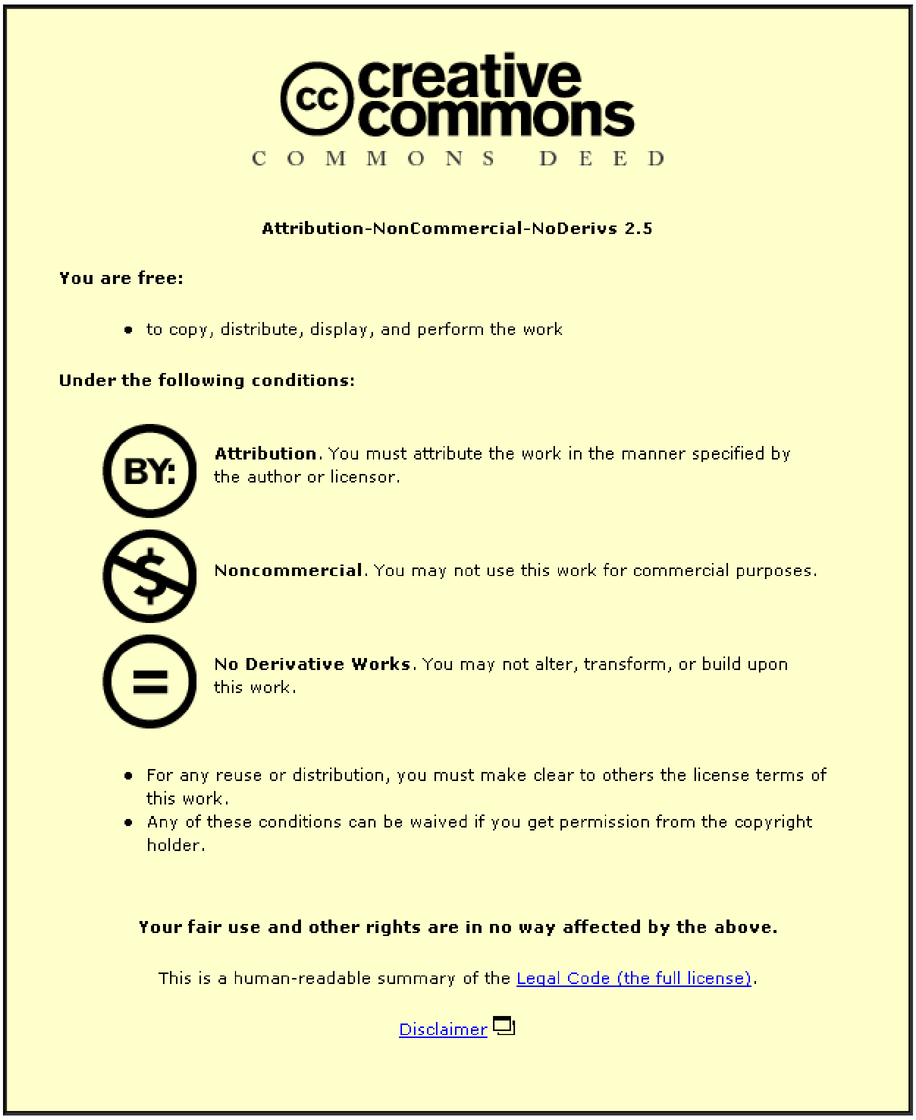


Noname manuscript No.
(will be inserted by the editor)

Analysis of a Buyer-Seller Watermarking Protocol for Trustworthy Purchasing of Digital Contents

Raphael C.-W. Phan [⋆] · **Bok-Min Goi** [⋆⋆] ·
Geong-Sen Poh · **Jongsung Kim** [⋆⋆⋆]

Received: date / Accepted: date

Abstract In ubiquitous environments where human users get to access diverse kinds of (often multimedia enabled) services irrespective of where they are, the issue of security is a major concern. Security in this setting encompasses both in the interest of the human users as well as their information and objects that they own. A typical kind of transaction interaction among users and/or machines in these environments is that of exchanging digital objects via purchases and/or ownership transfers, e.g. someone buying a song from iTunes via his iPhone, or downloading either bought or rented movies onto a portable DVD player. Here, there is a need to provide trustworthy protection of the rights of both parties; i.e. the seller's copyright needs to be protected against piracy, while on the other hand it has been highlighted in literature the need to protect innocent buyers from being framed. Indeed, if either party cannot be assured that his rights are protected when he is involved in transactions within such environments, he would shy away and instead prefer for instance the more conventional non-digital means of buying and selling. And therefore without active participation from human users and object owners it is difficult to fully kick off the actual realization of intelligent environments. Zhang *et al.* recently proposed a buyer-seller watermarking protocol without a trusted third party based on secret sharing. While it is a nice idea to eliminate the need of a trusted third party by distributing secret shares between the buyer and the seller

[⋆] Part of work done while the author was with the Laboratoire de sécurité et de cryptographie (LASEC), EPFL, Switzerland.

[⋆⋆] Part of work done while the author was with the Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.

[⋆⋆⋆] Corresponding author.

Electronic & Electrical Engineering, Loughborough University, U.K.
E-mail: r.phan@lboro.ac.uk
· Faculty of Engineering & Science,
Universiti Tunku Abdul Rahman (UTAR), Setapak, Malaysia.
E-mail: goibokmin@utar.edu.my
· Information Security Group, Royal Holloway, University of London, Egham, U.K.
E-mail: g.s.poh@rhul.ac.uk
· Department of e-Business, Kyungnam University, Korea
E-mail: jongsung.k@gmail.com

such that neither party has knowledge of the fingerprint embedded in a content, we show that it is possible for a buyer to remove his part of the fingerprint from the content he bought. This directly disproves the piracy tracing property claimed by the protocol. In fact, since piracy tracing is one of the earliest security applications of watermarking schemes, it raises doubts as to the soundness of the design of this protocol.

Keywords Security systems · trustworthy applications · content protection · transactions · digital rights protection · watermarking and fingerprinting protocol · buyer-seller · anonymity · unbinding property · secret sharing

1 Introduction

As users transact across virtual spaces within ubiquitous environments via their portable mobile smart devices like handhelds, PDAs, iPhones etc., the consumer business model has now moved to a setting where human consumers potentially purchase goods or services anywhere as long as they have access to their personal smart devices. The purchasing and subsequent downloading of songs (e.g. from iTunes), movies, music videos, etc is now so simple and inexpensive that users inadvertently involve themselves in such digital transactions as a matter taken for granted. And so, we have the situation where numerous amounts of digital content are bought and sold within this environment. Naturally, security issues arise that need to be addressed properly and trustworthily.

When a digital content is sold to a buyer B, there is a need to protect the seller's rights against cases where the buyer illegally redistributes copies of this content. Therefore, watermarking protocols are typically used to embed buyer-specific watermarks (a.k.a. fingerprints) into the content so that when an illegal copy is found, the extracted watermark reveals who the guilty buyer is.

However, it was not until [22] that the issue of protecting the buyer was raised. This is now known as the **customer's rights problem**. Briefly, this is caused by the implicit assumption that sellers are fully trusted, but if a seller is malicious, he can easily embed any buyer's fingerprint into his content and frame an innocent buyer for illegal distribution.

Building on this idea, [18] proposed the first of what is now a class of buyer-seller watermarking (BSW) protocols [18], [14], [1], [9], [16], [25] based on privacy homomorphic encryption schemes and watermarking schemes with linear embedding functions, though the more recent two [16], [25] protocols have the explicit design strategy such that they no longer require underlying watermarking schemes with the linearity property. Interestingly however, it is the absence of this property that is the starting point for our attack to work, as will be described in our Section III on protocol analysis.

In particular, we show in this paper that for a recent variant of the buyer-seller watermarking protocols, namely [25], it is possible for the buyer to remove his fingerprint from his copy of the bought content. This therefore directly disproves the **piracy tracing property** claimed by the protocol. In fact, since piracy tracing is one of the earliest security applications of watermarking protocols, it raises doubts as to the soundness of the design of this protocol.

2 Buyer-Seller Watermarking Protocols

These are protocols that provide content distribution between a buyer and a seller, in which the buyer of the content can be traced, while at the same time the seller cannot frame an honest buyer of illegal content redistribution. In addition, a malicious buyer cannot deny illegally redistributing content.

As mentioned earlier, BSW protocols were first proposed by [22] and later improved by [18]. [14] presented a protocol that also protects the buyer's privacy. Several buyer-seller protocol variants have been constructed since then, including the protocols proposed in [1], [2], [5], [6], [8], [9], [12], [13], [15], [16], [17], [21], and subsequent analyses appear in [10], [11], [20], [24], [5, 4, 23].

2.1 Parties Involved

A buyer-seller watermarking protocol involves a seller (S), who provides (or sells) content to a buyer (B), while an arbiter (A) settles disputes between the seller and buyer. A special trusted third party may also be involved. In many buyer-seller watermarking protocols [18, 14, 16], this role is played by a *watermark certification authority* (*WCA*), who is responsible for generating and certifying client watermarks. It is assumed that the seller and the buyer do not trust each other. It is also assumed that WCA and A will not conspire with the seller and/or the buyer.

2.2 Threats

The main security threats for BSW protocols can be classified from the perspective of which is the malicious party:

- *Seller.* A seller may frame a buyer. This happens when a seller inserts a unique watermark matching the buyer's identity into copies of the content and distributes this widely. Later the seller can accuse the buyer of illegal content redistribution by extracting this watermark from these copies.
- *Buyer.* There are two main threats:
  - A buyer may try to remove the watermark in the marked content.
  - A buyer may redistribute copies of content given by the seller, and later deny this fact when confronted by the seller.

2.3 Security Properties

These motivate the three main security properties of a buyer-seller watermarking protocol [14, 16]:

- *Traceability.* The identity of a legitimate, but dishonest, buyer who illegally redistributes content can be traced by the seller. This is the fundamental property expected of watermarking protocols used for copyright protection.
- *Framing Resistance.* An honest buyer cannot be falsely accused of illegal redistribution by the seller. This property relates to the customer's rights problem which motivated the introduction of BSW protocols.

- *Non-repudiation of Redistribution.* A dishonest buyer who has redistributed illegal copies of content cannot refute this fact. This allows the seller to prove the illegal act of the buyer to a third party arbiter. In this case framing resistance is a prerequisite since, without this property, a buyer can claim that it was the seller who redistributed copies of the content.

Some existing protocols [14, 16] include the protection of buyer's privacy as an additional security property, but in this paper we will only focus on the three fundamental properties.

2.4 Main Techniques

To fulfill the above mentioned security properties, the main idea is to prevent the seller from being able to determine the final marked copy given to the buyer while still allowing the seller to trace the identity of the buyer in illegally redistributed contents.

- For piracy tracing (*traceability*), BSW protocols deploy digital watermarking schemes [3].
- For *non-repudiation of redistribution*, BSW protocols deploy digital signature schemes such as RSA-OAEP to ensure that a dishonest client cannot repudiate the fact that copies of content were illegally distributed.
- To prevent the seller from framing a buyer (*framing-resistance*), most BSW protocols deploy asymmetric homomorphic encryption schemes such as Paillier [19] together with digital watermarking schemes such as the spread spectrum watermarking scheme [3] in a way that the party (i.e. the seller) who embeds his share of the watermark into the content has no idea what the final embedded watermark is. This technique is termed as *watermarking in the encrypted domain* [7]. As for who should generate the buyer watermark, there are two different techniques:
  - In the first technique introduced by Memon and Wong [18], a special trusted third party commonly known as the Watermark Certification Authority (WCA) was introduced to generate buyer watermarks, instead of letting the distributor to generate them; the WCA is fully trusted.
  - In the second technique, which was deployed by [25], the buyers are tasked to generate their own watermarks.

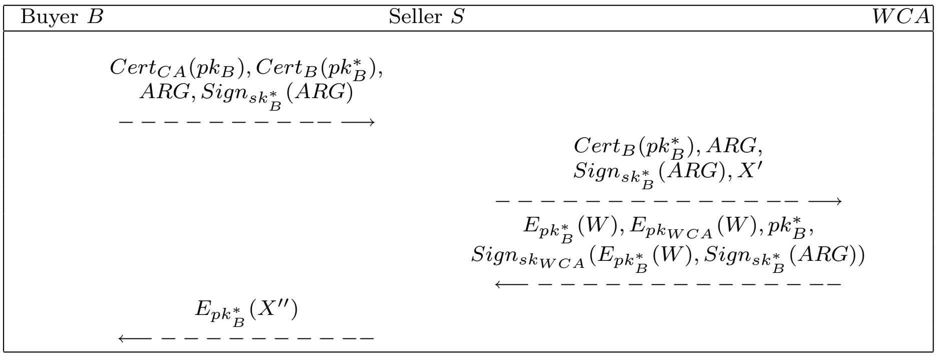
3 The Zhang *et al.* and Lei *et al.* Protocols

The [25] protocol basically inherits all the properties of its immediate predecessor the [16] protocol, but in addition its design strategy is such that there are only two parties involved, namely the buyer and the seller, and they do not need to interact with any TTP (WCA in this case) during the buying-selling stage except if a dispute arises later. The aim of this strategy is to eliminate the threat of conspiracy attacks [1, 9, 25]. Indeed, it is a major achievement to design a secure buyer-seller watermarking protocol that does not require a TTP.

Both BSW protocols comprise three subprotocols; namely, the *registration subprotocol*, the *watermarking subprotocol* and the *identification and arbitration subprotocol.* However, only the *registration subprotocol* and the *watermarking subprotocol*, which are relevant to the discussion in this paper are described. Note that the registration subprotocol for both BSW protocols are identical. For compactness of description, the Zhang *et al.* watermarking subprotocol and Lei *et al.* watermarking subprotocol are illustrated in Fig. 2 and Fig. 1, respectively. The notations used are as defined in Table 1.

Table 1 Notations

S	The seller who sells the digital content
B	The buyer who can buy contents anonymously
WCA	The watermark certification authority who can issue watermarks to buyers upon request and certify them
CA	Certification authority who can issue the (optionally anonymous) certificate and a pair of keys (pk, sk) for every party in the public-key infrastructure (PKI)
(pk_I, sk_I)	Public-private key-pair of user, I
(pk_B^*, sk_B^*)	An anonymous one-time key-pair generated by B
$Sign_{sk_I}(m)$	Signature of message, m signed by I with his private key, sk_I
$E_{pk_I}(m)$	Ciphertext of message, m encrypted with I's public key. Encryption can be done by anyone
$Cert_J(I)$	Digital certificate issued to party I by certification authority J. Anyone is able to verify the validity of the certificate, and the public key associated with a particular party can be easily obtained from his certificate
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 $n \leq m$
V	Watermark for indexing with n elements, $v_1, v_2, \ldots, v_n$, where $n \leq m$
X', X''	Watermarked content
$X + W$	Embed W into X with the embedding operation, $+$
ARG	An agreement which states the rights and obligations of seller and buyer, and uniquely binds a particular content X. This is to solve the *unbinding problem* in the original Memon-Wong BSW protocol [18], thus it can also be treated as a purchase order



Buyer B
Seller S
WCA
$Cert_{CA}(pk_B), Cert_B(pk_B^*),$
$ARG, Sign_{sk_B^*}(ARG)$
$Cert_B(pk_B^*), ARG,$
$Sign_{sk_B^*}(ARG), X'$
$E_{pk_B^*}(W), E_{pk_{WCA}}(W), pk_B^*,$
$Sign_{sk_{WCA}}(E_{pk_B^*}(W), Sign_{sk_B^*}(ARG))$
$E_{pk_B^*}(X'')$

Fig. 1 The Lei *et al.* Watermarking Subprotocol

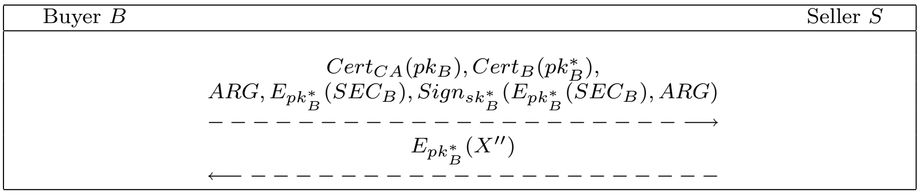

Buyer B
Seller S
$Cert_{CA}(pk_B), Cert_B(pk_B^*),$
$ARG, E_{pk_B^*}(SEC_B), Sign_{sk_B^*}(E_{pk_B^*}(SEC_B), ARG)$
$E_{pk_B^*}(X'')$

Fig. 2 The Zhang *et al.* Watermarking Subprotocol

3.1 The Registration Subprotocol

The buyer, B firstly applies to CA for an *anonymous certificate*[1] as follows:

1. B randomly generates an anonymous public-private key pair (pk_B, sk_B). He then sends pk_B to CA.
2. Upon approval, CA computes the anonymous certificate $Cert_{CA}(pk_B)$ and replies it to B.

Alternatively, if anonymity is not a concern, B can simply skip this subprotocol by carrying out the transaction using his normal digital certificate.

3.2 The Lei *et al.* Watermarking Subprotocol

Fig. 1 visualizes Lei *et al.*'s watermarking subprotocol and the details are as follows:

1. Firstly, B negotiates with the seller, S anonymously using his anonymous identity pk_B, on the honor of $Cert_{CA}(pk_B)$.
2. After the negotiation, the buyer randomly generates an anonymous (one time) public-private key pair (pk_B^*, sk_B^*) and sends $Cert_{CA}(pk_B)$, $Cert_B(pk_B^*)$, ARG and $sign_{sk_B^*}[ARG]$ to the seller. Note that the buyer is using his anonymous identity to generate the certificate $Cert_B(pk_B^*)$, hence the buyer's identity is not shown in the subject field.
3. Upon receiving the message from the buyer, the seller verifies the certificates and signatures. If pass, she embeds her watermark V into the X that the buyer wishes to purchase, and obtains $X' = X + V$. Then, she sends $Cert_B(pk_B^*)$, ARG, $sign_{sk_B^*}[ARG]$ and X' to WCA.
4. After validating the message from the seller, the WCA generates a unique watermark W, especially for this transaction (best-suited for X') and encrypts it with pk_{WCA} and pk_B^*. Note that the second encryption scheme has to be homomorphic with respect to the $+$. Then, he sends $E_{pk_{WCA}}[W]$, $E_{pk_B^*}[W]$, $sign_{sk_{WCA}}[E_{pk_B^*}[W]$, pk_B^* and $sign_{sk_B^*}[ARG]]$ back to the seller.
5. Due to homomorphic property, the seller is able to insert the second watermark in encrypted form into $E_{pk_B^*}[X']$ and obtains $E_{pk_B^*}[X'']$, where $X'' = X' + W$, without knowing the sk_B^*. Then, she delivers $E_{pk_B^*}[X'']$ to the buyer and stores all the necessary information in her database with respect to X.
6. Finally, the buyers receives his watermarked purchased content X'' by decrypting the message received from the seller with his sk_B^*.

[1] An anonymous certificate is just like a normal digital certificate except that the subject field contains a pseudonym but not the user's identity.

3.3 The Zhang *et al.* Watermarking Subprotocol

Fig. 2 visualizes Zhang *et al.*'s watermarking subprotocol and the details are as follows:

1. Similar to the Lei *et al.* protocol, B negotiates with S anonymously to set up a new ARG.
2. Then, B randomly generates an anonymous key pair (pk_B^*, sk_B^*) and a secret SEC_B. He sends $Cert_{CA}(pk_B)$, $Cert_B(pk_B^*)$, ARG, $Sign_{sk_B^*}(E_{pk_B^*}(SEC_B), ARG)$ and $E_{pk_B^*}(SEC_B)$, to the seller, S.
3. Upon receiving the message from B, then S checks the validity of the certificates and signature. If they pass the verification, S generates a random unique first-round watermark V and embeds it into the purchased digital multimedia content, X to obtain the first-round watermarked content, $X' = X+V$. Then he generates a secret SEC_S and computes the encrypted watermark $E_{pk_B^*}(W)$ where $W(= SEC_S + SEC_B)$ is the second-round watermark, using a public key cryptosystem which is privacy homomorphism with respect to the embedding operating $+$. Thanks to the homomorphism property, $E_{pk_B^*}(W)$ where $W = SEC_S + SEC_B$ can be obtained without decrypting $E_{pk_B^*}(SEC_B)$; in fact, this can not be done by S as he does not have the corresponding sk_B^*. Again, by using homomorphic public key cryptosystem, the seller can insert the second-round watermark W into X' in the encrypted domain to obtain $E_{pk_B^*}(X'')$. Then, S delivers $E_{pk_B^*}(X'')$ to B and stores the sales record for X.
4. Finally, with the knowledge of sk_B^*, B can decrypt the received $E_{pk_B^*}(X'')$ to obtain the final watermarked content X''.

For more details of both protocols, we refer the reader to [16, 25].

4 Attacking the Zhang *et al.* Protocol

It was claimed by [25] in their Section 4 that in their protocol, a buyer, B is unable to remove his fingerprint W from the copy X'' he had purchased. Hence, traceability (i.e. piracy tracing) was claimed. To be precise, the argument is that since $X'' = X' + W = X + V + W$, therefore since both X and V are unknown to B and further that only one share (out of two) of W is known to B, therefore B is not able to extract any information on W. In general, one can only remove an embedded watermark W if one knows the value of W.

Nevertheless, we show here that this can be circumvented for the Zhang *et al.* protocol, i.e. a buyer can remove his fingerprint hence invalidating the piracy tracing claim; and thus a dishonest buyer can then illegally redistribute the bought content. The problem stems from the fact that both secret shares SEC_B and SEC_S are embedded into the encrypted domain of X independently, and in the same way that any individual independent watermark, e.g. V is embedded, thus $X'' = X' + W = X + V + W = X + V + SEC_S + SEC_B$ can be viewed as having been embedded with 3 independent watermarks V, SEC_S and SEC_B. To the best of our knowledge, no other BSW protocol exhibits this. Therefore, with the knowledge of the value of any of these 3 watermarks, that watermark can be removed. In the case of B, he knows SEC_B, therefore he can remove SEC_B from X'' before illegally distributing it, thus all traces of B can no longer be found in the pirated copy.

In more detail, recall that a robust watermarking scheme is needed for the watermark embedding and extraction, the most common one being [3] used by all BSW variants to perform watermark embedding and extraction. This was also the one used by Zhang *et al.* as a concrete example in their Section 3.

The scheme first performs DCT on the content to obtain a set of DCT coefficients, which we denote as $x_1, x_2, \ldots, x_m$. Then a scaled version (let α be the scale factor) of the watermark is added to the DCT coefficients based on three possible variants of an insertion formula in [3]. For ease of description, we use the simplest one but we stress that our attack applies regardless of which is used. Let $W = w_1, w_2, \ldots, w_m$, then insertion of watermark W into the DCT coefficients $x_1, x_2, \ldots, x_m$ of some content X is:

$$x'_i = x_i + \alpha \cdot w_i, \tag{1}$$

where $x'_1, x'_2, \ldots, x'_m$ are the watermarked coefficients. In the case of the Zhang *et al.* protocol, the coefficients of X'' are:

$$x''_i = x_i + v_i + \alpha \cdot w_i = x_i + v_i + \alpha \cdot SEC_{S_i} + \alpha \cdot SEC_{B_i}. \tag{2}$$

Therefore, B can remove traces of SEC_B from X'' by doing:

$$x'_i = x''_i - \alpha \cdot SEC_{B_i} = x_i + v_i + \alpha \cdot SEC_{S_i}. \tag{3}$$

Note that the same problem fundamentally exists in Zhang *et al.*'s immediate predecessor [16]. Interestingly enough, this problem is a consequence of the design strategy of not requiring the underlying watermarking scheme to be linear in contrast to most existing buyer-seller protocol variants [18, 14, 1, 9]. By design, this relaxation relates to not including a secret permutation σ applied on W, thereby the underlying watermarking scheme need not be linear. Indeed, if the Zhang *et al.* protocol was designed with such a σ applied more specifically on SEC_B prior to insertion, then it seems this attack can be prevented. Yet, it was the non-requirement of linear underlying watermarking schemes (thus non-inclusion of σ) that was the explicit design strategy of these two protocols in the first place.

5 Discussion: Comparing the Security of Two Protocols

5.1 Resistance to Conspiracy Attacks

While the Zhang *et al.* protocol is based on the [16] protocol, yet in contrast, its design strategy clearly avoids the conspiracy attacks [1, 9, 25] where two or more parties involved in a protocol collude (conspire together) with each other to maliciously cheat another innocent party outside the collusion set. This is because since there are only two parties (the seller and the buyer) thus the notion of collusion becomes no longer meaningful.

For the case of Lei *et al.* however, one could argue that if one considers a setting similar to those considered in [1] then a conspiracy attack is possible, that involves collusion of the seller S and the watermark certification authority WCA, or collusion between the buyer B and the WCA. In more detail, for the first case: Although S on his own is unable to determine the value of the watermark W embedded into the content bought by B, by colluding with WCA he obtains W and therefore can embed it into any contents bought by B and frame B for illegally distributing them. For the second case: Since WCA is given the task of generating W, as well as the values $E_{pk^*_B}(W)$, $E_{pk_{WCA}}(W)$, $Sign_{sk_{WCA}}(E_{pk^*_B}(W), pk^*_B, Sign_{sk^*_B}ARG))$ − possibly used by S during the identification and arbitration protocol to identify a guilty buyer who distributes his bought copies illegally − then B can collude with the WCA to have a random watermark W generated that is not connected to B so that B would not be found guilty by the arbiter.

5.2 Non-Resistance to Piracy Tracing

Both the Zhang *et al.* and Lei *et al.* protocols do not require watermarking schemes with linearity property because by design they do not make use of a secret random permutation σ chosen by S and which is unknown to B.

What is intriguing is that the use of this would have protected the Zhang *et al.* protocol from our attack in Section III. In contrast, for the Lei *et al.* protocol it is possible to resist our attack even without the secret random permutation because there is an option (stated en passant by Lei *et al.* in [16]) to not have the entire X' sent but only a profile describing it. If this option is enforced, our attack will not apply.

The main problem why the Zhang *et al.* protocol falls to our attack is that while the Lei *et al.* protocol keeps B's watermark unknown to him, in contrast the Zhang *et al.* protocol allows B to choose the part of the watermark, i.e. SEC_B that uniquely binds B to a content. The other part of the watermark, i.e. SEC_S does not do so. To summarise, it does not matter how many parts are used to form the embedded watermark W, nor that not all parts are known to B. What matters is that the parts that bind B to the content must be unknown to B.

6 Conclusion

It is a nice idea to use secret sharing to solve both the problem of seller's and buyer's rights by distributing the secret shares of the watermark between both parties. However, if the embedding operation and the operator used to combine the shares are commutative, and further if the part of the watermark that binds B to the content is known to B, then it leads to our attack described above.

We do not see any way to fix the Zhang *et al.* protocol to still provide piracy tracing without eliminating its simplicity and basic structure. We remark that this is yet another example where an "improved" variant i.e. [25] is insecure while the predecessor i.e. [16] is not.

References

1. Choi JG, Sakurai K, Park JH (2003) Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party. In: Zhou J, Yung M, Han Y (eds) Applied Cryptography and Network Security - ACNS 2003, Springer-Verlag, Lecture Notes in Computer Science, vol 2846, pp 265–279
2. Choi JG, Park JH, Kwon KR (2004) Analysis of COT-based Fingerprinting Schemes: New Approach to Design Practical and Secure Fingerprinting Scheme. In: Fridrich JJ (ed) 6th International Workshop on Information Hiding - IH 2004, Springer-Verlag, Lecture Notes in Computer Science, vol 3200, pp 253–265

3. Cox IJ, Kilian J, Leighton T, Shamoon T (1997) Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans on Image Processing 6(12):1673–1687
4. Deng M, Preneel B (2008) Attacks on Two Buyer-Seller Watermarking Protocols and an Improvement for Revocable Anonymity. In: International Symposium on Electronic Commerce and Security, ICECS 2008, IEEE Computer Society, pp 923–929
5. Deng M, Preneel B (2008) On Secure and Anonymous Buyer-Seller Watermarking Protocol. In: Third International Conference on Internet and Web Applications and Services, ICIW 2008, IEEE Computer Society, pp 524–529
6. Deng M, Weng L, Preneel B (2008) Anonymous Buyer-Seller Watermarking Protocol with Additive Homomorphism. In: SIGMAP 2008 - International Conference on Signal Processing and Multimedia Applications, pp 300–307
7. Erkin Z, Piva A, Katzenbeisser S, Lagendijk RL, Shokrollahi J, Neven G, Barni M (2007) Protection and Retrieval of Encrypted Multimedia Content: When Cryptography Meets Signal Processing. EURASIP Journal on Information Security 2007:78,943, 20 pages, doi:10.1155/2007/78943
8. Frattolillo F, D'Onofrio S (2006) A Web Oriented and Interactive Buyer-Seller Watermarking Protocol. In: Security, Steganography, and Watermarking of Multimedia Content VIII, Proc. of SPIE, vol 6072, pp 718–716
9. Goi BM, Phan RCW, Yang Y, Bao F, Deng RH, Siddiqi MU (2004) Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity. In: Jakobsson M, Yung M, Zhou J (eds) Applied Cryptography and Network Security - ACNS 2004, Springer-Verlag, Lecture Notes in Computer Science, vol 3089, pp 369–382
10. Goi BM, Phan RCW, Siddiqi MU (2005) Cryptanalysis of a Generalized Anonymous Buyer-seller Watermarking Protocol of IWDW 2004. In: Enokido T, Yan L, Xiao B, Kim D, Dai YS, Yang LT (eds) Embedded and Ubiquitous Computing - EUC 2005, Springer-Verlag, Lecture Notes in Computer Science, vol 3823, pp 936–944
11. Goi BM, Phan RCW, Chuah HT (2007) Cryptanalysis of Two Non-anonymous Buyer-Seller Watermarking Protocols for Content Protection. In: Gervasi O, Gavrilova ML (eds) International Conference on Computational Science and Its Applications - ICCSA 2007, Springer-Verlag, Lecture Notes in Computer Science, vol 4705, pp 951–960
12. Ibrahim IM, El-Din SHN, Hegazy AFA (2007) An Effective and Secure Buyer-Seller Watermarking Protocol. In: Third International Symposium on Information Assurance and Security (IAS 07), IEEE Computer Society Press, pp 21–26
13. Ibrahim IM, El-Din SHN, Hegazy AFA (2007) An Effective and Secure Watermarking Protocol for Digital Rights Protection Over the Second-Hand Market. In: SECRYPT 2007 - International Conference on Security and Cryptography, pp 263–268
14. Ju HS, Kim HJ, Lee DH, Lim JI (2002) An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control. In: Lee PJ, Lim CH (eds) Information Security and Cryptology - ICISC 2002, Springer-Verlag, Lecture Notes in Computer Science, vol 2587, pp 421–432
15. Kuribayashi M, Tanaka H (2006) Fingerprinting Protocol for Online-Line Trade Using Information Gap between Buyer and Merchant. IEICE Trans on Fundamentals E89-A(4):1108–1115

16. Lei CL, Yu PL, Tsai PL, Chan MH (2004) An Efficient and Anonymous Buyer-Seller Watermarking Protocol. IEEE Trans on Image Processing 13(12):1618–1626
17. Leung A, Poh GS (2007) An Anonymous Watermarking Scheme for Content Distribution Protection using Trusted Computing. In: SECRYPT 2007 - International Conference on Security and Cryptography, INSTICC Press., pp 319–326
18. Memon N, Wong PW (2001) A Buyer-Seller Watermarking Protocol. IEEE Trans on Image Processing 10(4):643–649
19. Paillier P (1999) Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern J (ed) Advances in Cryptology - EUROCRYPT 1999, Springer-Verlag, Lecture Notes in Computer Science, vol 1592, pp 223–238
20. Phan RCW, Goi BM (2007) (In)Security of an Efficient Fingerprinting Scheme with Symmetric and Commutative Encryption of IWDW 2005. In: Digital Watermarking, 6th International Workshop - IWDW 2007, Springer-Verlag, Lecture Notes in Computer Science
21. Poh GS, Martin KM (2008) An Efficient Buyer-Seller Watermarking Scheme Based on Chameleon Encryption. In: Kim HJ, Katzenbeisser S, Ho ATS (eds) Digital Watermarking, Seventh International Workshop, IWDW 2008, Springer-Verlag, Lecture Notes in Computer Science
22. Qiao L, Nahrstedt K (1998) Watermarking schemes and protocols for protecting rightful ownerships and customer's rights. Journal of Visual Communication and Image Representation 9(3):194–210
23. Williams DM, Treharne H, Ho ATS, Culnane C (2008) Using a Formal Technique to Identify an Unbinding Attack on a Buyer-Seller Watermarking Protocol. In: ACM Workshop on Multimedia and Security, MM&Sec 2008, ACM, pp 205–214
24. Wu Y (2007) Security Flaws in Kuribayashi-Tanaka Fingerprinting Protocol. In: International Conference on Communications, ICC 2007, IEEE, pp 1317–1322
25. Zhang J, Kou W, Fan K (2006) Secure Buyer-Seller Watermarking Protocol. IEE Proceedings - Information Security 153(1):15–18

Biography

Raphael Phan is with the Electronic & Electrical Engineering department of Loughborough University, UK. He is General Chair of Mycrypt '05 and Asiacrypt '07 and annually serves in various technical program committees of cryptology and security conferences. He researches on diverse aspects of security and privacy.

Bok-Min Goi received his B.Eng degree in Electrical Engineering from University of Malaya (UM) in 1998, and the M.Eng.Sc and Ph.D degrees from Multimedia University (MMU) in 2002 and 2006, respectively. He is Associate Professor in the Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR). His research interests include cryptology, security protocols, information security, digital watermarking and embedded systems design.

Geong Sen Poh received the Bachelor degree and Master degree in computer science from Universiti Sains Malaysia, in 1999 and 2002 respectively. From 2002 to 2005 he worked as a researcher in MIMOS Berhad and then further his doctorate study with the Information Security Group, Royal Holloway, University of London. He obtained his PhD degree in 2009. He is now a senior researcher in MIMOS Berhad. His research interests include design and analysis of cryptographic protocols and digital watermarking.

Jongsung Kim obtained his Bachelor and Master degrees in mathematics from Korea university, Korea in 2000 and 2002, respectively. He received double Doctoral degrees on “Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms”, completed in November 2006 and February 2007 at the ESAT/COSIC group of Katholieke Universiteit Leuven and at Engineering in Information Security of Korea University, respectively. He had been a research professor at the Center for Information Security Technologies (CIST), Korea University, Korea, from March 2007 to August 2009. He has been an associate professor at the Department of e-Business, Kyungnam University, Korea, since September 2009. His research interests include symmetric crytosystems, digital forensic, side-channel attacks, ubiquitous computing systems and e-business. He serves in technical Program Committees of ISH ’05, ISA ’09, UASS ’09, UC-Sec ’09, SSDU ’09, SMPE ’09, MIMUC ’09 and ICUT ’09. He also serves as program co-chair of F2GC ’09 and as steering committee of MPIS ’09.