Bull. Korean Math. Soc. **46** (2009), No. 2, pp. 303–309
DOI 10.4134/BKMS.2009.46.2.303

A NOTE ON SELF-BILINEAR MAPS

Jung Hee Cheon and Dong Hoon Lee

Abstract. Cryptographic protocols depend on the hardness of some computational problems for their security. Joux briefly summarized known relations between assumptions related bilinear map in a sense that if one problem can be solved easily, then another problem can be solved within a polynomial time [6].

In this paper, we investigate additional relations between them. Firstly, we show that the computational Diffie-Hellman assumption implies the bilinear Diffie-Hellman assumption or the general inversion assumption. Secondly, we show that a cryptographic useful self-bilinear map does not exist. If a self-bilinear map exists, it might be used as a building block for several cryptographic applications such as a multilinear map. As a corollary, we show that a fixed inversion of a bilinear map with homomorphic property is impossible. Finally, we remark that a self-bilinear map proposed in [7] is not essentially self-bilinear.

1. Introduction

The Weil pairing on an elliptic curve have been used to solve cryptographic problems such as the discrete logarithm (DL) problem, the computational Diffie-Hellman (CDH) problem, the decisional Diffie-Hellman (DDH) problem [8]. After Joux proposed tripartite Diffie-Hellman protocol using the Weil paring, however, the Weil (or Tate) pairing is being used as a building block of interesting cryptographic protocols including ID-based schemes, a short signature scheme, self-blindable credentials, and key agreement [5, 1, 4, 2, 11, 9].

The *bilinear* property of the pairings plays an important role on pairing-based protocols. Given two groups G and H, a map $e : G \times G \to H$ is said to be bilinear if $e(g_1^{x_1}, g_2^{x_2}) = e(g_1, g_2)^{x_1 x_2}$ for all $x_i \in \mathbb{Z}$ and $g_i \in G$. Given a quadruple (g, g^x, g^y, g^z) the bilinear Diffie-Hellman (BDH) problem asks to find $e(g, g)^{xyz}$.

Received May 22, 2008.

2000 *Mathematics Subject Classification.* Primary 94A60, 11Y16, 68Q15.

Key words and phrases. cryptography, complexity, elliptic curves, pairing, self-bilinear map.

The first author was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. R01-2008-000-11287-0).

The security of most paring-based protocols relies on the BDH assumption, that is, the BDH problem is computationally infeasible. Joux [6] briefly summarized the relations between complexity assumptions in pairing-based cryptography. In this paper, we show that an additional relation exists. More precisely, the CDH assumption on H implies the BDH assumption or the general inversion (GI) assumption which is defined in Section 2.

On the other hand, we investigate the possibility of the existence of inversion of the bilinear map when one of inputs is fixed. We call such an inversion by the fixed inversion (FI). We show that the fixed inversion with homomorphic property does not exist by showing non-existence of a *self-bilinear* map, $e_s : G \times G \to G$ under the CDH assumption on G.

Recently, Lee presented a self-bilinear map $\mathcal{L} : A \times A \to A$, where A is a free R-module with rank two and R is a commutative ring with one [7]. However, the evaluation of $\mathcal{L}$ for a random input (s, t) is impossible unless the decomposition of s and t with respect to generators is not known. Thus $\mathcal{L}$ is not suitable to be used for other cryptographic applications. Moreover we can rewrite $\mathcal{L}$ as a non self-bilinear map.

The rest of the paper is organized as follows: In Section 2, we introduce bilinear maps and several CDH and BDH related problems and recall the known relations between assumptions. We present a new additional relation. In Section 3, we describe a concept of a self-bilinear map and its applications. Unfortunately we show that a cryptographic useful self-bilinear map does not exist and comment about the self-bilinear map presented by Lee [7]. We conclude in Section 4.

2. Bilinear map and hard problems

Throughout this paper, we denote G and H by cyclic groups of prime order p. We use the multiplicative group notations.

2.1. Bilinear map

A map $e : G \times G \to H$ is said to be *bilinear* provided that $e(g_1^{x_1}, g_2^{x_2}) = e(g_1, g_2)^{x_1 x_2}$ for all $x_i \in \mathbb{Z}/p\mathbb{Z}$ and $g_i \in G$. We denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}_p$. The Weil pairing for an elliptic curve is a good example of a bilinear map from an additive group of an elliptic curve to a multiplicative group of a finite field. In this paper, we assume that the bilinear map e has the following properties for practical purposes:

(1) Non-degenerate: There exists a $g \in G$ such that $e(g, g) \neq 1$.

(2) Efficient computable: There is a polynomially-bounded algorithm to compute $e(g_1, g_2)$ for any $g_1, g_2 \in G$.

In fact, the original Weil pairing does not satisfy the non-degeneracy, but a modified Weil pairing defined over supersingular curve has the above properties. A modified Weil paring is described in [1].

There are lots of protocols based on the Weil (or Tate) pairing including ID-based schemes, a short signature scheme, self-blindable credentials, and key agreement [1, 2, 4, 5, 9, 11].

2.2. Hard problems and its relations

Usual standard cryptographic protocols based on the discrete logarithms depend on one of the following assumptions for their security: the hardness of the discrete logarithm problem (DL), of the computational Diffie-Hellman problem (CDH), or of the decisional Diffie-Hellman problem (DDH).

- For any given two values g and g^x, the problem which computes x is called the *discrete logarithm problem* (DL).
- For any given two values g^{x_1} and g^{x_2}, the problem which computes $g^{x_1 x_2}$ is called the *computational Diffie-Hellman problem* (CDH).
- For given two distributions $\{(g^{x_1}, g^{x_2}, g^{x_1 x_2}) \mid x_1 \text{ and } x_2 \text{ are random}\}$ and $\{(g^{x_1}, g^{x_2}, g^r) \mid x_1, x_2 \text{ and } r \text{ are random}\}$, the problem which distinguishes the two distributions is called the *decisional Diffie-Hellman problem* (DDH).

Since bilinear Diffie-Hellman assumption was introduced by Boneh-Franklin [1], the security of most pairing-based protocols depends on the hardness of following problems:

- For any given 4-tuple $(g, g^{x_1}, g^{x_2}, g^{x_3})$, the problem which computes $e(g,g)^{x_1 x_2 x_3}$ is called the *bilinear Diffie-Hellman problem* (BDH).
- For given two distributions $\{(g^{x_1}, g^{x_2}, g^{x_3}, h^{x_1 x_2 x_3}) \mid x_1, x_2 \text{ and } x_3 \text{ are random}\}$ and $\{(g^{x_1}, g^{x_2}, g^{x_3}, h^r) \mid x_1, x_2, x_3 \text{ and } r \text{ are random}\}$, where $h = e(g,g)$, the problem which distinguishes the two distributions is called the *decisional bilinear Diffie-Hellman problem* (DBDH).

Joux considered the two types of inversion problem of the bilinear map, say the fixed inversion (FI) and the general inversion (GI).

- For a fixed $g \in G$ and any given $h \in H$, the problem which finds an inverse image g' such that $e(g, g') = h$ is called *fixed inversion problem* (FI).
- For any given $h \in H$, the problem which finds a pair (g_1, g_2) such that $e(g_1, g_2) = h$ is called *general inversion problem* (GI).

Joux gives the summary of the relations between complexity assumptions [6] (Figure 1). Each arrow in the figure goes from a complexity assumption to a weaker one. In other words, if a problem of weaker assumption is solved then so is a problem of stronger assumption.

2.3. Additional relation

Lemma 2.1. *Let $h, \bar{h} \in H$ for a cyclic group of order p. If we can solve CDH problem with a base element h, then we can also solve CDH problem with a*

$$\begin{tikzcd}
 & & \mathrm{CDH}_G \arrow[rr] \arrow[dr] & & \mathrm{DL}_G \arrow[d] & \\
\mathrm{DBDH} \arrow[r] \arrow[dr] & \mathrm{BDH} \arrow[ur] \arrow[dr] & \mathrm{GI} \arrow[r] & \mathrm{FI} \arrow[r] & \mathrm{DL}_H \arrow[r, leftrightarrow] & \mathrm{DL}_G \text{ or } \mathrm{GI} \\
 & \mathrm{DDH}_H \arrow[r] & \mathrm{CDH}_H \arrow[ur] & & &
\end{tikzcd}$$

Figure 1. Relations between complexity assumptions in pairing cryptography

base element $\bar{h}$ using $O(\log_2(p))$ computations of CDH problem with respect to h.

Proof. Suppose that we are given a triple $(\bar{h}, \bar{h}^x, \bar{h}^y)$ for any generator $\bar{h}$ of H. By assumption, we can easily compute CDH problem with respect to h. We call such a function by CDH_h.

Let $\bar{h} = h^s$ for some $s \in \mathbb{Z}_p$. Each of $h^{s^{2i}} = CDH_h(h, h^{s^i}, h^{s^i})$ and $h^{s^{i+1}} = CDH_h(h, h^{s^i}, h^s)$ can be computed. Hence $h^{s^{-1}} = h^{s^{p-2}}$ requires $O(\log_2 p)$ computations of CDH_h.

Since $h^{s^2xy} = CDH_h(h, h^{sx}, h^{sy})$, $\bar{h}^{xy} = CDH_h(h, h^{s^{-1}}, h^{s^2xy})$ can also be computed. □

Proposition 2.2. *If GI problem and BDH problem on H are easy, it is possible to solve CDH problem on H. Thus we have the additional following relation:*

$$CDH_H \to BDH \quad or \quad GI.$$

Proof. Suppose that we are given a triple $(\bar{h}, \bar{h}^x, \bar{h}^y)$ for some $\bar{h}$ of H. By Lemma 2.1, it is enough to show that we can compute h^{s^2xy}, where $h = e(g, g)$ and $\bar{h} = h^s$ for some s.

We can find (g_0, g_1, g_2, g_3) such that

$$e(g_0, g_1) = \bar{h}^x \text{ and } \quad e(g_2, g_3) = \bar{h}^y$$

since GI problem is easy.

Let $g_0 = g^t$ and $g_i = g_0^{a_i}$ for a positive integer t and a_i's. By assumption, we can easily solve BDH problem. Thus we call such a function by BDH. Then we can compute $(h^{s^2xy})^{t^{-1}}$ as follows:

$$BDH(g, g_1, g_2, g_3) = e(g, g)^{t^3 a_1 a_2 a_3} = (h^{s^2xy})^{t^{-1}}.$$

Let (g_4, g_5) be an inverse image of $(h^{s^2xy})^{t^{-1}}$, i.e., $e(g_4, g_5) = (h^{s^2xy})^{t^{-1}}$. Finally we can compute h^{s^2xy} as follows:

$$BDH(g, g_0, g_4, g_5) = e(g, g)^{t^4 a_1 a_2 a_3} = h^{s^2xy}.$$ □

3. Self-bilinear maps

Let $e : G \times G \to H$ be a bilinear map. As usual we assume that CDH problem on G is computationally infeasible for using cryptographic applications. Assume that a fixed inversion with homomorphic property exists. Such an inversion induces an injective homomorphism $\phi : H \to G$. Then we can construct a bilinear map $e_s : G \times G \to G$ such that

$$e_s : G \times G \to G, \quad (g_1, g_2) \mapsto \phi(e_s(g_1, g_2)).$$

Such a function is called *self-bilinear map.*

Self-bilinear maps might be useful in cryptographic applications. For example, we can construct a multilinear map $e_n : G^{\times n} \to G$ by

$$e_n(g_1, \ldots, g_n) = e_s(e_{n-1}(g_1, \ldots, g_{n-1}), g_n),$$

where $e_2 = e_s$ for any $n \geq 3$. This multilinear map can be used to make a multiparty key agreement protocol and several useful cryptographic applications [3].

3.1. Nonexistence of self-bilinear maps

Proposition 3.1. *Let G be a cyclic group of prime order p. If we have an efficiently computable non-degenerate bilinear map $e_s : G \times G \to G$, we can solve CDH problem on G by $O(\log p)$ evaluation of e_s.*

Proof. Let $g \in G$ and $e_s(g, g) = g^t$ for a positive integer t. Given a triple (g, g^x, g^y), one can compute $g^{t^{-2}} = g^{t^{p-3}}$ by at most $O(\log p)$ times e_s-computations since $e(g^{t^i}, g^{t^i}) = g^{t^{2i+1}}$ and $e_s(g^{t^i}, g) = g^{t^{i+1}}$.

Therefore we can solve the CDH problem as follows:

$$e_s(e_s(g^x, g^y), g^{t^{-2}}) = e_s(g^{txy}, g^{t^{-2}}) = g^{xy}. \qquad \square$$

Corollary 3.2. *Assume we have a non-degenerate bilinear map $e : G \times G \to H$ for two cyclic groups of prime order p. Then there is no injective homomorphism from H to G if the CDH problem on G is computationally infeasible.*

Verheul showed in [10] that if there is an injective homomorphism from the XTR subgroup to the associated supersingular curve, then the homomorphism can be utilized to make an oracle which computes the DH problem over XTR group. The proof technique is similar, but the above corollary gives the same result in more general situation.

3.2. Remarks on the Lee's self-bilinear map

Lee [7] presented a self-bilinear map $\mathcal{L} : A \times A \to A$, where A is a free R-module with rank two and proposed a few scheme based on the self-bilinear map. Let (S, T) be a generating pair for A. Lee also proposed key agreement and digital signature based on the self-bilinear map.

Consider elements $P = a_1S + b_1T$ and $Q = a_2S + b_2T$, where $a_1, a_2, b_1, b_2 \in R$. Then $L(P, Q)$ is defined by

$$\mathcal{L}(P, Q) = (a_1b_2 - b_1a_2)(\alpha S + \beta T)$$

for some fixed $\alpha, \beta \in R$. It is easy to show that $\mathcal{L}$ is a bilinear map.

The proposed key agreement (A-ECDH) is as follows:

(1) Let (S, T) be a pair of generators of A, which is a public system parameter. Alice and Bob select their private keys a and b at random and compute associated public keys aS and bS respectively.
(2) Alice sends $\mathcal{L}(aS, T)$.
(3) Bob computes $K = b(aS)$ and $h(K)$, where h is a cryptographic hash function and sends $J = h(K)\mathcal{L}(bS, T)$.
(4) Alice computes $K = a(bS)$ and $h(K)$. The shared secret computed by Alice is $ah(K)^{-1}J = ab\mathcal{L}(S, T)$. Also the secret computed by Bob is $b\mathcal{L}(aS, T)$. Therefore both Alice and Bob obtain the common secret.

The above scheme is not essentially based on the bilinear map. By the definition of $\mathcal{L}$, $\mathcal{L}(P, Q)$ cannot be evaluated for random elements $P, Q \in A$ unless the decomposition of P and Q with respect to (S, T) is not given. Hence $\mathcal{L}(aS, T)$ cannot be computed by any one except Alice. This is equivalent that Alice sends aU for a random value a and a fixed value U. Bob also sends bU for a random value b. Then they can compute the common secret abU. Therefore the above scheme is a just original elliptic curve Diffie-Hellman scheme.

In fact the bilinear map $\mathcal{L}$ can be stated as follows:

$$\begin{aligned} \mathcal{L} : \langle S \rangle \times \langle T \rangle &\to \langle U \rangle \\ (aS, bT) &\mapsto abU \end{aligned}$$

for a pair of generators of A and a fixed value $U \in A$. Thus $\mathcal{L}$ is essentially not a *self-bilinear* map.

4. Conclusion

Cryptographic protocols depend on the hardness of some computational problems such as DL, CDH, DDH, BDH, and DBDH problem for their security. Joux briefly described the relations between complexity assumptions in his survey paper [6]. We showed an additional relation exists.

Among the several trials on finding multilinear maps, one hopes to find a self-bilinear map. If there is an injective homomorphism from H to G, we can make a self-bilinear map. But we show that a self-bilinear map on G does not exist under the CDH assumption on G. Thus such an injective homomorphism cannot also exist. It is defined over a finitely generated free R-module A with rank two. However we cannot evaluate $\mathcal{L}$ for random inputs unless the decomposition of inputs with respect to the generators is known. This property is not preferable to cryptographic applications. In fact we can rewrite the map as a non self-bilinear map.

References

[1] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA), 213–229, Lecture Notes in Comput. Sci. **2139**, Springer, Berlin, 2001.

[2] D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), 514–532, Lecture Notes in Comput. Sci. **2248**, Springer, Berlin, 2001.

[3] D. Boneh and A. Silverberg, *Applications of multilinear forms to cryptography*, Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001), 71–90, Contemp. Math. **324**, Amer. Math. Soc., Providence, RI, 2003.

[4] J. Cha and J. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Public key cryptography—PKC 2003, 18–30, Lecture Notes in Comput. Sci. **2567**, Springer, Berlin, 2002.

[5] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Algorithmic number theory (Leiden, 2000), 385–393, Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.

[6] ———, *The Weil and Tate pairings as building blocks for public key cryptosystems*, Algorithmic number theory (Sydney, 2002), 20–32, Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002.

[7] H.-S. Lee, *A self-pairing map and its applications to cryptography*, Appl. Math. Comput. **151** (2004), no. 3, 671–678.

[8] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1639–1646.

[9] N. Smart, *Identity-based Authenticated Key Agreement Protocol based on Weil Pairing*, Electronic Letters, vol. 38, pp. 630–632, June 2002.

[10] E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, Advances in cryptology–EUROCRYPT 2001 (Innsbruck), 195–210, Lecture Notes in Comput. Sci. **2045**, Springer, Berlin, 2001.

[11] ———, *Self-blindable credential certificates from the Weil pairing*, Advances in cryptology–ASIACRYPT 2001 (Gold Coast), 533–551, Lecture Notes in Comput. Sci. **2248**, Springer, Berlin, 2001.

Jung Hee Cheon
ISaC and Department of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail address: jhcheon@snu.ac.kr

Dong Hoon Lee
ETRI Network and Communications Security Division
Deajeon 305-390, Korea
E-mail address: dlee@ensec.re.kr