Comments on a Buyer-Seller Watermarking Protocol for Large Scale Networks

Shuhua Wu[1,2] and Qiong Pu[2,3]
(Corresponding author: Shuhua Wu)
[1]Information Engineering University, Zhengzhou, China (Email: wushuhua726@sina.com)
[2]State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing, China
[3]CIMS Research Center, Tongji University, Shanghai, China
(Received April 9, 2010; revised and accepted May 22, 2010)

Abstract

Buyer-seller watermarking are protocols guaranteeing the buyer prevents false infringement accusations and the seller protects the watermark secrets from the buyer. Most recently, Chang et al. proposed an efficient and fair buyer-seller watermarking scheme for large scale networks quite recently. In this correspondence, we first shows its three weaknesses: the buyer can easily remove the watermark, the buyer can easily destroy the forensic information and the adversary can possibly learn about personal privacy of some honest customers. Thereafter, we suggest some countermeasures to defeat our described attacks while its merits are left unchanged.

Keywords: Buyer-seller protocol, secure watermark embedding, watermarking.

1 Introduction

In recent years, there is a rapid growth in the availability of multimedia content in digital form since it is much easier to adopt and distribute. However, content in digital form can be easily duplicated or copied. Therefore, it is quite important to develop copy protection or copy deterrence mechanisms. Digital watermarking is considered to be a feasible approach in preventing digital content from being illegally copied and distributed over the Internet [3, 4, 9]. Traditionally, the watermark is inserted solely by the seller. Therefore, both the buyer and the seller can access the watermarked content. When an unauthorized copy of the content is found, the forensic information can not exclusively identify the party who actually leaked the content. Thus the buyer-seller watermarking protocols are adopted to solve the aforesaid problem. In such protocols, the seller and the buyer jointly embed a watermark, which ensures that neither the watermark nor the watermarked content are available to the seller while the buyer receives a uniquely watermarked version but has no access to the unmarked original [5]. Due to usefulness, several watermarking schemes (e.g. [7, 10]) have been proposed over the past several years.

Recently, Katzenbeisser et al. [5] proposed an efficient watermarking protocol using a secure watermark embedding algorithm [8]. However, as noted by Chang et al. [2], this protocol is still not practical enough due to high computational cost for buyers. They further argued that Katzenbeisser et al.'s assumption that all messages are exchanged over private and authenticated channels is too demanding in real-world environments [2]. To overcome the drawbacks of the aforementioned scheme, Chang et al. proposed an efficient and fair buyer-seller watermarking scheme for large scale networks quite recently [2]. In order to be suitable for heterogeneous network environments (for example, a buyer may utilize low-power mobile devices to purchase digital content through wireless networks), it transfers heavy-burden operations (such as public key cryptography) from the buyer to a powerful server. Chang et al. claimed that their scheme can well protect both the owners' copyright and the customers' right and undeniably trace unauthorized copies under the assumption that the core protocol runs over public communication channels. In this correspondence, we first demonstrate that the scheme fails to achieve the security goals as claimed. More specially, the buyer can easily remove the watermark and destroy the forensic information. On the other hand, the adversary can possibly learn about personal privacy of some honest customers. Thereafter, we suggests some countermeasures to defeat our described attacks while its merits are left unchanged.

2 Review of Lemma et al.'s Secure Watermark Embedding Approach

Like Katzenbeisser et al.'s scheme [5], Chang et al.'s watermarking protocol is also based on the secure watermark embedding algorithms proposed in [8]. We now recall the

secure watermark embedding algorithms. Here, we just follow the description in [5].

Let $\mathbf{c}$ be a piece of content, represented as a vector of quantized real numbers —either samples in the spatial/temporal domain or coefficients in a transform domain (e.g., DCT or wavelet coefficients). The representation of $\mathbf{c}$ eventually determines the watermark embedding domain. We denote by a vector $\mathbf{W}$ a watermark sequence that will be embeded in the content $\mathbf{c}$. The secure watermark embedding approach is based on partial encryption [6, 8], where perceptually significant parts of the content are distorted by a random vector $\mathbf{k}$. As in [5], the symbol "$\oplus/\ominus$" denotes an additive/subtractive operation on two vectors (or sequences). Then, $\mathbf{W} \oplus \mathbf{k}$, in which the watermark $\mathbf{W}$ is heavily distorted by a noise sequence $\mathbf{k}$, can be interpreted as an encrypted watermark. Analogously, $\mathbf{c} \ominus (\mathbf{W} \oplus \mathbf{k})$ is interpreted as an encrypted version of watermarked content $\mathbf{c} \ominus \mathbf{W}$. That is because, by choosing a suitable transform and a distribution of the sequence $\mathbf{k}$, the secure embedding scheme is believed to satisfy the following requirements.

- Removing the randomness $\mathbf{k}$ from either $\mathbf{W} \oplus \mathbf{k}$ or $\mathbf{c} \ominus (\mathbf{W} \oplus \mathbf{k})$ is of comparable hardness as breaking the watermark robustness (i.e., removing the watermark from $\mathbf{c} \ominus \mathbf{W}$).
- Given a content $\mathbf{c}$ and an encrypted watermarked content sequence $\mathbf{c} \ominus (\mathbf{W} \oplus \mathbf{k})$, obtaining a (high-quality) watermarked object $\mathbf{c} \ominus \mathbf{W}$, which has a very low correlation with $\mathbf{k}$, is of comparable hardness as watermark removal.

Hereby, encrypted watermark embedding is performed by subtracting the encrypted watermark from the content, which yields an encrypted version of watermarked content $\mathbf{c} \ominus \mathbf{W}$. The client is given, besides an encrypted watermarked content sequence $\mathbf{c} \ominus (\mathbf{W} \oplus \mathbf{k})$, the randomness $\mathbf{k}$, which allows him or her (by adding the received sequence to the encrypted watermarked content $\mathbf{c} \ominus (\mathbf{W} \oplus \mathbf{k})$) to remove the noise $\mathbf{k}$ and obtain the watermarked content $\mathbf{c} \ominus \mathbf{W}$. Therefore, during decryption, no access to the original content $\mathbf{c}$ and watermark $\mathbf{W}$ is required. More information is referred to [8] about the secure embedding approach which additively/subtractively distorts suitably selected transform coefficients with a noise sequence $\mathbf{k}$ (see [8] for a simple implementation that utilizes discrete cosine transform (DCT) coefficients).

In addition, it is possible to detect an encrypted watermark $\mathbf{W} \oplus \mathbf{k}$ in a potentially watermarked content $\mathbf{c}'$, albeit at a larger error rate. The watermark detector employed in [8] is a correlation detector that bases its decision on the correlation $\langle \mathbf{c}', \mathbf{W} \rangle$. Given a heavily distorted version $\mathbf{W} \oplus \mathbf{k}$ of the watermark, it is still possible to perform watermark detection in encrypted watermark $\mathbf{W} \oplus \mathbf{k}$ since the distortion is linear and the key sequence $\mathbf{k}$ is chosen at random : $\langle \mathbf{c}', \mathbf{W} \oplus \mathbf{k} \rangle = \langle \mathbf{c}', \mathbf{W} \rangle + \langle \mathbf{c}', \mathbf{k} \rangle \approx \langle \mathbf{c}', \mathbf{W} \rangle$. Thus, the correlation between the encrypted watermark $\mathbf{W} \oplus \mathbf{k}$ and the content $\mathbf{c}'$ gives a rough estimate of the correlation between $\mathbf{c}'$ and the embedded watermark $\mathbf{W}$. However, due to the introduction of additional noise in the watermark, the detection is not as accurate as the detection with $\mathbf{W}$; in particular, the false positives and false negatives probabilities of the detector will increase.

3 Review of Chang et al.'s Watermarking Scheme

This section describes the buyer-seller watermarking scheme proposed by Chang et al. [2], starting with some notations and definitions. Here, we just follow the description in [2].

The participants can be categorized into three entities: WCA entity is a unique and trusted watermark combination authority, buyer entity is the set $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$, and the seller entity is the set $\mathcal{S} = \{S_1, S_2, \cdots, S_n\}$. And $ID_{WCA}, ID_{B_i}, ID_{S_j}$ represent the identity of WCA, B_i, S_j respectively, where $1 \leq i \leq m$ and $1 \leq j \leq n$. Let $\mathcal{E}$ be an elliptic curve defined on a finite field F_p and G be a base point with the prime order q over $\mathcal{E}$. WCA is assumed to have a private/public key pair (x_{WCA}, Y_{WCA}), where $x_{WCA} \in Z_q^*$ (which is assumed under restricted protection) and $Y_{WCA} = x_{WCA} * G$. Thereafter, $h(\cdot)$ denotes a strong collision-free hash function and behaves like random oracles [1]; $E_X[m]$ denotes the symmetric encryption that the message m is encrypted using key X; $\Gamma_{WCA}[m]$ denotes the asymmetric encryption that the message m is encrypted using WCA's public key.

Chang et al.'s scheme involves three protocols: the registration protocol, the watermarking protocol (core protocol), and the identification and arbitration protocol. We will briefly recall them respectively in subsequent sections.

3.1 Registration Protocol

Before acquiring a copy of digital content $\mathbf{c}$, each buyer B_i needs to register with WCA to apply his own private delegation master key for future watermarking protocol. WCA only performs the following steps once time for each buyer B_i.

R1. For each B_i, WCA generates the master secret δ_{B_i}, which satisfies the following equation $h(x_{WCA} \| ID_{B_i}) = h(ID_{B_i} \| ID_{WCA}) \cdot \delta_{B_i} \mod q$, where $\|$ denotes a concatenation operation.

R2. WCA computes $\gamma_{B_i} = \delta_{B_i} * G = (x_{B_i}, y_{B_i})$; and $d = x_{B_i} \mod q$. Also, WCA computes $e_{B_i} = h(d \| ID_{WCA})$ and $s_{B_i} = \delta_{B_i} - x_{WCA} \cdot e_{B_i} \mod q$.

R3. WCA computes $h(\delta_{B_i} \| ID_{WCA})$ as the master delegation key for B_i and then delivers the computed result along with (e_{B_i}, s_{B_i}) which can be treated as the certificate, to B_i securely.

Eventually, WCA destroys all the computed results but only records the mapping relation of the buyer's ID_{B_i}

and $h(\delta_{B_i})$ for future arbitration between the buyer and the seller.

3.2 Watermarking Protocol

The primary goal is to provide a buyer to obtain a legal watermarked digital content from the seller and achieve mutual authentication among a buyer B_i, the seller S_j, and WCA. Chang et al. [2] stresses that all messages in the protocol are exchanged over public communication channels, which is quite different from those in Katzenbeisser et al.'s protocol [5]. The simplified description of the new protocol is given in Figure 1. A more detailed description of the protocol follows.

W1. Initially, B_i generates a seed value *seed* and a random element $N_B \in_R Z_q^*$, which are used to generate a part of valid watermark and to establish a common session key, respectively. Next, B_i utilizes $h(\delta_{B_i} \| ID_{WCA})$ to encrypt the generated results and the identity of S_j, i.e., $E_{h(\delta_{B_i} \| ID_{WCA})}[seed,\ ID_{S_j},\ N_B]$. Simultaneously, for the identifier of the requested content C_{ID}, B_i computes $h(h(seed \ \|N_B) \ \|C_{ID} \ \|ID_{S_j})$. B_i eventually sends to the seller S_j the items: $(e_{B_i},\ s_{B_i}) \ \|C_{ID} \ \|h(h(seed \ \|N_B) \ \|C_{ID} \ \|ID_{S_j}) \ \|E_{h(\delta_{B_i} \| ID_{WCA})} \ [seed,\ ID_{S_j},\ N_B]$.

W2. According to the received items, S_j generates a transaction number n. Also, S_j randomly generates a valid watermark w and computes the ciphertext $\Gamma_{WCA}[n,\ w,\ ts]$, where ts is the current timestamp. Finally, S_j sends to WCA the items: $(e_{B_i},\ s_{B_i}) \ \|E_{h(\delta_{B_i} \| ID_{WCA})} \ [seed,\ ID_{S_j},\ N_B] \ \|ID_{S_j} \ \|\Gamma_{WCA} \ [n,\ w,\ ts]$. It is worth noting that S_j temporarily preserves the item $h(h(seed \ \|N_B) \ \|C_{ID} \ \|ID_{S_j})$ for future authentication.

W3. Upon receiving the messages from S_j, WCA firstly utilizes the received (e_{B_i}, s_{B_i}) and the private key x_{WCA} to compute $\delta_{B_i} = s_{B_i} + x_{WCA} \cdot e_{B_i} \mod q$. Next, WCA computes $\gamma'_{B_i} = s_{B_i} * G + e_{B_i} * Y_{WCA} = (x'_{B_i}, y'_{B_i})$ and $d' = x'_{B_i} \mod q$. And then, WCA utilizes the computed d' and the identity ID_{WCA} to calculate $h(d' \| ID_{WCA})$. If the computed result $h(d' \| ID_{WCA})$ is equal to the received e_{B_i}, WCA authenticates the buyer B_i successfully. Simultaneously, WCA derives $h(\delta_{B_i} \| ID_{WCA})$ to decrypt $E_{h(\delta_{B_i} \| ID_{WCA})}[seed, ID_{S_j}, N_B]$. After that, WCA also utilizes the private key x_{WCA} to decrypt all messages in $\Gamma_{WCA}[n, w, ts]$. If the retrieved ID_{S_j} equals the transmitted identity from the seller and the decrypted timestamp ts is under the reasonable interval, WCA authenticates the seller S_j successfully. To provide digital right for the buyer B_i, WCA will generate a valid watermark sequence $\mathbf{w}'$ from the retrieved *seed* and the transaction number n. Next, WCA combines the final valid watermark $\mathbf{W} = \mathbf{w} \oplus \mathbf{w}'$ and randomly generates the key $\mathbf{k}$, which is used to distort the watermark $\mathbf{W}$, to compute $\mathbf{W}' = \mathbf{W} \oplus \mathbf{k}$.

To establish a fresh session key with B_i, WCA generates a random element $N_{WCA} \in_R Z_q^*$ to compute the common session key $h(N_B \| N_{WCA})$, which is used to encrypt the messages $\{n, N_B, N_{WCA}, \mathbf{k}\}$. To being authenticated by the seller, WCA needs to calculate $h(see \| N_B)$. Simultaneously, WCA derives the evident key $h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})$, which is used to encrypt the messages $\{seed, \mathbf{w}, \mathbf{k}, N_B, N_{WCA}\}$ for future identification and arbitration. Finally, WCA forwards to S_j the following items: $E_{h(N_B \| N_{WCA})}$ $[n,\ N_B,\ N_{WCA},\ \mathbf{k}]$ $\|N_{WCA}$ $\|h(see \ \|N_B)$ $\|\mathbf{W}'$ $\|E_{h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})}$ $[seed,\ \mathbf{w},\ \mathbf{k},\ N_B,\ N_{WCA}]$.

W4. When S_j receives these messages, he firstly retrieves $h(seed \| N_B)$ and then computes $h(h(seed \| N_B) \ \|C_{ID} \ \|ID_{S_j})$. If the computed result is equal to the previously received $h(h(seed \ \|N_B) \ \|C_{ID} \ \|ID_{S_j})$ from the buyer B_i in Step W2, then S_j authenticates both WCA and B_i. Simultaneously, S_j updates the transaction database by storing the tuple $(n,\ C_{ID},\ \mathbf{W}',$ $(e_{B_i},\ s_{B_i}),\ E_{h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})}$ $[seed,\ \mathbf{w},\ \mathbf{k},\ N_B,$ $N_{WCA}])$. After updating the transaction database, S_j embeds the distorted watermark $\mathbf{W}'$ into the requested content $\mathbf{c}$ by computing $\mathbf{c} \ominus \mathbf{W}'$. Finally, S_j transmits to B_i the items: $E_{h(N_B \| N_{WCA})}$ $[n,\ N_B,$ $N_{WCA},\ \mathbf{k}]$ $\|N_{WCA}$ $\|\mathbf{c} \ominus \mathbf{W}'$.

W5. After receiving the message from S_j, B_i retrieves N_{WCA} to derive the fresh session key $h(N_B \| N_{WCA})$ and then verifies the previously generated random element N_B by decrypting $E_{h(N_B \| N_{WCA})}[n, N_B, N_{WCA}, \mathbf{k}]$. If the verification is succeeded, then B_i can remove the distorted sequence $\mathbf{k}$ to obtain the watermarked version of the content $\mathbf{c} \ominus \mathbf{W}$ from the distorted content $\mathbf{c} \ominus \mathbf{W}'$ by computing $\mathbf{c} \ominus \mathbf{W}' \oplus \mathbf{k}$.

3.3 Identification and Arbitration Protocol

When a suspicious digital content $\mathbf{c}'$, which may be owned by the specified seller S_j, is found over the Internet, the protocol can be utilized to trace the identity of the specified buyer, who purchased $\mathbf{c}'$ in the earlier transaction, with undeniable evidences.

Once S_j discovers $\mathbf{c}'$, she uses the encrypted watermarks $\mathbf{W}' = \mathbf{W} \oplus \mathbf{k}$ stored in the transaction database to perform watermark detection in $\mathbf{c}'$. When finding the corresponding item with the highest correlation value over the predefined confidence level, S_j collects the associated information: $(\mathbf{c},\ \mathbf{W}',\ n,\ (e_{B_i}, s_{B_i})$ $E_{h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})}[seed, \mathbf{w}, \mathbf{k}, N_B, N_{WCA}])$, and then sends them along with $\mathbf{c}'$ to the judge J.

Then J proceeds to ask WCA to use x_{WCA} to recover the evident key $h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})$ and then decrypt $E_{h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})}[seed, \mathbf{w}, \mathbf{k}, N_B, N_{WCA}])$.

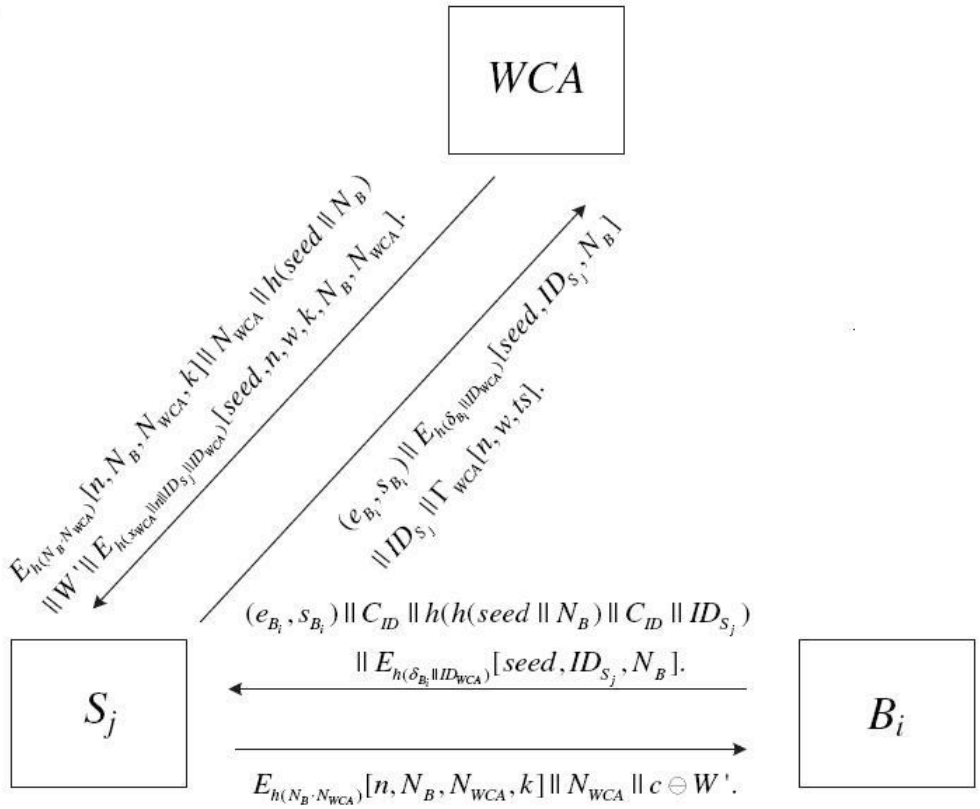

Figure 1: Chang et al.'s watermarking protocol [2]

Next, J verifies the decrypted transaction number and watermark. If the verification fails, J rejects the case, otherwise, J utilizes the decrypted $\mathbf{k}$ to recover the final valid watermark $\mathbf{W} = \mathbf{w} \oplus \mathbf{w}'$ from $\mathbf{W}' = \mathbf{W} \oplus \mathbf{k}$. Finally, J verifies the presence of $\mathbf{W}$ in $\mathbf{c}'$ and the irrelevance between $\mathbf{k}$ and $\mathbf{c}'$ under the threshold of a predetermined confidence level. If it indeed holds, $\mathbf{c}'$ is an unauthorized copy. To trace the distributor, J simultaneously asks WCA to utilize x_{WCA} and the certificate (e_{B_i}, s_{B_i}) to derive the master secret δ_{B_i}. Once δ_{B_i} is derived, WCA can compute $h(\delta_{B_i})$ and confirm the real identity of B_i.

4 Weaknesses of Chang et al.'s Scheme

We now describe the weaknesses that are found in the above scheme. It is worth noting that Chang et al. assumes that all messages in the watermarking protocol (Section 3.2) are exchanged over public communication channels and WCA in their scheme is always a trusted party. Under such assumptions, Chang et al. claimed that their scheme could achieve the following security goals. However, we will demonstrate the claim is incorrect.

Firstly, they claimed that the buyer in their scheme was unable to remove the watermark from the digital watermarked content. I do admit, if only given $\mathbf{c} \ominus \mathbf{W}$, it is impossible for B_i to remove $\mathbf{W}$ in it. However, if the buyer is a malicious eavesdropper, she can easily obtain $\mathbf{W}' = \mathbf{W} \oplus \mathbf{k}$ by wiretapping the exchanged messages in W3 and then use it along with the received item $\mathbf{c} \ominus \mathbf{W}'$ in W4 to recover the original content by computing $(\mathbf{c} \ominus \mathbf{W}') \oplus \mathbf{W}' = \mathbf{c}$. As a result, digital watermarking techniques that are used to protect the seller's copyright will be defeated completely. In addition, the unbinding problem will arise as well.

Secondly, they claimed that their scheme was traceable, which meant that any buyer who had distributed the digital content unlawfully could be identified using the identification and arbitration protocol. I do admit, if both the seller and the buyer follow the watermarking protocol honestly, the malicious buyer who tries to deny the purchased content will be detected during the identification and arbitration phase. However, if the buyer is an active adversary, she just modifies the partial transcripts $E_{h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})}$ [*seed*, $\mathbf{w}$, $\mathbf{k}$, N_B, N_{WCA}] exchanged in W3 into a random bit string of the same length. And the modification can not be detected by the seller and the latter will store the received item in the transaction database. After the transaction is finished, the buyer may distribute the digital content unlawfully in the Internet. Then, if the seller finds such an unauthorized copy of the digital content and makes an infringement accusation, the responsible distributor can deny the purchased content successfully. That is because, when J asks WCA to use x_{WCA} to recover the evident key $h(x_{WCA} \| n \| ID_{S_j} \| ID_{WCA})$ and then decrypt modi-

fied ciphertext pointing to $E_{h(x_{WCA}\|n\|ID_{S_j}\|ID_{WCA})}$ [*seed*, $\mathbf{w}$, $\mathbf{k}$, N_B, N_{WCA}]) in the identification and arbitration protocol, the probability that for J to get any meaningful results from decryption for verification is next to zero. As a result, the suspicion can not be justified.

Thirdly, they claimed that their scheme could protect the buyer's privacy well because the behavior of users was done anonymously in their scheme. I do admit, nobody, except WCA, can trace the real identity of a buyer, since for each buyer B_i, a self-verified token (e_{B_i}, s_{B_i}) can be interpreted as a temporary identity. However, it is still possible to collecting information about some customer's behavior and the tracking of some user although the acute identity is unknown. That is because one buyer (or its identity) corresponds to only one such self-verified token (e_{B_i}, s_{B_i}) according to the registration protocol. In addition, it is possible to infer a buyer's real identity through data mining techniques if the same user frequently purchases digital contents. As a result, the buyer's personal privacy can not be well-protected.

In addition, we find Chang et al.'s scheme has the following drawback: it puts a large amount of trust into WCA. Let's assume WCA is also an eavesdropper who has obtained $\mathbf{c} \ominus \mathbf{W}'$ by wiretapping the exchanged messages in W4. Then she can easily derive the watermarked content $\mathbf{c} \ominus \mathbf{W}$ from it by computing $(\mathbf{c} \ominus \mathbf{W}') \oplus \mathbf{k} = \mathbf{c} \ominus \mathbf{W}$ since she also knows $\mathbf{k}$. On the other hand, she can always trace the real identity of B_i. Therefore, the privacy of the purchase behavior of the buyer will be fully leaked to the malicious WCA. Furthermore, if WCA is also an active attacker, she can easily impersonate the legitimate buyer B_i to purchase digital content since she can record the master secret δ_{B_i}, the master's delegation $h(\delta_{B_i}\|ID_{WCA})$ and the certificate (e_{B_i}, s_{B_i}) for the buyer B_i in the registration phase and then use them to play an role of B_i successfully in the watermarking protocol.

5 Countermeasure

In this section, we figure out what is wrong with the protocol and how to fix it.

The vulnerability to the first attack stems from an absence of confidentiality protection on message $\mathbf{W}'$ in the Chang et al.'s watermarking protocol. And the vulnerability to the second attack stems from an absence of authentication of message $E_{h(x_{WCA}\|n\|ID_{S_j}\|ID_{WCA})}$ [*seed*, $\mathbf{w}$, $\mathbf{k}$, N_B, N_{WCA}]) (denoted by α for simplicity). The simplest way to resolve the security problem with Chang's scheme on the first two attacks would be to establish a fresh session key shared by WCA and S_j to protect them. To achieve this goal, S_j generates a random element $N_S \in_R Z_q^*$ and also encrypts it using WCA's public key: i.e. computes the ciphertext $\Gamma_{WCA}[n, w, N_S, ts]$. Eventually, S_j sends to the seller S_j the new ciphertext instead of $\Gamma_{WCA}[n, w, ts]$ in W2. Upon receiving it, WCA will compute $E_{h(N_S\|N_{WCA})}(\mathbf{W}'\|h(\alpha))$ and send to S_j this new item instead $\mathbf{W}'$ in plain. Then S_j will compute the session key $h(N_S\|N_{WCA})$ and decrypt the received ciphertext to retrieve $\mathbf{W}'$ and $h(\alpha)$. Finally, S_j will use the received α to compute $h(\alpha)$ and compare it with the decrypted $h(\alpha)$. If they are equal, S_j believes that the received α has not been modified on the way and the decrypted $\mathbf{W}'$ has been kept secret. Otherwise, S_j rejects the case.

The vulnerability to the third attack stems from the determined relation between B_i's identity and its certificate (e_{B_i}, s_{B_i}). That is, one buyer (or its identity) corresponds to only one such self-verified token (e_{B_i}, s_{B_i}) according to the registration protocol. The simplest way to resolve the security problem with Chang's scheme on the third attack would be to include a random number r in the computation the master secret δ_{B_i}. More specifically, WCA generates the master secret δ_{B_i}, which satisfies the following equation $h(x_{WCA}\|ID_{B_i}) = h(ID_{B_i}\|ID_{WCA}\|r) \cdot \delta_{B_i} \bmod q$. Accordingly, WCA records the mapping relation of the buyer's ID_{B_i} and $h(ID_{B_i}\|ID_{WCA}\|r)$ for future arbitration between the buyer and the seller. As a result, one buyer may be allowed to have multiple master secrets, multiple master delegation keys and multiple certificates. Therefore, B_i can apply a number of anonymous certificates simultaneously and randomly chooses one for each transaction.

Finally, we have to stress that, in order to overcome the aforesaid drawback, each buyer has to hold a public key pair of an asymmetric encryption scheme or a signature scheme, which requires the operation of a full PKI to manage digital certificates for end users. After so many years, public key infrastructures are still limited to a small scale or closed domains [11]. Therefore, any schemes depending on PKI support can not be applied quite widely. On the other hand, such protocols can not work well with heterogamous environments, for example, a buyer may utilize low-power mobile devices to purchase digital content through wireless network, since public key cryptography involves expensive computational operations and the buyer's device may not bear the heavy burden operations. Therefore, the security engineers, who are responsible for the design and development of the watermarking scheme, must realize it.

6 Conclusion

In this correspondence, we have shown the weaknesses of Chang et al.'s watermarking scheme for large scale networks. And, we have suggested some countermeasures to fix its problems while its merits are left unchanged.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China (No. 61101112) and China Postdoctoral Science Foundation (2011M500775).

References

[1] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," *Proceedings of ACM Annual Conference on Computer and Communications Security*, pp. 62-73, 1993.

[2] C. C. Chang, H. C. Tsai, Y. P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," *Computers and Security*, vol. 29. pp. 269-277, 2010.

[3] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, "Reversible watermarking: Current status and key issues," *International Journal of Network Security*, vol. 2, no. 3, PP. 161-171, May 2006.

[4] T. Kalker, *Digital Video Watermarking for DVD Copy Protection*, Multimed. Arch. Storage, Sept. 1999.

[5] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," *IEEE Transactions on Forensics and Security*, vol. 3, no. 4, pp. 783-786, 2008.

[6] D. Kundur, "Video fingerprinting and encryption principles for digital rights management," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 918-932, Jun. 2004.

[7] C. L. Lei, P. L. Yu, P. L. Tsai, and M. H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1618-1626, 2004.

[8] A. Lemma, S. Katzenbeisser, M. Celik, and M. van der Veen, "Secure watermark embedding through partial encryption," *Proceedings of 5th International Workshop Digital Watermarking*, LNCS 4283, pp. 433-445, Springer-Verlag, 2006.

[9] N. Memon and P. W. Wong, "Protecting digital media content," *Communications on ACM*, vol. 4, pp. 11-24, July 1998.

[10] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 9, no. 4, pp. 643-649, 2001.

[11] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, June 2002.

Shuhua Wu is a Ph.D. candidate at Information Engineering University, Zhengzhou. His research interest is information security.

Qiong Pu is a Ph.D. candidate at Tongji University. Her research interest is communication security.