Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity

Bok-Min Goi[1], Raphael C.-W. Phan[2], Yanjiang Yang[3], Feng Bao[3], Robert H. Deng[3], and M.U. Siddiqi[1]

[1] Multimedia University, 63100 Cyberjaya, Malaysia
{bmgoi,umar}@mmu.edu.my
[2] Information Security Research (iSECURES) Lab,
Swinburne Sarawak Institute of Technology, 93576 Kuching, Malaysia
rphan@swinburne.edu.my
[3] Institute for Infocomm Research,
21 Heng Mui Keng Terrace, Singapore 119613
{yanjiang, baofeng, deng}@i2r.a-star.edu.sg

Abstract. By combining techniques of watermarking and fingerprinting, a sound buyer-seller watermarking protocol can address the issue of copyright protection in e-commerce. In this paper, we analyze the security of two recent anonymous buyer-seller watermarking protocols proposed by Ju *et. al* and Choi *et. al* respectively, and prove that they do not provide the features and security as claimed. In particular, we show that i) the commutative cryptosystem used in Choi *et. al*'s protocol fails to prevent the watermark certification authority (WCA) from discovering the watermark (fingerprint) chosen by the buyer; ii) for both protocols, the seller can discover the watermark chosen by the buyer if he colludes with the WCA. Hence, these protocols cannot guard against conspiracy attacks. We further show that these protocols only provide "partial" anonymity, ie. the buyer's anonymity is guaranteed only if WCA is honest. Our results suggest that the security of these protocols must assume the honesty of WCA, contrary to the designers' original claim. Finally, we propose a new anonymous buyer-seller watermarking protocol which is more secure and efficient, and provides true anonymity.

Keywords: Watermarking, Fingerprinting, Traitor Tracing, Copyright Protection, Anonymity.

1 Introduction

All types of multimedia information can be stored and processed within a computer in digital form. Furthermore, they can be transmitted losslessly over a noisy digital communication networks. However, since the duplication of digital multimedia content results in perfectly identical copies, the copyright protection issue is a main problem that needs to be addressed. *Digital watermarking*

M. Jakobsson, M. Yung, J. Zhou (Eds.): ACNS 2004, LNCS 3089, pp. 369–382, 2004.

[SKT98,HK99,VP99,WPD99,CMB02] and *digital fingerprinting* [WNR83,ZK95, PS96,PW97,PS00] are well recognized as two main classes of techniques for the copyright protection over digital data. They constitute two facets of copyright protection in the context of electronic marketplaces. More specifically, watermarking works by imperceptibly embedding a *seller* specific mark, which upon extraction enables provable ownership; fingerprinting embeds a *buyer* specific mark, which upon extraction identifies the buyer who has illegally disseminated the underlying digital data. For more details of the types of watermarking and fingerprinting schemes, the reader is referred to [CSP03]. A *buyer-seller watermarking protocol* [MW01,JKLL02,CC03,CSP03] is one that incorporates techniques of watermarking and fingerprinting to protect the rights of both the buyer and the seller.

In this paper, we concentrate on *anonymous* buyer-seller watermarking protocols in the sense that buyers can buy goods anonymously, but nevertheless can be identified by enforcement authorities if they redistribute the goods illegally. Anonymity has become one of the main service requirements, especially in e-commerce. The buyer is unwilling to disclose his identity (his public key in particular) when purchasing any content, since this could leak his privacy information, ie. lifestyle, personal interests, and embarrassing details.

A sound anonymous buyer-seller watermarking protocol is expected to fulfill the following requirements [PW97,JKLL02,CSP03]:

1. **Anonymity**: A buyer is able to purchase digital goods anonymously.
2. **Unlinkability**: Given two marked digital items, no one can decide whether or not they were purchased by the same buyer.
3. **Traceability**: The buyer who has illegally distributed digital goods (traitor/copyright violater) can be traced.
4. **No Framing**: An honest buyer should not be falsely accused by a malicious seller or other buyers.
5. **No Repudiation**: The buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or a security breach of the seller's system.
6. **Collusion Tolerance**: An attacker should not be able to find, generate, or delete the fingerprint by comparing the marked copies, even if they have access to a large number of copies.

1.1 Previous Work

Pfitzman and Waidner [PW97] are known to be the first to propose the concept of anonymous fingerprinting, in correspondence with the needs to achieve personal privacy in the overall context of e-commerce. However, their proposed scheme, based on secure two-party computation, is impractical since the underlying blocks are too complex to be efficient.

Afterwards, Pfitzman and Sadeghi suggested a method [PS00] without relying on two-party computations, but it is not practical either, because the building block [BS95] uses long codes for embedding.

The first-known buyer-seller watermarking protocol is due to Memon and Wong [MW01], and this was later extended by Ju *et. al* [JKLL02] to provide for anonymity of the buyer. Basically, a buyer-seller watermarking protocol is a combination of digital watermarking and digital fingerprinting. This type of protocol is a good model in the sense that it satisfies virtually all the requirements listed above. However, a problem with such a protocol is that it assumes a trusted *watermark certification authority* and a trusted *judge*. In other words, security of the system is based on the assumption that the seller will not collude with the watermark certification authority nor the judge (no conspiracy attack). Other buyer-seller watermarking protocols are due to Chang and Chung [CC03], and Cheung *et. al* [CLW04] but they do not provide any anonymity.

A recent work by Choi *et. al* [CSP03] claims to overcome this limitation of needing a trusted third party (TTP) by presenting a buyer-seller watermarking protocol secure against conspiracy attacks; but we will show in the next few sections that this is not the case.

1.2 Outline of This Paper

In this paper, we analyze the security of two recent anonymous buyer-seller watermarking protocols due to Ju *et. al* [JKLL02] and Choi *et. al* [CSP03]. We show that they fail to provide the features and security as claimed by their designers. In particular, these protocols cannot combat against the conspiracy attack [CSP03] where a seller colludes with the watermark certificate authority (WCA) in order to discover the watermark chosen by the buyer, and hence recreate the buyer's copy. We also show that even when protocol failures notwithstanding, the underlying commutative cryptosystem used in Choi *et. al*'s protocol still cannot prevent the WCA from discovering the actual watermark chosen by the buyer.

Furthermore, we show that these protocols can only provide "partial" anonymity, namely that the buyer's anonymity is guaranteed only if the WCA is honest. Finally, we propose a *truly* anonymous buyer-seller watermarking protocol without TTP that is more efficient and secure against conspiracy attacks. This protocol provides full anonymity in the sense that its security does not involve any WCA and hence does not have to depend on such parties to be honest. Our approach is that to ensure true anonymity, the buyer should generate his own private watermark, W and so other parties are not able to collude with each other to mount an attack to recreate the watermarked digital content sold to the buyer.

In Section 2, we discuss preliminary concepts and notations used in this paper. We review in Section 3 the protocols due to Ju *et. al* [JKLL02] and Choi *et. al* [CSP03]. We then present an attack on the commutative cryptosystem used in Choi *et. al*'s protocol, as well as conspiracy attacks on both protocols. In Section 4 we present our new protocol. We conclude in Section 5 and also highlight topics for further research.

2 Preliminaries

In this section, we briefly review the preliminary concepts required for an understanding of the rest of this paper.

2.1 Cryptographic Primitives

Since all protocols discussed in this paper use public key cryptography [RSA78, MOV97], we will briefly describe it in this subsection. In public key cryptosystems, each agent, A possesses a public key, pk_A which is easily obtainable from a certification authority center, CA. A also possesses a secret private key, sk_A, which is the inverse of pk_A. For convenience, we stick to $pk_A = g_A^{sk_A} \bmod p$, where p is a large prime (such that $(p-1)/2$ is also a prime) and g_A chosen by A is a generator of the multiplicative group, Z_p^* of order $(p-1)$. Also, unless otherwise specified, all arithmetic operations are performed under Z_p^*. We denote $E_k(m)$ to mean the message, m encrypted with the key, k. Any agent can encrypt a message for A using pk_A, but only A can decrypt this message with sk_A. This ensures *confidentiality*. Furthermore, A can sign a message by encrypting it with sk_A, denoted as $sign_{sk_A}(m)$, so that anybody can verify by using pk_A the identity of A and that the message really originated from A. This provides *authentication* and *non-repudiation*.

All parties − the seller, the buyer and the watermark certification authority (WCA) − have registered with the CA, and have their own pair of keys, which are $(pk_A, sk_A), (pk_B, sk_B)$ and (pk_C, sk_C) respectively.

Definition 1: (Homomorphic Cryptosystem) [CF85,BY87,MW01]. A cryptosystem E^h is said to be homomorphic if it forms a (group) homomorphism. That is, for a certain defined operation, $\otimes$, then given ciphertexts $E^h(x)$ and $E^h(y)$ for some unknown plaintexts x and y, anyone can compute $E^h(x \otimes y)$, or vice-versa, even without the private key. For example, the RSA cryptosystem [RSA78] is homomorphic with respect to the multiplication operation. As in [MW01], we assume that the public-key cryptosystem we are using is a privacy homomorphism with respect to the watermark insertion operation.

Definition 2: (Commutative Cryptosytem) [CSP03]. A cryptosystem E^c is said to be commutative, if for a multiple encrypted (decrypted) message, the same resultant ciphertext (plaintext) will be obtained, irrespective of its order of encryption. That is, $E^c_{K1}(E^c_{K2}(x)) = E^c_{K2}(E^c_{K1}(x))$ and $D^c_{K2}(E^c_{K1}(E^c_{K2}(x))) = E^c_{K1}(x)$ where $D(.) = E^{-1}(.)$.

Since one of our attacks in Section 3 exploits the special properties of the ElGamal-type [ZVM03] commutative cryptosystem chosen by Choi *et. al* [CSP03] for use in their protocol, we will briefly review it here:

ElGamal-type Commutative Cryptosystem [CSP03]. Consider two communicating parties, Alice and Bob, having respectively

$$K_A = \{(p, g_A, x_A, y_A) : y_A = g_A^{x_A} \pmod p\}$$
$$K_B = \{(p, g_B, x_B, y_B) : y_B = g_B^{x_B} \pmod p\}$$

where x_A and y_A (respectively x_B and y_B) are the private-public key-pair of Alice (respectively Bob). Suppose Alice encrypts first. To encrypt message m, Alice chooses a random number r_A and the obtains the ciphertext C_A consisting of two parts c_{A1} and c_{A2}, ie., $C_A = (c_{A1}, c_{A2})$, where

$$c_{A1} = g_A^{r_A} \bmod p, \quad c_{A2} = m * y_A^{r_A} \bmod p$$

Bob chooses a random number r_B and in turn encrypts Alice's ciphertext. The resulting C_B has two parts c_{B1} and c_{AB}, ie., $C_B = (c_{B1}, c_{AB})$, where

$$c_{B1} = g_B^{r_B} \bmod p, \quad c_{AB} = m * y_A^{r_A} * y_B^{r_B} \bmod p$$

The final ciphertext of the commutative cryptosystem thus consists of *three* parts, $C = (c_{A1}, c_{B1}, c_{AB})$. Note that C_A and C share an element c_{A1}, which will be exploited in one of our attacks in Section 3.2.

Now consider the decryption process. Suppose Alice decrypts first. She computes $c_{AB} * (c_{A1}^{x_A})^{-1} = m * y_B^{r_B} \pmod p$ using her private key x_A. Then Bob continues to compute $m * y_B^{r_B} * (c_{B1}^{x_B})^{-1} = m \pmod p$ using his private key x_B. Note that the order of decryptions similarly does not affect the final decryption result.

2.2 Notations

For ease of explanation, we use the notations similar to those in [JKLL02,CSP03], as follows:

3 Protocols and Attacks

In this section, we first briefly review the two protocols due to Ju *et. al* [JKLL02] and Choi *et. al* [CSP03], and then proceed with our attacks.

Both protocols comprise three phases, namely *watermark generation*, *watermark insertion*, *copyright violator identification*. Aside from the *watermark generation* phase, the two protocols are similar to each other.

For simplicity, we depict the watermark generation phase of the two protocols in Figures 1 and 2 respectively, and the common watermark insertion phase in Figure 3. We omit the copyright violator identification phase since it is irrelevant to our attacks. We refer the interested reader to [JKLL02,CSP03] for details.

Note that in Figure 1, $e = E_{pk_J}(\overline{sk}_B)$ is computed by encrypting with the judge's public key, pk_J. In Ju *et. al*'s protocol, there is a distinction between the

A	Alice, the seller who sells the digital multimedia content
B	Bob, the buyer who can buy contents anonymously
C	Carol, the watermark certification authority (WCA) who can issue watermarks to buyers upon request and certify them
CA	certification authority who can issue the certificate and a pair of keys (pk, sk) for every agent in the public-key infrastructure (PKI)
X	original content with m elements, $x_1, x_2, \ldots, x_m$
W	watermark with n elements, $w_1, w_2, \ldots, w_n$, where $n \leq m$
X', X''	watermarked content
$X \otimes W$	embed W into X with the embedding operation,$\otimes$
σ	random permutation function chosen (only known) by Alice
$cert$	a certificate computed by Bob
$E^h(.)/D^h(.)$	encryption/decryption algorithm of a public-key cryptosystem with homomorphic property
$E^c(.)/D^c(.)$	encryption/decryption algorithm of a commutative cryptosystem

judge, J and the WCA, Carol. This need for a judge as a trusted third party (TTP) was eliminated in Choi *et. al*'s protocol.

Meanwhile in Figure 2, $(\overline{sk}_{B1}, \overline{pk}_B = g^{\overline{sk}_{B1}})$ is an *anonymous key-pair* generated by the buyer, Bob to achieve his anonymity while purchasing. Bob convinces Carol of his possession of $\overline{sk}_{B1}$ via a zero-knowledge proof [C87]. Authenticity of this key-pair is certified by Carol as indicated by s_i, $i = 1 \ldots k$.

Finally, Figure 3 illustrates the common watermark insertion phase which is similar between both protocols, except that ew_j, s_j and W_j are used in Choi *et. al*'s protocol while ew, s and W are used in Ju *et. al*'s protocol. Also, Bob gets in the end a watermarked copy X'' of X that Alice cannot reproduce since she does not know the corresponding private key $\overline{sk}_{B1}$ and W_j even if she colludes with Carol. Plus, since Bob does not know σ, he cannot remove $\sigma(W_j)$ from X'', and neither can he remove V which is unknown to him.

3.1 Attacking the Protocol Due to Ju *et. al*

We first review two previous conspiracy attacks on Ju *et. al*'s protocol, and then further present our attack on it.

Conspiracy Attack I [CSP03]: Collusion of the Seller, the Watermark Certification Authority and the Judge. First, the seller, Alice sends the received $\overline{pk}_B$ and s from the buyer, Bob to the Watermark Certification Authority, Carol. Carol can easily go through her database of stored values and obtain the corresponding $E_{pk_J}(\overline{sk}_B)$ and pass it to the judge. The judge can decrypt it and then returns $\overline{sk}_B$ to Carol and Alice. By knowing $\overline{sk}_B$, w can be decrypted and W will be obtained. Hence, Alice can recreate Bob's watermarked copy, X''.

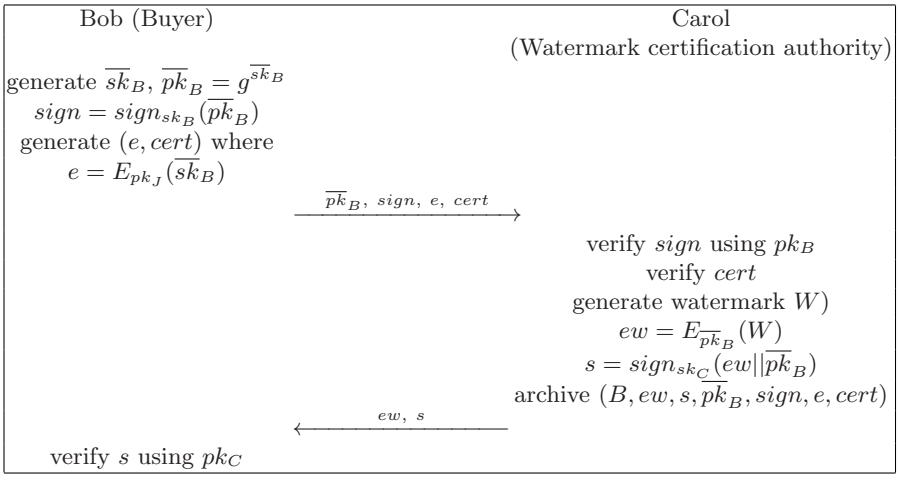

Fig. 1. Watermark Generation due to Ju *et. al* [JKLL02]

Conspiracy Attack II [CSP03]: Collusion of the Seller and the Judge. Alice can intercept the message communicated from Bob to Carol through an insecure channel and obtain $E_{pk_J}(\overline{sk}_B)$ and $\overline{pk}_B$. Alice forwards these together with $E^h_{\overline{pk}_B}(X'')$ to the judge. The judge can easily decrypt $E_{pk_J}(\overline{sk}_B)$ to get $\overline{sk}_B$ and further use that to decrypt $E^h_{\overline{pk}_B}(X'')$ to obtain X''. Hence, Alice can receive X'' if he colludes with the judge.

In addition to these two attacks, we present another new conspiracy attack, as follows:

Conspiracy Attack III [New]: Collusion of the Seller and the Watermark Certification Authority. Carol always knows and can record the watermark W which is sent to and used by the buyer. Consequently, once Alice colludes with Carol, she can obtain this and recreate Bob's copy easily since she has all the information needed, namely X, V, $\overline{pk}_B$ and σ.

By right, Carol should not store the unique watermark used by the buyer, Bob. However, it is quite hard − in fact, impossible − to prevent Carol from doing so, because in this protocol, Carol is the one who generates the watermark. It is this limitation that is the basis behind why a watermarking protocol falls to conspiracy attacks. We will show in Section 4 how to combat against this by presenting a new protocol that does not suffer from this and hence is resistant to conspiracy attacks.

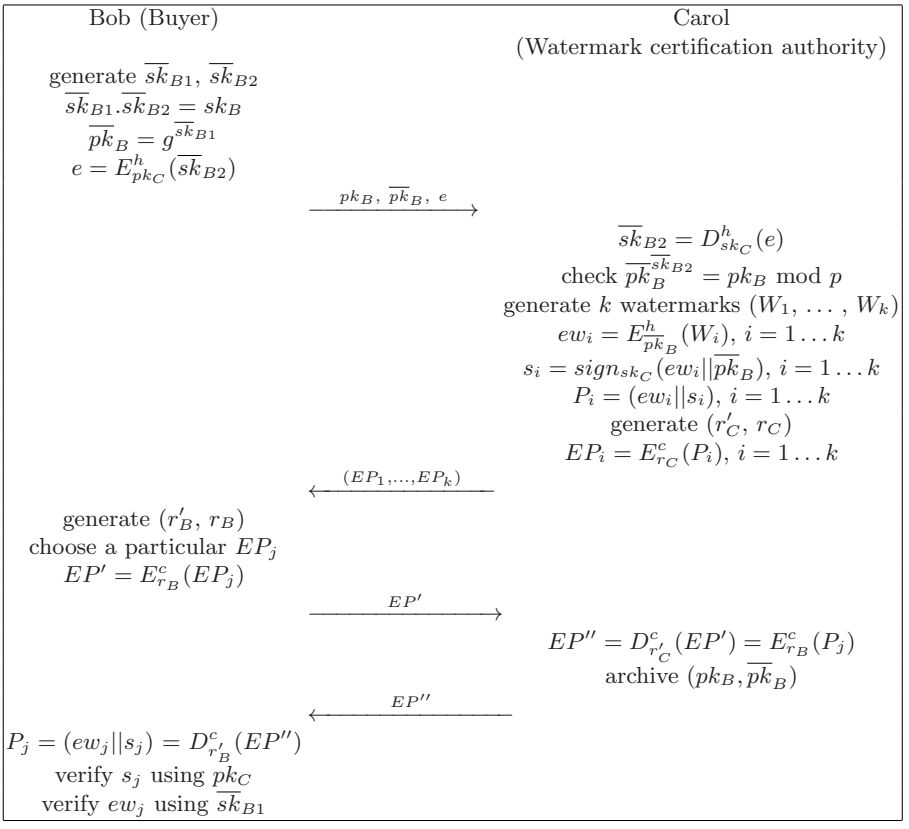

Fig. 2. Watermark Generation due to Choi *et. al* [CSP03]

3.2 Attacking the Protocol Due to Choi *et. al*

In this section, we first show that the commutative cryptosystem used in Choi *et. al*'s protocol fails to prevent the watermark certification authority from knowing the actual mark (fingerprint) chosen by the buyer. Second, we further show that even in the case where a secure commutative cryptosystem is chosen, the protocol itself cannot prevent conspiracy attacks by the seller and the watermark certification authority. In particular, the seller is able to discover the actual mark by colluding with the watermark certification authority and simply exploiting the encrypted watermark presented by the buyer.

Attack on the Commutative Cryptosystem. Recall that to prevent the watermark certification authority, Carol, from colluding with the seller, Alice, the protocol is intended to conceal the actual watermark chosen by the buyer, Bob, from Carol while at the same time enable Carol to certify this watermark. The adopted method as listed in Figure 2 works as follows. Carol first generates

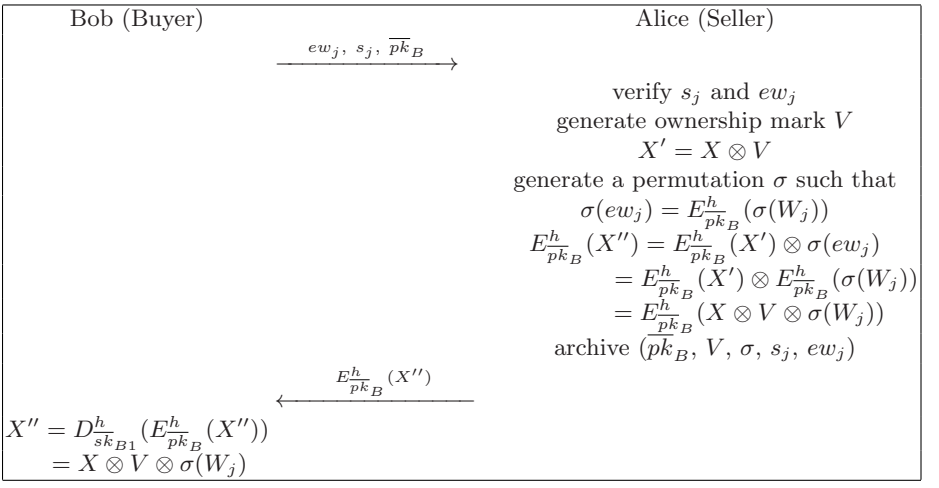

Fig. 3. Watermark Insertion of Both Protocols

k watermarks (W_1,..., W_k) and computes

$$\begin{aligned} ew_i &= E^h_{\overline{pk}_B}(W_i),\ i = 1 \ldots k \\ s_i &= sign_{sk_C}(ew_i || \overline{pk}_B), i\ = 1 \ldots k \\ P_i &= (ew_i || s_i),\ i = 1 \ldots k \\ EP_i &= E^c_{r_C}(P_i),\ i = 1 \ldots k \end{aligned} \tag{1}$$

where (r'_C, r_C) is respectively Carol's private and public key-pair for the commutative cryptosystem. Carol then sends (EP_1,...,EP_k) to Bob who selects a particular one (EP_j) and encrypts it with his key-pair (r'_B, r_B):

$$EP' = E^c_{r_B}(EP_j). \tag{2}$$

Bob sends EP' to Carol, who then decrypts it yielding EP'' as

$$EP'' = D^c_{r'_C}(EP') = E^c_{r_B}(P_j). \tag{3}$$

Carol sends EP'' to Bob. Bob then decrypts EP'' using r'_B to obtain P_j and in turn W_j. Note that in the interactions, it is anticipated that from EP' and EP'', Carol cannot determine the actual EP_j or P_j chosen by the buyer since Carol does not know r'_B.

The commutative cryptosystem explicitly specified by Choi *et. al* [CSP03] for use in their protocol is an ElGamal-type cryptosystem (See Section 2.1). Therefore, we have (r'_B, r_B) = (x_B, $y_B = g_B^{x_B} \mod p$) and (r'_C, r_C) = (x_C, $y_C = g_C^{x_C} \mod p$), and EP_i in (1) becomes

$$EP_i = E^c_{r_C}(P_i) = (g_C^{r_C} \bmod p,\ P_i * y_C^{r_C} \bmod p),\ i = 1 \ldots k. \tag{4}$$

Further, EP' in (2) becomes

$$EP' = E^c_{r_B}(EP_j) = (g_C^{r_C} \bmod p,\ g_B^{r_B} \bmod p,\ P_j * y_C^{r_C} * y_B^{r_B} \bmod p). \quad (5)$$

It is obvious that when Bob sends EP' to Carol, Carol can easily learn the particular EP_j (in turn W_j) chosen by Bob by simply comparing the first elements of EP' and EP_i, $i = 1 \ldots k$. This attack suggests that the commutative cryptosystem chosen by Choi *et. al* actually fails to attain its anticipated objective, ie., to prevent Carol from learning the actual mark chosen by Bob. It is worth noting that the first element ($g_C^{r_C} \bmod p$) must be included in EP' as indicated in (5) since it is needed (See Section 2.1) in the decryption process by Carol.

The most straightforward way to prevent this attack is to replace the ElGamal-type cryptosystem chosen by Choi *et. al* with alternative commutative cryptosystems that do not succumb to this attack.

Further, note that Carol uses the same random number r_C to encrypt all EP_i, $i = 1 \ldots k$ (See [CSP03], Section 4.1). This causes yet another serious problem because at the end of the watermark generation phase, Bob eventually learns the P_j, so by equation (6) he can compute $y_C^{r_C} \bmod p$. With $y_C^{r_C} \bmod p$ in place, Bob can learn via the same equation all the values of the other P_i's, and in turn the corresponding values of W_i, $i = 1 \ldots k$. This might not be desirable in practice.

Conspiracy Attack on the Protocol. We further demonstrate that the protocol itself is vulnerable to a conspiracy attack by Alice and Carol, even if we assume the underlying commutative cryptosystem is secure.

In the watermarking insertion phase (see Figure 3), Bob sends the chosen ew_j, s_j, $\overline{pk}_B$ to Alice for the purpose of watermark insertion. By colluding with Carol, Alice will know the set of possible watermarks $W_1, W_2, \ldots, W_k$ generated for Bob. Then, for $i = 1 \ldots k$, she computes all the values, $ew_i = E^h_{\overline{pk}_B}(W_i)$ and compares them with the ew_j that she received from Bob. The buyer's chosen watermark will then simply be the corresponding W_i.

Alternatively, Alice could forward ew_j and $\overline{pk}_B$ to Carol. By $\overline{pk}_B$, Carol determines the set of ew_i, $i = 1 \ldots k$ that have been produced for Bob. Then Carol compares the received ew_j from Alice with ew_i, $i = 1 \ldots k$. Note that ew_i, $i = 1 \ldots k$, are originally produced by Carol, so she knows the corresponding plaintexts although she cannot decrypt them! It becomes clear that the plaintext of the matching item among ew_i, $i = 1 \ldots k$, is $W_i = W_j$. Upon successfully retrieving W_j, Carol gives it to Alice. In this way, the conspiracy attack by Alice and Carol succeeds. As a matter of fact, to facilitate the process of matching, it suffices for Carol to simply maintain a table for each user as follows:

$ew_i = E^h_{\overline{pk}_B}(W_i)$	W_i
ew_1	W_1
ew_2	W_2
...	...
ew_k	W_k

Once Alice knows the watermark chosen by Bob, many important features of the anonymous buyer-seller watermarking protocol would end up getting compromised. First, traitor tracing does not hold any more since both the seller and the buyer might possibly be the traitor. Second, non-framing fails because an honest buyer may be falsely accused by a dishonest seller. Third, due to the fact both the seller and the buyer can misbehave, non-repudiation obviously no longer holds.

3.3 Failure to Provide True Anonymity

Here, we further remark on the "anonymity" provided by both the protocols proposed by Ju *et. al* [JKLL02] and Choi *et. al* [CSP03]. During the watermark generation phase, for Ju *et. al*'s protocol, Carol uses Bob's public key, pk_B to verify the *sign* from Bob, and so Carol knows Bob's identity. Similarly, in Choi *et. al*'s protocol, Bob sends pk_B along with $\overline{pk}_B$ to Carol. Therefore, Carol would be able to associate $\overline{pk}_B$ to Bob's identity, and so although the anonymous key-pairs appear anonymous to Alice, they are by no means anonymous to Carol. This suggests that buyer anonymity in the protocols is achieved only when the watermark certification authority, Carol, can be trusted, and hence both protocols only achieve "partial anonymity".

4 Our Proposed Protocol

We propose a new truly anonymous buyer-seller watermarking protocol where the buyer is allowed to generate his own secret watermark and hence is the only party who knows it. This is essential to protect the buyer's security from conspiracy attacks, and to ensure his privacy. The watermark generation phase is given in Figure 4, while our watermark insertion phase is identical to Figure 3. Note that only a total of 4 messages are communicated in our protocol (during the entire watermark generation and insertion phases).

The main intuition is that the buyer, Bob enlists the help of a certification authority, CA to certify his chosen anonymous public key, $\overline{pk}_B$. In this way, only CA knows where $\overline{pk}_B$ came from. CA is the one who issues public key certificates containing public and private key-pairs of all agents (including Alice, Bob and Carol) in a public-key infrastructure (PKI) and hence is definitely trustable, otherwise no PKI would be secure and no public and private key-pairs would be binding or confidential. Note that there is no need for a separate watermark certification authority, Carol in this case.

Copyright Violater Identification. When Bob is suspected, the judge will request by law for him to disclose the unique self-generated watermark, W and then compute the deterministic encryption $E^h_{\overline{pk}_B}(W)$. The result is compared with the stored ew in the CA's database, whose integrity can be validated by using s: (i) if they are not the same, B will be guilty because of giving a fraudulent

watermark, (ii) if yes, then, the judge will proceed to extract the embedded watermark in multimedia content. Finally, the extracted watermark is compared with $\sigma(W)$. If they match, then B is guilty, otherwise, B is innocent. Alice is not able to recreate X'' because he does not know the unique W. Note that Bob does not need to disclose his identity during the identification process. The interested reader is also referred to [JKLL02] for more details on the identification process.

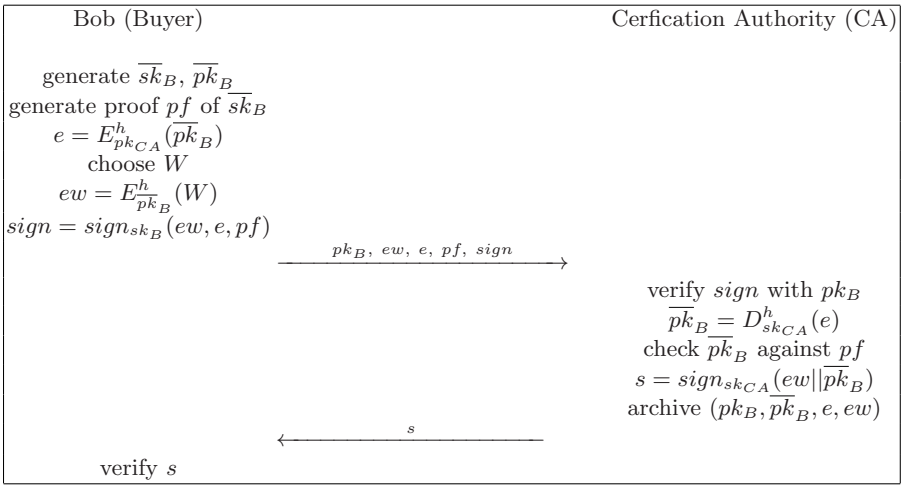

Fig. 4. Watermark Generation of Our Proposed Protocol

5 Conclusions and Open Problems

We have shown that the two recent anonymous buyer-seller watermarking protocols due to Ju *et. al* [JKLL02] and Choi *et. al* [CSP03] are insecure against conspiracy attacks, contradicting their exact security claims. With the success of conspiracy attacks, many important features including traitor tracing and non-repudiation are completely compromised.

We have further shown that protocol failures notwithstanding, the commutative cryptosystem chosen by Choi *et. al* in their protocol makes it insecure in that it cannot prevent the watermark certification authority from discovering the watermark chosen by the buyer.

Though the main claim by Choi *et. al* is that their protocol eliminates the need for a trusted third party, our results have shown that this is not the case at all. On the contrary, the security of their protocol depends entirely on the honesty of the watermark certification authority which is a trusted third party. Further, we have also shown that their protocol does not provide true anonymity since in this case one has to again rely on the honesty of the watermark certification authority.

We further pose some interesting open problems for future work:

- Security analysis of the proposed protocols on their security with different block cipher modes of operation, and underlying cryptographic and watermarking algorithms.
- Design of buyer-seller watermarking protocols for multi-transactions involving multiple copies. There are two issues involved here. First, for a certain content, X, which supposing can only be sold to n different buyers, how do current protocols handle this? In particular, how do we ensure that a seller does not sell more copies of X than what is allowed, or that he does not resell an already-sold copy? Second, on the buyer side, suppose a buyer wishes to buy more than one copy of the same content, X from the same seller. How do current protocols keep track of how many identical copies of X that have been bought by the same buyer from the same seller? One way that we foresee to tackle the second issue is to tag a unique identification number to each content, including identical contents, so that even if two or more contents are identical, they would cause different X values to be input to the protocols.

References

[BS95] D. Boneh, J. Shaw, *Collusion-Secure Fingerprinting for Digital Data*, Crypt'95, LNCS 963, pp.452-465, 1995.

[BY87] E.F. Brickell, Y. Yacobi, *On Privacy Homormorphisms*, Eurocrypt'87, LNCS 304, pp.117-125, 1987.

[CC03] C.C. Chang, C.Y. Chung, *An Enhanced Buyer-Seller Watermarking Protocol*, Proc. ICCT2003, pp. 1779-1783, 2003.

[C87] D. Chaum, *An Improved Protocol for Demonstrating Possession of Discrete Logarithms and some Generalizations*, Eurocrypt'87, LNCS 307, pp. 127-141, 1987.

[CLW04] S.-C. Cheung, H.-F. Leung, C. Wang, *A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents*, Proc. 37th Hawaii International Conference on System Sciences, Hawaii, p. 40094a, 2004.

[CSP03] J.G. Choi, K. Sakurai, J.H. Park, *Does it Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party*, Proc. Applied Cryptography and Network Security '03, LNCS 2846, pp. 265-279, 2003.

[CF85] J.D. Cohen, M.J. Fischer, *A Robust and Verifiable Cryptographically Secure Election Scheme (extended abstract)*, Proc. IEEE 26th Annu. Symp. Foundations Computer Science, Portland, p. 372-382, 1985.

[CMB02] I.J. Cox, M.L. Miller, J.A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.

[HK99] F. Hartung, M. Kutter, *Multimedia Watermarking Techniques*, Proc. IEEE, vol. 87, pp. 1079-1107, July 1999.

[JKLL02] H.S. Ju, H.J. Kim, D.H. Lee, J.I. Lim, *An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control* , ICISC'02, LNCS 2587, pp. 421-432, 2002.

[MW01] N. Memon, P.W. Wong, *A Buyer-Seller Watermarking Protocol*, IEEE Transactions on Image Processing, vol. 10, no. 4, pp.643-649, 2001.

[MOV97] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[PS00] B. Pfitzman, A.R. Sadeghi, *Coin-Based Anonymous Fingerprinting*, Eurocrypt'99, LNCS 1592, pp.150-163, 2000.

[PS96] B. Pfitzman, M. Schunter, *Asymmetric Fingerprinting*, Eurocrypt'96, LNCS 1070, 1996, pp. 84-95.

[PW97] B. Pfitzman, W. Waidner, *Anonymous Fingerprinting*, Eurocrypt'97, LNCS 1233, pp. 88-102, 1997.

[RSA78] R.L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[SKT98] M. Swanson, M. Kobayashi, A. Tewfik, *Multimedia Data Embedding and Watermarking Technologies*, Proc. IEEE, vol. 86, pp. 1064-1087, June 1998.

[VP99] G. Voyatzis and I. Pitas. The Use of Watermarks in the Protection of Digital Multimedia Products. Proc. IEEE, Vol. 87, pp. 1197-1207, July 1999.

[WNR83] N.R. Wagner, *Fingerprinting*, IEEE Symposium on Security and Privacy, pp.18-22, 1983.

[WPD99] R. Wolfang, C. Podilchuk, E. Delp, *Perceptual Watermarks for Digital Images and Video*, Proc. IEEE, vol. 87, pp. 1108-1126, July 1999.

[ZK95] J. Zhao, E. Koch, *Embedding Robust Labels Into Images For Copyright Protection*, International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, 1995.

[ZVM03] W. Zhao, V. Varadharajan, Y. Mu, *A Secure Mental Poker Protocol Over the Internet*, Australasian Information Security Workshop 2003, Conference in Research and Practice in Information Technology, Vol. 21, Feb. 2003.