Cryptanalysis of a Generalized Anonymous Buyer-Seller Watermarking Protocol of IWDW 2004

Bok-Min Goi¹, Raphael C.-W. Phan², and M.U. Siddiqi^{1,*}

¹ Centre for Cryptography and Information Security (CCIS),
Faculty of Engineering, Multimedia University,
63100 Cyberjaya, Malaysia
`bmgoi@mmu.edu.my`

² Information Security Research (iSECURES) Lab,
Swinburne University of Technology (Sarawak Campus),
93576 Kuching, Malaysia
`rphan@swinburne.edu.my`

Abstract. In this paper, we analyze the security of a generalized anonymous buyer-seller watermarking protocol recently proposed by Choi and Park at IWDW 2004. We prove that it has not met the designers' intended security criteria by showing that an attacker can actually: (1) discover the unique buyer's watermark which was chosen by the watermark certificate center (*WCC*), and (2) decrypt the encrypted watermarked digital content without any extra cost. Also, it is surprising to note that when designing their protocol, the designers did not take into consideration the conspiracy attacks.

Keywords: Digital Watermarking, Buyer-Seller Watermarking Protocol, Cryptanalysis, Copyright Protection.

1 Introduction

In this information age, all types of multimedia information are being stored and processed in digital form, because of many advantages over the traditional analog counterpart. Unfortunately, since the duplication of digital multimedia content results in perfectly identical copies, many multimedia content providers are hesitant to sell/distribute their content digitally. *Digital watermarking* [15, 5] and *digital fingerprinting* [12, 13] are mainly designed to overcome this problem—the *copyright protection issue*. A *buyer-seller watermarking protocol* is a combination of both; more precisely, it allows to trace redistribution of the digital contents by extracting the original buyer's information (fingerprint) and to prove the content owner by extracting the sellers' information (watermark) from the redistributed contents. Therefore, it does protect the rights and interests of not only the seller

* The first author acknowledges the Malaysia IRPA grant (04-99-01-00003-EAR).

but also of the buyer. In the literature, many buyer-seller watermarking protocols have been proposed [1-4, 7-10].

In this paper, we analyze the security of a generalized anonymous buyer-seller watermarking protocol recently proposed by Choi and Park at IWDW 2004 [3]. At first glance, the new protocol looks quite attractive because it can be generalized to *multi-purchase environments* where a set of buyers can purchase multiple distinct contents from a set of sellers, and this solves the open problem stated in Goi *et al.* [7]. However, we show that it does not achieve the security criteria set out by the designers, namely that an attacker can actually: (1) discover the unique buyer watermark chosen by the watermark certificate center (*WCC*), and (2) decrypt and obtain the encrypted watermarked digital content. It is also surprising that when designing the protocol, the designers did not consider security against *conspiracy attacks* when in fact even Memon and Wong [10] – the designers of the original buyer-seller watermarking protocol – had commented that it is undesirable to place complete trust on a single source, including the watermark certification center, and that such attacks had already been considered extensively in this literature [8, 3, 7]. To solve the conspiracy attack, we refer readers to Goi *et al.* [7] where the buyer should generate his own private watermark and convince the certificate authority that s/he owns the secret watermark, via the zero-knowledge proof protocol.

1.1 Related Work

In 1998, Qiao and Nahrstedt [14] presented an *owner-customer* watermarking protocol that solved the problem of rightful ownership. Unfortunately, it is a *symmetric scheme* and does not guarantee the buyer's security. The first truly buyer-seller watermarking protocol that withheld the buyer's unique watermark (fingerprint) from the seller was proposed by Memon and Wong [10]. The Memon-Wong protocol is an *asymmetric scheme* where even the seller is not able to reproduce the unique watermarked content. Since then, several variants of this protocol have been proposed in the literature, including the Chang-Chung protocol and Cheung *et al.* protocol which were proposed at ICCT '03 [1] and HICSS '04 [2], respectively. Also worth mentioning is the Lei *et al.* protocol [9] which is based on the unbinding problem.

Independently of these, the issue of the importance of "anonymity" was raised by Ju *et al.* at ICISC '02 [8] when they presented an anonymous version of the Memon-Wong protocol. Choi *et al.* later at ACNS '03 [3] presented conspiracy attacks on the Ju *et al.* variant and further modified it such that it resists these attacks. However, Goi *et al.* at ACNS '04 [7] showed that the Choi *et al.* protocol was still insecure against conspiracy attacks and also can not provide *full anonymity*. They then proposed a variant that achieves full anonymity. Finally, Choi and Park at IWDW '04 generalized on their earlier ACNS '03 work of [3] to multi-purchase environments. They also claimed that their protocol can be implemented for mobile communication by employing mobile agents with an extra step - *delegation* step. A comparison of security features and primitive

requirements of various proposed buyer-seller watermarking protocols is shown in Table 1.

Table 1. Comparison of Security Features and Primitive Requirements of Various Buyer-Seller Watermarking Protocols

		Memon 01 [10]	Ju 02 [8]	Chang 03 [1]	Choi 03 [3]	Cheung 04 [2]	Goi 04 [7]	Lei 04 [9]	Choi 04 [3]
Services & Security Provided	Anonymity	×	✓	×	✓	×	✓	✓	✓
	Conspiracy attacks	×	×	×	×	×	✓	×	×
	Multi-purchase	×	×	×	×	×	×	×	✓
Primitive Requirements	Homomorphic [†]	✓	✓	×	✓	✓	✓	×	✓
	Commutative [‡]	×	×	×	✓	✓	×	×	×
	Linearity [†]	✓	✓	✓	✓	×	✓	×	✓

[†] : Homomorphic encryption algorithm and linear watermarking scheme are defined in subsection 2.2.

[‡] : An encryption algorithm is said to be *commutative*, if for a multiple encrypted (decrypted) message the same resultant ciphertext (plaintext) will be obtained irrespective of its the order of encryption [7].

1.2 Security Criteria

We describe in this subsection some security criteria that are expected to be achieved by a sound anonymous buyer-seller watermarking protocol, as follows [7, 3]:

- **Anonymity.** A buyer’s identity is protected, unless s/he is found guilty.
- **Unlinkability.** Nobody is able to determine whether the different watermarked contents are purchased by the same buyer.
- **Traceability.** The buyer who has illegally redistributed watermarked contents can be traced.
- **No-Framing.** Nobody can accuse an honest buyer.
- **Non-Repudiation.** The guilty buyer cannot deny that the unauthorized copies of the content were not created by him.

Obviously, the security of a seller-buyer watermarking protocol is dependent on the underlying watermarking scheme. Hence, the used watermarking scheme must be collusion tolerant; more precisely, nobody can find and delete the embedded watermark (invisible type) from the content without knowing the watermark.

2 Preliminaries

2.1 Notations

For ease of explanation, we stick to the notations used in [3] as follows:

S	the seller who sells the digital multimedia content
B	the buyer who can buy watermarked contents anonymously
RC	the agent who can verify the buyer's identity and issue the buyer anonymous certificates, $Cert(y_1)$
WCC	the agent who can issue watermarks to buyers upon request and certify them
CA	certification authority who can issue the certificate and a pair of keys (x, y) for every agent in the PKI
X	original content with m elements $x_1, x_2, \dots, x_m$
W	watermark with n elements $w_1, w_2, \dots, w_n$ generated by WCC , where $n \leq m$
V	watermark with n elements $v_1, v_2, \dots, v_n$ generated by the seller, where $n \leq m$
X', X''	watermarked content
$X \otimes W$	embed watermark, W into X with insertion operation, $\otimes$
σ	random permutation function chosen by S
t	total number of contents to be purchased
$text$	valid set of operations that the agent is allowed to perform while using the certificates
$\parallel$	string concatenation

2.2 Building Blocks

The protocols discussed here use *public key cryptography* [11]; each agent, A possesses a pair of keys: public key, y_A and private key x_A — which are obtained from a certificate authority center (CA). For convenience, we stick to $y_A \equiv g^{x_A} \bmod p$, where p is a large prime such that $\frac{p-1}{2}$ is also a prime, and g is a generator of the multiplication group, Z_p . All arithmetic operations are performed under Z_p , unless otherwise specified. We denote $E_y(m)$ to mean the message, m encrypted with the public key, y . Any agent can encrypt a message for A using y_A , but only A can decrypt this message with x_A : $D_{x_A}[E_{y_A}(m)]$. Furthermore, A can sign a message by encrypting it with x_A , denoted as $sign_{x_A}(m)$. We assume that all agents have registered with the CA beforehand and have their own pair of keys: the seller, S with (x_S, y_S) , the buyer, B with (x_B, y_B) , RC with (x_R, y_R) and WCC with (x_W, y_W) . Also, the public-key encryption algorithm used in this paper must be homomorphic. A well-known homomorphic encryption algorithm is the RSA with respect to the multiplication operation.

Besides robustness, in terms of various digital processing operations, printing and re-scanning, and collusion attacks, the underlying watermarking scheme adopted must have *linearity* property. This is because the seller needs to permute the original watermark generated by WCC with a random permutation function, σ before embedding it into the content. The detailed watermark embedding process is described as follows:

$$\begin{aligned}
 X' &= X \otimes \sigma(W) \\
 &= (x_1, x_2, \dots, x_m) \otimes \sigma(w_1, w_2, \dots, w_n) \\
 &= (x_1 \otimes w_{\sigma(1)}), (x_2 \otimes w_{\sigma(2)}), \dots, (x_n \otimes w_{\sigma(n)}), x_{n+1}, x_{n+2}, \dots, x_m
 \end{aligned}$$

Therefore, the robust Cox's invisible watermarking algorithm [5] is a suitable choice and has intensively been used in Memon-Wong protocol and its variants.

3 An Overview of the Choi-Park Protocol

Basically, there are four steps involved in the Choi-Park Protocol: (1) Registration, (2) Watermarking generation, (3) Watermark insertion, and (4) Copyright violator identification.

In order to ensure that Choi-Park protocol works, several typos and mistakes in [3] have to be corrected. They are:

- **Registration step:** Firstly, RC should keep $(y_B, y_1, \text{cert}(y_1))$ in database RC_DB , but not $(y_B, y_2, \text{cert}(y_1))$. Further, although the designers did not consider this, x_{B_2} has to be stored in database RC_DB . This is because x_{B_2} is later used during the Copyright violator identification step to prove and disclose the buyer's identity if s/he is found guilty; i.e., $y_1^{x_{B_2}} = y_B$.
- **Watermark generation step:** Note that $(k_1, k_2, \dots, k_t) \in Z_p$ have to be chosen carefully, so that the obtained $y_i^* = (y_1^{k_i}, g^{k_i})$ contains no zero element of $y_1^{k_i}$, for $i = 1, 2, \dots, t$. Otherwise, the encryption function: $E_{y_i^*}(m) = (m \cdot y_1^{k_i} \| g^{k_i})$ would turn out to be trivial.
- **Watermark insertion step:** The validity of $\text{sign}_{B_i} = \text{sign}_{x_{B_1}}(\text{text}_i)$ is verified by S using $y_1 = g^{x_{B_1}}$ (anonymous public key of x_{B_1}) but not y_i^* . Hence, B has to send y_1 to S . (This will cause the protocol to become linkable although it still provides anonymity service.) Furthermore, according to the definition of the encryption function as used in [3], the final encrypted watermarked digital content should be defined as $E_{y_i^*}(X_i'') = E_{y_i^*}(X_i \otimes V_i \otimes \sigma_i(W_i) \cdot y_1^{k_i} \| g^{k_i})$, and not, $E_{y_i^*}(X_i'') = E_{y_i^*}(X_i \otimes V_i \otimes \sigma_i(W_i) \cdot y_i^* \| g^{k_i})$. Therefore, the decryption function is performed as follows:

Fig. 1. Choi-Park Protocol: Registration

Fig. 2. Choi-Park Protocol: Watermark Generation **Fig. 3.** Choi-Park Protocol: Watermark Insertion

$$\begin{aligned}
 D_{x_{B_1}}[E_{y_i^*}(X_i'')] &= \frac{X_i \otimes V_i \otimes \sigma_i(W_i) \cdot y_1^{k_i}}{(g^{k_i})^{x_{B_1}}} \\
 &= \frac{X_i \otimes V_i \otimes \sigma_i(W_i) \cdot y_1^{k_i}}{y_1^{k_i}} = X_i \otimes V_i \otimes \sigma_i(W_i) \quad (1)
 \end{aligned}$$

Choi and Park claimed here that only the buyer with the secret information, x_{B_1} can perform the decryption and then obtain the final watermarked content, X_i^n . However, we prove in Section 4 that it is not true.

For compactness of description, all these steps, except for step (4), are illustrated in Figures 1, 2 and 3, respectively. The proposed protocol is efficient because each step can be completed in one round. During the registration step, as shown in Figure 1, by providing y_1 (which is used for achieving anonymity), B convinces RC of possession of x_{B_1} via a zero-knowledge proof [6]. We omit the copyright violator identification step as it is straightforward and irrelevant to our attacks and discussions in this paper. We refer interested readers to [3] for further details.

4 Attacking the Choi-Park Protocol

The main problem of the Choi-Park protocol is the encryption process during the watermark generation step: WCC encrypts each watermark W_i with $y_i^* = (y_1^{k_i}, g^{k_i})$ such that, $Enc_W_i = E_{y_i^*}(m) = (m \cdot y_1^{k_i} \| g^{k_i})$, for $i = 1, 2, \dots, t$. However, y_i^* , together with Enc_W_i and $sign_W_i$, are sent in clear form, both during the watermark generation step and during the watermark insertion step. This causes a serious security flaw and the protocol becomes totally insecure. More precisely, upon receiving/intercepting these messages, the seller/ anyone can decrypt Enc_W_i to obtain the watermark W_i even without k_i , and x_{B_1} (which are secretly kept by WCC and the buyer, respectively). This is because one can compute $(y_1^{k_i})^{-1}$, the inverse of $y_1^{k_i}$ easily. For instance, the well-known extended Euclidean algorithm [11] can be used for computing multiplicative inverses in Z_p , where p is an n -bit prime integer. The computational complexity of the given algorithm is only $O((\lg p)^2)$ or $O(n^2)$; in other words, it can be done in polynomial time.

Upon computing $(y_1^{k_i})^{-1}$, we multiply it with $Enc_W_i = (W_i \cdot y_1^{k_i} \| g^{k_i})$ (note that doing so is equivalent to decryption) to recover W_i . This disproves the claims in [3] that only the buyer with knowledge of x_{B_1} can decrypt Enc_W_i to get the unique watermark W_i based on Eq.(1). This causes several serious security issues, some of which are further explained in detail in following subsections.

4.1 Attacking the Buyer's Security

By a Malicious Seller. Once a malicious seller has obtained the unique buyer's watermark, W_i as described above, then with all other the necessary information, i.e., X, V_i, σ_i that he has access to, he can reproduce and redistribute illegally the watermarked content for his own gain. When the illegal watermarked content is found in the market, the innocent buyer will be accused. Hence, "no-framing" and "non-repudiation" cannot be provided.

By any Outsider. With the knowledge of W_i , an attacker can simply embed it into a digital content which is not (never) purchased by the buyer, who may never be aware of this. Again, an innocent buyer will be accused.

4.2 Attacking the Seller's Security

As mentioned above, with the information $y_1^{k_i}$, the decryption process can be carried by anyone. Firstly, an attacker intercepts the encrypted watermarked digital content, $E_{y_i^*}(X_i)$ during the watermark insertion step and then decrypts it to obtain the watermarked content, X_i , although s/he does not pay to the seller.

5 Discussions

Our attack exploited the fact that $y_i^* = (y_1^{k_i}, g^{k_i})$ is sent in the clear, and that the encryption method used by the designers is mere multiplication with $y_1^{k_i}$ (followed by concatenation with g^{k_i}), and correspondingly, the decryption (see equation (1)) is simply division with the same, which translates to multiplication with the multiplicative inverse of $y_1^{k_i}$. Although x_{B_1} was used in the generation of y_1 and can therefore be used in the decryption process, the fact is that even without x_{B_1} , decryption can still be done with y_1 . This is very clear from equation (1). This is quite different from the encryption and decryption processes used in RSA-type schemes where both involved exponentiations.

Finally, it is very surprising that during the design of their protocol Choi and Park did not take into consideration of the conspiracy attacks. It is obvious that once the seller colludes with *RC* or *WCC*, the anonymity and other security services provided by the protocol will be compromised totally. In order to solve this, the buyer should be responsible to generate his/her own private watermark and convince the certificate authority that s/he owns the secret watermark, via the zero-knowledge proof protocol, as proposed by Goi *et al.* in [7].

6 Conclusions

In this paper, we have shown that Choi and Park protocol is flawed. This is due to the leak of y_i^* during the protocol that allows an attacker to discover the unique buyer watermark and also further decrypt the encrypted watermarked digital content. Therefore, it cannot provide “no framing” and “non-repudiation”, “unlinkability” and “untraceability” security criteria, even if the underlying watermarking scheme is secure. Furthermore, the protocol is not secure against conspiracy attacks.

References

1. C.C. Chang and C.Y. Chung. An Enhanced Buyer-Seller Watermarking Protocol. In *Proceedings of ICCT '03*, pp. 1779-1783, 2003.
2. S.C. Cheung, H.F. Leung and C. Wang. A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents. In *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37)*, January 2004.

3. J.G. Choi and J.H. Park. A Generalization of an Anonymous Buyer-Seller Watermarking Protocol and Its Application to Mobile Communications. In *Proceedings of IWDW '04*, LNCS 3304, pp. 232-243, 2005.
4. J.G. Choi, K. Sakurai, and J.H. Park. Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party. In *Proceedings of ACNS '03*, LNCS 2846, pp. 265-279, 2003.
5. I.J. Cox, J. Kilian, T. Leighton and T. Shamoon. Secure Spread Spectrum Watermarking for Images, Audio and Video. In *IEEE Trans. on Image Processing*, vol. 6, no.12, pp.1673-1678, 1997.
6. D. Chaum. An Improved Protocol for Demonstrating Possession of Discrete Logarithms and some Generalizations. In *Proceedings of Eurocrypt '87*, LNCS 307, pp. 127-141, 1987.
7. B.M. Goi, R.C.-W. Phan, Y. Yang, F. Bao, R.H. Deng and M.U. Siddiqi. Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and An Improvement for True Anonymity. In *Proceedings of ACNS '04*, LNCS 3089, pp. 369-382, 2004.
8. H.S. Ju, H.J. Kim, D.H. Lee and J.I. Lim. An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control. In *Proceedings of ICISC '02*, LNCS 2587, pp. 421-432, 2002.
9. C.-L. Lei, P.-L. Yu, P.-L. Tsai and M.-H. Chan. An Efficient and Anonymous Buyer-Seller Watermarking Protocol. In *IEEE Trans. on Image Processing*, vol. 13, no. 12, pp. 1618-1626, 2004.
10. N. Memon and P.W. Wong. A Buyer-Seller Watermarking Protocol. In *IEEE Trans. on Image Processing*, vol. 10, no.4, April 2001.
11. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography", CRC Press, 1997.
12. B. Pfizmann and A.R. Sadeghi. Coin-Based Anonymous Fingerprinting. In *Proceedings of Eurocrypt '99*, LNCS 1592, pp. 150-164, 1999.
13. B. Pfizmann and M. Waidner. Anonymous Fingerprinting. In *Proceedings of Eurocrypt '97*, LNCS 1233, pp. 88-102, 1997.
14. L. Qiao and K. Nahrstedt. Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights. In *J. Visual Commun. Image Representation*, vol. 9, pp. 194-210, 1998.
15. G. Voyatzis and I. Pitas. The Use of Watermarks in the Protection of Digital Multimedia Products. In *Proc. IEEE*, Vol. 87, pp. 1197-1207, July 1999.