Attacks on Two Buyer-Seller Watermarking Protocols and an Improvement for Revocable Anonymity

Mina Deng and Bart Preneel
IBBT-COSIC, K.U.Leuven
Belgium

1. Introduction

The recent success of the Internet and the rapid development of information technology facilitate the proliferation of e-commerce, where all types of multimedia information can easily be stored, traded, replicated, and distributed in digital form without a loss of quality. As a main advantage over traditional commercial means, e-commerce brings convenience and efficiency for trading activities between sellers and buyers. However, it also enables illegal replications and distributions of digital products at a low cost. In this regard, there are many multimedia content providers still hesitating to sell and distribute their products over the Internet. Therefore, digital copyright protection is a main concern that needs to be addressed. On the other hand, how to protect the rights and provide security for both the seller and the buyer is another challenge for e-commerce.

In the realm of security, encryption and digital watermarking are recognized as promising techniques for copyright protection. *Encryption* is to prevent unauthorized access to a digital content. The limitation is that once the content is decrypted, it doesn't prevent illegal replications by an authorized user. *Digital watermarking (*Cox et al., 2001, 1997), (Hartung & Kutter, 1999), complementing encryption techniques, provides provable copyright ownership by imperceptibly embedding the seller's information in the distributed content. Similarly, *digital fingerprinting* is to trace and identify copyright violators by embedding the buyer's information in the distributed content.

The literature of fingerprinting research can be categorized as fingerprinting for generic data, e.g. c-secure fingerprinting code (Boneh & Shaw, 1995), fingerprinting for multimedia data (Wang et al., 2005), (Trappe et al., 2003), (Liu et al., 2005), and fingerprinting protocols, e.g. the ones based on secure two-party computations (Pittzmann & Schunter, 1996), (Pfitzmann & Waidner, 1997) or based on coin-based constructions (Pfitzmann & Sadeghi, 1999, 2000), (Camenisch, 2000).The shortcoming of these fingerprinting schemes lies in the inefficiency of the implementations (Ju et al., 2002). On the other hand, the literature can also be categorized as symmetric schemes, asymmetric schemes, and anonymous schemes. In *symmetric schemes* (Blakley et al., 1986), (Boneh & Shaw, 1995), (Cox et al., 1997), both the seller and the buyer know the watermark and the watermarked content.

Problem solved	(Memon& Wong)	(Ju et al.)	(Choi et al.)	(Goi et al.)	(Lei et al.)	(Zhang et al.)	(Shao)	(Ibrahim et al.)	Ours
Piracy tracing	√	√	√	√	√	√	√	√	√
Customer's rights	√	√	√	√	√	√	√	√	√
Unbinding					√	√	√	√	√
Conspiracy				√		√			√
Dispute resolution		√			√		√	√	√
Anonymity/unlinkability									√

Table 1. Comparison of some existing buyer-seller watermarking protocols with our protocol

As a consequence, it is possible for a malicious seller to frame an innocent buyer, or for an accused buyer to repudiate the guilt. This *customer's rights problem* in symmetric schemes was first pointed out (Qiao & Nahrstedt, 1998), and the problem can be solved by *asymmetric schemes* (Pittzmann & Schunter, 1996), (Pfitzmann & Waidner, 1997), (Biehl & Meyer, 1997) where only the buyer can obtain the exact watermarked or fingerprinted copy, and hence the buyer cannot claim that an pirated copy was originated from the seller. When a pirated copy is found, the seller is able to obtain a means to identify and prove the copyright violation to a trusted third party. Moreover, in order to provide the buyer's anonymity, *anonymous schemes* (Pfitzmann & Sadeghi, 1999, 2000) further make use of a registration service to eliminate the need of exposing the buyer's identity to the seller.

A *buyer-seller watermarking protocol* is one that combines encryption, digital watermarking, and other techniques to ensure rights protection for both the buyer and the seller in e-commerce. A complete and sound buyer-seller watermarking protocol is expected to solve the following problems.

1. **The piracy tracing problem:** once a pirated copy is found, the seller should be able to trace and identify the copyright violator.
2. **The customer's rights problem:** when a watermark is inserted solely by the seller, the seller may benefit from framing attacks to an innocent buyer or it causes unsettled disputes. On the other hand, the accused buyer of distributing an unauthorized copy may claim that the copy originated from the seller or there existed a security breach in the seller's system.
3. **The unbinding problem:** upon discovering a pirated copy, the seller can fabricate piracy by transplanting the buyer's watermark into another digital content. Therefore, it is necessary to bind a chosen watermark with a specific transaction.
4. **The anonymity problem:** the identity of a buyer should remain unexposed during transactions unless he is proven to be guilty.
5. **The conspiracy problem:** malicious parties may collude with each other and mount attacks to frame an innocent buyer or to confound the tracing by removing the watermark from the digital content.
6. **The dispute problem:** the arbitrator should be able to resolve disputes, without the buyer revealing his identity or private key.

Accordingly, a buyer-seller watermarking protocol should provide the following security properties as the strategic design principle.

1. **Traceability:** a copyright violator should be able to be traced and identified.

2. **Non-framing:** nobody can accuse an honest buyer.
3. **Non-repudiation:** a guilty buyer cannot deny his responsibility for a copyright violation caused by him.
4. **Dispute resolution:** the copyright violator should be identified and adjudicated without him revealing his private information, e.g. private keys or watermark.
5. **Conspiracy resistance:** no colluded parties should be able to frame an innocent buyer or to confound the tracing by removing the watermark from the digital content.
6. **Anonymity:** a buyer's identity is undisclosed until he is judged to be guilty.
7. **Unlinkability:** nobody can determine whether the different watermarked contents are purchased by the same buyer or not.

1.1 Analysis of the Existing Work

The literature is rich of relevant buyer-seller watermarking protocols. Qiao and Nahrstedt (Qiao & Nahrstedt, 1998), first pointed out the *customer's rights problem* in the watermarking protocols for piracy tracing. However, their scheme is symmetric and doesn't guarantee the buyer's security. The first known asymmetric buyer-seller watermark protocol was introduced by Memon and Wong (Memon & Wong, 2001), and it was improved by Ju et al. (Ju et al., 2002). Since the first introduction of the concept, several alternative design solutions have been proposed. Due to the space limit, instead of a full security analysis, we summarize the analysis and point out the shortcomings of each previous protocols (Choi et al., 2003), (Goi et al., 2004), (Lei et al., 2004), (Zhang et al., 2006), (Shao, 2007), and (Ibrahim et al., 2007). Except that the piracy tracing problem and the customer's rights problem are solved in the early schemes, the existing solutions to the other problems are either impractical or incomplete, as depicted in Table 1. Comparison of some existing buyer-seller watermarking protocols with our protocol

1. **The piracy tracing problem.** All of these protocols are able to resolve the piracy tracing problem, and provide a mechanism for the seller to trace and recover the identity of a guilty buyer.
2. **The customer's rights problem.** All these protocols can solve the customer's rights problem, since the protocols are designed asymmetric, i.e., the seller doesn't know the exact value of the buyer's watermark, neither does she know the final watermarked digital content that the buyer gets. Therefore, the accused buyer for a illegal replication or distribution cannot claim that the copy is originated from the seller or a security breach in the seller's system.
3. **The unbinding problem.** Lei et al. (Lei et al., 2004) addressed *the unbinding problem* in (Memon & Wong, 2001), (Ju et al., 2002), (Choi et al., 2003), (Goi et al., 2004) and provided a mechanism to bind a specific transaction of a digital content to a specific buyer, such that a malicious seller cannot transplant the watermark embedded in a digital content to another higher-priced content. The similar design principle is applied in (Zhang et al., 2006) and (Shao, 2007).
4. **The conspiracy problem.** Choi et al. (Choi et al., 2003) pointed out the *conspiracy problem* of (Memon & Wong, 2001), (Ju et al., 2002) where a malicious seller can collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer. Goi et al. (Goi et al., 2004) found the conspiracy problem couldn't be solved through commutative cryptosystems of (Choi et al., 2003), and further point out that the schemes of (Memon & Wong, 2001), (Ju et al., 2002), (Choi et al., 2003) are vulnerable

against *conspiracy attacks*, and show that the protocol's security shouldn't rely on any third party. Zhang et al. (Zhang et al., 2006) apply the idea of (Goi et al., 2004)and ensure that the buyer's watermark is generated by the buyer, instead of a watermark certificate authority (*WCA*). According to our analysis, we conclude that the protocols of (Lei et al., 2004), (Shao, 2007), and (Ibrahim et al., 2007) cannot resist the conspiracy attack, where a malicious seller can collude with a third party, such that the seller can discover the buyer's watermark.

5. **The anonymity problem.** Memon and Wong's protocol (Memon & Wong, 2001) requires the seller to know the buyer's identity to carry out a transaction. Protocols of (Ju et al., 2002), (Choi et al., 2003) improve (Memon & Wong, 2001) by applying an anonymous key pair in each transaction. However, both protocols require the *WCA* to know the buyer's identity, which means that the buyer's anonymity is not preserved against conspiracy attacks. In (Goi et al., 2004), the buyer is required to request a signature from the certification authority (*CA*) of the public key infrastructure (*PKI*) to generate a watermark. However, (Goi et al., 2004) cannot solve the anonymity problem efficiently, since before each transaction, the buyer has to contact the *CA* for a new signature. (Lei et al., 2004), (Zhang et al., 2006), (Shao, 2007) apply anonymous certificates, i.e., digital certificates without real identities of applicants. Unfortunately, transaction unlinkability is not provided: during all transactions, the anonymous certificate stays the same, unless the buyer contacts the *CA* before each transaction for a new certificate, which is impractical for real life applications.
6. **The dispute problem.** Zhang et al. (Zhang et al., 2006) presented a scheme, derived from (Lei et al., 2004), where no trusted third party (*TTP*) is required in the watermark generation phase and the conspiracy problem is solved. Unfortunately, we find the existence of *dispute resolution problem* in (Zhang et al., 2006), in order to resolve disputes the buyer is required to cooperate and reveal his secret key or his secret watermark to the judge or to the *CA*, which is unrealistic in real-life applications. Similarly, schemes of (Memon & Wong, 2001), (Choi et al., 2003), (Goi et al., 2004) all require the accused but possible innocent buyer to disclose his identity or private key. Moreover, these protocols don't operate properly if the underlying cryptosystem is probabilistic, because the data encrypted by the judge or the *CA* may not be equal to the data provided by the seller. In (Ju et al., 2002), the buyer creates a key escrow cipher to escrow his anonymous private key at the judge. The problem is that the buyer's secrecy would not be protected against conspiracy attacks if the judge was malicious. In (Lei et al., 2004), the judge requests the buyer's watermark from the *WCA*, and hence the security depends on the trustworthiness of the *WCA.*

1.2 Our Approach

From the above analysis, we show that none of the existing protocols fulfils the design requirements. Our contribution of this paper is twofold: first, we analyze the security and present attacks on the protocols by Lei et al. (Lei et al., 2004), and Ibrahim et al. (Ibrahim et al., 2007), and prove that neither of them is able to provide security for the buyer and/or the seller as claimed. Further, both protocols require to employ deterministic cryptosystems. Unfortunately, all efficient privacy homomorphic cryptosystems are probabilistic (Fontaine & Galand, 2007), and both protocols require a privacy homomorphism for watermark insertion in the encrypted domain. In this regard, we can prove that both protocols are not able to work properly as designed to be. Next, we point out that the buyer's anonymity or the transaction unlinkability is not provided by these two protocols. Second, we propose an anonymous buyer-seller watermarking protocol, which is secure and fair for both the seller and the buyer. Our protocol employs privacy homomorphic cryptosystems to protect the buyer's secret watermark, and group signature schemes to provide revocable anonymity of the buyer. The proposed protocol is an improvement of the early work (Deng & Preneel, 2008), (Zhang et al., 2006).

The rest of the paper is organized as follows. The security of the protocol by Lei et al. is analyzed in Sec. 0. The security of the protocol by Ibrahim et al. is analyzed in Sec. 0. Some cryptographic primitives are reviewed in Sec. 0. A generalized model of anonymous buyer-seller watermarking protocol is defined in Sec. 0. The proposed protocol is explained in Sec. 0. Finally, the security analysis is provided in Sec. 0 and the conclusion is drawn in Sec. 0.

2. Attacks on the Protocol of Lei et al.

In the protocol of (Lei et al., 2004), the players are the seller Alice *A*, the buyer Bob *B*, the certificate authority *CA*, the watermark certificate authority *WCA*, and the arbitrator *J*. The protocol comprises three phases, namely the registration protocol, the watermark generation and insertion protocol, and the identification and arbitration protocol. We provide an overview of the protocol in Fig. 1, Fig. 2, and Fig. 3. Notations are explained in Table 2. Notations and abbreviations

2.1 Attack on the Buyer's Security

Collusion of the seller and the *WCA*. In the protocol, Alice generates her watermark V and embeds V to the original content X, $X' = X \oplus V$. The *WCA* generates Bob's watermark W, and sends Alice the two encrypted values of W with Bob's encryption key pk_{B^*} and *WCA*'s encryption key pk_{WCA}, respectively. Alice embeds the encrypted watermarked, $E_{pk_{B^*}}(X'') = E_{pk_{B^*}}(X') \oplus E_{pk_{B^*}}(W)$. When malicious Alice colludes with an untrustworthy *WCA*, Alice sends $E_{pk_{B^*}}(W)$ back to the *WCA*. The *WCA* recovers W via decryption, and sends W to Alice. After Alice obtains W, she knows all the necessary information X, V, W to reproduce the watermarked content X'' for Bob.

Lei et al. assume that the *WCA* will not reveal Bob's information to Alice. However, the assumption is unrealistic. Because there is no technical enforcement for the *WCA* not to reveal any private information to Alice, the conspiracy attack is effective. Once Alice gets Bob's watermark, any important features of the protocol would end up getting compromised. First, the piracy traceability won't be achieved, since both the buyer and the seller might be the traitor. Second, non-framing fails, even though the unbinding problem is solved in the protocol. Alice is able to frame an innocent Bob by reproducing and redistributing the watermarked content X''. Third, non-repudiation fails, even though *B* doesn't know W and cannot remove W from X''. A malicious Bob can deny his guilt by claiming that the pirated copy was created by Alice or a security breach in Alice's computing system. In fact, this attack weakens the security for both the buyer and the seller.

$\mathcal{A}$	Alice, the seller and the copyright holder
$\mathcal{B}$	Bob, the buyer who purchases the desired digital contents from the seller
CA	A trustworthy certificate authority in the PKI
$\mathcal{J}$	An arbiter who adjudicates lawsuits against the infringement of copyright and intellectual property
WCA	A watermark certificate authority to generate or approve the watermark of the buyer
$E_{pk_i}(\cdot), D_{sk_i}(\cdot)$	Encryption and decryption operation
$sign_{sk_i}(m), \mathtt{Vf}(pk_i, m, sig)$	The signature creation and verification operation
$H(\cdot)$	A collision resistant hash function
UKg	The user key generation algorithm applied by a user i to obtain a personal public and private key pair
GSig	The group signing algorithm applied by a group member i to a message m
GVf	The group signature verification algorithm to verify the signature on m with the group public key gpk
Open	The opening algorithm applied by the opener to claim the identity of the group member who has produced the signature of m, and generate a proof of the claim
Judge	The judge algorithm which aims to verify that certain group member i produced a signature of m with a proof
ARG	An agreement between the buyer and the seller that uniquely binds the particular transaction to X
$Cert_{CA}(pk_B)$	Bob's anonymous certificate for pk_B issued by the CA
$Cert_{pk_B}(pk_B^*)$	Bob's anonymous certificate for pk_B^* issued by Bob on the honer of pk_B
$Cert_C A(B)$	Bob's public key certificate issued the CA
$Cert_B$	Bob's certificate issued by CA in the group signature registration phase
B	The identity of Bob
$X, X^{'}, X^{''}$	The original content, the watermarked content after the first embedding, the final watermarked content for Bob
$\oplus$	Watermark embedding operation
$det(X, Y)$	Non-blind watermark extraction operation with inputs as the watermarked content and the original content
$gpk, gmsk, gsk_B$	The group public key, group manager's secret key, and Bob's group signature key.
$(pk_B, sk_B), (upk_B, usk_B)$	Bob's key pairs used in the group joining phase
(pk_B^*, sk_B^*)	Bob's one-time anonymous public private key pair for each transaction
$reg[B]$	The registration table populated by the CA to store the group registration information of Bob
sig_B	Bob's signature to pk_B signed with usk_B
σ	Bob's group signature to pk_B^* signed with gsk_B
$c_{esc}, pf_{sk_B^*}$	Bob's key escrow cipher $E_{pk_{CA}}(sk_B^*)$ and its proof
V, W_A, W_B	V, W_A are the seller's watermarks, W_B is the buyer's watermark, generated in each transaction
1^k	If $k \in \mathbb{N}$, then 1^k denotes the string of k ones.

Table 2. Notations and abbreviations

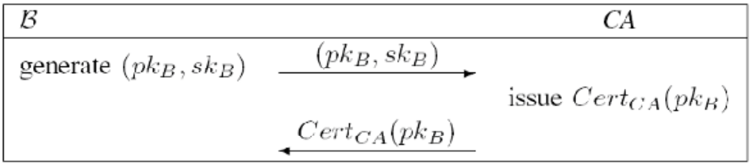


Fig. 1. The registration protocol in Lei et al.'s protocol (Lei et al., 2004).

2.2 Attack on the Seller's Security

Collusion of the buyer and the *WCA*. Besides the conspiracy attack explained above, a malicious buyer and the untrustworthy *WCA* can also collude. In this case, the *WCA* informs Bob the actual value of W directly, so that it is possible for Bob to remove his watermark from the watermarked digital content. Therefore, non-repudiation won't hold, and the protocol fails to provide security for the seller.

2.3 Failure for Probabilistic Cryptosystems

In the arbitration and identification protocol, the WCA is required by the arbitrator J to decrypt $E_{pk_{WCA}}(W)$ and obtain the Bob's watermark W. Then J performs a validation on the correctness of the value $E_{pk_{WCA}}(W)$ sent by Alice, by computing the encryption of W obtained from the WCA with the buyer's public key pk_{B^*} as $E_{pk_{WCA}}(W)$. If $E_{pk_{B^*}}(W)$ is not the same as $E_{pk_{B^*}}'(W)$, then J rejects the case and the protocol halts. It is obvious that this verification won't work using probabilistic cryptosystems. As explained in Sec. The buyer-seller watermarking protocol requires watermarking insertion to be performed in the encrypted domain, and it should be achieved by employing privacy homomorphic cryptosystems. However, all efficient privacy homomorphic cryptosystems are probabilistic (Fontaine & Galand, 2007). As a result, the protocol fails to function properly as claimed.

2.4 Failure for Unlinkability

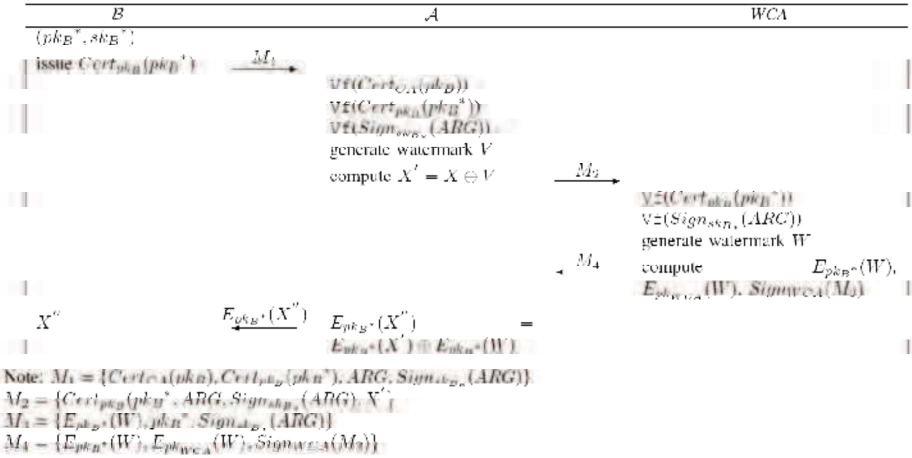

$\mathcal{B}$
$\mathcal{A}$
WCA
(pk_{B^*}, sk_{B^*})
issue $Cert_{pk_B}(pk_{B^*})$
M_1
$V\stackrel{?}{=}(Cert_{CA}(pk_B))$
$V\stackrel{?}{=}(Cert_{pk_B}(pk_{B^*}))$
$V\stackrel{?}{=}(Sign_{sk_{B^*}}(ARG))$
generate watermark V
compute $X' = X \ominus V$
M_2
$V\stackrel{?}{=}(Cert_{pk_B}(pk_{B^*}))$
$V\stackrel{?}{=}(Sign_{sk_{B^*}}(ARG))$
generate watermark W
M_4
compute $E_{pk_{B^*}}(W)$, $E_{pk_{WCA}}(W)$, $Sign_{WCA}(M_2)$
X''
$E_{pk_{B^*}}(X'')$
$E_{pk_{B^*}}(X'') = E_{pk_{B^*}}(X') \oplus E_{pk_{B^*}}(W)$
Note: $M_1 = \{Cert_{CA}(pk_B), Cert_{pk_B}(pk_{B^*}), ARG, Sign_{sk_{B^*}}(ARG)\}$
$M_2 = \{Cert_{pk_B}(pk_{B^*}), ARG, Sign_{sk_{B^*}}(ARG), X'\}$
$M_3 = \{E_{pk_{B^*}}(W), pk_{B^*}, Sign_{sk_{B^*}}(ARG)\}$
$M_4 = \{E_{pk_{B^*}}(W), E_{pk_{WCA}}(W), Sign_{WCA}(M_3)\}$

Fig. 2. The watermark generation and insertion protocol in Lei et al.'s protocol (Lei et al., 2004).

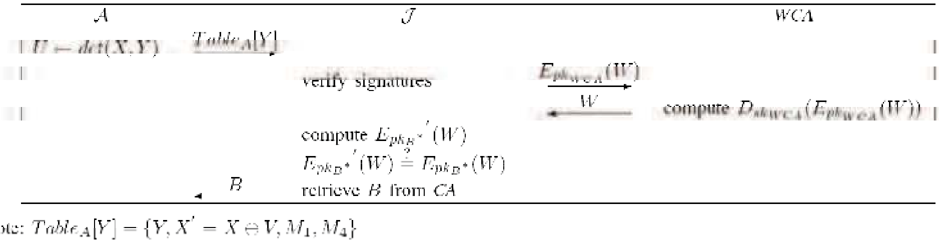
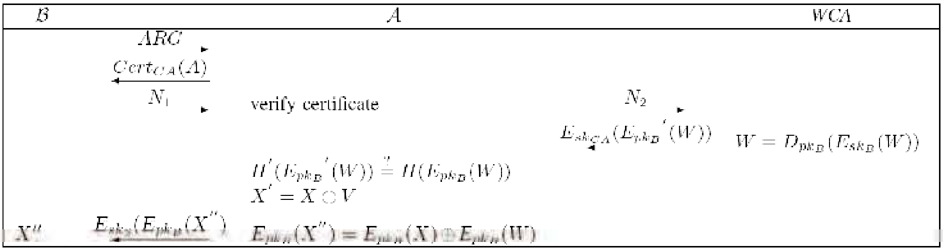

$\mathcal{A}$
$\mathcal{J}$
WCA
$U \leftarrow det(X, Y)$
$Table_A[Y]$
verify signatures
$E_{pk_{WCA}}(W)$
W
compute $D_{sk_{WCA}}(E_{pk_{WCA}}(W))$
compute $E_{pk_{B^*}}'(W)$
$E_{pk_{B^*}}'(W) \stackrel{?}{=} E_{pk_{B^*}}(W)$
B
retrieve B from CA
Note: $Table_A[Y] = \{Y, X' = X \ominus V, M_1, M_4\}$

Fig. 3. The identification and arbitration protocol in Lei et al.'s protocol (Lei et al., 2004).

In the protocol, Bob first obtains an anonymous certificate $Cert_{CA}(pk_B)$ from the CA, i.e., a digital certificate without the real identity of the applicant, in order to provide the buyer's anonymity. As Lei et al. claimed, by issuing the anonymous certificate to Bob, the CA is responsible for binding this anonymous certificate to Bob's identity. In each transaction with Alice, Bob generates an one-time key pair (pk_{B^*}, sk_{B^*}), and creates a certificate of pk_{B^*} on the honour of the certified public key pk_B. Unfortunately, the protocol fails to provide transaction unlinkability: during all transactions from the seller to the buyer, the public key anonymous certificate $Cert_{CA}(pk_B)$ stays the same, unless the buyer contacts the CA before each transaction to acquire a new certificate, which is impractical for real-life applications.

3. Attacks on the Protocol of Ibrahim et al.

The players involved in the protocol (Ibrahim et al., 2007), are the seller *A*, the buyer *B*, the certificate authority *CA*, and the arbitrator *J*. The protocol comprises two phases, namely the watermark generation and insertion protocol and the identification and arbitration protocol. The watermark generation and insertion protocol is reviewed in Fig. 4.


B
A
WCA
ARG
$Cert_{CA}(A)$
N_1
verify certificate
N_2
$E_{sk_{CA}}(E_{pk_B}'(W))$
$W = D_{pk_B}(E_{sk_B}(W))$
$H'(E_{pk_B}'(W)) \overset{?}{=} H(E_{pk_B}(W))$
$X' = X \oplus V$
X''
$E_{sk_B}(E_{pk_B}(X'')$
$E_{pk_B}(X'') = E_{pk_B}(X) \oplus E_{pk_B}(W)$

Note: $N_1 = \{E_{pk_B}(W), E_{sk_B}(H(ARG)), E_{pk_{CA}}(E_{sk_B}(W)), E_{sk_B}(H(H(ARG)) + H(W)), Cert_C A(B)\}$
$N_2 = \{E_{pk_{CA}}(E_{sk_B}(W)), Cert_C A(B)\}$

Fig. 4. The watermark generation and insertion protocol in Ibrahim et al.'s protocol (Ibrahim et al., 2007).

3.1 Attack on the Seller's Security

In the protocol, Bob generates his secret watermark W, and W is approved by the *CA*. The watermarked content is $X'' = X \oplus V \oplus W$, V is Alice's watermark. Since Bob knows W, it is possible for Bob to remove his watermark W from the watermarked content X''. Hence, the protocol fails to provide non-repudiation and traitor traceability.
Ibrahim et al. assume that it is impossible for Bob to remove W from X'', because Bob doesn't have access of the original content X nor the watermark embedding algorithm. Unfortunately, the assumption is unrealistic, and it can be combated by employing a blind watermarking scheme (Kutter & Petitcolas, 1999), (Eggers et al., 2000), where the original content is not required to remove the watermark. On the other hand, there is no technical enforcement to ensure that Bob can't get the knowledge of the watermarking algorithm employed in the protocol. In fact, according to Kerckhoffs' principle in cryptography, "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge." "The system must not require secrecy and can be stolen by the enemy without causing trouble" (Kerckhoffs, 1883). Therefore, the attack is effective and non-repudiation fails. The protocol fails to provide both the basic requirement of traitor traceability and the seller's security.

3.2 Failure for Probabilistic Cryptosystems

In the watermark generation and insertion protocol, after Alice receives the encrypted value $E_{SK_{CA}}(E_{PK_B}'(W))$ from the CA, Alice decrypts $E_{SK_{CA}}(E_{PK_B}'(W))$ using the CA's public key pk_{CA}, and then computes the message digest of the result $E_{PK_B}'(W)$, as $H'(E_{PK_B}'(W))$. Next, Alice computes the message digest of $E_{PK_B}(W)$ sent earlier by Bob, as $H(E_{PK_B}(W))$. Alice compares $H'(E_{PK_B}'(W))$ and $H(E_{PK_B}(W))$. The protocol continues if they equal, else the protocol halts. Therefore, the protocol fails with probabilistic cryptosystems, because $E_{PK_B}{}'(W)$ computed by the CA and $E_{PK_B}(W)$ provided by Bob would be different. Then Alice would consider the protocol failed, and halt the protocol. Following the same reasoning of the similar attack on the Lei et al.'s protocol, we can prove that the protocol fails to employ privacy homomorphic probabilistic cryptosystems.

3.3 Failure for Anonymity and Unlinkability

The protocol doesn't specify the registration subprotocol. In each transaction with Alice, Bob provides Alice his PKI certificate $Cert_{CA}(B)$ issued by a trustworthy CA. Since $Cert_{CA}(B)$ is not an anonymous certificate, Alice can identify Bob. Therefore, Bob's anonymity is not preserved whatsoever. It is clear that the protocol fails to provide anonymity and unlinkability for the buyer.

4. Cryptographic Primitives

4.1 Privacy Homomorphism

A privacy homomorphism refers to a cryptosystem *E* which is homomorphic with respect to some binary operators $\circ_M$ in the plaintext space *M* and $\circ_C$ in the ciphertext space *C*, such that

$$\forall m_1, m_2 \in M : E(m_1 \circ_M m_2) = E(m_1) \circ_C E(m_2)$$

Homomorphic cryptosystems can be classified as two groups, namely those security relies on the *"decisional composite residuosity assumption" (DCRA)*, and those of the *ElGamal* class based on *"decisional Diffie-Hellman assumption" (DDH)*. The strongest security level a privacy homomorphism can reach is *IND-CPA*, instead of *IND-CCA2*. The state of the art of privacy homomorphic cryptosystems is presented in (Fontaine & Galand, 2007). For instance, the deterministic *RSA cryptosystem* (Rivest et al., 1978) and the *ElGamal cryptosystem (*ElGamal, 1985) are multiplicative privacy homomorphism. In contrast to deterministic *RSA*, *ElGamal* is *IND-CPA*. The *Goldwasser-Micali cryptosystem* (Goldwasser & Micali, 1982), the *Paillier cryptosystem* (Paillier, 1999), and *Paillier's* generalization the *Damgård-Jurik cryptosystem* (Damgåard & Jurik, 2001) are additive privacy homomorphism.

4.2 Group Signature

Group signatures (Chaum & van Heyst, 1991), (Camenisch & Stadler, 1997) enable group members, each with its own private signature key to produce signatures on behalf of the group. Group signature schemes can either be for static groups, where the identities of group members are fixed in the group setup phase; or for dynamic groups, which allow to update group members with time. Dynamic schemes have the advantage that instead of assigning a high level of trust to a single group manager, the group manager is separated as an issuer, to issue private signature keys to the group members, and an opener, to open signatures. This provides more security with a lower level of trust. The security properties of static and dynamic group signature schemes are formalized in (Bellare et al., 2003, 2005) as follows:

1) **Anonymity** allows group members to create signatures anonymously, such that it is hard for an adversary, not in possession of the group manager's opening key to recover the identity of the signer.
2) **Traceability** permits the signer's anonymity to be revoked by the group manager in case of misuse, and ensures that no colluded group members can create unverifiable signatures, or signatures that can't be traced back to some member of the coalition.
3) **Non-frameability** requires that no adversary can produce a signature in the name of a user unless the latter indeed produced it.

4.3 Verifiable Encryption

Verifiable encryption schemes enable the encrypter to ensure that the plaintext satisfies certain application-dependent properties without compromising secrecy. It can be employed in numerous applications including escrow schemes (Young & Yung, 1998), (Poupard & Stern, 2000), group signature and identity escrow schemes (Ateniese et al., 2000), (Kilian & Petrank, 1998), and digital payment with revocable anonymity (Frankel et al., 1996), (Camenisch et al., 1996). Specific schemes are proposed in (Camenisch & Shoup, 2003) for both discrete-log based and factoring based schemes. In our proposed scheme, verifiable encryption is used for key escrow, such that the buyer can prove to the seller that the plaintext is valid without revealing any private information, and hence the buyer's privacy is preserved.

5. Model of Anonymous Buyer-Seller Watermarking Protocols

Let $X_0 \in \{0,1\}^*$ be the cover data, X be the set of all watermarked copies of X_0, and k be a security parameter as a common input for all algorithms. An anonymous buyer-seller watermarking protocol involves four parties: a seller Alice A that is the copyright holder, a buyer Bob B, a certificate authority CA that functions as a group manager, and a judge J that adjudicates lawsuits against the infringement of copyrights. The protocol consists of the following three subprotocols.

1. *Reg*: the registration protocol consists of an algorithm *Set-CA* and a protocol *Reg-CAB*. *Set-CA* is a probabilistic key setup algorithm to generate group manager's public key gpk and private keys (ok, ik) of the *CA*. *Reg-CAB* is a probabilistic two-party protocol (*Reg-CA, Reg-B*) between the *CA* and the buyer *B*. Their common input are *B*'s identity B and gpk. The *CA*'s secret input is (ok, ik). *B*'s output is his private group signature key gsk_B. The *CA* stores *B*'s group certificate $Cert_B$ and the buyer's identity B in a registration table as $reg[B]$.
2. *WK*: a two-party protocol (*WK-A,WK-B*) between the seller *A* and the buyer *B*. Their common input is gpk. *A*'s secret input are the cover data X_0 and a transaction number ϕ, and *A*'s output is a transaction record in $Table_A$. *B*'s secret input is *B*'s group signature key gsk_B, and *B*'s output is a watermarked copy $X' \in \mathrm{X}$.

3. *Arb*: a three-party protocol (*Arb-A, Arb-J, Arb-CA*) among *A*, *J*, and the *CA*. *A* and *J* 's input are a pirated copy $Y \in \mathrm{X}$, the cover data X_0, and a record in $Table_A$. The *CA*'s input are (gpk, ok, ik) and the list of buyer's certificates in the registration table reg. The *CA*'s output is the identity id of a guilty buyer with a proof τ. *J* verifies τ and provides *A* the output as id or an empty string ε in case of failure.

Note that the registration protocol *Reg* is required to be performed once in the setup-phase by the *CA* for each new buyer. The watermarking protocol WK should be executed multiple times for multiple transactions between the buyer and the seller. The arbitration protocol *Arb* is executed for dispute resolution.

6. Proposed Protocol

The proposed buyer-seller watermarking protocol involves four players: the seller Alice, the buyer Bob, the trustworthy *CA* that functions as a group manager, and an arbitrator. The protocol consists of three phases. First, Bob registers at the *CA* before the purchase in the registration protocol. Second, Bob only needs to contact Alice during transactions in the watermark generation and insertion protocol. Third, in case Alice found a pirated copy, the identification and arbitration protocol enables her to identify the copyright violator, with the help of the judge and the *CA*.

The following assumptions should hold in the protocol, otherwise, the security properties cannot be guaranteed. We assume a public key infrastructure *PKI* is well deployed, such that each entity has a *PKI* certificate issued by the *CA*. The *CA* is assumed to be trustworthy, because the *PKI* should be secure. For consistency, we assume that the digital content is a still image, although the protocol can be applied to other multimedia formats such as audio or video. Note that the security of the protocol depends on the security of the underlying watermarking and cryptographic building blocks. Hence, the watermarking scheme employed should be collusion resistant. In particular, nobody is able to detect and delete the embedded watermark from a content without knowing the watermark. Our scheme employs the privacy homomorphism of the Paillier cryptosystem (Paillier, 1999) and Cox et al.'s robust collusion resistant watermarking scheme (Cox et al., 1997). Camenisch et al.'s verifiable encryption scheme (Camenisch & Shoup, 2003) is employed for the key escrow of the buyer's private key at the *CA*, such that the buyer can prove to the seller that the plaintext is valid without revealing the secrecy. We choose to employ the dynamic group signature proposed by Bellare et al. (Bellare et al., 2005) as an example.

6.1 Registration Protocol

The registration protocol, performed between the buyer Bob and the *CA*, is depicted in Fig. **5**.

1) In the group key generation phase, the CA generates a tuple $(gpk, gmsk)$. The group public key gpk consists of a public encryption key pk_e, a certificate verification key pk_s, and some security parameters. The manager secret key $gmsk$ is the decryption key sk_e corresponding to pk_e. The certificate creation key is sk_s, corresponding to pk_s.

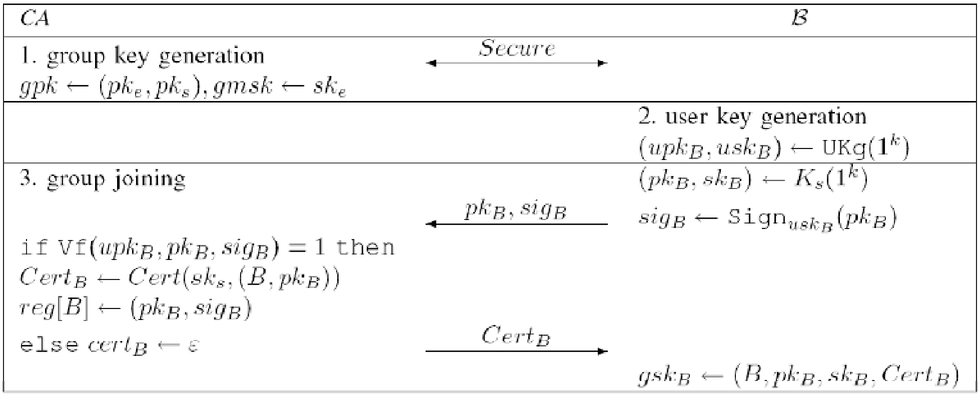
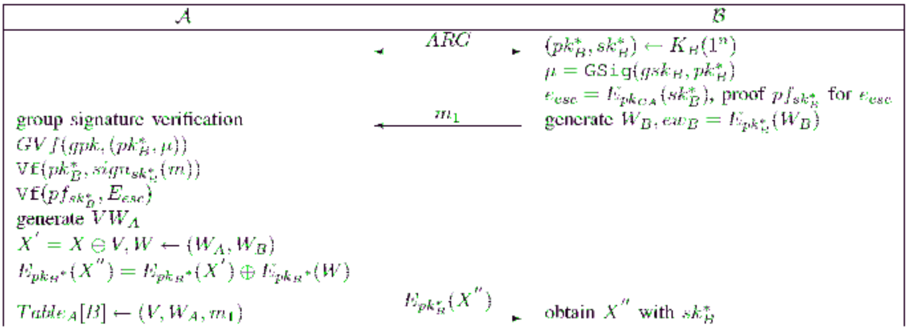
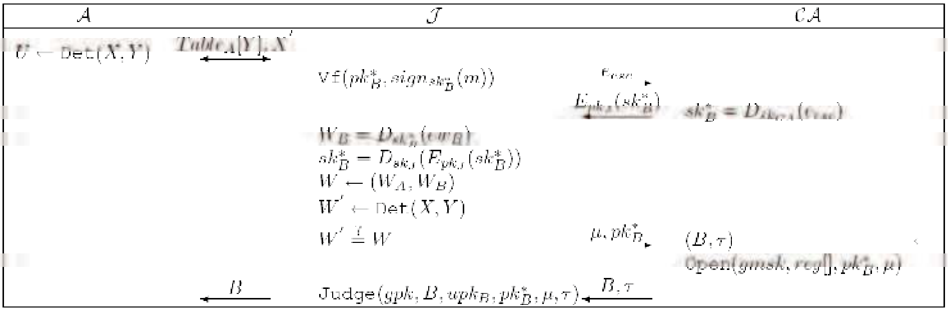

CA
$\mathcal{B}$
1. group key generation
$gpk \leftarrow (pk_e, pk_s), gmsk \leftarrow sk_e$
Secure
2. user key generation
$(upk_B, usk_B) \leftarrow \mathtt{UKg}(1^k)$
3. group joining
$(pk_B, sk_B) \leftarrow K_s(1^k)$
pk_B, sig_B
$sig_B \leftarrow \mathtt{Sign}_{usk_B}(pk_B)$
$\mathtt{if\ Vf}(upk_B, pk_B, sig_B) = 1\ \mathtt{then}$
$Cert_B \leftarrow Cert(sk_s, (B, pk_B))$
$reg[B] \leftarrow (pk_B, sig_B)$
$\mathtt{else}\ cert_B \leftarrow \varepsilon$
$Cert_B$
$gsk_B \leftarrow (B, pk_B, sk_B, Cert_B)$

Fig. 5. The registration protocol performed between the buyer *B* and the *CA*.


$\mathcal{A}$
$\mathcal{B}$
ARC
$(pk_B^*, sk_B^*) \leftarrow K_B(1^n)$
$\mu = \mathtt{GSig}(gsk_B, pk_B^*)$
$e_{esc} = E_{pk_{CA}}(sk_B^*)$, proof $pf_{sk_B^*}$ for e_{esc}
group signature verification
m_1
generate W_B, $ew_B = E_{pk_B^*}(W_B)$
$GVf(gpk, (pk_B^*, \mu))$
$\mathtt{Vf}(pk_B^*, sign_{sk_B^*}(m))$
$\mathtt{Vf}(pf_{sk_B^*}, E_{esc})$
generate VW_A
$X' = X \ominus V, W \leftarrow (W_A, W_B)$
$E_{pk_B*}(X'') = E_{pk_B*}(X') \oplus E_{pk_B*}(W)$
$Table_A[B] \leftarrow (V, W_A, m_1)$
$E_{pk_B^*}(X'')$
obtain X'' with sk_B^*

Note: $m = \{pk_B^*, \mu, ARG, cw_B, pf_{sk_B^*}, c_{esc}\}, m_1 = \{m, sign_{sk_B^*}(m)\}$

Fig. 6. The watermark generation and embedding protocol performed between the seller *A* and the buyer *B*.


$\mathcal{A}$
$\mathcal{J}$
CA
$U \leftarrow \mathtt{Det}(X, Y)$
$Table_A[Y], X'$
$\mathtt{Vf}(pk_B^*, sign_{sk_B^*}(m))$
e_{esc}
$E_{pk_J}(sk_B^*)$
$sk_B^* = D_{sk_{CA}}(e_{esc})$
$W_B = D_{sk_B^*}(ew_B)$
$sk_B^* = D_{sk_J}(E_{pk_J}(sk_B^*))$
$W \leftarrow (W_A, W_B)$
$W' \leftarrow \mathtt{Det}(X, Y)$
$W' \overset{?}{=} W$
μ, pk_B^*
(B, τ)
$\mathtt{Open}(gmsk, reg[], pk_B^*, \mu)$
B
$\mathtt{Judge}(gpk, B, upk_B, pk_B^*, \mu, \tau)$
B, τ

Note: $\mu = \mathtt{GSig}(gsk_B, pk_B^*)$

Fig. 7. The copyright violator identification and arbitration protocol performed among the seller *A*, the judge *J*, and the *CA*.

2) To join the group, Bob generates a public and private key pair (upk_B, usk_B), and a signing and verifiction key pair (pk_B, sk_B). Bob sends to the CA his signature sig_B on pk_B with the key usk_B.
3) After the signature is verified, the CA issues the group membership to Bob by issuing a certificate of pk_B and Bob's identity B. Then the CA stores Bob's public key and Bob's signature (pk_B, sig_B) in the registration table reg.
4) Bob receives the certificate $Cert_B$ and derives his group signature key gsk_B from the tuple $(B, pk_B, sk_{B,} Cert_B)$.

6.2 Watermark Generation and Embedding Protocol

The watermark generation and insertion protocol, as depicted in Fig. **6**, can be executed multiple times for multiple transactions between the seller Alice and the buyer Bob. In order to uniquely bind a particular transaction to the item of interest X, Alice and Bob first negotiate a purchase agreement *ARG* on transaction specifications.

1) Bob generates a one-time anonymous public and private key pair (pk_{B^*}, sk_{B^*}), and signs the public key pk_{B^*} with his group signature key gsk_B. For key escrow, Bob encrypts the secret key sk_{B^*} with the *CA*'s encryption key pk_{CA}, and computes a verifiable proof $pf_{sk_{B^*}}$ for the escrow cipher e_{esc}, in order to assure Alice that the encrypted message is valid without compromising sk_{B^*}. For each transaction, Bob generates a unique watermark W_B, in compliance with the features of the content X for robustness, and transfers the encrypted watermark and all the other public information m to Alice.
2) Alice verifies Bob's signature and verifiable proof, as well as Bob's group signature on his anonymous public key. Similarly, Alice generates two unique watermarks V and W_A for each transaction. The first round of watermark insertion is performed as:

$$X' = X \oplus V \qquad (1)$$

Note that the sole purpose of V, is to be used as a key to search the sales record in case Alice finds a pirated copy of her products (Memon & Wong, 2001), (Lei et al., 2004).

3) Alice computes the composite watermark W in the encrypted domain by employing privacy homomorphism:

$$E_{pk_{B^*}}(W) = E_{pk_{B^*}}(W_A) \times E_{pk_{B^*}}(W_B) = E_{pk_{B^*}}(W_A + W_B) \qquad (2)$$

4) Alice performs the second round of watermark insertion:

$$E_{pk_{B^*}}(X'') = E_{pk_{B^*}}(X') \otimes E_{pk_{B^*}}(W) = E_{pk_{B^*}}(X' \oplus W) \qquad (3)$$

Where $\oplus$ denotes the watermark insertion operation in the message space, and $\otimes$ denotes the corresponding operation in the encrypted domain. Note that the computation is possible because we assume the encryption $E_{pk_{B^*}}(\bullet)$ is privacy homomorphic with respect to $\oplus$. Alice stores W_A, V, W_A and Bob's information in $Table_A$, and delivers the encrypted content X'' to Bob.

5) After decryption $D_{sk_{B^*}}(E_{pk_{B^*}}(W))$, Bob obtains the watermarked content X'' from Alice.

6.3 Identification and Arbitration Protocol

The identification and arbitration protocol is executed among the seller Alice *A*, an judge *J*, and the *CA*, as depicted in Fig. **7**.

1) In case Alice finds a pirated copy Y of X, she extracts the watermark U from Y, and searches the sales record by correlating U with every V in $Table_A$. Then she provides all relevant information together with the intermediate watermarked content X' to *J*.
2) If the signature provided by Alice is verified, *J* accepts the case and forwards the seller's key escrow cipher to the *CA* to recover the private key of the buyer.
3) The *CA* decrypts the cipher, recovers the key, and returns the encrypted value $E_{pk_J}(sk_{B^*})$ to *J*.
4) After *J* obtains the buyer's key by decryption $D_{sk_J}(E_{pk_J}(sk_{B^*}))$, he further obtains the buyer's secret watermark $W = D_{sk_{B^*}}(ew)$. Then *J* compares the extracted watermark from X' and Y provided by Alice, with the one that is derived from the recovered watermarks (W_A, W_B) from the buyer and the seller. If they match with a high correlation, the suspected buyer is proven to be guilty. Otherwise, the buyer is innocent. Note that until now, the buyer's identity is unexposed.
5) To recover the buyer's identity, *J* orders the *CA* to open the buyer's group signature, with the group manager's secret key $gmsk$.
6) Upon receiving the recovered identity B and a claim proof τ, *J* verifies the *CA*'s claim.
7) If verified, *J* closes the case and announces that the buyer with identity B is guilty.

7. Security Analysis

In this section, we analyze the security properties of the proposed scheme. The soundness and completeness of the protocol rely on the security and robustness of the underlying cryptographic and watermarking primitives.

1. **Non-framing (buyer's security).** Alice only knows the encrypted content $E_{pk_{B^*}}(X'')$, but she doesn't know the watermarked content delivered to Bob X'', neither does she know Bob's secret watermark W_B. Therefore, Alice cannot accuse Bob by distributing replicas of X'' herself. That is, the customer's rights problem is solved. On the other hand, Bob is able to generate his watermark and there is no third party involved in the watermark generation phase. Therefore, Alice cannot recover Bob's watermark via conspiracy attacks. Further, the unbinding problem is solved because Alice can't forge Bob's signature that explicitly binds $E_{pk_{B^*}}(W_B)$, pk_{B^*} to *ARG*, which in turn binds to a particular transaction of X. In this regard, it is infeasible for Alice to transplant Bob's watermark to another content to fabricate piracy.
2. **Non repudiation (seller's security).** Bob only knows his watermark W_B, but not the composite watermark W generated from the watermarks of Alice and Bob. On the other hand, there is no third party involved in the protocol, so Bob cannot obtain any secret information via conspiracy attacks. Therefore, it is infeasible for Bob to remove his watermark W_B from the watermarked content X'', neither can he claim that the copy was created by Alice or a security breach of Alice's system. Because only Bob knows sk_{B^*} and W_B, no one can forge Bob's copy.
3. **Traceability.** The protocol provides a mechanism that, once a pirated copy is found, Alice can provide the judge with sufficient information related to the particular transaction. The judge is able to identify the privacy violator with the help of the *CA*, due to the traceability property of the underlying group signature scheme.
4. **Dispute resolution.** When a dispute occurs, even without Bob providing his secret key sk_{B^*} or his secret watermark W_B, the judge can still recover sk_{B^*} from the *CA*, with the help of the key escrow cipher e_{esc} and the proof $pf_{sk_{B^*}}$. Once sk_{B^*} is recovered, the judge knows W and can further arbitrate if the suspected Bob is guilty or not.
5. **Conspiracy resistance.** Bob is able to generate his own wat ermark and there is no third party involved in the watermark generation and insertion protocol. It enables the scheme to be conspiracy resistant.
6. **Revocable anonymity.** The essential protection of the buyer's privacy is by taking advantage of the group signature scheme and the one-time anonymous public and private key pair. Before the purchase, Bob requests a group signature key gsk_B from the trustworthy *CA*, which in turn takes responsibility to bind Bob's signature key to Bob's identity. In each transaction with Alice, Bob uses an anonymous public and private key pair (pk_{B^*}, sk_{B^*}) and generates a signature μ to pk_{B^*} with the group signature key gsk_B. By the anonymity property introduced by the underlying group signature scheme (Bellare et al., 2005), it is computationally infeasible for an adversary, not in possession of the opener's opening key ok, to recover the identity of the signer from its signature. Note that the *CA* is trustworthy, otherwise the group signature

scheme would not be secure. In case of disputes, Alice collects the transaction information and sends μ , pk_{B^*} , *ARG*, ew_B , $pf_{sk_{B^*}}$ and e_{esc} to the judge for arbitration. The information can only prove someone with an anonymous key pk_{B^*} has bought the product X , but it doesn't disclose the identity of Bob. Only when Bob is adjudicated to be guilty, the judge can send a legal order for the *CA* to recover Bob's identity. Therefore, Bob's anonymity is not revoked by the *CA* only until he is adjudicated to be guilty.

7. **Unlinkability.** Unlinkability is provided in the proposed protocol because of the unlinkability property introduced by the underlying group signature and Bob's one-time key pair (pk_{B^*}, sk_{B^*}) . Given the list of sales information, no one can relate two transactions together as if they were from the same buyer.
8. **Mutual authentication.** Man-in-the-middle attacks on the protocol are infeasible. First, the *PKI* is well deployed to ensure mutual authentication between entities, as the basic requirement of a secure protocol. Second, all messages are transferred in a secure communication channel, such that eavesdropping is infeasible.

8. Conclusion

In this paper, we present attacks on two buyer-seller watermarking protocols proposed by Lei et al. (Lei et al., 2004) and Ibrahim et al. (Ibrahim et al., 2007), and prove that neither of these protocols is able to provide security for the buyer or the seller as claimed. Further, we point out that both protocols are not able to work properly when employing homomorphic probabilistic cryptosystems. We also address the anonymity and unlinkability problem in these protocols. We propose an improved protocol, which is secure and fair for both the seller and the buyer. Our protocol employs privacy homomorphic cryptosystems and group signature schemes, in order to protect the secrecy of the buyer and the seller, and to preserve revocable anonymity of the buyer. Comparing with early work, our scheme is able to provide all the required security properties of a secure and anonymous buyer-seller watermarking protocol, namely non-framing, non-repudiation, traceability, mutual authentication, dispute resolution, anonymity and unlinkability.

9. Acknowledgment

The work reported here has been funded in part by the European Community's Sixth Framework Programme under grant number 034238, SPEED project - Signal Processing in the Encrypted Domain. The work reported reflects only the authors' views; the European Community is not liable for any use that may be made of the information contained herein. This work was also supported in part by the Concerted Research Action (GOA) AMBioRICS 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy).

10. References

Ateniese, G., Camenisch, J., Joye, M. & Tsudik, G. (2000), A practical and provably secure coalition-resistant group signature scheme, LNCS 1880, pp. 255-270.

Bellare, M., Micciancio, D. & Warinschi, B. (2003), Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions, in 'Topics in Cryptology - Eurocrypt 2003', LNCS 2656, Springer-Verlag, pp. 614-629.

Bellare, M., Shi, H. & Zhang, C. (2005), Foundations of group signatures: the case of dynamic groups, in 'Topics in Cryptology - CT-RSA 2005', LNCS 3376, Springer-Verlag, pp. 136-153.

Biehl, I. & Meyer, B. (1997), Protocols for collusion-secure asymmetric fingerprinting, in 'Proc. 14th STACS', LNCS 1200, Springer-Verlag, pp. 213-222.

Blakley, G. R., Meadows, C. & Prudy, G. B. (1986), Fingerprinting long forgiving messages, in 'Advances in Cryptology CRYPTO 85', LNCS 218, Springer-Verlag, pp. 180-189.

Boneh, D. & Shaw, J. (1995), Collusion-secure fingerprinting for digital data, LNCS 963, pp. 452-465.

Camenisch, J. (2000), Efficient anonymous fingerprinting with group signatures, in 'ASIACRYPT', LNCS 1976, Springer-Verlag, pp. 415-428.

Camenisch, J. L. & Stadler, M. A. (1997), Efficient group signature schemes for large groups, in 'Adv. in Cryptology - CRYPTO97', LNCS 1294, pp. 410-424.

Camenisch, J., Maurer, U. M. & Stadler, M. (1996), Digital payment systems with passive anonymity-revoking trustees, in 'ESORICS', pp. 33-43.

Camenisch, J. & Shoup, V. (2003), Practical verifiable encryption and decryption of discrete logarithms, in 'Adv. in Cryptology - Crypto 2003', LNCS 2729, Springer-Verlag, pp. 126-144.

Chaum, D. & van Heyst, E. (1991), Group signatures, in `Advances in Cryptology - EUROCRYPT 1991', LNCS 547, pp. 257-265.

Cox, I., Kilian, J., Leighton, T. & Shamoon, T. (1997), `Secure spread spectrum watermarking for multimedia', IEEE Transactions on Image Processing 6(12), 1673-1687.

Cox, I., Miller, M., Bloom, J. & Miller, M. (2001), Digital Watermarking: Principles & Practice, The Morgan Kaufmann Series in Multimedia Information and Systems, Morgan Kaufmann.

Damgård, I. & Jurik, M. (2001), A generalisation, a simplification and some applications of Paillier's probabilistic public-key system, in '4th International Workshop on Practice and Theory in Public-Key Cryptography', LNCS 1992, Springer-Verlag, pp. 119-136.

Deng, M. & Preneel, B. (2008), On secure and anonymous buyer-seller watermarking protocol, in 'International Conference on Internet and Web Applications and Services', IEEE, pp. 524-529.

Eggers, J., Su, J. & Girod, B. (2000), A blind watermarking scheme based on structured codebooks, in 'Secure Images and Image Authentication, IEE Colloq.', pp. 4/1-4/6.

ElGamal, T. (1985), A public key cryptosystem and a signature scheme based on discrete logarithms, in 'Adv. in Cryptology - CRYPTO84', LNCS 196, pp. 10-18.

Fontaine, C. & Galand, F. (2007), `A survey of homomorphic encryption for non-specialists', EURASIP Journal on Information Security. http://www.hindawi.com/RecentlyAcceptedArticlePDF.aspx?journal=IS&number=13801.

Frankel, Y., Tsiounis, Y. & Yung, M. (1996), Indirect disclosure proof: Achieving. efficient fair on-line e-cash, in 'Advances in Cryptology - Asiacrypt 1996', LNCS 1163, pp. 286-300.

Goi, B.-M., Phan, R. C.-W., Yang, Y., Bao, F., Deng, R. H. & Siddiqi, M. U. (2004), Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity, in 'Applied Cryptography and Network Security', LNCS 2587, pp. 369-382.

Goldwasser, S. & Micali, S. (1982), Probabilistic encryption and how to play mental poker hiding all partial information, in 'Proceedings of the 14th Annual ACM Symposium on the Theory of Computing', pp. 365-377.

Hartung, F. & Kutter, M. (1999), Multimedia watermarking techniques, Vol. 87, pp. 1079-1107. Invited paper.

Ibrahim, I. M., El-Din, S. H. N. & Hegazy, A. F. A. (2007), An effective and secure buyer-seller watermarking protocol, in 'Third International Symposium on Information Assurance and Security, 2007. IAS 2007', pp. 21-28.

Jae-Gwi Choi, Kouichi Sakurai, J.-H. P. (2003), Does it need trusted third party? design of buyer-seller watermarking protocol without trusted third party, in 'Applied Cryptography and Network Security', LNCS 2846, pp. 265-279.

Ju, H.-S., Kim, H.-J., Lee, D.-H. & Lim, J.-I. (2002), `An anonymous buyer-seller watermarking protocol with anonymity control', Information Security and Cryptology – ICISC, pp. 421-432.

Kerckhoffs, A. (1883), `La cryptographie militaire', Journal des sciences militaires IX, 5-83.

Kilian, J. & Petrank, E. (1998), Identity escrow, LNCS 1462, pp. 169-185.

Kutter, M. & Petitcolas, F. A. P. (1999), A fair benchmark for image watermarking systems, in 'SPIE Security and Watermarking of Multimedia Contents', Vol. 3657, pp. 226-239.

Lei, C.-L., Yu, P.-L., Tsai, P.-L. & Chan, M.-H. (2004), 'An efficient and anonymous buyer-seller watermarking protocol', IEEE Transactions on Image Processing 13(12), 1618-1626.

Liu, K., Trappe, W., Wang, Z., Wu, M. & Zhao, H. (2005), Multimedia Fingerprinting Forensics for Traitor Tracing, EURASIP Book Series on Signal Processing and Communications, Hindawi Publishing Co.

Memon, N. D. & Wong, P. W. (2001), 'A buyer-seller watermarking protocol', IEEE Transactions on Image Processing 10(4), 643-649.

Paillier, P. (1999), Public-key cryptosystems based on composite degree residuosity classes, in 'Advances in Cryptology EUROCRYPT 1999', LNCS 1592, Springer-Verlag, pp. 223-238.

Pfitzmann, B. & Sadeghi, A. R. (1999), Coin-based anonymous fingerprinting, in 'Advances in Cryptology EUROCRYPT 1999', LNCS 1592, Springer-Verlag, pp. 150-164.

Pfitzmann, B. & Sadeghi, A. R. (2000), Anonymous fingerprinting with direct non-repudiation, in 'Advances in Cryptology ASIACRYPT 2000', LNCS 1976, Springer-Verlag, pp. 401-414.

Pfitzmann, B. & Waidner, M. (1997), Anonymous fingerprinting, in 'Advances in Cryptology EUROCRYPT 1997', pp. 88-102.

Pfitzmann, B. & Schunter, M. (1996), Asymmetric fingerprinting, in 'Advances in Cryptology EUROCRYPT 1996', LNCS 1070, Springer-Verlag, pp. 84-95.

Poupard, G. & Stern, J. (2000), Fair encryption of RSA keys, in 'Adv. in Cryptology – EUROCRYPT 2000', LNCS 1807, pp. 172-190.

Qiao, L. & Nahrstedt, K. (1998), 'Watermarking schemes and protocols for protecting rightful ownership and customer's rights', Journal of Visual Communication and Image Representation 9(3), 194 - 210.

Rivest, R. L., Shamir, A. & Adelman, L. M. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', Communication of the ACM 21(2), 120-126.

Shao, M.-H. (2007), A privacy-preserving buyer-seller watermarking protocol with semi-trust third party, in 'Trust, Privacy and Security in Digital Business', LNCS 4657, pp. 44-53.

Trappe, W., Wu, M., Wang, Z. J. & Liu, K. J. R. (2003), 'Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation', IEEE Transactions on Image Processing 51(4), 1069 - 1087.

Wang, Z. J., Wu, M., Zhao, H. V., Trappe, W. & Liu, K. J. R. (2005), 'Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation', IEEE Transactions on Image Processing 14(6), 804 - 821.

Young, A. & Yung, M. (1998), Auto-recoverable auto-certifiable cryptosystems, in 'EUROCRYPT 1998', pp. 17-31.

Zhang, J., Kou, W. & Fan, K. (2006), Secure buyer-seller watermarking protocol, in 'IEE Proceedings Information Security', Vol. 153, pp. 15-18.

Mina Deng was born in Sept. 1981, Beijing, China. She received MSc. degree in electrical engineering from the Katholieke Universiteit Leuven, Belgium, in 2004.

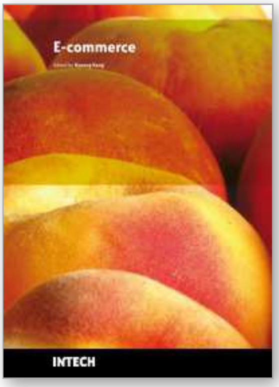
She is currently a PhD student at the Computer Security and Industrial Cryptography (COSIC) research lab, department of electrical engineering, Katholieke Universiteit Leuven, Belgium. She also works as a security and privacy researcher for the Interdisciplinary institute for BroadBand Technology (IBBT) Belgium. She has been involved in serval European research projects, such as "SPEED-Signal Processing in the Encrypted Domain" (2007-present), the European Networks of Excellence "FIDIS-Future of Identity in the Information Society" (2004-present) and "ECRYPT-European Network of Excellence for Cryptology" (2004-2008) by European Commission-Framework Program 6 (EC-FP6).

Ms Deng's research interests include cryptography, security and privacy, identity management, and electronic service applications, such as DRM, e-commerce, e-health, etc. She received "Outstanding Achievement Award for best student research paper", granted by the New Zealand State Services Commission in 2008, and the "Barco/VIK-Prize" as the Belgian Flemish best engineering thesis prize in 2003.

Bart Preneel received a Master's Degree in electrical engineering and the Doctorate in applied sciences (cryptology) from the Katholieke Universiteit Leuven (Belgium) in 1987 and 1993 respectively.

He is currently full professor at the Katholieke Universiteit Leuven. He was visiting professor at five universities in Europe and was a research fellow at the University of California at Berkeley. He has authored and co-authored more than 200 reviewed scientific publications and is inventor of two patents. His main research interests are cryptography and information security.

Prof. Preneel is president of the IACR (International Association for Cryptologic Research) and of L-SEC vzw. (Leuven Security Excellence Consortium), an association of 60 companies and research institutions in the area of e-security. He is a member of the Editorial Board of the Journal of Cryptology, the IEEE Transactions on Forensics and Information Security, and the International Journal of Information and Computer Security. He has participated to more than 20 research projects sponsored by the European Commission, for four of these as project manager. He has been program chair of ten international conferences (including Eurocrypt 2000, SAC 2005 and ISC 2006) and he has been invited speaker at more than 30 conferences. In 2003, he has received the European Information Security Award in the area of academic research, and he received an honorary Certified Information Security Manager (CISM) designation by the Information Systems Audit and Control Association (ISACA).



E-commerce
Edited by Kyeong Kang

ISBN 978-953-7619-98-5
Hard cover, 284 pages
Publisher InTech
Published online 01, February, 2010
Published in print edition February, 2010

E-commerce provides immense capability for connectivity through buying and selling activities all over the world. During the last two decades new concepts of business have evolved due to popularity of the Internet, providing new business opportunities for commercial organisations and they are being further influenced by user activities of newer applications of the Internet. Business transactions are made possible through a combination of secure data processing, networking technologies and interactivity functions. Business models are also subjected to continuous external forces of technological evolution, innovative solutions derived through competition, creation of legal boundaries through legislation and social change. The main purpose of this book is to provide the reader with a familiarity of the web based e- commerce environment and position them to deal confidently with a competitive global business environment. The book contains a numbers of case studies providing the reader with different perspectives in interface design, technology usage, quality measurement and performance aspects of developing web-based e-commerce.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821