(In)Security of an Efficient Fingerprinting Scheme with Symmetric and Commutative Encryption of IWDW 2005

Raphael C.-W. Phan[1] and Bok-Min Goi[2] ⋆

[1] Laboratoire de sécurité et de cryptographie (LASEC),
Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland
raphael.phan@epfl.ch
[2] Centre for Cryptography and Information Security (CCIS),
Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Malaysia
bmgoi@mmu.edu.my

Abstract. We analyze the security of a fingerprinting scheme proposed at IWDW 2005. We show two results, namely that this scheme (1) does not provide *seller security*: a dishonest buyer can repudiate the fact that he redistributed a content, and (2) does not provide *buyer security*: a buyer can be framed by a malicious seller.

Keywords: Watermarking, fingerprinting, security issues, combination of data hiding and cryptography, buyer-seller, repudiation, framing.

1 Introduction

Two of the most celebrated applications of watermarking are *copyright protection* and *piracy protection*. For this, a robust watermarking scheme is employed to embed the content owner's mark to prove his ownership; and to embed a mark (so called a fingerprint) of the content buyer so that the content binds to the buyer and any dishonest buyer who later redistributes this content can be traced.

An interesting body of literature in watermarking has formed around the design and analysis of buyer-seller watermarking (BSW) schemes, which are typically protocols that allow marks identifying both the seller (it is commonly assumed that the owner is the seller) and the buyer to be embedded into the content, so that copyright and piracy protection can be provided. In addition to ensuring this basic *seller security*, BSW schemes also provide *buyer security* [34], i.e., an honest buyer is assured that he cannot be framed by malicious sellers.

⋆ The second author acknowledges the Malaysia eScience grants (01-02-01-SF0032, 01-02-01-SF0060).

Related Work. It turns out that designing secure BSW schemes is more subtle than first thought. For instance, the original proposal that highlighted the need to provide buyer security in [34], was shown inadequate in [25] since the seller knows the final copy of the fingerprinted content and may well have redistributed this himself.

Meanwhile, a few subsequent BSW schemes proposed with different additional features like anonymity [20], without trusted third parties (TTP) [10] and extension for multiple purchases [11] were later found to have security problems [10, 19, 18]. A few more recent schemes can be found in [24, 37, 38].

BSW schemes typically employ techniques from both watermarking and cryptography. See [13, 21, 33] for cautions when integrating the two fields.

This Paper. We show the first known analysis of a recent BSW scheme proposed by Yong and Lee at IWDW 2005 [37]. Our results indicate that this scheme does not provide seller security and buyer security, properties that are desired by any basic BSW scheme.

Section 2 gives the preliminaries and notations used throughout this paper. We describe the Yong-Lee BSW scheme in Section 3, and then present our attacks in Section 4. Section 5 gives some concluding remarks.

2 Preliminaries

We list here basic requirements of a secure anonymous buyer-seller watermarking scheme (the interested reader can refer to [25, 37] for details):

- **Traceability**. The buyer who has illegally redistributed watermarked contents can be traced.
- **Non-Repudiation**. The guilty buyer cannot deny having illegally redistributed copies of the content.
- **Non-Framing**. No one can accuse an honest buyer.
- **Privacy: Anonymity and Unlinkability**. Without obtaining an illegally distributed copy, the seller cannot identify the buyer. Also, the purchases of honest buyers should not be linkable even by a collusion of all sellers, registration center and other buyers.

Note that in any BSW scheme, it is assumed that the underlying watermarking scheme used for embedding is collusion-tolerant and robust.

2.1 Cryptographic Preliminaries

In a *public key cryptosystem* [26], each party A possesses a pair of public-private keys (y_A, x_A) obtainable from a certificate authority or registration center RC. For convenience, we let $y_A \equiv g^{x_A} \bmod p$ [26], where p is a large prime and g is a generator of the multiplicative group $\mathbb{Z}_p^*$ of order $(p-1)$. Also, unless otherwise specified, all arithmetic operations are performed in $\mathbb{Z}_p^*$. Any party can encrypt a message for A using y_A, but only A can decrypt this message with x_A. This ensures *confidentiality*. Furthermore, A can sign a message by encrypting it with x_A, denoted as $sign_{x_A}(M)$, so that anybody can verify by using y_A that the message really originated from A. This provides *authentication* and *non-repudiation*. Note however that it is common knowledge not to use the same key-pair for both encryption and signature.

Both the seller and the buyer have registered with the registration center RC, and have their own pair of keys which are (y_A, x_A) and (y_B, x_B), respectively. Note that the RC also has its own public-private key pair (y_{RC}, x_{RC}).

2.2 Notations

For ease of explanation, we use the following common notations for BSW schemes:

S	the seller who owns and sells the digital content X
B	the buyer who buys the digital content
RC	registration center who can issue certificates
J	the judge
$\otimes$	fingerprint embedding (watermarking) operation
X	original content with t elements $(x_1, x_2, ..., x_t)$
X'	fingerprinted content, where $X' = X \otimes F$ for a fingerprint F
$H(\cdot)$	collision-resistant hash function
$E_U(x)$	public-key encryption of x under party U's public key
$Enc_K(x)$	symmetric-key encryption of x under secret key K
$CEnc_K(x)$	commutative symmetric-key encryption of x under secret key K

3 The Yong-Lee Anonymous BSW Scheme

We describe the anonymous BSW scheme by Yong and Lee proposed at IWDW 2005 [37]. As is common for this type of scheme, it consists of three phases; i.e. *registration*, *fingerprinting* and *identification*. For better illustration, we depict the registration phase and fingerprinting phase in Fig. 1.

Registration. This phase involves two parties: the buyer B and registration center RC. Both are assumed to have public and private key pairs, i.e., x_I is the private key of party I while its public key is $y_I = g^{x_I}$. Certificates issued by RC are signed by its private key x_{RC}, and can be publicly verified by anyone using RC's public key y_{RC}.

1. B randomly chooses two secret values $x_1, x_2 \in \mathbb{Z}_p^*$ such that $x_1 + x_2 = x_B \in \mathbb{Z}_p^*$. Then B sends $(y_B, y_1 = g^{x_1}), E_{RC}(x_2)$ to RC, and convinces via zero knowledge to RC of its possession of x_1.
2. RC decrypts $E_{RC}(x_2)$ and computes $y_2 = g^{x_2}$ and checks that $y_1 y_2 = y_B$. If verified, it returns to B a certificate $Cert(y_1)$ which states the correctness of y_1 and the registration of B.

Repeating this phase several times allows B to obtain several different pairs (y_1, x_1) which it will use as its unlinkable and anonymous key pairs.

Fingerprinting. This phase involves two parties: the buyer B and the seller S.

1. B sends y_1, $Cert(y_1)$ and *payment* to S as a purchase request for the digital content X.

2. On receiving this, S verifies $Cert(y_1)$ and generates two fingerprints F_B^0 and F_B^1 for B, i.e.,

$$F_B^i = \{f_B^{i,1}, f_B^{i,2}, \ldots, f_B^{i,t}\}, i = \{0, 1\}.$$

3. S generates two identical copies of the digital content X^0 and X^1, and splits each copy into t frames, i.e.,

$$X^i = \{x^{i,1}, x^{i,2}, \ldots, x^{i,t}\}, i = \{0, 1\}.$$

4. S then embeds F_B^i into each of the t frames of X^i for $i = \{0, 1\}$, by using the specific embedding construction in [14], to obtain

$$X_B^i = \{x_B^{i,1}, x_B^{i,2}, \ldots, x_B^{i,t}\}, i = \{0, 1\},$$

where

$$x_B^{i,j} = x^{i,j} \otimes f_B^{i,j} \quad , i = \{0, 1\}, j = \{1, \ldots, t\}.$$

Buyer, B		**Registration Center,** RC
Randomly select:		
$x_1, x_2 \in_R \mathbb{Z}_p^*$ s.t. $x_1 + x_2 = x_B$		
Compute y_1 and encrypt x_2:		
$y_1 = g^{x_1}$, $E_{RC}(x_2)$.	$\xrightarrow{y_B, y_1, E_{RC}(x_2)}$	Decrypt $E_{RC}(x_2)$ using x_{RC}.
		Compute: $y_2 = g^{x_2}$.
		Check: $y_1 \cdot y_2 \stackrel{?}{=} y_B$.
	$\xleftarrow{Cert(y_1)}$	If pass, return $Cert(y_1)$.

(a) Registration Phase

Buyer, B		**Seller,** S
	$\xrightarrow{y_1, Cert(y_1), payment}$	Verify $Cert(y_1)$ (using y_{RC}).
		If pass, generate and embed:
		$F_B^i = \{f_B^{i,1}, f_B^{i,2}, \ldots, f_B^{i,t}\}$,
		$X^i = \{x^{i,1}, x^{i,2}, \ldots, x^{i,t}\}, i = \{0, 1\}$,
		$X_B^i = \{x_B^{i,1}, x_B^{i,2}, \ldots, x_B^{i,t}\}$ where
		$x_B^{i,j} = x^{i,j} \otimes f_B^{i,j}$.
		Generate 2 secret keys K_0 and K_1:
		$K_i = \{k_{i,1}, k_{i,2}, \ldots, k_{i,t}\}, i = \{0, 1\}$.
		Encrypt and obtain:
		$\mathcal{X}_B^i = \{\mathbf{x}_B^{i,1}, \mathbf{x}_B^{i,2}, \ldots, \mathbf{x}_B^{i,t}\} = Enc_{K_i}(X_B^i)$.
		Encrypt K_0 and K_1 (using K_S):
		$C_i = \{CEnc_{K_S}(k_{i,1}), CEnc_{K_S}(k_{i,2}), \ldots, CEnc_{K_S}(k_{i,t})\}$
		$= \{c_{i,1}, c_{i,2}, \ldots, c_{i,t}\}$.
Randomly generate:	$\xleftarrow{\mathcal{X}_B^0, \mathcal{X}_B^1, C_0, C_1}$	
$L_B = \{l_1, l_2, \ldots, l_t\}$		
for $l_j = \{0, 1\}$.		
Then construct:		
$C' = \{c'_1, c'_2, \ldots, c'_t\}$		
where $c'_j = c_{l_j, j}$.		
Encrypts C' (using K_R):		
$D_1 = \{d_1, d_2, \ldots, d_{\frac{t}{2}}\}$ and		
$D_2 = \{d_{\frac{t}{2}+1}, \ldots, d_t\}$, where		
$d_i = CEnc_{K_R}(c'_i)$.	$\xrightarrow{D_1}$	Decrypt D_1 (using K_S):
		$U_1 = \{u_1, u_2, \ldots, u_{\frac{t}{2}}\}$, where
Decrypt U_1 (using K_R).	$\xleftarrow{U_1}$	$u_i = CEnc_{K_S}^{-1}(d_i) = CEnc_{K_R}(k_{l_j, j})$.
Then, decrypt 1^{th} $t/2$ frames:		
$\mathbf{x}_B^{l_j, j}$ for $j = \{1, 2, \ldots, \frac{t}{2}\}$.		
Generate:		
$T_B = E_J(L_B)$ and $sig_{x_1}(T_B)$.	$\xrightarrow{T_B, sig_{x_1}(T_B), D_2}$	Verify (using y_1) $sig_{x_1}(T_B)$.
		If verified, it decrypts D_2 (using K_S):
Decrypt U_2 (using K_R).	$\xleftarrow{U_2, sig_{x_S}(T_B)}$	$U_2 = \{u_{\frac{t}{2}+1}, \ldots, u_t\}$.
Then, decrypt 2^{nd} $t/2$ frames:		
$X_B = \{x_B^{l_1,1}, x_B^{l_2,2}, \ldots, x_B^{l_t,t}\}$.	$\xrightarrow{TN_B = E_J(H(X_B), H(X_B) \oplus H(L_B))}$	Record $Rec_B =$
		$\langle y_1, Cert(y_1), F_B^0, F_B^1, T_B, sig_{x_1}(T_B), TN_B \rangle$.

(b) Fingerprinting Phase

Fig. 1. Yong-Lee Anonymous BSW Scheme

5. S generates two secret key vectors K_0 and K_1. Each key vector consists of t randomly selected keys:

$$K_i = \{k_{i,1}, k_{i,2}, \ldots, k_{i,t}\}, i = \{0, 1\}.$$

6. S encrypts each of the t frames of X_B^i ($i = \{0, 1\}$) using each of the t keys of K_i, using symmetric key encryption $Enc_K(\cdot)$. This produces two encrypted digital content vectors $\mathcal{X}_B^0$ and $\mathcal{X}_B^1$ of frames, such that

$$\begin{aligned}\mathcal{X}_B^i &= \{\mathbf{x}_B^{i,1}, \mathbf{x}_B^{i,2}, \ldots, \mathbf{x}_B^{i,t}\} \\ &= Enc_{K_i}(X_B^i) \\ &= Enc_{k_{i,j}}(x_B^{i,j}), i = \{0, 1\}, j = \{1, \ldots, t\}.\end{aligned}$$

7. S randomly selects a secret key K_S and encrypts the two key vectors K_0 and K_1 via commutative encryption $CEnc_K(\cdot)$, producing two encrypted key vectors C_0 and C_1, i.e.

$$\begin{aligned}C_i &= \{c_{i,1}, c_{i,2}, \ldots, c_{i,t}\} \\ &= \{CEnc_{K_S}(k_{i,1}), CEnc_{K_S}(k_{i,2}), \ldots, CEnc_{K_S}(k_{i,t})\}, i = \{0, 1\}.\end{aligned}$$

   S sends $(\mathcal{X}_B^0, \mathcal{X}_B^1, C_0, C_1)$ to B.

8. B randomly generates a t-bit integer $L_B = \{l_1, l_2, \ldots, l_t\}$ for $l_j = \{0, 1\}, j = \{1, \ldots, t\}$, restricted to the fact that L_B should not be all 0 or all 1. It then constructs a new encrypted vector $C' = \{c'_1, c'_2, \ldots, c'_t\}$ where $c'_j = c_{l_j,j}$. To elaborate, this means that each c'_j is either $c_{0,j}$ or $c_{1,j}$ depending on the bit l_j of L_B.

9. B randomly chooses a secret key K_R and encrypts C' via commutative encryption to obtain an encrypted vector that it halves into two consecutive parts $D_1 = \{d_1, d_2, \ldots, d_{\frac{t}{2}}\}$ and $D_2 = \{d_{\frac{t}{2}+1}, \ldots, d_t\}$, where

$$\begin{aligned}d_i &= CEnc_{K_R}(c'_i) \\ &= CEnc_{K_R}(CEnc_{K_S}(k_{l_j,j})) \\ &= CEnc_{K_S}(CEnc_{K_R}(k_{l_j,j})).\end{aligned}$$

   B sends D_1 to S.

10. S decrypts D_1 with K_S to get the vector $U_1 = \{u_1, u_2, \dots, u_{\frac{t}{2}}\}$, where

$$\begin{aligned} u_i &= CEnc_{K_S}^{-1}(d_i) \\ &= CEnc_{K_S}^{-1}(CEnc_{K_S}(CEnc_{K_R}(k_{l_j,j}))) \\ &= CEnc_{K_R}(k_{l_j,j}). \end{aligned}$$

   S sends U_1 to B.

11. B now obtains $t/2$ decryption keys by decrypting each u_i with key K_R, and can thus decrypt the first $t/2$ frames of the encrypted digital content $\mathbf{x}_B^{l_j,j}$ for $j = \{1, 2, \dots, \frac{t}{2}\}$.

12. B generates $T_B = E_J(L_B)$ and a signature $sig_{x_1}(T_B)$. These are evidence for resolving piracy disputes in future. B sends $(T_B, sig_{x_1}(T_B), D_2)$ to S.

13. S verifies $sig_{x_1}(T_B)$ with y_1. If verified, it decrypts D_2 with K_S to obtain the vector $U_2 = \{u_{\frac{t}{2}+1}, \dots, u_t\}$, where u_i is similar to that in Step (10.). S sends $(U_2, sig_{x_S}(T_B))$ to B.

14. B now obtains the remaining $t/2$ decrypting keys by decrypting each u_i of U_2 with key K_R, thus it can decrypt the remaining $t/2$ frames of $\mathcal{X}_B^{l_j,j}$ for $j = \{\frac{t}{2}+1, \dots, t\}$. Hence, B now has the complete fingerprinted content X_B, i.e.

$$X_B = \{x_B^{l_1,1}, x_B^{l_2,2}, \dots, x_B^{l_t,t}\}.$$

   B sends $TN_B = E_J(H(X_B), H(X_B) \oplus H(L_B))$ to S.

15. S records $Rec_B = \langle y_1, Cert(y_1), F_B^0, F_B^1, T_B, sig_{x_1}(T_B), TN_B \rangle$ in its database.

Identification. This phase involves three parties: the seller S, the judge J and the registration center RC.

1. After finding an illegally redistributed digital content, S extracts the fingerprint from it. S then sends $\mathcal{X}_B^0$ and $\mathcal{X}_B^1$ with the transaction record Rec_B to the judge J.
2. J decrypts T_B and TN_B and checks that L_B corresponds to $\mathcal{X}_B$, and that T_B was signed by B. It verifies the presence of frames of either F_B^0 or F_B^1 in X_B based on L_B. If all are verified, it sends y_1 to RC and asks for the identity of B, and informs S.

4 Insecurity of the Yong-Lee BSW Scheme

Attacking the Seller Security. The security of the seller is captured by the notion of *traceability* and *non-repudiation.*

Nevertheless, we show how the seller security can be defeated by a malicious buyer. The attack follows.

1. B performs an entire **fingerprinting** protocol session with S, thus in the end B has the content X_B and S has recorded $Rec_B = \langle y_1, Cert(y_1), F_B^0, F_B^1, T_B, sig_{x_1}(T_B), TN_B\rangle$ in its database.
2. B initiates another **fingerprinting** protocol session with S, this time requesting for some other digital content X'. During the protocol, B proceeds normally, except that it reuses the y_1, $Cert(y_1)$, T_B, $sig_{x_1}(T_B)$, TN_B from the previous session. It is clear that S will correctly verify y_1 from $Cert(y_1)$, and T_B from $sig_{x_1}(T_B)$. Furthermore S cannot check TN_B since it is encrypted for only J to decrypt.
3. Thus in the end B obtains the fingerprinted X'_B and S records $Rec'_B = \langle y_1, Cert(y_1), F_B'^0, F_B'^1, T_B, sig_{x_1}(T_B), TN_B\rangle$ in its database.
4. B can repeat this as many times as it wishes. Now B can pirate all the fingerprinted content X'_B it received from its sessions with S except for the first, X_B.
5. When S discovers that X'_B has been redistributed and initiates the **identification** protocol, B can counter that it only bought once from S, for the digital content X_B. It can argue that the other X'_B have nothing to do with him, but that S reused y_1, $Cert(y_1)$, T_B, $sig_{x_1}(T_B)$, TN_B to frame him for distributing X'_B.
6. The judge J cannot reach a conclusion in favour of S because TN_B will not correspond to X'_B since it corresponds only to X_B.

This attack shows to some extent a failure of *traceability* since B cannot be judged guilty for redistributing X'_B. This also shows a failure of *non-repudiation* because the only part that binds to B for which B cannot repudiate is $T_B = E_J(L_B)$, which is independent of the digital content bought by B.

Attacking the Buyer Security. The security of the buyer is captured by the notion of *non-framing.* Additionally, when privacy is desired then this is captured by *anonymity* and *unlinkability.*

We demonstrate two cases for which *non-framing* can be violated. The first follows, by exploiting T_B.

1. S guesses all possible values of L_B and for each guess checks if $T_B = E_J(L_B)$. Since L_B is only a 32-bit vector, this requires just 2^{32} trials.
2. S does the **fingerprinting** protocol steps 3 and 4 for X', where the old fingerprints F_B^0 and F_B^1 are reused, and embedded into any other content X' for which S wants to frame B. This gives $X_B'^0$ and $X_B'^1$.
3. Since L_B has been obtained, S knows the fingerprinting pattern chosen by B. So S can embed the same pattern into any other content X'. Denote the fingerprinted content as X_B'.
4. S computes $TN_B' = E_J(H(X_B'), H(X_B') \oplus H(L_B))$.
5. S initiates the **identification** protocol to frame B for pirating X_B', by sending $X_B'^0$ and $X_B'^1$ together with transaction record $Rec_B' = \langle y_1, Cert(y_1), F_B^0, F_B^1, T_B, sig_{x_1}(T_B), TN_B' \rangle$ to the judge J.
6. J decrypts T_B and TN_B' and will correctly verify that L_B corresponds to X_B', and that T_B was signed by B. It will also correctly detect in X_B' the presence of the fingerprinting pattern based on L_B. Thus, this will cause J to agree that B has pirated X_B', and it will send y_1 to RC to ask for the identity of B, and informs S.

The second attack below also violates *non-framing* in the sense that even if B was dishonest and redistributed X_B, it should only be held guilty for X_B and not for any other content X_B' for which it did not redistribute. This is in line with the common legal system. If this is violated, it is still unfair to B; for instance if X_B is some inexpensive content whose copyright is claimed by S only for a brief period thus B might feel it is ok to redistribute among friends after some time. However, once X_B is obtained by S it can frame B for redistributing some other very expensive content X_B' and for which it holds copyright indefinitely. The attack follows.

1. S does not know the fingerprinting pattern based on L_B that was selected by B to be embedded into content X to form X_B. However, S does have the copies of X_B^0 embedded with F_B^0, and of X_B^1 embedded with F_B^1.
   Proceeding frame by frame in sequence, S compares each frame of X_B with each frame of X_B^0 and of X_B^1. Since each frame is processed independently (like in electronic code book way), S will successfully obtain the fingerprinting pattern L_B.
2. The rest of the attack steps is similar to the steps 2 to 6 of the first attack above.

Our first attack exploits the fact that L_B can be bruteforced in practice, and that T_B can be used for verifying these guesses. Even if L_B is too long to be bruteforced in practice (but this is not the case for the Yong-Lee scheme), our second attack still applies. It exploits the fact that the seller S knows the fingerprint set $\{F_B^0, F_B^1\}$ used to embed into the content thus it can know the fingerprinting pattern chosen by the buyer B by simple frame comparison once a copy of the fingerprinted content X_B is available. In both attacks, the major flaw we exploit is the same for which we exploited in our attack on Seller Security in the previous subsection: that the only thing that binds to the buyer B is $sig_{x_1}(T_B)$, which is independent of the content bought by B. This allows the seller S to transplant the same fingerprinting pattern to any other content for as many times as it wishes to frame B.

5 Concluding Remarks

The Yong-Lee BSW scheme attempts to eliminate the inefficiency of some existing BSW schemes by using symmetric key encryption and commutative encryption. The flaws that we have demonstrated on this scheme do not stem from the use of these encryption methods, but exploits the fact that the scheme was not sufficiently binding a buyer to the content. This causes a buyer to repudiate and thus get away with illegal redistribution of bought content, breaking seller security. This also makes it easier for a seller to transplant a buyer's fingerprint to other contents for framing, thus breaking buyer security.

Our results show that the Yong-Lee scheme does not offer the security for which it is designed to provide, and therefore leaves doubts on the design of this scheme, considering the state of the art of BSW schemes thus far, and the fact that the Yong-Lee BSW scheme is a fairly recent proposal that should have taken the state of the art into its design consideration. We caution against simple fixes that patch our attacks in this paper since experience has shown that the break-and-fix cycle loops indefinitely, for instance see [17–19, 30–32] where attacks were applied to protocols [8–11, 20, 22, 6, 36] that improved on existing ones. We suggest instead, that if BSW schemes are required, to consider other schemes like [24, 38] that have not yet been shown to fall to any attacks that counter their design goals.

References

1. F. Bao, R.H. Deng and P. Feng. An Efficient and Practical Scheme for Privacy Protection in the E-commerce of Digital Goods. *Proceedings of ICICS '00*, LNCS 2836, pp. 162-170, 2001.

2. G. Blakley, C. Meadows and G.B. Purdy. Fingerprinting Long Forgiving Messages. *Advances in Cryptology - CRYPTO '85*, LNCS 218, pp. 180-189, 1986.
3. D. Boneh and J. Shaw. Collusion-secure Fingerprinting for Digital Data. *Advances in Cryptology - CRYPTO '95*, LNCS 963, pp. 452-465, 1995.
4. R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Publishing, U.S., 2001.
5. E.F. Brickell and Y. Yacobi. On Privacy Homormorphisms. *Advances in Cryptology - EUROCRYPT '87*, LNCS 304, pp. 117-125, 1987.
6. J.W. Byun, D.H. Lee and J. Lim. Efficient and Provably Secure Client-to-Client Password-based Key Exchange Protocol. *Proceedings of APWeb '06*, LNCS 3841, pp. 830-836, 2006.
7. D. Chaum. An Improved Protocol for Demonstrating Possession of Discrete Logarithms and some Generalizations. *Advances in Cryptology - EUROCRYPT '87*, LNCS 307, pp. 127-141, 1987.
8. C.C. Chang and C.Y. Chung. An Enhanced Buyer-Seller Watermarking Protocol. *Proceedings of ICCT '03*, pp. 1779-1783, 2003.
9. S.C. Cheung, H.F. Leung and C. Wang. A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents. *Proceedings of HICSS-37*, January 2004.
10. J.-G. Choi, K. Sakurai and J.H. Park. Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party. *Proceedings of ACNS '03*, LNCS 2846, pp. 265-279, 2003.
11. J.-G. Choi and J.H. Park. A Generalization of an Anonymous Buyer-Seller Watermarking Protocol and Its Application to Mobile Communications. *Proceedings of IWDW '04*, LNCS 3304, pp. 232-243, 2005.
12. J.-G. Choi, J.H. Park and K.R. Kwon. Analysis of COT-based Fingerprinting Schemes: New Approaches to Design Practical and Secure Fingerprinting Scheme. *Proceedings of IH '04*, LNCS 3200, pp. 253-265, 2004.
13. I.J. Cox, G.J. Doerr and T. Furon. Watermarking is Not Cryptography. *Proceedings of IWDW '06*, LNCS 4283, pp. 1-15, 2006.
14. I.J. Cox, J. Kilian, T. Leighton and T. Shamoon. Secure Spread Spectrum Watermarking for Images, Audio and Video. *IEEE Trans. on Image Processing*, vol. 6, no. 12, pp. 1673-1678, 1997.
15. J. Domingo-Ferrer. Anonymous Fingerprinting based on Committed Oblivious Transfer. *Proceedings of PKC '99*, LNCS 1560, pp. 43-52, 1999.
16. J. Domingo-Ferrer. Anonymous Fingerprinting of Electronic Information with Automatic Identification Redistributors. *IEE Electronics Letters*, vol. 43, no. 13, pp. 1303-1304, 1998.
17. B.-M. Goi, R.C.-W. Phan and H.-T. Chuah. Cryptanalysis of Two Non-Anonymous Buyer-Seller Watermarking Protocols for Content Protection. *Proceedings of DC-SMDC '07, in ICCSA '07*, LNCS 4705, pp. 951-960, 2007.
18. B.-M. Goi, R.C.-W. Phan and M.U. Siddiqi. Cryptanalysis of a Generalized Anonymous Buyer-Seller Watermarking Protocol of IWDW 2004. *Proceedings of SecUbiq '05, in EUC Workshops '05*, LNCS 3823, pp. 936-944, 2005.
19. B.-M. Goi, R.C.-W. Phan, Y. Yang, F. Bao, R.H. Deng and M.U. Siddiqi. Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and An Improvement for True Anonymity. *Proceedings of ACNS '04*, LNCS 3089, pp. 369-382, 2004.
20. H.S. Ju, H.J. Kim, D.H. Lee and J.I. Lim. An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control. *Proceedings of ICISC '02*, LNCS 2587, pp. 421-432, 2002.

21. S. Katzenbeisser. On the Integration of Watermarks and Cryptography. *Proceedings of IWDW '03*, LNCS 2939, pp. 50-60, 2004.
22. J. Kim, S. Kim, J. Kwak and D. Won. Cryptanalysis and Improvement of Password-Authenticated Key Exchange Scheme between Clients with Different Passwords. *Proceedings of ICCSA '04*, LNCS 3043, pp. 895-902, 2004.
23. M. Kuribayashi and H. Tanaka. A New Anonymous Fingerprinting Scheme with High Enciphering Rate. *Progress in Cryptology - INDOCRYPT '01*, LNCS 2247, pp. 30-39, 2001.
24. C.-L. Lei, P.-L. Yu, P.-L. Tsai and M.-H. Chan. An Efficient and Anonymous Buyer-Seller Watermarking Protocol. *IEEE Trans. on Image Processing*, vol. 13, no. 12, December 2004.
25. N. Memon and P.W. Wong. A Buyer-Seller Watermarking Protocol. *IEEE Trans. on Image Processing*, vol. 10, no. 4, April 2001.
26. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, U.S., 1997.
27. B. Pfitzmann and A.R. Sadeghi. Coin-Based Anonymous Fingerprinting. *Advances in Cryptology - EUROCRYPT '99*, LNCS 1592, pp. 150-164, 1999.
28. B. Pfitzmann and M. Schunter. Asymmetric Fingerprinting. *Advances in Cryptology - EUROCRYPT '96*, LNCS 1070, pp. 84-95, 1996.
29. B. Pfitzmann and M. Waidner. Anonymous Fingerprinting. *Advances in Cryptology - EUROCRYPT '97*, LNCS 1233, pp. 88-102, 1997.
30. R.C.-W. Phan and B.-M. Goi. Cryptanalysis of an Improved Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) Scheme. *Proceedings of ACNS '05*, LNCS 3531, pp. 33-39, 2005.
31. R.C.-W. Phan and B.-M. Goi. Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange using Different Passwords. *Proceedings of ACNS '06*, LNCS 3989, pp. 226-238, 2006.
32. R.C.-W. Phan and B.-M. Goi. Cryptanalysis of Two Provably Secure Cross-Realm C2C-PAKE Protocols. *Progress in Cryptology - Indocrypt '06*, LNCS 4329, pp. 104-117, 2006.
33. R.C.-W. Phan and H.-C. Ling. Flaws in Generic Watermarking Protocols based on Zero-Knowledge Proofs. *Proceedings of IWDW '04*, LNCS 3304, pp. 184-191, 2005.
34. L. Qiao and K. Nahrstedt. Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights. *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194-210, 1998.
35. W. Trappe, M. Wu and K. Liu. Collusion-resistant Fingerprinting for Multimedia. *Proceedings of IEEE ICASSP '02*, pp. 3309-3312, 2002.
36. Y. Yin and L. Bao. Secure Cross-Realm C2C-PAKE Protocol. *Proceedings of ACISP '06*, LNCS 4058, pp. 395-406, 2006.
37. S. Yong and S.-H. Lee. An Efficient Fingerprinting Scheme with Symmetric and Commutative Encryption. *Proceedings of IWDW '05*, LNCS 3710, pp. 54-66, 2005.
38. J. Zhang, W. Kou and K. Fan. Secure Buyer-Seller Watermarking Protocol. *IEE Proceedings - Information Security*, vol. 153, no. 1, pp. 15-18, 2006.

Acknowledgement

We are grateful for suggestions by anonymous referees of IWDW '07 to give emphasis in our discussion on whether the Yong-Lee scheme can be fixed to counter our attacks. This has been duly treated in the Concluding Remarks above. Part of this work was done while the first author was attending the smoothly run IACR-sponsored Eurocrypt 2007 conference in Barcelona. We thank God for His many blessings.