_1\cdot\mathbf{c}_2 & \text{Case (ii)},\\ \mathbf{c}_2\cdot e\left(\mathbf{g}_1,\ \text{proj}_2(\mathbf{c}_1)\right) & \text{Case (iii)},\\ \mathbf{c}_1\cdot e\left(\mathbf{g}_1,\ \text{proj}_2(\mathbf{c}_2)\right) & \text{Case (iv)}.\end{cases}$$

Here, we set

Case (i): $\mathbf{c}_1,\mathbf{c}_2\in G_1^2\times G_2^2$,

Case (ii): $\mathbf{c}_1,\mathbf{c}_2\in G_T^4$,

Case (iii): $\mathbf{c}_1\in G_1^2\times G_2^2$, $\mathbf{c}_2\in G_T^4$,

Case (iv): $\mathbf{c}_2\in G_1^2\times G_2^2$, $\mathbf{c}_1\in G_T^4$.

Dec: for a ciphertext $\mathbf{c}$, proceed with one of the following:

1) Case 1: $\mathbf{c}\in G_T^4$. Compute $\mathbf{w}=\pi_T(\mathbf{c})\in G_T^4$. For $i=1,2,\ldots,t$, compute $\mathbf{y}_i=\mathbf{w}^{n/p_i}$, compute $\mathbf{z}_i=\pi_T\left(e(\mathbf{g}_1,\mathbf{g}_2)\right)^{n^3/p_i^3}$, compute $\alpha_i=\log_{\mathbf{z}_i}\mathbf{y}_i$. Compute $\alpha=\text{CRT}_{q_1,\ldots,q_t}(\alpha_1,\ldots,\alpha_t)$. Output α as the plaintext.

2) Case 2: $\mathbf{c}=((c_{11},c_{12}),(c_{21},c_{22}))\in G_1^2\times G_2^2$. Compute $\mathbf{w}=\pi_1\left(\text{proj}_1(\mathbf{c})\right)\in G_1^2$. For $i=1,2,\ldots,t$, compute $\mathbf{y}_i=\mathbf{w}^{n/p_i}$, compute $\mathbf{z}_i=\left(\pi_1(\mathbf{g}_1)\right)^{n^2/p_i^2}$, compute $\alpha_i=\log_{\mathbf{z}_i}\mathbf{y}_i$. Compute $\alpha=\text{CRT}_{q_1,\ldots,q_t}(\alpha_1,\ldots,\alpha_t)$. Output α as the plaintext.

2. Correctness of Our Construction

Recall the fact that $H_i\subset\ker(\pi_i)$ and $e\left(\pi_1(\mathbf{g}_1),\pi_2(\mathbf{g}_2)\right)=\pi_T\left(e(\mathbf{g}_1,\mathbf{g}_2)\right)$. Now, we check the correctness of our construction. First, we want to show that Dec(sk, Enc(pk, m)) = m. We consider Enc(pk, m) = $\mathbf{c}$, which has the following form:

$$\mathbf{c}=\left(\mathbf{g}_1^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}\cdot\mathbf{h}_1^{\,r},\mathbf{g}_2^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}\cdot\mathbf{h}_2^{\,r'}\right).$$

Then, we have the following, successively:

1) $\mathbf{w}=\pi_1\left(\text{proj}_1(\mathbf{c})\right)=\pi_1(\mathbf{g}_1)^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}$.

2) $\mathbf{y}_i=\mathbf{w}^{\frac{n}{p_i}}=\pi_1(\mathbf{g}_1)^{m_i\cdot\frac{n^2}{p_i^2}}$,

3) $\alpha_i=\log_{\mathbf{z}_i}\mathbf{y}_i=m_i$, where $\mathbf{z}_i=\left(\pi_1(\mathbf{g}_1)\right)^{\frac{n^2}{p_i^2}}$.

Therefore, we have

$$\alpha=\text{CRT}_{q_1,\ldots,q_t}(m_1,\ldots,m_t)=m.$$

Now, we check the correctness of Eval$_\times$ in our construction. The input of the algorithm Eval$_\times$ is of the form $\mathbf{c},\mathbf{c}'\in G_1^2\times G_2^2$ such that Enc(pk, m) = $\mathbf{c}$ and Enc(pk, m') = $\mathbf{c}'$ for some $m,m'\in Z_N$. Then, we get the following, successively:

1) $$\begin{aligned}\mathbf{c}_\times&=\text{Eval}_\times\left(\text{pk},(\mathbf{c},\mathbf{c}')\right)\\&=e\left(\text{proj}_1(\mathbf{c}),\text{proj}_2(\mathbf{c}')\right)\\&=e\left(\mathbf{g}_1^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}}\mathbf{h}_1^{\,r},\mathbf{g}_2^{\frac{m'_1n}{p_1}+\cdots+\frac{m'_tn}{p_t}}\mathbf{h}_2^{\,r'}\right).\end{aligned}$$

2) $$\begin{aligned}\mathbf{w}&=\pi_T(\mathbf{c}_\times)\\&=e\left(\pi_1(\mathbf{g}_1)^{\frac{m_1n}{p_1}+\cdots+\frac{m_tn}{p_t}},\pi_2(\mathbf{g}_2)^{\frac{m'_1n}{p_1}+\cdots+\frac{m'_tn}{p_t}}\right).\end{aligned}$$

3) $$\begin{aligned}\mathbf{y}_i&=\mathbf{w}^{\frac{n}{p_i}}=e\left(\pi_1(\mathbf{g}_1)^{\frac{m_in}{p_i}},\pi_2(\mathbf{g}_2)^{\frac{m'_in}{p_i}}\right)^{\frac{n}{p_i}}\ \ldots\ldots..(*)\\&=e\left(\pi_1(\mathbf{g}_1),\pi_2(\mathbf{g}_2)\right)^{\frac{m_im'_in^3}{p_i^3}}\\&=\pi_T\left(e(\mathbf{g}_1,\ \mathbf{g}_2)\right)^{\frac{m_im'n^3}{p_i^3}}.\end{aligned}$$

4) $\alpha_i=\log_{\mathbf{z}_i}\mathbf{y}_i=m_im'_i$, for $\mathbf{z}_i=\pi_T\left(e(\mathbf{g}_1,\mathbf{g}_2)\right)^{\frac{n^3}{p_i^3}}$.

The equality (*) above is true from the fact that

$$e\left(\pi_1(\mathbf{g}_1)^{\frac{m_in}{p_i}},\pi_2(\mathbf{g}_2)^{\frac{m'_jn}{p_j}}\right)=1\quad\text{if } i\neq j.$$

Therefore, we have

$$\alpha=\text{CRT}_{q_1,\ldots,q_t}\left(m_1m'_1,\ldots,m_tm'_t\right)=mm'.$$

Because the multiplications of the group elements correspond to the addition of the exponents, one can similarly show the correctness of Eval_+.

3. Security Analysis

As in Freeman's BGN cryptosystem, the IND-CPA security of our scheme is based on the hardness of the subgroup decision for $H_j \subset G_j^2$.

Theorem 2. If the subgroup decision problems of $H_j \subset G_j^2$ for randomly chosen subgroups H_j are hard, then the new scheme in our construction is IND-CPA secure.

Proof. It is enough to show that if there is a successful IND-CPA adversary X against our encryption scheme, then we can construct a successful solver D of the subgroup decisional problem of $H_j \subset G_j^2$ for some j (= 1 or 2). Without loss of generality, we assume $j = 1$ and the subgroup decision problem for $j = 2$ is hard. For a given instance $\left(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \mathbf{z}_1 \in G_1^2\right)$ of the subgroup decision problem for $j = 1$, D acts as the challenger of an IND-CPA security game to the adversary X against our encryption with $\mathrm{pk} = \left(e, \mathbf{g}_j \in G_j^2, \mathbf{h}_j \in H_j, j = 1,2\right)$ for randomly chosen $\left(H_2 = \langle \mathbf{h}_2 \rangle, G_2 = \langle \mathbf{g}_2 \rangle\right)$. For the given messages m_0, m_1, which are arbitrarily chosen by the IND-CPA adversary X, the challenger D chooses random $b \in \{0,1\}$ and computes $\mathbf{c}_b = \left(\mathbf{g}_1^{\phi(m_b)} \mathbf{z}_1^{r_1}, \mathbf{g}_2^{\phi(m_b)} \mathbf{h}_2^{r_2}\right)$, where

$$\phi(m_b) = \sum \frac{m_{b,i} n}{p_i} \text{ with } \mathrm{mod}_{q_1,\ldots,q_t}(m_b) = (m_{b,1}, \ldots, m_{b,t}).$$

Challenger D sends $\mathbf{c}_b$ to adversary X and then X responds with $b' \in \{0,1\}$. Challenger D outputs 1, which means $\mathbf{z}_1 \in H_1$, if and only if $b' = b$.

We consider three IND-CPA security games with respect to the same public key, $\mathrm{pk} = \left(e, \mathbf{g}_j \in G_j^2, \mathbf{h}_j \in H_j, j = 1,2\right)$. The differences of each game are from the construction of the ciphertext to be challenged in the following way:

1) $\mathrm{Game}_0 : \mathbf{c}_b' = \left(\mathbf{g}_1^{\phi(m_b)} \mathbf{h}_1^{r_1}, \mathbf{g}_2^{\phi(m_b)} \mathbf{h}_2^{r_2}\right)$,

2) $\mathrm{Game}_1 : \mathbf{c}_b'' = \left(\mathbf{g}_1^{\phi(m_b)} \overrightarrow{w_1}^{r_1}, \mathbf{g}_2^{\phi(m_b)} \mathbf{h}_2^{r_2}\right)$

for randomly chosen $\overrightarrow{w_1} \in G_1^2$,

3) $\mathrm{Game}_2 : \mathbf{c}_b''' = \left(\mathbf{g}_1^{\phi(m_b)} \overrightarrow{w_1}^{r_1}, \mathbf{g}_2^{\phi(m_b)} \overrightarrow{w_2}^{r_2}\right)$

for randomly chosen $\mathbf{w}_1 \in G_1^2$ and $\mathbf{w}_1 \in G_2^2$.

We note that Game_0 is exactly the same as the IND-CPA security of our encryption scheme. From the hardness of the subgroup decision problem for $H_2 \subset G_2^2$, $\mathbf{c}_b''$ and $\mathbf{c}_b'''$ are indistinguishable for any probabilistic polynomial time adversary; therefore, we see that Pr[X wins Game_1] – Pr[X wins Game_2] is negligible. Because $\mathbf{c}_b'''$ is uniformly distributed in $G_1^2 \times G_2^2$, we see that Pr[X wins Game_2] = 1/2.

For challenger D, as a solver of the subgroup decision problem, we have

$$\begin{aligned}
&\Pr[D(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \vec{\mathbf{z}}_1 \in H_1) = 1] \\
&\quad = \Pr[\text{X wins } \mathrm{Game}_0] \\
&\quad = \epsilon(n), \\
&\Pr[D(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \mathbf{z}_1 \in^{rand} G_1^2) = 1] \\
&\quad = \Pr[X \text{ wins } \mathrm{Game}_1] \\
&\quad = \Pr[X \text{ wins } \mathrm{Game}_2] + \mathrm{negl}(n) \\
&\quad = 1/2 + \mathrm{negl}(n).
\end{aligned}$$

Therefore, we see that

$$\begin{aligned}
&|\Pr[D(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \mathbf{z}_1 \in H_1) = 1] \\
&\quad - \Pr[D(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \mathbf{z}_1 \in^{rand} G_1^2) = 1]| \\
&\quad = |\epsilon(n) - \frac{1}{2} + \mathrm{negl}(n)|.
\end{aligned}$$

Because X is a successful IND-CPA adversary against our scheme, we see that $\epsilon(n) - 1/2$ is non-negligible; therefore, $|\epsilon(n) - 1/2 + \mathrm{negl}(n)|$ is non-negligible. Thus, D is a successful solver of the subgroup decision problem $\left(H_1 = \langle \mathbf{h}_1 \rangle, G_1^2 = \langle \mathbf{g}_1 \rangle, \mathbf{z}_1 \in G_1^2\right)$. ■

Now, we analyze the strength of the subgroup decision assumption of $H_j \subset G_j^2$ with $|G_j| = n = p_1 \cdots p_t$ for randomly chosen subgroup H_j.

Theorem 3. The subgroup decision assumption of $H_j \subset G_j^2$ for randomly chosen subgroup H_j is equivalent to the DDH assumption in the cyclic group G_j with $|G_j| = n$ for $j = 1, 2$.

Proof. We prove only the case where $j = 1$; the proof for $j = 2$ is similar. Suppose that one can solve the subgroup decision problem of group G_1^2 for a randomly chosen subgroup with non-negligible probability. Suppose that an instance $(u, v, y, z) \in G_1^4$ of DDHP in G_1 is given. We consider a subgroup $H_1 = \langle (u^a, v^b) \rangle$ of G_1^2 for randomly chosen $a, b \in Z_n^*$ so that H_1 can be considered as a randomly chosen subgroup of G_1^2. Now, consider a tuple $\mathbf{w}' = (y^a, z^b) \in G_1^2$. We see that the following hold:

1) $\mathbf{w}' \in H_1$,

2) $(y, z) \in \langle (u, v) \rangle$,

3) (u, v, y, z) is a DDH tuple in G_1.

By solving the subgroup decision problem of G_1^2 for the randomly given subgroup $H_1 = \langle (u^a, v^b) \rangle$ and $\mathbf{w}' = (y^a, z^b) \in G_1^2$, one can correctly decide whether (u, v, y, z) is a DDH tuple in G_1. Therefore, we see that one can solve the DDHP in G_1 by using a solver of the subgroup decision problem of G_1^2. For the proof of the converse, suppose that the DDHP in G_1 is solvable with non-negligible probability. We consider the subgroup decision problem of G_1^2 for $H_1 = \langle u, v) \rangle (\subset G_1^2$ and $(y, z) \in G_1^2$. We see that the following are equivalent for

http://dx.doi.org/10.4218/etrij.16.0115.0630

randomly chosen $a \in Z_n^*$:

1) (u^a, v^a, y^a, z^a) is a DDH tuple in G_1,

2) $(y^a, z^a) \in H_1$,

3) $(y, z) \in H_1$.

By solving the DDHP in G_1 for the random instance (u^a, v^a, y^a, z^a), one can solve the given instance of the subgroup decision problem of G_1^2. Therefore, we see that one can solve the subgroup decision problem of G_1^2 by using a solver of the DDHP in G_1. ■

Now, by the results of Theorems 1–3, we see that our construction using the pairing $\hat{e}: G_1 \times G_2 \to G_T$, where $G_j = \langle g_j \rangle$ and $|G_j| = n = p_1 p_2 \cdots p_t$, is IND-CPA secure if p_i is large enough to guarantee the DDH assumption on the cyclic group $G_{j,p_i} = \langle g_j^{n/p_i} \rangle$ for all $i = 1, 2, \ldots, t$ and $j = 1, 2$.

4. Selection of Parameters for Current Security Level

For the current security level (that is, 112-bit security until the year 2030 [3], [4]), it is required that $(q^k - 1)/n = \ell$ is of 2,048 bits for the pairing $\hat{e}: G_1 \times G_2 \to G_T$ with $|G_1| = |G_2| = |G_T| = n$ and embedding degree k. Recall that G_2 is a subgroup of an elliptic curve group over the finite field F_q, and G_T is a subgroup of the multiplicative group $F_{q^k}^*$. Because G_1 is a subgroup of the elliptic curve group $E(F_q)$, it is assumed that $\log n \le \log q$. We can expand the message size to t times larger than the BGN cryptosystem by using $|G_i| = p_1 p_2 \ldots p_t$. According to reports [3], [4], to guarantee the DDH assumption on G_i until the year 2030, it is recommended as $\log p_i \sim 224$. Table 4 suggests the suitable parameters of our construction for a 112-bit security level.

According to Table 1, for a 112-bit security level, using the embedding degree as $k = 1, 2$ expands the message by up to nine times. We note that the ciphertexts belong to either $G_1^2 \times G_2^2$ or $G_T^4 \subset (F_{q^k})^4$. Therefore, the bit-size of ciphertext in our scheme is at most 16,384.

Table 5 presents selection parameters for a 112-bit security level in Freeman's construction using prime product pairing [5]. In the prime case as in Table 2, a relatively small q can be used to encrypt a message. However, expanding the size of a message as much as up to t times by using the naive approach of direct CRT requires t implementations of the initial scheme, which makes it impractical for large t, such as t = 9. In particular, for any choice of embedding degree, we see that the ciphertext after Eval$_\times$ is an element in $\left(G_T^4\right)^9 \subset \left(F_{q^k}\right)^{36}$, which means that its bit-size is about 73,728. We also note that this is 4.5 times larger than our construction using composite pairing.

In the case of k = 2, we need a pairing-friendly curve with ratio log q/log n = 1, which is very rare in the construction of the current pairing-friendly elliptic curves of composite order. Finding an efficient pairing-friendly elliptic curve of composite degree with rate log q/log n = 1 is an interesting subject of future research. Currently, selecting an embedding degree of k = 1 in our scheme is the most efficient solution, and it expands the size of a message by up to nine times that achieved by using Freeman's product pairing of prime order.

Table 4. Selecting parameters for 112-bit security.

k	1	2	4	6	12
log q	4,096	2,048	1,024	683	342
log n	2,048	2,048	1,024	683	342
t	9	9	4	3	1

Table 5. Prime (n) order case of 112-bit security.

k	1	2	4	6	12
log q	2,048	1,024	512	342	224
log n	224	224	224	224	224

V. Conclusion

In this paper, we presented how to expand the message size of the BGN cryptosystem using a product pairing of composite order. We use composite order not to provide the security of the scheme but to expand the message size. The security of our scheme is based on the DDH assumption on the subgroups of prime order of the underlying composite pairing group. We also presented how to select parameters that expand the message size more efficiently.

References

[1] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," Theory of Cryptography-TCC 2005, Springer Verlag, LNCS 3378, 2005, pp. 325–341.

[2] J. Tibor and S. Jorg, "On the Analysis of Cryptographic Assumptions in the Generic Ring Model," *J. Cryptology*, vol. 26, no. 2, Apr. 2013, pp. 225–245.

[3] Fact Sheet Suite B Cryptography, NSA. Accessed June 1, 2015. https://www.nsa.gov/ia/programs/suiteb_cryptography/

[4] Algorithms for Qualified Electronic Signatures, BNetzA, BSI, Feb. 2013, updated with BSI Draft, Oct. 2013.

[5] D. Freeman, "Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups," *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2010, pp. 44–61.

[6] A. Guillevix, "Comparing the Pairing Efficiency over Composite Order and Prime Order Elliptic Curves," *Appl. Cryptography Netw. Security*, *Springer LNCS*, vol. 7954, 2013, pp. 357–372.

[7] H.-S. Lee and S. Lim, "A Depth Specific Description of Somewhat Homomorphic Encryption and its Applications," *Appl. Math. Inf. Sci.*, vol. 9, no. 3, 2015, pp. 1345–1353.

[8] D. Boneh, K. Rubin, and A. Silverberg, "Finding Composite Order Ordinary Elliptic Curves Using the Cocks-Pinch Method," *J. Number Theory*, vol. 131, 2011, pp. 832–841.

[9] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(P) and its Cryptographic Significance," *IEEE Trans. Inf. Theory*, vol. 24, no. 1, Jan. 1978, pp. 106–110.

[10] N. Koblitz, "A Security in Composite-Order Pairing-Based Protocols with Embedding Degree K>2," Cryptology ePrint Archive Report 2010, p. 227.

[11] X. Zhang and D. Lin, "Efficient Pairing Computation on Ordinary Elliptic Curve of Embedding Degree 1 and 2," *Cryptography Coding*, *LNCS*, vol. 7089, 2011, pp. 309–326.

[12] M. Scott, "Computing the Tate Pairing," *Topic Cryptography*, *LNCS*, vol. 3376, 2005, pp. 293–304.

Soo Kyung Eom received her PhD degree in mathematics from Ewha Womans University, Seoul, Rep. of Korea, in 2011. She is a post-doctoral scholar at the Institute of Mathematical Sciences, Ewha Womans University. Her main research interests include pairing-based cryptography, such as efficiency and security issues for pairing computation and construction of elliptic curves.

Hyang-Sook Lee received her PhD degree in mathematics from Northwestern University, Evanstone, IL, USA, in 1993. She is currently a professor with the Department of Mathematics, Ewha Womans University, Seoul, Rep. of Korea. Her research interests are pairing-based cryptography, especially pairing computations, constructing pairing friendly curves, digital signatures, and public key cryptography.

Seongan Lim received her PhD degree in mathematics from Purdue University, West Lafayetle, IN, USA, in 1995. She is currently a research professor at the Institute of Mathematical Sciences, Ewha Womans University, Seoul, Rep. of Korea. Her research interests include public key cryptography and privacy preserving protocols.

http://dx.doi.org/10.4218/etrij.16.0115.0630