An Investigator Unearths Illegal Behavior via a Subliminal Channel

Chin-Ling Chen[1,2], Tzay-Farn Shih[1], Kun-hao Wang[2], Chien-Hung Chen[1], Woei-Jiunn Tsaur[3]

[1] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taiwan
[2] School of Information Engineering, Changchun Sci-Tech University, China
[3] Computer Center, National Taipei University, Taiwan
clc@mail.cyut.edu.tw, tfshih@cyut.edu.tw, wkhyoyo@163.com, bitz823@hotmail.com, wjtsaur@mail.ntpu.edu.tw

Abstract

With the rapid development of the Internet, the number of criminal cases has greatly increased. Therefore, determining how to avoid and reduce illegal behaviors has become an important issue. For example: illegal insider trading of enterprises, commercial spying, etc. Illegal insider trading occurs when somebody in an enterprise trades based on non-public information obtained during the performance of the insider's duties at the corporation, or in breach of a fiduciary or other relationship of trust and confidence, or where the non-public information was misappropriated from the company. In this paper, we propose a novel scheme to protect investigators' safety and ensure the security of the collected evidence via a subliminal channel. We use a cryptographic mechanism to solve the replay attack, forgery attack, non-repudiation, untraceable and authentication issues. Our scheme not only protects investigators' identity and safety but also constitutes a fair arbitration mechanism.

Keywords: Subliminal channel, Fair arbitration, Security, Non-repudiation, Insider trading

1 Introduction

With the rapid development of the Internet, people can easily to access Internet resources; however, ready access may also cause increased illegal behavior to occur. In real life, illegal behavior occurs frequently. We often hear news about insider trading in different enterprises. Insider trading can cause the enterprise and shareholders to suffer significant losses.

The subliminal channel was first proposed by Simmons in 1983 [1-3]. Subliminal channels are employed for secret communication; like a signal, it is set up beforehand. These channels can be used to send subliminal messages to the receiver, but the subliminal messages cannot be accessed except through the specified receiver. Harn and Gong [4] proposed a digital signature with a subliminal channel in 1997. Their paper showed how to construct a digital signature scheme with a broadband subliminal channel; it did not require the subliminal receiver to share the transmitter's secret signing key. Lin et al. [5] proposed a digital signature with multiple subliminal channels and its applications. The proposed scheme can provide more than one independent subliminal message.

Many illegal cases or transactions often happen in real life. Therefore, developing a fair mechanism to ensure the legal rights of each party is an important task. In 1997, Franklin and Reiter [6] proposed achieving a fair exchange with a semi-trusted third party. Zhou and Gollman [7] proposed a fair non-repudiation protocol in 1996. Their scheme provided both a fair and non-repudiated protocol.

In 2009, Chen and Liu [8] proposed a traceable E-cash transfer system via subliminal channel as protection against blackmail; they sent the blackmail message to a victim's bank via a subliminal channel. Solving the threat of blackmail on an E-cash transfer system is an important issue. The scheme not only can be employed against blackmail attack, but it can also provide a traceable E-cash system. In 2010, Chen and Liao [9] proposed a fair online payment system for digital content via a subliminal channel. Their scheme protects a consumer's ownership and offers an intact arbitration mechanism to ensure the fairness of transactions between customer and shop.

In this paper, we propose a novel scheme to protect the investigator's identity such that the evidence of illegal behavior is kept secure for official agents to make a fair arbitration via a subliminal channel. The investigator can uncover illegal transactions. When the investigating organization notifies the police to arrest a criminal, the evidence of illegal activity will be sent to official agents to make a fair arbitration.

The proposed scheme should have the following capabilities:

(1) Against replay attack [10-11]: A replay attack occurs when an attacker copies the message between

[*] Corresponding Author: Chin-Ling Chen; E-mail: clc@mail.cyut.edu.tw

DOI: 10.3966/160792642018031902025

two parties and replays it to one or more parties to achieve the replay attack.

(2) Against forgery attack [12]: In a forgery attack an attacker masquerading as the legal party transmits the message to obtain the other party's trust, and achieve the forgery attack.

(3) Non-repudiation [13-14]: Non-repudiation refers to the ability to ensure that the parties can't deny the authenticity of their signature on the message which they sent.

(4) Untraceable [15-16]: Untraceable is an important issue in electronic cash payment system. Other people cannot trace the sender when they get the transmission message.

(5) Fair arbitration [14, 17]: Fair arbitration is a necessary mechanism. It not only protects both parties' rights but also makes a fair arbitration.

The rest of our paper is organized as follows. In Section 2, we introduce the framework of our scheme. In Section 3, we make a security analysis of our scheme. In Section 4, we discuss the communication cost and computation cost of our scheme. Finally, we offer a conclusion regarding our scheme.

2 Our scheme

There are five parties involved in our scheme:

(1) Criminal (C): The malicious person/organization.

(2) Investigator (I): A person who investigates an illegal behavior.

(3) Investigating Organization (IO): The organization doing the investigation.

(4) Official Agent (OA): A trustworthy and fair arbitrator.

(5) Police (P): The police agency.

The following notations are used in our scheme:

Notations

SK_X	the X's private key
PK_X	the X's public key, where $PK_X = g^{SK_I} \bmod p$, where g is a randomly chosen generator of the multiplicative group Z
$K_{X\text{-}Y}$	the session key between X and Y
$Sig_{I_1}, Sig_{I_2}, Sig_{I_3}$	the signatures of the investigator
T_X	the timestamp which is generated by X
M_S	the subliminal message
M_{evi}	the criminally-related evidence
$C_{X\text{-}Y}$	the cipher message transferred from X to Y
$H()$	a one-way hash function
$E_{K_{X-Y}}(M) / D_{K_{X-Y}}(M)$	use the session key K_{X-Y} to encrypt/decrypt message M
Z	the secret number which is shared by IO and OA
II	The information of the crimes, for example: video, picture, image
$\oplus$	the XOR operation
$\|\|$	concatenation operation

The overview of our scheme is shown in Figure 1.

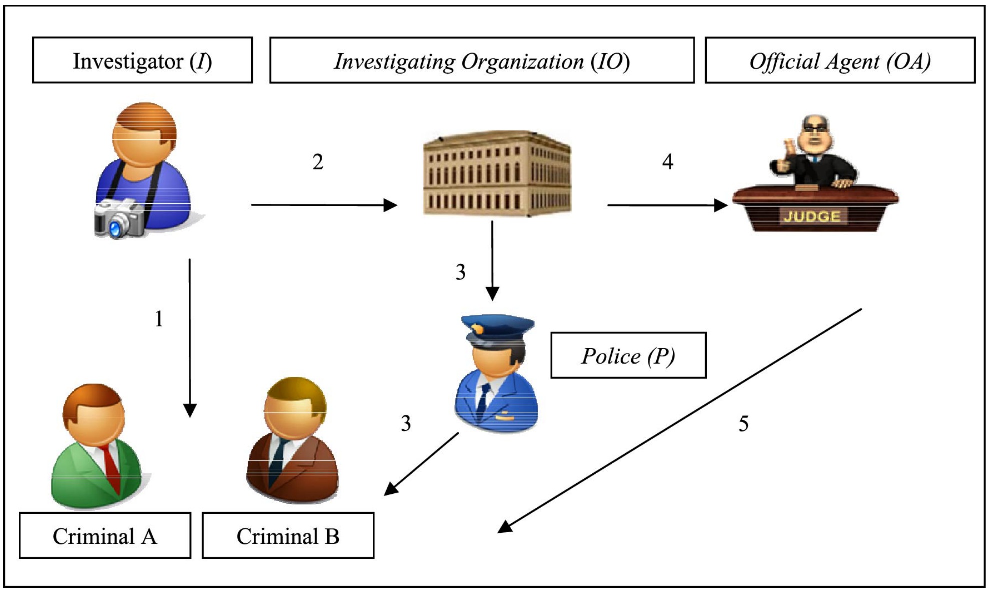

Figure 1. Overview of our scheme

Step 1. I→ Criminals A & B: When criminals A and B engage in an illegal behavior, I collects the information on their illegal behaviors.

Step 2. I→ IO: I sends a secret message to IO via the subliminal channel.

Step 3. IO→ P→ Criminal A & B: When IO receives the subliminal message, IO will notify the police to arrest criminals A & B.

Step 4. IO→ OA: IO sends the evidence of an illegal activity to OA.

Step 5. OA extracts the evidence message from IO's message and verifies if the activity of A and B is illegal.

2.1 The initial phase

First, I, IO and OA generate the key pairs. IO and OA share the secret number Z. I and IO make the subliminal message M_S to build a subliminal channel. SK_I is I's private key and PK_I is I's public key, where $PK_X = g^{SK_I} \bmod p$.

2.2 The investigation phase

The IO dispatches an investigator to go undercover. When the criminal has engaged in illegal behavior, the investigator collects information on the illegal behavior. I sends the investigation results to IO. After that, the IO notifies police to arrest the criminal who has engaged in the illegal behavior. The scenario of the Investigation phase is shown in Figure 2.

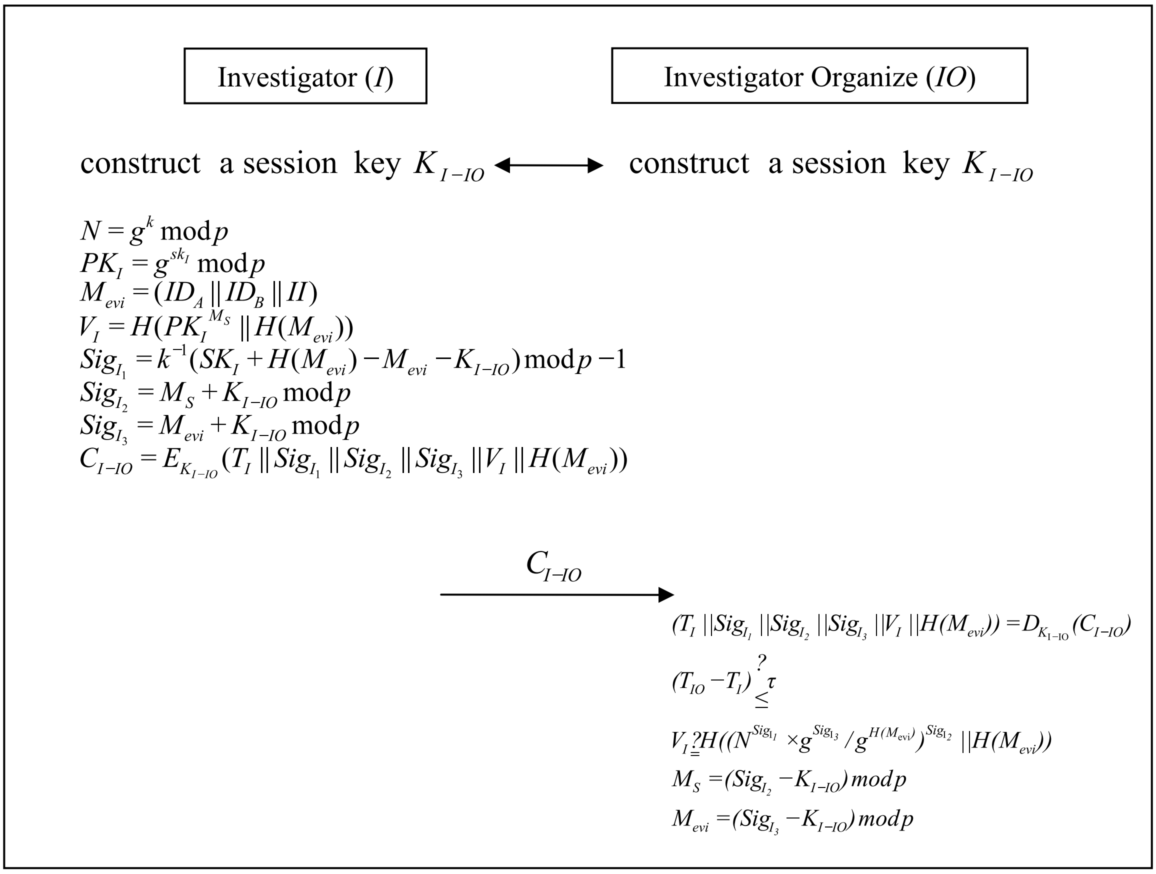
Investigator (*I*)
Investigator Organize (*IO*)
construct a session key K_{I-IO}
construct a session key K_{I-IO}
$N = g^k \bmod p$
$PK_I = g^{sk_I} \bmod p$
$M_{evi} = (ID_A \| ID_B \| II)$
$V_I = H(PK_I^{M_S} \| H(M_{evi}))$
$Sig_{I_1} = k^{-1}(SK_I + H(M_{evi}) - M_{evi} - K_{I-IO}) \bmod p-1$
$Sig_{I_2} = M_S + K_{I-IO} \bmod p$
$Sig_{I_3} = M_{evi} + K_{I-IO} \bmod p$
$C_{I-IO} = E_{K_{I-IO}}(T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi}))$
C_{I-IO}
$(T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi})) = D_{K_{I-IO}}(C_{I-IO})$
$(T_{IO} - T_I) \overset{?}{\leq} \tau$
$V_I \overset{?}{=} H((N^{Sig_{I_1}} \times g^{Sig_{I_3}} / g^{H(M_{evi})})^{Sig_{I_2}} \| H(M_{evi}))$
$M_S = (Sig_{I_2} - K_{I-IO}) mod p$
$M_{evi} = (Sig_{I_3} - K_{I-IO}) mod p$

Figure 2. The scenario of the investigation phase

Step 1. I and IO construct a session key K_{I-IO} [18]. **(1)**

Step 2. I randomly chooses a parameter k, $k \in [0, p]$ and gcd(k, p-1) = 1, and then computes the following parameters:

$$N = g^k \bmod p \tag{2}$$

$$PK_I = g^{SK_I} \bmod p \tag{3}$$

The investigator collects the information on the illegal behavior and makes an evidence message:

$$M_{evi} = (ID_A \| ID_B \| II) \tag{4}$$

Afterwards, I uses the subliminal message M_S and PK_I to compute the parameter V_I :

$$V_I = H(PK_I^{M_S} \| H(M_{evi})) \tag{5}$$

Then I uses the secret key SK_I and session key K_{I-IO} to compute the signatures: Sig_{I_1} , Sig_{I_2} and Sig_{I_3} as follows:

$$Sig_{I_1} = k^{-1}(SK_I + H(M_{evi}) - M_{evi} - K_{I-IO}) \bmod p - 1 \tag{6}$$

$$Sig_{I_2} = M_S + K_{I-F} \bmod p \tag{7}$$

$$Sig_{I_3} = M_{evi} + K_{I-F} \bmod p \tag{8}$$

After that, I uses the session key K_{I-IO} to encrypt the message ($T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi})$):

$$C_{I-IO} = E_{K_{I-IO}}(T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi})) \tag{9}$$

Then I send the cipher message C_{I-IO} to IO.

Step 3. After receiving the cipher message C$_{I\text{-}IO}$ at T$_{IO}$, IO uses the session key K$_{I\text{-}IO}$ to decrypt the message:

$$(T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi})) = D_{K_{I-IO}}(C_{I-IO}) \quad \textbf{(10)}$$

After that, IO checks the validity of timestamp T$_I$:

$$(T_{IO} - T_I) \overset{?}{\leq} \tau \quad \textbf{(11)}$$

τ is the valid time interval between I and IO. If it holds, IO verifies I's identity:

$$V_I \overset{?}{=} H((N^{Sig_{I_1}} \times g^{Sig_{I_3}} / g^{H(M_{evi})})^{Sig_{I_2}} \| H(M_{evi})) \quad \textbf{(12)}$$

If Equation (13) holds, IO obtains the subliminal message M$_S$ and the evidence message M$_{evi}$. Then IO uses the session key K$_{I\text{-}IO}$ to extract the subliminal message M$_S$ and M$_{evi}$ as follows:

$$M_S = (Sig_{I_2} - K_{I-IO}) \bmod p \quad \textbf{(13)}$$

$$M_{evi} = (Sig_{I_3} - K_{I-IO}) \bmod p \quad \textbf{(14)}$$

IO notifies the police to arrest the criminal.

In some application environments tags must be access controlled. Even though user may hold a registered mobile RFID reader, when querying a RFID tag, the system may still need to confirm the query limitations of that mobile RFID reader. Thus, RFID tags cannot send sensitive EPC arbitrarily.

2.3 The arbitration Phase

IO sends the evidence message and subliminal message to OA. Then, OA uses the evidence to arbitrate this case. The scenario of the arbitration phase is shown in Figure 3.

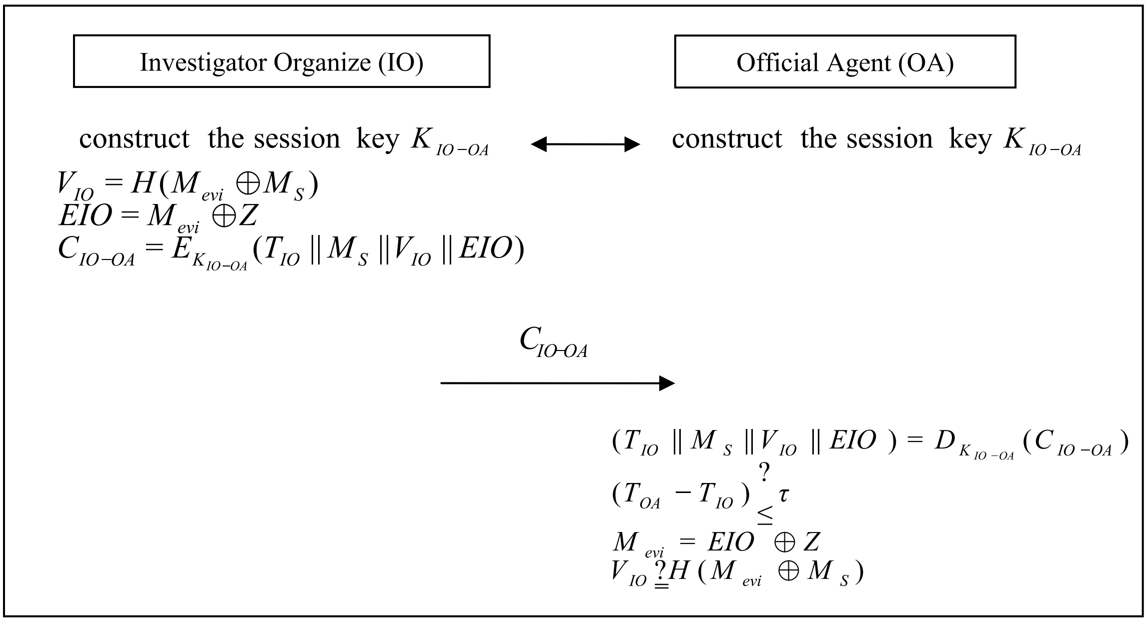
Investigator Organize (IO)
Official Agent (OA)
construct the session key K_{IO-OA}
construct the session key K_{IO-OA}
$V_{IO} = H(M_{evi} \oplus M_S)$
$EIO = M_{evi} \oplus Z$
$C_{IO-OA} = E_{K_{IO-OA}}(T_{IO} \| M_S \| V_{IO} \| EIO)$
$C_{IO\text{-}OA}$
$(T_{IO} \| M_S \| V_{IO} \| EIO) = D_{K_{IO-OA}}(C_{IO-OA})$
$(T_{OA} - T_{IO}) \overset{?}{\leq} \tau$
$M_{evi} = EIO \oplus Z$
$V_{IO} \overset{?}{=} H(M_{evi} \oplus M_S)$

Figure 3. The scenario of the arbitration phase

Step 1. IO and OA construct a session key K$_{IO\text{-}OA}$. **(15)**

Step 2. IO computes the parameter V$_{IO}$ **(16)**

$$V_{IO} = H(M_{evi} \oplus M_S),$$

and then computes the parameter EIO:

$$EIO = M_{evi} \oplus Z \quad \textbf{(17)}$$

After that, IO uses the session key K$_{IO\text{-}OA}$ to encrypt the timestamp T$_{IO}$, subliminal message M$_S$, parameter V$_{IO}$ and EIO:

$$C_{IO-OA} = E_{K_{IO-OA}}(T_{IO} \| M_S \| V_{IO} \| EIO) \quad \textbf{(18)}$$

Then IO sends the cipher message C$_{IO\text{-}OA}$ to the OA.

Step 3. After receiving the cipher message C$_{IO\text{-}OA}$ at T$_{OA}$, OA uses the session key K$_{IO\text{-}OA}$ to decrypt the message:

$$(T_{IO} \| M_S \| V_{IO} \| EIO) = D_{K_{IO-OA}}(C_{IO-OA}) \quad \textbf{(19)}$$

Then OA checks the timestamp T$_{OA:}$

$$(T_{OA} - T_{IO}) \overset{?}{\leq} \tau \quad \textbf{(20)}$$

If it holds, OA extracts the evidence message:

$$M_{evi} = EIO \oplus Z \quad \textbf{(21)}$$

After that, OA uses the evidence M$_{evi}$ and subliminal message M$_S$ to verify V$_{IO:}$

$$V_{IO} \overset{?}{=} H(M_{evi} \oplus M_S) \quad \textbf{(22)}$$

If the above equation holds, this case will enter the arbitration phase.

2.4 The Official Agent arbitration phase

In this phase, OA makes a fair arbitration by examining IO's evidence. IO takes the related evidence of illegal activity and crime information to OA. Then OA uses the related information and evidence to make a fair arbitration. The flowchart of the official agent arbitration phase is shown in Figure 4.

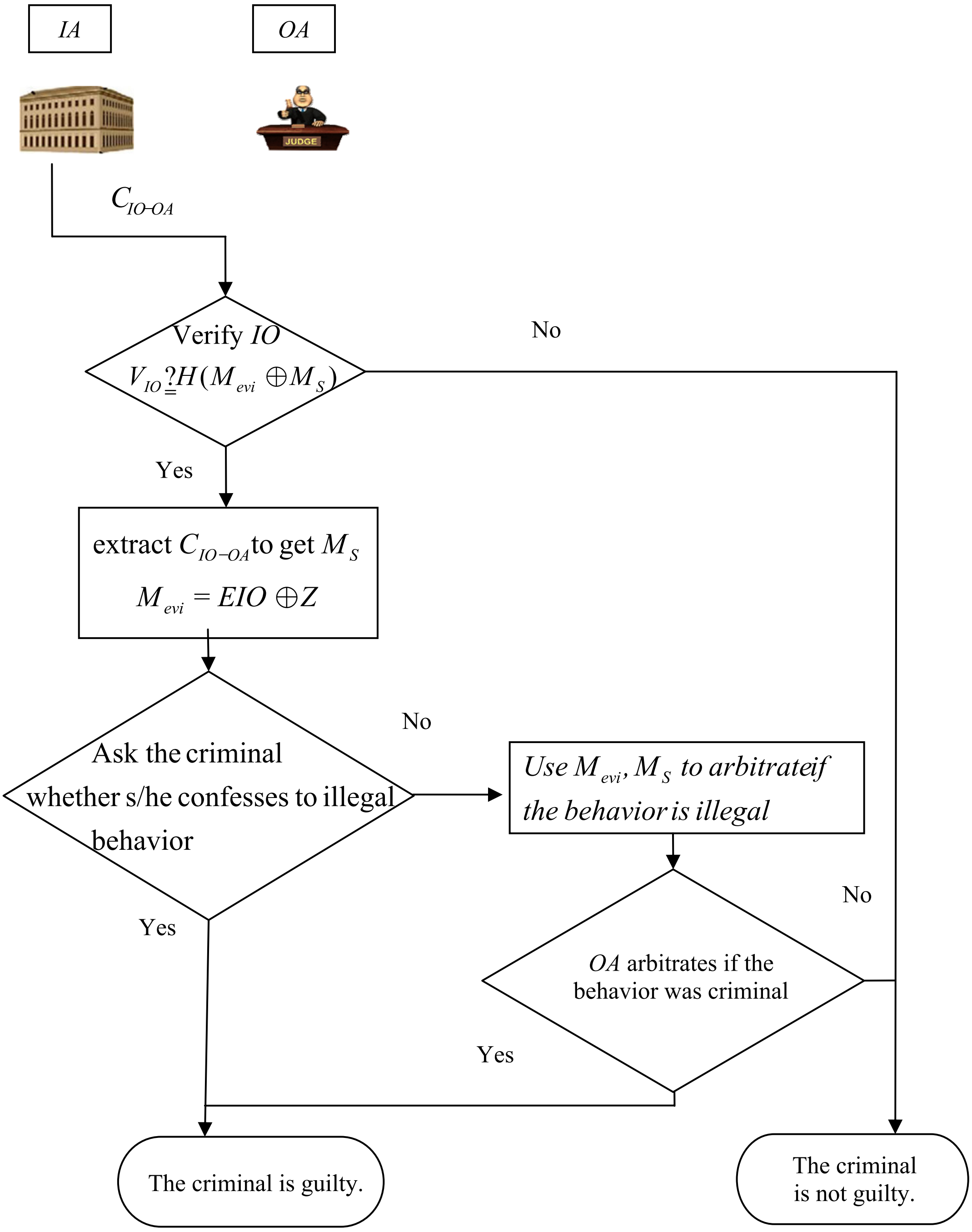
IA
OA
JUDGE
$C_{IO\text{-}OA}$
Verify IO
$V_{IO} \overset{?}{=} H(M_{evi} \oplus M_S)$
No
Yes
extract C_{IO-OA} to get M_S
$M_{evi} = EIO \oplus Z$
Ask the criminal whether s/he confesses to illegal behavior
No
Use M_{evi}, M_S to arbitrateif the behavior is illegal
Yes
OA arbitrates if the behavior was criminal
No
Yes
The criminal is guilty.
The criminal is not guilty.

Figure 4. The flowchart of the official agent arbitration phase

Step 1. IO sends the message $C_{IO\text{-}OA}$ to OA.

Step 2. When receiving the message $C_{IO\text{-}OA}$ from the IO, OA uses the session key $K_{IO\text{-}OA}$ to extract the message. Then OA uses Equation (22) to verify IO's identity.

If it holds, OA decrypts the subliminal message M_S and the evidence message M_{evi} (refer to Equations (19) and (21), respectively).

Step 3. After that, OA extracts the subliminal message and the evidence message to the criminal, and asks the criminal whether s/he confesses the illegal behaviors.

Step 4. If the criminal denies the case, OA will arbitrate the case in accordance with the subliminal message and the evidence message.

3 Security Analyses

3.1 Replay Attack

Because the timestamp T$_{IO}$ and T$_I$ is variable for each transaction, if a malicious attacker or criminal's partner wants to replay message C$_{IO\text{-}OA}$ (where $C_{IO-OA} = E_{IO-OA}(T_{IO} \| M_S \| V_{IO} \| EIO)$) and C$_{I\text{-}IO}$ (where $C_{I-IO} = E_{K_{I-IO}}(T_I \| Sig_{I_1} \| Sig_{I_2} \| Sig_{I_3} \| V_I \| H(M_{evi}))$) it will fail. So, the attacker cannot achieve the replay attack.

3.2 Forgery Attack

According to our scheme, if an attacker wants to forge the message, it is hard to do so. When IO receives the message, it must verify I's identity. Consequently, the attacker cannot achieve the forgery attack.

The derivation of the verification is shown as follows:

$$\begin{aligned}
&H((N^{Sig_{I_1}} \cdot g^{Sig_{I_3}} / g^{H(M_{evi})})^{Sig_{I_2} - K_{I-IO}} \| H(M_{evi})) \\
&= H((N^{Sig_{I_1}} \cdot g^{Sig_{I_3}} / g^{H(M_{evi})})^{M_s} \| H(M_{evi})) \\
&= H(((g^k)^{Sig_{I_1}} \cdot g^{Sig_{I_3}} / g^{H(M_{evi})})^{M_s} \| H(M_{evi})) \\
&= H(((g^k)^{k^{-1}(SK_I + H(M_{evi}) - M_{evi} - K_{I-IO})} \cdot g^{Sig_{I_3}} / g^{H(M_{evi})})^{M_s} \| H(M_{evi})) \\
&= H(((g^{SK_I + H(M_{evi}) - M_{evi} - K_{I-IO}} \cdot g^{M_{evi} + K_{I-IO}} / g^{H(M_{evi})})^{M_s} \| H(M_{evi})) \\
&= H(((g^{SK_I})^{M_s} \| H(M_{evi})) \\
&= H((PK_I{}^{M_s} \| H(M_{evi})) \\
&= V_I
\end{aligned}$$

3.3 Non-repudiation Issue

Our protocol involves the digital signature mechanism; we solve the non-repudiation issue. In the investigation phase, I cannot deny that I sent the subliminal message *M$_S$* and evidence message *M$_{evi}$* to IO because IO received and verified I's signature Sig_{I_1} Then, when receiving the message from IO, OA verified IO's signature. So, OA cannot deny the behavior via the digital signatures. The verifications are shown in Table 1.

Table 1. The non-repudiation issues

Non-repudiation proof	Proof issuer	Proof holder	Verification
$(V_I, Sig_{I_1}, Sig_{I_2}, Sig_{I_3}, M_S, M_{evi})$	I	IO	$V_I \overset{?}{=}$ $H((N^{Sig_{I_1}} \times g^{Sig_{I_3}} / g^{H(M_{evi})})^{Sig_{I_2} - K_{I-IO}} \| H(M_{evi}))$
$(V_I, Sig_{I_1}, M_S, M_{evi})$	IO	OA	$V_{IO} \overset{?}{=} H(M_{evi} \oplus M_S)$

3.4 Untraceable Issue

In our scheme, I and IO use the subliminal message to build the subliminal channel. Because we involve the subliminal message M$_S$ in an exponential operation: ($V_I = H(PK_I{}^{M_S} \| H(M_{evi}))$, the M$_S$ is difficult to obtain. If the M$_S$ is exposed, it will face the exponential operation problem. On the other hand, we use the session key to encrypt the signature and another parameter; it can protect the signature and the parameter will be exposed. Therefore, I's identity is untraceable via the subliminal message.

3.5 Fair Arbitration

In the arbitration phase, after receiving the message C$_{I\text{-}IO}$, OA will verify the IO's identity: $V_{IO} \overset{?}{=} H(M_{evi} \oplus M_S)$. The OA extracts the message C$_{I\text{-}OA}$ to obtain M$_S$ and computes the M$_{evi}$. Then OA uses M$_{evi}$ and M$_S$ to ask if the criminal confesses to illegal behavior. If the criminal denies this case, OA will arbitrate it based on M$_{evi}$ and M$_S$. Such a design can ensure that the criminal does not suffer from unfair arbitration.

4 Discussions

We show the computation cost and communication cost in Tables 2 and 3, respectively. We involve the evidence message M$_{evi}$ ($H((N^{Sig_{I_1}} \cdot g^{Sig_{I_3}} / g^{H(M_{evi})})^{Sig_{I_2} - K_{I-IO}} \| H(M_{evi}))$)

and subliminal message M$_s$ ($V_I = H(PK_I{}^{M_s} \| H(M_{evi}))$ in the exponential operation. Based on the discrete logarithm problem, the attacker cannot attack successfully. Therefore, it also enhances the system security. Although it requires more computation cost, the communication cost performance is good, as shown in Table 3.

Table 2. The computation cost of our scheme

Phase	computation cost
Investigation Phase	$2T_H$+$4T_{Sub}$+$3T_{Add}$+$2T_{Asym}$+$8T_{Exp}$
Arbitration Phase	$1T_H$ +$4T_{XOR}$ +$2T_{Asym}$

Notes. T_H is the time complexity of one-way hash function; T_{Sub} is the time complexity of subtraction; T_{Add} is the time complexity of addition; T_{Asym} is the time complexity for executing an asymmetric encryption / decryption operation; T_{Exp} is the time for executing the modular exponential operation; T_{Mut} *is the* time complexity for executing the modular multiplication; T_{XOR} is the time for exclusion or operation.

Table 3. The communication cost of our scheme

Phase	Communication cost	Data transmission time (ms)	
		300 Kbps	2 Mbps
Investigation Phase	2|*p*|+2|*H*|+|*p*-1|+|*t*|+|*sk*|	11.36+(|*sk*|/300)	1.704 +(|*sk*|/2048)
Arbitration Phase	2|*M*|+|*H*|+|*t*|+|*sk*|	0.64+(|*sk*|/300)	0.093+(|*sk*|/2048)

Notes. |*p*| is the length of a large prime (1024 bits); |*M*| is the length of the message (8 bits); |*H*| is the length of hash function (160 bits); |*t*| is the length of timestamp (16 bits); |*sk*| is the total communication amount (bits) during the construction of the session key.

5 Conclusions

We propose an investigator unearthing an illegal transaction via a subliminal channel. The proposed scheme can defend against the replay attack and forgery attack. It not only protects the investigator's safety, but also ensures the illegal evidence's reality. Because we use a subliminal channel to find and send evidence of illegal behavior to the investigating organization, it is difficult to unmask the investigator's identity. On the basis of the non-repudiated evidence (M_S and M_{evi}), our scheme achieves fair arbitration. The communication cost and computation cost of our scheme is acceptable.

Acknowledgements

This research was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract number MOST 106-2622-E-305-001-CC2, MOST 106-2221-E-324-013 and MOST 103-2632-E-324-001-MY3.

References

[1] G. J. Simmons, The Prisoner's Problem and the Subliminal Channel, D. Chaum (Ed.), *Advances in Cyptology*, Plenum Press, 1984, pp. 51-67.

[2] G. J. Simmons, The Subliminal Channel and Digital Signatures, *Proc. of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, Paris, France, 1984, pp. 364-378.

[3] G. J. Simmons, Subliminal Communication Is Easy Using the DSA, *Eurocrypt 93*, Lofthus, Norway, 1993, pp. 218-232.

[4] L. Harn, G. Gong, Digital Signature with A Subliminal Channel, *IEEE Proceedings-Computers and Digital Techniques*, Vol. 144, No. 6, pp. 387-389, November, 1997.

[5] D. R. Lin, C. I. Wang, Z. K. Zhang, D. J. Guan, A Digital Signature with Multiple Subliminal Channels and Its Applications, *Computers & Mathematics with Applications*, Vol. 60, No. 2, pp. 276-284, July, 2010.

[6] M. K. Franklin, M. K. Reiter, Fair Exchange with a Semi-trusted Third Party, *Proceedings of the 4th ACM Conference on Computer and Communications Security*, Zurich, Switzerland, 1997, pp. 1-5.

[7] J. Zhou, D. Gollman, A Fair Non-repudiation Protocol, *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, Oakland, CA, 1996, pp. 55-61.

[8] C. L. Chen, M. H. Liu, A Traceable E-cash Transfer System against Blackmail via Subliminal Channel, *Electronic Commerce Research and Applications*, Vol. 8, No. 6, pp. 327-333, November-December, 2009.

[9] C. L. Chen, J. J. Liao, A Fair Online Payment System for Digital Content via Subliminal Channel, *Electronic Commerce Research and Applications*, Vol. 10, No. 3, pp. 279-287, May-June, 2011.

[10] D. He, M. Ma, Y. Zhang, C. Chen, J. Bu, A Strong User Authentication Scheme with Smart Cards for Wireless Communications, *Computer Communications*, Vol. 34, No. 3, pp. 367-374, March, 2011.

[11] C. L. Chen, M. S. Lu, J. W. Li, C. Gong, L. Zhao, A Secure Public Transport Multimedia on Demand System for VANET, *Journal of Internet Technology*, Vol. 16, No. 7, pp. 1177-1188, December, 2015.

[12] A. K. Awasthi, K. Srivastava, R. C. Mittal, An Improved Timestamp-based Remote User Authentication Scheme, *Computers & Electrical Engineering*, Vol. 37, No. 6, pp. 869-874, November, 2011.

[13] W. J. Tsaur, Secure Communication for Electronic Business Applications in Mobile Agent Networks, *Expert Systems with Applications*, Vol. 39, No. 1, pp. 1046-1054, January, 2012.

[14] Y. Wang, M. H. Au, W. Susilo, Optimistic Fair Exchange in the Enhanced Chosen-key Model, *Theoretical Computer Science*, Vol. 562, pp. 57-74, January, 2015.

[15] C. L. Chen, M. L. Chiang, D. K. Li, W. C. Lin, A Novel Lottery Protocol for Mobile Environments, *Computers &*

Electrical Engineering, Vol. 49, pp. 146-160, January, 2016.

[16] Z. Eslami, M. Talebi, A New Untraceable off-line Electronic Cash System, *Electronic Commerce Research and Applications*, Vol. 10, No. 1, pp. 59-66, January-February, 2011.

[17] S. J. Lin, D. C. Liu, An Incentive-based Electronic Payment Scheme for Digital Content Transactions over the Internet, *Journal of Network and Computer Applications*, Vol. 32, No. 3, pp. 589-598, May, 2009.

[18] Internet Engineering Task Force (IETF) Working Group, *Diffie-Hellman Key Agreement Method*, RFC 2631, June, 1999.

Biographies

Chin-Ling Chen received his Ph.D. from National Chung Hsing University, Taiwan in 2005. From 1979 to 2005, He was a senior engineer at Chunghwa Telecom Co., Ltd. He is currently a distinguished professor. His research interests include cryptography and network security. He has published over 80 articles in SCI/SSCI international journals.

Tzay-Farn Shih received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taiwan, in 2006. He is presently an associate professor of Computer Science and Information Engineering at Chaoyang University of Technology. His research interests include computer simulation, computer networks, wireless networks and wireless sensor networks.

Kun-hao Wang received his PhD from JiLin University, China in 2014. He is a teacher in Changchun Sci-Tech University. His main research is bioinformatics, digital media and computer graphics. He has published two articles in SCI international journals.

Chien-Hung Chen received the B.S. degree in Department of Computer Science and Information Engineering from Chaoyang University of Technology, Taichung Taiwan in 2011. He received his Master's degree in the Department of Computer Science and Information Engineering, Chaoyang University of Technology in 2013. His research interests focus on information security.

Woei-Jiunn Tsaur received his Ph.D. degree from National Taiwan University of Science and Technology, Taiwan, in 1998. Since 2016, he has been with the Computer Center at National Taipei University, Taiwan, where he is currently a Full Professor. His research interests include network security and applied cryptography.