A Receiver Deniable Encryption Scheme
Bo Meng¹, and JiangQing Wang²
¹ School of Computer South-Center University for Nationalities, Wuhan, China
Email: mengscuec@gmail.com
² School of Computer South-Center University for Nationalities, Wuhan, China
Email: wjqing2000@yahoo.com.cn

Abstract—A practical efficient receiver deniable encryption scheme based on BCP commitment scheme and idea of Klonowski et al. is proposed in the paper. The analysis of the proposed schemes is also presented.

Index Terms—deniable encryption, BCP commitment scheme, protocol security

I. INTRODUCTION

Deniable encryption can be used against revealing information that the owner of the information may decrypt it in an alternative way to a different plaintext. Namely if this user opens all his inputs including the claimed encrypted message to a coercer, the coercer fails to prove the validity or invalidity of the opened message.

The notion of deniable encryption was introduced by Canetti et al. in 1996 [1]. Deniable encryption is an important cryptographic primitive, essential in all cryptographic protocols where a coercive adversary comes to play with high potential. Deniable encryption can be used to develop the receipt-freeness and coercion-resistance in the internet/electronic voting protocols and ineletronic bidding, electronic auctions and secure multiparty computation.

In the last several decades people have focused on developing more practical efficient deniable encryptions. Canetti et al. [2] propose a public-key deniable encryption, which includes basic and party deniable schemes, and a shared-key deniable encryption, which includes a one-time-pad and plan-ahead shared-key deniable schemes. Assangne and Weimann [3] propose a deniable encryption file system called Rubberhose file system. But their deniable can not be used in network communication. Rjasková [4] proposes a sender-deniable public-key deniable encryption based on RSA cryptosystem. The deniable encryption is very inefficient. Sending 1 bit through the deniable encryption means sending 10⁵ bits through the public channel. Klonowski et al. [5] expand the schemes [2] and propose a receiver deniable encryption scheme based on the ElGamal cryptosystem and apply it to implement the covert channel. But their deniable scheme is not suitable to the large scale networks.

The rest of this paper is organized as follows: Section II presents the proposed efficient receiver deniable encryption scheme. Section III gives an analysis of the security property. Finally, the conclusions are given in Section IV.

II. THE PROPOSED PRACTICAL EFFICIENT RECEIVER DENIABLE ENCRYPTION SCHEME

A. Assumptions and Model

We define a receiver-deniable encryption scheme as a scheme by which, the receiver is able to lie about the decrypted message to a coercer and hence, escape coercion. On one hand, the receiver is able to decrypt the correct message, on the other hand, all the information held by the receiver when opened to a coercer, do not allow this coercer to verify the encrypted message or the coercer can not find the message is a fake message. Consequently, approaching the receiver becomes useless from the very beginning.

The participants in our scheme are the sender, the receiver and the coercive adversary. As usual, the sender is assumed to be beyond the reach of any coercer while the receiver is possibly coerced.

The coercer has the power to approach the receiver coercing him to reveal the decrypted message, the decryption key and all the parameters he used during decryption. In our proposed receiver deniable encryption scheme, we assume that the coercer has the ability to eavesdrop the communication channels.

B. The proposed deniable encryption scheme

The proposed deniable encryption scheme consists of preliminaries, encryption, decryption and dishonest opening phases. In preliminaries phase the sender and receiver generate their public/private keys based on BCP cryptosystem. At the same time the receiver generate his public/private keys based on ElGamal cryptosystem [10, 11]. In encryption phase the sender produces the ciphertext (c, φ) using the idea of Klonowski et al [5] and commitment B = C(r, m) based on BCP commitment scheme. In decryption phase the receiver encrypt scheme based on mediated RSA PKI and oblivious transfer protocol. But deniability in the scheme is worth discussing. All above these schemes is either low efficient or is implemented with physical assumptions or is not suitable to the large scale networks.

Motivated by this we propose an efficient deniable encryption scheme based on idea of Klonowski et al. [5] and the BCP commitment scheme and cryptosystem [9].

Corresponding author: Bo Meng, School of Computer South-Center University for Nationalities, Wuhan, China, 430074.
decrypts $B = C (r, m)$ with his private key based on BCP cryptosystem gets the message $m$. In dishonest opening phase the receiver decrypt $(\check{\phi}, \phi)$ with his private key based on ElGamal cryptosystem and gets the random number $r_1, r_2$. Then he uses $m$ and $r_2$ to generate $m'$ which has $B = C (r, m) = C (r, m')$. Finally he provides $m'$ and $r_1$ to coercer and escape the coercion owning to coercer can not find $m'$ is a fake message.

**Preliminaries**

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a \in \mathbb{Z}_N$</td>
<td>$\check{\phi}$</td>
</tr>
<tr>
<td>$g^{a \cdot \text{ord}(G)} \mod N^2$</td>
<td>$\phi$</td>
</tr>
<tr>
<td>$h \mod N^2$</td>
<td>$G_{\text{hash}(v_2)}^{r_1}$</td>
</tr>
<tr>
<td>${p, q, g, h}$; $a$</td>
<td>$r_1, r_2, m_2 \cdot d, N_2 \mod N_2 / 2$</td>
</tr>
<tr>
<td>$r_1, r_2, m_2 \cdot d, N_2 / 2$</td>
<td>$B \cdot G_{\text{hash}(v_2)}^{r_1}$</td>
</tr>
</tbody>
</table>

Figure 1. Preliminaries

The receiver chooses a random element $a \in \mathbb{Z}_N$, and sets $g = a^{-1} \mod N^2$, publishes publicly $(N, g)$. Then the sender gets $(N, g)$ and chooses a random number $a \in [1, \text{ord}(G)]$, computes $h = g^a \mod N^2$ and publish publicly $(g)$. The public key of the receiver is given by the triplet $(N, g, h)$, while the corresponding secret key is private key $(p, q)$. At the same time the sender can generates his public key $(N, g, h)$ and private key $a$ based on BCP cryptosystem. Finally he creates his private key $a$ and public key $y = g^a \mod p$ according to ElGamal cryptosystem. Because everyone can know the public key $(N, g, h)$ of the sender, the receiver can get the sender’s private key $a$ owning to the knowledge of $h = g^a \mod N^2$ and $N = p \cdot q$. Figure 1 describes the key generation of the sender and receiver. Note that $a$ is the private key of the sender based on both ElGamal cryptosystem and BCP cryptosystem. Figure 1 describes the preliminaries.

**Encryption**

The sender choose random numbers $r_1, r_2 \in \mathbb{Z}_N$, after that the sender generate the message $m \in \mathbb{Z}_N$, which will be sent to the receiver in deniable encryption scheme. The sender computes $B = C (r, m) = C (r_1, m) = h^r (1 + mN) \mod N^2$ based on BCP commitment scheme. Generating the fake message $m'$, he can find $r_1 = r_2 + (m - m')d \mod N \mod N \div 2$ which make $B = C (r_2, m') = C (r_1, m')$. Then he computes $(\check{\phi} = g_{\text{hash}(v_2)}, \phi = (g_{\text{hash}(v_2)} \cdot r_1^{-d} \cdot r_2)$ using ElGamal cryptosystem. $(\check{\phi}, \phi)$ is the ciphertext of $r_2$. Finally he sends $(\check{\phi}, \phi)$ and $B = C (r, m)$ to the receiver. Figure 2 describes the procedure of encryption.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r_2 \cdot {g}$</td>
<td>$m \cdot a$</td>
</tr>
<tr>
<td>$B = C (r, m) = C (r_1, m')$</td>
<td>$\check{\phi} \cdot \phi \cdot h \cdot 1 \cdot mN \cdot h^r$</td>
</tr>
<tr>
<td>$r_1, r_2, m_2 \cdot d, N_2 \mod N_2 / 2$</td>
<td>$B \cdot G_{\text{hash}(v_2)}^{r_1}$</td>
</tr>
</tbody>
</table>

Figure 2. Procedure of encryption

**Decryption**

The receiver uses the private key $(p, q)$ to recover $m = \frac{D - 1 \mod N^2}{N} \cdot \pi \mod N$ based on BCP cryptosystem. Figure 3 describes the procedure of decryption.

**Dishonest Opening**

The receiver uses the private key $a$ to recover the plaintext $r_2 = \check{\phi} \cdot \phi^{-a} = (g^a \cdot r_1) \cdot r_2 (g_{\text{hash}(v_2)} \cdot r_1)^{-a}$, then he can compute $\text{hash}(r_1)$, and gets $r_1 = \check{\phi} \cdot G_{\text{hash}(v_2)}^{r_1}$. The receiver computes $A_1 = g^a \mod N^2$ and $A_2 = g^a \mod N^2$ based on BCP cryptosystem, then he recovers $m_1 = \frac{B / (A_1^a \cdot 1 \mod N^2)}{N}$ and...
In order to escape the coercion the receiver must generate a fake message $m'$. With $m'$, the coercer can get $B = C(r', m') = C(r, m) = C(r_2, m)$.

Given $r'' = r_1$, according the proposed deniable encryption scheme, the receiver can get $m' = \frac{C(r, m)}{h'' - 1} \mod N^2$. Finally the receiver can claim $m'$ is sent by the sender. The coercer can not found the truth.

Hence the proposed deniable encryption scheme is receiver deniability.

IV. CONCLUSION

In this paper we propose a practical efficient receiver deniable encryption scheme based on BCP commitment scheme and idea of Klonowski et al. [5]. The proposed scheme is a one-move scheme without any pre-encryption information required to be sent between the sender and the receiver prior to encryption. Moreover, the overhead is low in term of the size of the ciphertext.

REFERENCES


**Bo Meng** was born in 1974 in People’s Republic of China. He received his M.S. degree in computer science and technology, Ph.D. degree in traffic information engineering and control from Wuhan University of Technology, at Wuhan, People’s Republic of China, in 2000, 2003, respectively. From 2004 to 2006, he works in Wuhan University, People’s Republic of China as Postdoctoral researcher in information security.

Currently he is an Associate Professor of school of computer, South-Center University for Nationalities, in People’s Republic of China. He has authored/coauthored over 40 papers in International/National journals and conferences. His current research interests include electronic commerce, internet voting, and protocol security.

**JiangQing Wang** was born in 1964 in People’s Republic of China. She received his M.S. degree and Ph.D. degree in computer science and technology from Wuhan University, at Wuhan, People’s Republic of China, in 1989, 2007, respectively. From 2000 to 2001, she is a visiting scholar in Chonbuk National University, South Korea. From 2006 to 2007, she gets a visiting scholar position in University of Wisconsin in USA.

Currently she is a professor and dean of school of computer, South-Center University for Nationalities, in People’s Republic of China. She has authored/coauthored over 50 papers in International/National journals and conferences. Her current research interests include protocol security, artificial intelligence. She has overall charge of a National Natural Science Funds of China