A Note on Bilinear Groups of a Large Composite Order

Zhengjun Cao[1], Lihua Liu[2,*]

Abstract

We remark that the structure of bilinear groups of a large composite order (at least 1024 bits) could make group operation inefficient and lose the advantages of elliptic curve cryptography which gained mainly from smaller parameter size. As of 2013, the longest parameter recommended by NIST for elliptic curves has 571 bits. From the practical point of view, such an algebraic structure is unlikely applicable to cryptographic schemes.

Keywords: bilinear groups of composite order; homomorphic public-key encryption.

1 Introduction

The use of elliptic curves in cryptography was suggested independently by N. Koblitz [4] and V. Miller [6] in 1985. It is well-known that the advantages of elliptic curve cryptography are mainly gained from smaller parameter size. It is generally accepted that a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key [3].

Weil pairing plays a key role in elliptic curve cryptography. In 1993, Menezes, Okamoto and Vanstone [7] suggested to use Weil pairing to reduce elliptic curve logarithms to logarithms in a finite field. In 2001, Boneh and Franklin [2] proposed a fully functional identity-based encryption scheme based on Weil pairing. Since then, an abundance of research has been published on the efficient implementation of these pairings (modified Weil pairing, Tate pairing), as well as cryptographic schemes using bilinear pairings. Except the general restrictions on the domain parameters for an elliptic curve E over a finite field $\mathbb{F}_q$, these bilinear pairings require that the underlying groups

[1]Department of Mathematics, Shanghai University, Shanghai, China. [2]Department of Mathematics, Shanghai Maritime University, Shanghai, China. liulh@shmtu.edu.cn

should be of prime order $n\,(> 2^{160})$ so that the ECDLP is resistant to all known attacks, such as Pohlig-Hellman attack, Pollard's rho attack. Thus, it is necessary that the cardinality $\#E(\mathbb{F}_q)$ should be divisible by a sufficiently large prime n.

In 2005, Boneh, Goh and Nissim [1] introduced the subgroup decision problem over bilinear groups of a large composite order n so that it supports a homomorphic public key encryption. They assume that it is hard to decide if an element in a subgroup, without knowing the factorization of n. Since then, researchers have proposed some cryptographic schemes [5, 10, 11] based on subgroup decision problem. It seems that the algebraic structure (bilinear groups of a large composite order) facilitates the security arguments of these protocols [5, 10, 11].

In this note we would like to stress that bilinear groups of a large composite order (at least 1024 bits) could make group operation very slow. So far, there are no testing reports on this topic. From the practical point of view, such an algebraic structure is unlikely applicable to cryptographic schemes although it facilitates to design some complicated cryptographic protocols.

2 Bilinear groups of composite order

Let $\mathcal{G}$ be a group generation algorithm that takes security parameter 1^λ as input and outputs tuple $(p, q, \mathbb{G}, \mathbb{G}_1, e)$ where p and q are distinct primes, $\mathbb{G}$ and $\mathbb{G}_1$ are cyclic groups of order $n = p\,q$, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is a non-degenerate bilinear map, i.e., it satisfies: (i) bilinear: for $\forall\, g_1, g_2 \in \mathbb{G}$ and $\forall\, a, b \in \mathbb{Z}$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{a\,b}$; (ii) non-degenerate: for generator g of $\mathbb{G}$, $e(g, g)$ generates $\mathbb{G}_1$.

Let $\mathbb{G}_p$ and $\mathbb{G}_q$ denote the subgroups of $\mathbb{G}$ of order p and q, respectively. Then $\mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q$. If g is a generator of $\mathbb{G}$, then g^q and g^p are generators of $\mathbb{G}_p$ and $\mathbb{G}_q$, respectively. Let g_p and g_q denote the generators of $\mathbb{G}_p$ and $\mathbb{G}_q$, respectively. For all random elements $h_p \in \mathbb{G}_p$ and $h_q \in \mathbb{G}_q$, We have

$$e(h_p, h_q) = 1$$

because $e(h_p, h_q) = e(g_p^a, g_q^b)$ for some integers a, b, and $e(g_p^a, g_q^b) = e(g^{q\,a}, g^{p\,b}) = e(g, g)^{p\,q\,a\,b} = 1$ for some generator g in $\mathbb{G}$.

We here stress that the subgroup decision assumption over a bilinear group $\mathbb{G}$ requires a large composite order n so that it is resistant to all known factoring methods.

3 Boneh-Goh-Nissim homomorphic encryption

In 2005, Boneh, Goh and Nissim [1] introduced the subgroup decision problem over bilinear groups of a large composite order n so that it supports a homomorphic public key encryption. We now relate the scheme as follows.

KeyGen(τ): Given a security parameter $\tau \in Z^+$, run $\mathcal{G}(\tau)$ to obtain a tuple $(q_1, q_2, \mathbb{G}, \mathbb{G}_1, e)$. Let $n = q_1 q_2$. Pick two random generators $g, u \overset{R}{\leftarrow} \mathbb{G}$ and set $h = u^{q_2}$. Then h is a random generator of the subgroup of $\mathbb{G}$ of order q_1. The public key is $PK = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$. The private key is $SK = q_1$.

Encrypt(PK, M): Assume the message space consists of integers in the set $\{0, 1, \cdots, T\}$ with $T < q_2$. To encrypt a message m using public key PK, pick a random $r \overset{R}{\leftarrow} \{0, 1, \cdots, n-1\}$ and compute

$$C = g^m h^r \in \mathbb{G}.$$

Output C as the ciphertext.

Decrypt(SK, C): To decrypt a ciphertext C using the private key $SK = q_1$, observe that

$$C^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m$$

Let $\hat{g} = g^{q_1}$. To recover m, it suffices to compute the discrete log of C^{q_1} base $\hat{g}$. Since $0 \le m \le T$ this takes expected time $\tilde{O}(\sqrt{T})$ using Pollard's lambda method.

Extension: The authors [1] pointed out that anyone can multiply two encrypted messages once using the bilinear map. Set $g_1 = e(g, g)$ and $h_1 = e(g, h)$. Then g_1 is of order n and h_1 is of order q_1. Also, write $h = g^{\alpha q_2}$ for some (unknown) $\alpha \in \mathbb{Z}$. Suppose there are two ciphertexts $C_1 = g^{m_1} h^{r_1} \in \mathbb{G}$ and $C_2 = g^{m_2} h^{r_2} \in \mathbb{G}$. To build an encryption of the product $m_1 \cdot m_2$ mod n given only C_1 and C_2, do: 1) pick a random $r \in \mathbb{Z}_n$, and 2) set $C = e(C_1, C_2) h_1^r \in \mathbb{G}_1$. Then

$$C = e(C_1, C_2) h_1^r = e(g^{m_1} h^{r_1}, g^{m_2} h^{r_2}) h_1^r = g_1^{m_1 m_2} h_1^{m_1 r_2 + r_2 m_1 + \alpha q_2 r_1 r_2 + r} = g_1^{m_1 m_2} h_1^{\tilde{r}} \in \mathbb{G}_1$$

where $\tilde{r} = m_1 r_2 + r_2 m_1 + \alpha q_2 r_1 r_2 + r$ is distributed uniformly in $\mathbb{Z}_n$ as required. Thus, C is a uniformly distributed encryption of $m_1 m_2$ mod n, but in the group $\mathbb{G}_1$ rather than $\mathbb{G}$. Note that the system is still additively homomorphic in $\mathbb{G}_1$.

4 On the large parameters in Boneh-Goh-Nissim homomorphic encryption

In Ref.[1] the authors remark that the Boneh-Goh-Nissim homomorphic encryption resembles the Paillier [9] and the Okamoto-Uchiyama [8] encryption schemes. But it is flawed. The Paillier system is constructed *over a multiplicative subgroup of integers modulo* n^2, where $n = p\,q$, p, q are two large primes. The Okamoto-Uchiyama encryption is constructed *over a multiplicative group over ring* $\mathbb{Z}/n\mathbb{Z}$, where $n = p^2 q$, p, q are two large primes. Unlike the Paillier system and the Okamoto-Uchiyama encryption, the Boneh-Goh-Nissim encryption is constructed *over a bilinear group* $\mathbb{G}$ *of a large composite order* $n = q_1 q_2$, where q_1, q_2 are two large primes so as to prevent the adversary from factoring n.

Let E be an elliptic curve defined over $\mathbb{F}_q$. The number of points in $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$, is called the order of E over $\mathbb{F}_q$. Hasse's theorem provides tighter bounds for $\#E(\mathbb{F}_q)$.

Theorem 1 (Hasse) *Let* E *be an elliptic curve defined over* $\mathbb{F}_q$. *Then*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

So far, bilinear groups used in cryptographic protocols are derived *only* from elliptic curves. To construct a bilinear group with a large composite order n, it requires a large q by the Hasse theorem. If n is of 1024 bits, then the parameter q should be of more bits. As we mentioned before, in classical elliptic curve cryptograph it requires that the parameter q is about of 160 bits. Apparently, a large parameter q (at least 1024 bits) makes group operation inefficient and loses the advantages of elliptic curve cryptograph gained mainly from smaller parameter size.

Remark. As we know, a homomorphic encryption enables "computing with encrypted data". It is a useful tool for secure protocols. The Boneh-Goh-Nissim encryption solves the problem of constructing 'doubly homomorphic' encryption schemes where one may both 'add and multiply'. The multiplicative homomorphism was due to properties of bilinear maps and the knowledge of factoring the order n. Although the Boneh-Goh-Nissim encryption is somewhat impractical, it answered the long standing open question about 'doubly homomorphic' encryption. It seems difficult to rule out its theoretical importance.

References

[1] Boneh, D., Goh, E., Nissim, K.: Evaluating 2-dnf formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325-341. Springer, Heidelberg (2005)

[2] Boneh D., Franklin M.: Identity-Based Encryption from the Weil Pairing. In: Kilian J. (ed.) CRYPTO'2001. LNCS, vol. 2139, pp. 213-229. Springer, Heidelberg (2001)

[3] Hankerson D., Menezes A., Vanstone S.: Guide to Elliptic Curve Cryptography. Springer, Heidelberg (2004)

[4] Koblitz, N: Elliptic curve cryptosystems. Mathematics of Computation 48 (177): 203-209 (1987)

[5] Liu J., Yuen T., Zhou J.: Forward secure ring signature without random oracles. In: Qian S. et al. (eds.) ICICS'2011. LNCS, vol.7043, pp. 1-14. Springer, Heidelberg (2011)

[6] Miller, V: Use of elliptic curves in cryptography. CRYPTO 85: 417-426 (1985)

[7] Menezes A., Okamoto T., Vanstone S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory 39(5): 1639-1646 (1993)

[8] Okamoto T., Uchiyama S.: A new public-key cryptosystem as secure as factoring. In: Nyberg K. (ed.) Eurocrypt'1998. LNCS, vol. 1403, pp. 308-318. Springer, Heidelberg (1998)

[9] Pallier P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern J. (ed.), Eurocrypt'1999. LNCS, vol. 1592, pp. 223-238. Springer, Heidelberg (1999)

[10] Seo J., Kobayashi T., Ohkubo M., Suzuki K.: Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts. In: Jarecki S., Tsudik G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 215-234, Springer, Heidelberg (2009)

[11] Shacham H., Waters B.: Efficient ring signatures without random oracles. In: PKC'2007, LNCS, vol. 4450, pp. 166-180. Springer, Heidelberg (2007)