Anonymous Fingerprinting as Secure as the Bilinear Diffie-Hellman Assumption

Myungsun Kim, Jongseong Kim, and Kwangjo Kim

International Research center for Information Security (IRIS),
Information and Communications University (ICU),
58-4, Hwaamdong, Yuseong-gu, Daejeon, 305-732, Korea.
{ms.kim,jskim224,kkj}@icu.ac.kr

Abstract. The illegal copying and redistribution of digitally-stored information is a crucial problem to distributors who electronically sell digital data. Fingerprinting provides a means which a copyright owner can trace illegal redistributors of electronic information. Various fingerprinting schemes have appeared as techniques for copyright protection from symmetric fingerprinting by Boneh and Shaw [3], asymmetric fingerprinting by Pfitzmann and Schunter [14], and anonymous fingerprinting by Pfitzmann and Waidner [15]. In most of previous schemes, the computational capability of clients has been assumed to roughly be equal to each other and even to their servers. In particular, the key size of known algorithms for fingerprinting schemes keeps back from their practical implementation. In this paper, we propose a scheme for anonymous fingerprinting based on the bilinear Diffie-Hellman problem and prove its security. Our scheme exhibits all computations are performed more efficiently than previous schemes and the key size is quite reasonable for practical use.

Keywords: Anonymous, asymmetric, and symmetric fingerprinting, Bilinear Diffie-Hellman problem, Intellectual property protection, Security reduction

1 Introduction

According to the progress of computer networks and development of the Internet, protection of digitally-stored information property has become a crucial problem to be solved. A lot of research work has been invested into the design of methods that technically support the copyright protection of digital data. One class of such methods consists of techniques called *fingerprinting schemes*. The other class of such methods is called *watermarking schemes*. Watermarking is clearly one of the reasonable alternatives to solve several problems such as violation of ownership and illegal distribution of the copy. It enables the owner of digital property to embed some information in the digital contents and to extract it. On the other hand, fingerprinting allows a buyer to embed the information related to himself, and enables a merchant to trace the buyer from the illegally redistributed copy.

In general, fingerprinting schemes are classified into two different classes called *symmetric* fingerprinting schemes [2, 3, 17] and *asymmetric* fingerprinting schemes [14, 18]. While in symmetric schemes the merchant fingerprints the data item, asymmetric schemes achieve this in an interactive protocol between the buyer and the merchant where the buyer also embeds his own secret. At the end of the protocol only the buyer knows the fingerprinted data item. The advantage of the asymmetric schemes over the symmetric schemes is for the merchant to obtain a proof of treachery that convinces any honest third party.

The two aforementioned classes of fingerprinting schemes do not preserve privacy because buyers are required to identify themselves to the merchant for the purpose of fingerprinting. Purchasing digital items, especially in open networks, reveals information about the buyer' shopping behavior. Such buyer-profiles are very appealing to commercial misuse. Thus it is desirable for buyers to be capable of purchasing fingerprinted digital items anonymously and remain anonymous as long as they do not distribute the digital contents illegally. To solve this problem, *anonymous asymmetric* fingerprinting schemes were first proposed by Pfitzmann and Waidner [15]. Since then, various anonymous fingerprinting schemes have been proposed in [10, 11, 8, 9, 13, 5]. The construction in [10, 11, 8] is based on general two-party computation. The scheme [9] uses oblivious transfer protocols. Later, Kuribayashi and Tanaka [13] focused on improving enciphering rate. Another approach for constructing anonymous fingerprinting schemes based on group signatures was suggested by Camenisch in [5].

However, most of the previous fingerprinting schemes, especially anonymous cases, have not taken into account the computational capability of buyers. From the practical point of view, the key size of known algorithms for previous fingerprinting schemes keeps back from their practical implementation. In this paper, we propose a scheme for anonymous fingerprinting based on the bilinear Diffie-Hellman problem and analyze its security emphasizing that all computations can be performed efficiently and quite reasonable with respect to the key size.

The outline of this paper is as follows: Section 2 gives a brief introduction of fingerprinting schemes and primitives adopted in this paper. Section 3 contains several notations and formal statements for our definition of security. We proceed in Section 4 by presenting our proposal. We then discuss the security of the proposed method in Section 5 and present the brief comparison with previous schemes in Section 6. Finally, we make concluding remarks in Section 7.

2 Preliminaries

In this section, we introduce some basic techniques used in our scheme. First we review various fingerprinting techniques. Next we state briefly the bilinear Diffie-Hellman problem exploited in the conventional scheme in [1, 6].

2.1 Fingerprinting

Digital contents such as image, music, and movie are easily copied without any degradation. Fingerprinting is a cryptographic scheme for the copyright protection of digital contents assisted by a watermarking technique. And the scheme can deter people from executing illegal redistribution of digital contents by making it possible for the merchant to identify the original buyer of the redistributed copy, where we call her a traitor. The fingerprinting schemes can be classified into the following three classes.

Symmetric. The operation to embed a fingerprint is performed only by a merchant. Therefore, the merchant cannot convince any third party of the traitor's treachery even if the merchant has detected the identity of a traitor in the content.

Asymmetric. Fingerprinting is an interactive protocol between a buyer and a merchant. After the purchase, only the buyer obtains the copy with a fingerprint. If the merchant has found the illegally distributed copy somewhere, he can identify the traitor and prove to the third party.

Anonymous (asymmetric). A buyer can purchase a fingerprinted content without revealing his identity to a merchant, however the merchant can identify the traitor when he finds the illegally distributed copy. It also retains the asymmetric property.

Most fingerprinting schemes have a collusion problem. Suppose that digital contents are distributed with different fingerprints. If a collusion group who has obtained those contents compares fingerprints of their contents, they easily capture all fingerprints from their contents. Therefore the collusion group can remove original fingerprints, interpolate gaps, and resell the digital contents without worrying about being traced. This collusion problem was first studied by Blakley *et al.* [2] and practical solution against collusion was dealt with by Boneh and Shaw [3].

2.2 Bilinear Diffie-Hellman problem

We can make use of any bilinear map on an elliptic curve to construct a group $\mathbb{G}$ in which the computational Diffie-Hellman (C-DH) problem is intractable, but the decisional Diffie-Hellman (D-DH) problem is tractable [1,4].

Let E be an elliptic curve over a base field K and let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of order m for some large prime m. Our scheme makes use of a *bilinear* map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ between these two groups. The bilinear map must satisfy the following properties.

i. *Bilinearity*: For all $P, Q, R \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_m^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ or $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$ and $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$.

ii. *Non-degeneracy*: If $\hat{e}(P, Q) = 1$ for all $Q \in \mathbb{G}_1$, then $P = \mathcal{O}$, where $\mathcal{O}$ is a point at infinity.

iii. *Computability*: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

Since the $\mathsf{D\text{-}DH}$ problem in $\mathbb{G}_1$ is easy, we cannot use the $\mathsf{D\text{-}DH}$ problem to build cryptosystems in the group $\mathbb{G}_1$. Instead, the security of our protocol is based on a variant of the $\mathsf{C\text{-}DH}$ problem called the bilinear Diffie-Hellman ($\mathsf{B\text{-}DH}$) problem.

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order m and let P be a generator of $\mathbb{G}_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map.

Definition 1. *The* $\mathsf{B\text{-}DH}$ problem *in* $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ *is the following: given* (P, aP, bP, cP) *for some* $a, b, c \in \mathbb{Z}_m^*$, *compute* $v \in \mathbb{G}_2$ *such that* $v = \hat{e}(P, P)^{abc}$.

Definition 2. *A randomized algorithm* $\mathcal{IG}$ *is a* $\mathsf{B\text{-}DH}$ parameter generator *if*

1. *$\mathcal{IG}$ takes a security parameter* $0 < k \in \mathbb{Z}$,
2. *$\mathcal{IG}$ runs in polynomial time in k, and*
3. *$\mathcal{IG}$ outputs the description of two groups* $\mathbb{G}_1, \mathbb{G}_2$ *and the description of a bilinear map* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.

We require that the groups have the same prime order $m = |\mathbb{G}_1| = |\mathbb{G}_2|$. We denote the output of $\mathcal{IG}$ by $\mathcal{IG}(1^k)$. A concrete example of the $\mathsf{B\text{-}DH}$ parameter generator is given in [1].

3 Definitions of security

In this section, we present some definitions that should be satisfied by a fingerprinting scheme and its security.

3.1 Bilinear Diffie-Hellman assumption

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order m and let P be a generator of $\mathbb{G}_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map.

Definition 3. *An algorithm $\mathcal{A}$ has an* advantage $\mathsf{Adv}^{\mathsf{B\text{-}DH}}(\mathcal{A}) = \epsilon$ *in solving* $\mathsf{B\text{-}DH}$ *in* $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$ *if*

$$\mathsf{Adv}^{\mathsf{B\text{-}DH}}(\mathcal{A}) \triangleq \Pr\left[\mathcal{A}(P, aP, bP, cP) = \hat{e}(P, P)^{abc}\right] \geq \epsilon,$$

where the probability is over the random choice of $\langle a, b, c \rangle \in \mathbb{Z}_m^*$, *the random choice of* $P \in \mathbb{G}_1^*$, *and the random bits of* $\mathcal{A}$.

The security of our fingerprinting scheme is intrinsically based on the intractability of the $\mathsf{B\text{-}DH}$ problem. We formally describe this assumption, called the bilinear Diffie-Hellman intractability assumption (B-DHIA).

A (τ, ϵ)-$\mathsf{B\text{-}DH}$-attacker for the groups is a probabilistic polynomial time(PPT) algorithm $\mathcal{A}$ running in time τ that given a $\mathsf{B\text{-}DH}$ parameter generator $\mathcal{IG}$ stated in Section 2 solves the $\mathsf{B\text{-}DH}$ problem if for a sufficiently large k:

$$\Pr\left[\mathcal{A}(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, aP, bP, cP) = \hat{e}(P, P)^{abc} \;\middle|\; \begin{array}{l} \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle \leftarrow \mathcal{IG}(1^k); \\ P \leftarrow \mathbb{G}_1^*; \\ \langle a, b, c \rangle \leftarrow \mathbb{Z}_m^* \end{array}\right] \geq \epsilon.$$

We denote this probability by $\mathsf{Succ}_{\mathcal{IG}}^{\mathsf{B\text{-}DH}}(\mathcal{A})$.

Definition 4 (B-DHIA). *Given a* $\mathsf{B\text{-}DH}$ *parameter generator* $\mathcal{IG}$ *the* $\mathsf{B\text{-}DH}$ *problem is* (τ, ϵ)-intractable *if there is no* (τ, ϵ)*-attacker* $\mathcal{A}$ *for the groups.*

3.2 Model of anonymous fingerprinting

A model given in [5] was focused on fingerprinting using group signatures. We describe the more general model of anonymous fingerprinting schemes.

Definition 5 (AAF protocol). *An anonymous (asymmetric) fingerprinting* (AAF) *protocol* $\mathcal{P}_{\mathsf{fing}} = \{\mathsf{FKG}_R, \mathsf{FReg}_{RB}, \mathsf{FAuth}_{MB}, \mathsf{FFing}_{MB}, \mathsf{FIden}_{MR}\}$ *involving a buyer* B*, a merchant* M*, and a registration authority* R *is defined by the followings:*

- FKG_R*: A PPT algorithm for* R*. Invoking the* $\mathsf{B\text{-}DH}$ *parameter generator* $\mathcal{IG}$*, it outputs* R*'s secret key and the corresponding public key, which is published authentically.*
- FReg_{RB}*: A probabilistic two-party protocol between* B *and* R*.* B *registers at* R *and at the end each party obtains a registration record.* B *outputs his anonymous public-key and obtains certificates on pseudonym pairs.*
- FAuth_{MB}*: A probabilistic two-party protocol between* B *and* M*.* B *authenticates himself to* M *using the certificate from the sub-protocol* FReg_{RB}*.*
- FFing_{MB}*: A probabilistic two-party protocol between* B *and* M*.* B *buys the data item from* M *and jointly fingerprints it with him. The output to* M *is a purchase record and the main output to* B *is the fingerprinted data item.*
- FIden_{MR}*: A probabilistic two-party protocol between* R *and* M*. If* M *finds an illegally redistributed copy, he extracts some information from this copy. The output to* M *is a proof which also contains the description of the corresponding data item and the real identity of a traitor.* R *examines the proof received from* M *by using the corresponding public information and makes a decision.*

Now we can define the security of the AAF scheme. The definition allows the security of the proposed protocol to be reduced to that of the underlying hard problem.

Definition 6. *A protocol* $\mathcal{P}_{\mathsf{fing}} = \{\mathsf{FKG}_R, \mathsf{FReg}_{RB}, \mathsf{FAuth}_{MB}, \mathsf{FFing}_{MB}, \mathsf{FIden}_{MR}\}$ *is a* secure AAF *protocol if:*

1. ***Correctness:*** *All sub-protocols should terminate successfully whenever all players* B*,* M*, and* R *are honest.*
2. ***Registration security:*** *Without compromising the private key* x_B *of* B*, the registration protocol* FReg_{RB} *provides authentication to* B*.*
3. ***Anonymity:*** *Without obtaining a particular and an illegally redistributed copy,* M *cannot identify* B *through* FAuth_{MB} *and* FFing_{MB}*.*

A (t, ε)-AAF-**breaker** for $\mathcal{P}_{\mathsf{fing}}$ is a PPT Turing machine $\varDelta$ running in time t that satisfies three conditions of Definition 6 at least with probability $\varepsilon = \mathsf{Succ}_{\mathcal{P}}^{\mathsf{AAF}}(\varDelta)$. Then the fingerprinting scheme is (t, ε)-AAF-**secure** if there is no (t, ε)-AAF-breaker $\varDelta$.

4 The protocol

In this section, we propose a secure fingerprinting scheme which provides anonymity and overcomes the drawbacks from previous schemes. In Domingo's schemes [10, 11], the registration protocol is a 4-pass and his schemes require many exponential operations. Our scheme is a 3-pass registration protocol and requires one addition, one scalar multiplication, and one pairing operation over an elliptic curve under the assumption that pre-computations are possible. The identification protocol in our scheme preserves the same advantage.

Our AAF protocol $\mathcal{P}_{\mathsf{fing}}^{\mathsf{B\text{-}DH}}$consists of three sub procedures: registration, fingerprinting, and identification. The registration procedure involves the key generation algorithm and the fingerprinting procedure may be divided into buyer's authentication process and fingerprinting process. Our scheme is constructed as follows:

4.1 Registration procedure

R invokes the key generation algorithm FKG_R at first. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of order m for some large prime m, P be an arbitrary generator of $\mathbb{G}_1$, and $\hat{e}$ be a bilinear map such that

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2 .$$

Assume that both B and R have the $\mathsf{B\text{-}DH}$ public-key pairs as in [1]. R uses its secret key to issue certificates which can be verified using R's public key. The public keys of R and all buyers are supposed to be known and certified. The buyer's secret key is $x_B = s_1 s_2 s_3 \in \mathbb{Z}_m^*$ and his public key is $y_B = \hat{e}(x_B P, P) = \hat{e}(P,P)^{s_1 s_2 s_3} \in \mathbb{G}_2$.

Protocol [registration] – FReg_{RB}

1. R chooses a secret random $x_R \in \mathbb{Z}_m^*$ and sends $T_R = x_R P$ to B.
2. B uses secret keys s_1, s_2, and s_3 in $\mathbb{Z}_m^*$ and computes X and Y such that

$$X = s_1 s_2 P \quad \text{and} \quad Y = s_1 s_2 s_3 P + T_R.$$

   B convinces R in zero-knowledge of possession of s_1, s_2 and s_3. Note that Y plays a role of anonymous public-key of B.
3. R checks that $\hat{e}(Y,P) = y_B \cdot \hat{e}(P, T_R)$. If valid, R computes $T = \hat{e}(X, T_R)$. Otherwise terminates the protocol. R returns to B the certificates $\mathsf{Cert}(T)$, $\mathsf{Cert}(Y \| x_R)$, and x_R. The certificates issued by R state the correctness of T and Y.
4. On receiving certificates, B verifies that $T = \hat{e}(X, T_R)$. He views (Y, T) as a pseudonym pair and keeps it safely.

The registration protocol works as shown in Figure 1.

B		R
		Choose $x_R \in \mathbb{Z}_m^*$ Compute $T_R = x_R P$
	$\xleftarrow{\quad T_R \quad}$	
Choose $s_1, s_2, s_3 \in \mathbb{Z}_m^*$ Compute $X = s_1 s_2 P$ and $Y = s_1 s_2 s_3 P + T_R$		
	$\xrightarrow{\quad X, Y \quad}$	
		Check $\hat{e}(Y, P) = y_B \cdot \hat{e}(P, T_R)$ Compute $T = \hat{e}(X, T_R)$ Issue $\mathsf{Cert}(T)$ and $\mathsf{Cert}(Y \| x_R)$
	$\xleftarrow{\mathsf{Cert}(T), \mathsf{Cert}(Y \| x_R), x_R}$	
Verify $T_R = x_R P, T = \hat{e}(X, T_R)$ Keep (x_R, T, Y)		

Fig. 1. The registration protocol FReg_{RB}

4.2 Fingerprinting procedure

From the conceptual point of view, fingerprinting is similar to secure contract signing in some respects. One can capture such a similarity from the following fingerprinting protocol. Assume that the B-DH signature given in [6] or its variants may be used here. If possible, we call the signing algorithm $\mathsf{Sign}(\cdot, \ldots, \cdot)$ and the verifying algorithm $\mathsf{Verify}(\cdot, \cdot, \cdot)$. Assume that a variant of a secure multiparty computation given in [7] may be constructed under the B-DH assumption.

Protocol [fingerprinting] – ($\mathsf{FAuth}_{MB}, \mathsf{FFing}_{MB}$)

1. B sends $Y, [T, \mathsf{Cert}(T)]$, and text to M, where text is a string identifying his purchase. B outputs a B-DH signature sig on text with the secret key (s_1, s_2, s_3, x_R). The signature sig is not sent to M.
2. M verifies the certificate $\mathsf{Cert}(T)$ on T and stores $[T, \mathsf{Cert}(T)]$ as his purchase record.
3. B and M initiate a secure two-party computation assumed as above. M's inputs are T, Y, text, and item, where item denotes the original information to be fingerprinted. B's inputs are $x_R, \mathsf{sig}, s_1, s_2$, and $\mathsf{Cert}(Y \| x_R)$. The computations are performed as follows:
   i. $\mathsf{val}_1 = \mathsf{Verify}_1(\mathsf{text}, \mathsf{sig}, Y)$. The B-DH signature sig on text is verified by the anonymous public-key Y. The output val_1 is a Boolean variable

only seen by M which is true if and only if the signature verification is completed successfully.

ii. $\mathsf{val}_2 = \mathsf{Verify}_2(Y, \mathsf{Cert}(Y\|x_R), s_1, s_2, x_R, T)$. Firstly, the certificate $\mathsf{Cert}(Y\| x_R)$ on Y is verified. Secondly, it is checked whether $T = \hat{e}(s_1 s_2 P, x_R P)$. The output is also a Boolean variable only seen by M which is true if and only if the two aforementioned checks are completed successfully.

iii. $\mathsf{item}^\star = \mathsf{Fing}(\mathsf{item}, \mathsf{emb})$. A collusion-tolerant fingerprinting algorithm as used in [3, 17] is applied to embed emb into the original information item, where

$$\mathsf{emb} = \mathsf{text}\|\mathsf{sig}\|Y\|\mathsf{Cert}(Y\|x_R)\|s_1\|s_2\|x_R\|T. \tag{1}$$

As a consequence, the fingerprinted information $\mathsf{item}^\star$ is obtained as output and is only seen by B. In the above two-party computation, M allows him to obtain outputs first and, unless val_1 and val_2 are both true, B does not get his output $\mathsf{item}^\star$.

From the overall point of view, the fingerprinting protocol can be divided into two steps as following: buyer authentication and secure two-party computation. The former works as depicted on Figure 2, and the latter works as shown in Figure 3.

B		M
	$\xrightarrow{Y, [T, \mathsf{Cert}(T)], \mathsf{text}}$	
Select $k \in_{\mathcal{R}} \mathbb{Z}_m^*$		Verify $\mathsf{Cert}(T)$
$\mathsf{sig} = \mathsf{Sign}(\mathsf{text}, s_1, s_2, s_3, x_R, k)$		Record $[T, \mathsf{Cert}(T)]$

Fig. 2. Buyer authentication of fingerprinting protocol FAuth_{MB}

4.3 Identification procedure

When M detects illegal redistribution of $\mathsf{item}^\star$, he performs the identification protocol on the ground of information extracted from $\mathsf{item}^\star$ and the purchase record. On finding an illegal copy redistributed, M extracts emb. The extracted information contains the values specified by Eq. (1) and is combined with the purchase record $[T, \mathsf{Cert}(T)]$ by M in order to provide a redistribution proof.

Protocol [identification] – FIden_{MR}

1. The signature sig on text is verified using the pseudonym public-key Y.

B's input	Secure two-party computation	M's input
		$T, Y, \mathsf{text}, \mathsf{item}$ $\longleftarrow$
$x_R, \mathsf{sig}, s_1, s_2,$ $\mathsf{Cert}(Y \\| x_R)$ $\longrightarrow$		
	$\mathsf{val}_1 = \mathsf{Verify}_1(\mathsf{text}, \mathsf{sig}, Y)$ $\longrightarrow$	val_1
	• $\mathsf{Verify}(\mathsf{sig}, \mathsf{text}, Y)$	
	$\mathsf{val}_2 = \mathsf{Verify}_2(Y, \mathsf{Cert}(Y \\| x_R), s_1, s_2, x_R, T)$ $\longrightarrow$	val_2
	• Verify $\mathsf{Cert}(Y \\| x_R)$	
	• Check $T = \hat{e}(s_1 s_2 P, x_R P)$	
$\mathsf{item}^\star$ $\longleftarrow$	$\mathsf{item}^\star = \mathsf{Fing}(\mathsf{item}, \mathsf{emb})$	
	• $\mathsf{emb} = \mathsf{text} \\| \mathsf{sig} \\| Y \\| \mathsf{Cert}(Y \\| x_R) \\| s_1 \\| s_2 \\| x_R \\| T$	

Fig. 3. Secure two-party computation of fingerprinting protocol FFing_{MB}

2. The value x_R links the certificates T and Y. In addition, the value x_R cannot be altered since it is part of the certificates.
3. The value x_R proves that the owner of the pseudonym public-key Y is the same as the owner of T. This is because, according to the registration protocol, R only reveals x_R to B after B has provided such that $T = \hat{e}(s_1 s_2 P, x_R P)$. Therefore, provided that the $\mathsf{B\text{-}DH}$ problem is hard, B cannot produce a correct value T without knowing x_R in polynomial time.
4. In consequence, in order to identify an illegally redistributing buyer, M attempts to raise the public keys of buyers to x_R such that $\hat{e}(Y, P) = y_B \cdot \hat{e}(P, P)^{x_R}$. Now the dishonest buyer has been identified. Note that x_R cannot be forged by M to unjustly accuse a buyer because T and Y are publicly certified.

5 Analysis of security

We analyze in this section the security of the construction proposed in Section 4.

Theorem 1. *Under the B-DHIA, the protocol* $\mathcal{P}_{\mathsf{fing}}^{\mathsf{B\text{-}DH}}$ *is a secure* AAF *protocol.*

Proof.

The first condition of Definition 6 follows immediately from the description of $\mathcal{P}_{\mathsf{fing}}^{\mathsf{B\text{-}DH}}$. The theorem now follows from the following two lemmas.

Lemma 1. *Under the B-DHIA, let the* $(\mathsf{FKG}_R, \mathsf{FReg}_{RB})$ *be a sub-protocol of* $\mathcal{P}_{\mathsf{fing}}^{\mathsf{B\text{-}DH}}$*. Let* Δ *be a breaker against the* AAF *security of* $\mathcal{P}_{\mathsf{fing}}^{\mathsf{B\text{-}DH}}$ *within a time bound* t *and with at least success probability* ε*. Then there exists an adversary*

$\mathcal{A}$ that (τ, ϵ)-breaks the B-DH *problem whose running time $\tau = O(t_{on} \cdot \varepsilon^{-1} + t_{off})$, and success probability*

$$\mathsf{Succ}^{\mathsf{B\text{-}DH}}_{\mathcal{IG}}(\mathcal{A}) \geq \frac{1}{16 \cdot \varepsilon},$$

where denote by t_{on} its on-line running time and by t_{off} its off-line running time.

Proof(sketch).

R only sees X, Y, and zero-knowledge proofs. It is clear that the zero-knowledge proofs leak no information on B. If we don't consider the zero-knowledge proofs, R requires knowledge of x_B to find the value Y' such that $Y' + T_R = y_B$. With considering the zero-knowledge proofs, then the breaker Δ without knowing x_B can compute X, Y such that $X = s_1 s_2 P$, $Y = x_B P + T_R$. Hence, the breaker can solve the B-DH problem, which contracts the B-DHIA. That is, the breaker Δ is reduced to the adversary $\mathcal{A}$. The detail of proof refers to [12]. □

The registration protocol $(\mathsf{FKG}_R, \mathsf{FReg}_{RB})$ provides buyer authentication without compromising the private key x_B of B. This means that the protocol $\mathcal{P}^{\mathsf{B\text{-}DH}}_{\mathsf{fing}}$ meets the second condition of Definition 6.

Lemma 2. *Assume that a secure two-party computation on the* B-DH *problem is feasible. Under the B-DHIA, let the $(\mathsf{FAuth}_{MB}, \mathsf{FFing}_{MB})$ be a sub-protocol of $\mathcal{P}^{\mathsf{B\text{-}DH}}_{\mathsf{fing}}$. Let Δ be a breaker against the* AAF *security of $\mathcal{P}^{\mathsf{B\text{-}DH}}_{\mathsf{fing}}$ within a time bound t and with at least success probability ε. Then there exists an adversary $\mathcal{A}$ that (τ, ϵ)-breaks the* B-DH *problem whose running time $\tau = O(t_{on} \cdot \varepsilon^{-1} + t_{off})$, and success probability*

$$\mathsf{Succ}^{\mathsf{B\text{-}DH}}_{\mathcal{IG}}(\mathcal{A}) \geq \frac{1}{\tau \cdot \varepsilon},$$

where denote by t_{on} its on-line running time and by t_{off} its off-line running time.

Proof(sketch).

In the fingerprinting protocol, M knows Y, $[T, \mathsf{Cert}(T)]$, and outputs of a secure two-party computation that are val_1 and val_2. However, if the secure two-party computation is infeasible, the only way for M to know x_R is to solve the B-DH problem such that $T = \hat{e}(X, x_R P) = \hat{e}(P, P)^{s_1 s_2 x_R}$ using $\mathsf{Cert}(T)$. If it is possible to solve in polynomial-time bound, then the attacker $\mathcal{A}$ violates the B-DHIA. Therefore, the breaker Δ is reduced to the adversary $\mathcal{A}$. The detail of proof refers to [12]. □

An honest buyer who follows the fingerprinting protocol $(\mathsf{FAuth}_{MB}$, $\mathsf{FFing}_{MB})$ will not be identified if the secure two-party computation on the B-DH problem is feasible. This means that the protocol $\mathcal{P}^{\mathsf{B\text{-}DH}}_{\mathsf{fing}}$ meets the third condition of Definition 6.

In the sequel, we have the breaker Δ against the AAF security with respect to the adversary $\mathcal{A}$ with running time τ and at least success probability ϵ such that running time is bounded t, and the success probability

$$\mathsf{Succ}^{\mathsf{AAF}}_{\mathcal{P}}(\Delta) < \frac{1}{16 \cdot \varepsilon} + \frac{1}{\tau \cdot \varepsilon}.$$

This completes the proof of the theorem. □

6 Comparison

The proposal gains an advantage over previous schemes with respect to the key size because the proposal works on an elliptic curve. Therefore, our construction increases efficiency and, at the same time, decreases computation quantity. Table 1 and 2 show the comparison. We denote by E the cost of modular exponentiation, by M the cost of modular multiplication, by S the cost of the point multiplication on an elliptic curve, by P the cost the pairing on an elliptic curve, by A the cost of point addition on an elliptic curve, by R the number of rounds in given protocol, and by N the number of public key in directory.

Table 1. Computation Complexity

Protocol	Scheme [10]	Scheme [8]	Our scheme
Registration	$6\mathsf{E}$	$7\mathsf{E}$	$1\mathsf{S}+1\mathsf{P}$
	$1\mathsf{M}$	$2\mathsf{M}$	$1\mathsf{A}$
Fingerprinting	$5\mathsf{E}$	$4\mathsf{E}$	$2\mathsf{P}$
	$1\mathsf{M}$	$2\mathsf{M}$	0
Identification	$3\mathsf{E}+N/2$	$(3+1)\mathsf{E}$	$1\mathsf{S}+2\mathsf{P}$
	$2\mathsf{M}$	$3\mathsf{M}$	0

Table 2. Communication Complexity

Protocol	Scheme [10]	Scheme [8]	Our scheme
Registration	$4\mathsf{R}$	$2\mathsf{R}$	$3\mathsf{R}$
Fingerprinting	$6\mathsf{R}$	$6\mathsf{R}$	$6\mathsf{R}$
Identification	$\frac{N}{2}\mathsf{R}$	$\frac{N}{2}\mathsf{R}$	$\frac{N}{2}\mathsf{R}$

7 Concluding Remarks

We proposed a practical protocol suitable for anonymous fingerprinting which is computationally much simpler than previous protocols.

As future works, firstly we have to replace the zero-knowledge proof by a more efficient protocol in the registration protocol. Secondly, we should realize the secure two-party computation on the $\mathsf{B\text{-}DH}$ problem used in the fingerprinting protocol.

References

[1] D. Boneh and M. Franklin, "ID-based encryption from the Weil-pairing", *Advances in Cryptology – Crypto '2001*, LNCS 2139, Springer-Verlag, pp. 213–229, 2001.

[2] G. R. Blakley, C. Meadows, and G. B. Purdy, "Fingerprinting long forgiving messages", *Advances in Cryptology – Crypto 1985*, LNCS 218, Springer-Verlag, pp. 180–189, 1986.

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data", *Advances in Cryptology – Crypto 1995*, LNCS 963, Springer-Verlag, pp. 452–465, 1995.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil-pairing", *Advances in Cryptology – Asiacrypt '2001*, LNCS 2248, Springer-Verlag, pp. 514–532, 2001.

[5] J. Camenisch, "Efficient anonymous fingerprinting with group signatures", *Advances in Cryptology – Asiacrypt 2000*, LNCS 1976, Springer-Verlag, pp. 415–428, 2000.

[6] J. Cha and J. Cheon, "An identity-based signature from gap Diffie-Hellman groups", Available from *http://eprint.iacr.org*, 2002.

[7] D. Chaum, I. Damgård, and J. van de Graaf, "Multiparty computations ensuring privacy of each party's input and correctness of the result", *Advances in Cryptology – Crypto 1987*, LNCS 293, Springer-Verlag, pp. 87–119. 1988.

[8] C. Chung, S. Choi, Y. Choi, and D. Won, "Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors", *ICISC 2000*, LNCS 2015, Springer-Verlag, pp. 221-234, 2001.

[9] J. Domingo-Ferrer, "Anonymous fingerprinting based on committed oblvious transfer", *PKC 1999*, LNCS 1560, Springer-Verlag, pp. 43–52, 1999.

[10] J. Domingo-Ferrer, "Anonymous fingerprinting of electronic information with automatic identification redistributors", *IEE Electronics Letters*, Vol. 43, No. 13, 1998.

[11] J. Domingo-Ferrer and H. Herrera-Joancomartí, "Efficient smart-card based anonymous fingerprinting", *Smart Card Research and Advanced Application – CARDIS 1998*, 1998.

[12] M.S. Kim and K.J. Kim, "A new identification scheme base on the bilinear Diffie-Hellman problem", *ACISP 2002*, LNCS 2384, Springer-Verlag, pp. 362–378, 2002.

[13] M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting scheme with high enciphering rate", *Indocrypt 2001*, LNCS 2247, Springer-Verlag, pp. 30–39, 2001.

[14] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting", *Advances in Cryptology – Eurocrypt 1996*, LNCS 1070, Springer-Verlag, pp. 84–95, 1996.

[15] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting", *Advances in Cryptology – Eurocrypt 1997*, LNCS 1233, Springer-Verlag, pp. 88–102, 1997.

[16] A.-R. Sadeghi, "How to break a semi-anonymous fingerprinting scheme", *Information Hiding, 4th International Workshop 2001*, LNCS 2137, Springer-Verlag, pp. 384–394, 2001.

[17] W. Trappe, M. Wu, and K.J. R. Liu, "Collusion-resistant fingerprinting for multimedia",IEEE International Conference on *Acoustics, Speech, and Signal Processing*, Vol. 4, pp. 3309–3312, 2002.

[18] H. Yoshiura, R. Sasaki, and K. Takaragi, "Secure fingerprinting using public-key cryptography", *Security Protocols-6th International Workshop*, LNCS 1550, Springer-Verlag, pp. 83–89, 1998.