Electronic Funds Transfer Protocol Using Domain-verifiable Signcryption Scheme

Moonseog Seo and Kwangjo Kim

ICU, 58-4 Hwaam-dong, Yusong-gu
Taejon, 305-350, S. KOREA
{msseo,kkj}@icu.ac.kr

Abstract. In this paper, we propose Domain-verifiable signcryption scheme, which is applied to the Electronic Funds Transfer(EFT) protocol, that only predetermined n participants within the domain of protocol participants can decrypt their own part of message and verify whole transaction. The computational cost of our scheme is as low as that of Zheng's scheme assuming that Trusted Third Party(TTP) must be used to keep partial information for participants confidential and multi-verification. Our scheme does not require the role of TTP.

1 Introduction

The Electronic Funds Transfer(EFT) protocol is most widely used for transfering money between the financial institutions. The protocol requires both confidentiality and authentication services simultaneously. Efficiency is a factor that must be fulfilled in financial systems. The efficiency is achieved by applying signcryption scheme to EFT protocol. The Signcryption[9], which is first proposed by Zheng, is a new cryptographic primitive called *"catch two birds with single stone"* scheme. This simultaneously fulfills both the functions of signature and encryption in a single logical step, and reduces computational cost which is significantly lower than that required by the traditional signature-then-encryption paradigm [3, 6, 9].

In application to EFT protocol in multiple participants environment, the signcryption scheme needs modification so that only predetermined n participants within a domain can decrypt their own part of message and verify whole transaction. We call this modified signcryption scheme Domain-verifiable signcryption scheme where domain means a set of participants involved in a transaction protocol. In Zheng's signcryption scheme, the unsigncryption (decryption and signature verification) needs the recipient's private key; therefore, only the recipient can verify the signature. So, Zheng's signcryption schemes have some constraints to be used in applications where a signature needs to be validated by any others. To overcome this problem, Bao and Deng[1] modified Zheng's signcryption scheme such that verification of a signature no longer needs the recipient's private key. However, Bao and Deng's scheme is not as efficient computationally as Zheng's scheme. Also in their scheme, the message must be decrypted before it is verified by other people ending up losing confidentiality. To maintain the confidentiality and also to be used in firewall application, Gamage, Leiwo and Zheng[4] proposed the signcryption for third-party verification. But in this scheme, whereas any verifier can verify the signature, only one person can obtain the whole plaintext message.

In EFT protocol usage, there exist many participants for one transaction. A transaction consists of secret information to be processed by each participant. Each participant requires confidentiality for his own secret information. Also all participants need authentication of that whole transaction. Signcryption schemes[1, 4, 9] proposed previously cannot be directly used in this situation.

In this paper, we propose Domain-verifiable signcryption scheme based on Gamage, Leiwo and Zheng's signcryption that can be easily applicable to the EFT and Secure Electronic Transaction(SET) protocol[7] that many participants within domain can keep their own part of message confidentially and verify the whole transaction. Also we sketch EFT protocol between two banks using the Domain-verifiable signcryption. The computational cost of our scheme is as low as Zheng's scheme with assuming that Trusted Third-Party(TTP) must be used for keeping partial information for participants confidential and multi-verification. When we use Domain-verifiable signcryption, we can construct EFT protocol without interaction of TTP.

The rest of the paper is organized as follows. The signcryption schemes proposed until now are described briefly in Section 2. The proposed scheme for domain-verification is discussed in Section 3. Section 4 provides the application of our scheme with financial EFT protocol. Finally concluding remarks are given in Section 5.

2 Related Work

We describe three signcryption schemes proposed until now. The original signcryption primitive proposed in [9] by Zheng combines the sign-then-encrypt two step process to create a secure authenticated message into a single logical step with significant savings in both computational and transmission costs. A disadvantage for some applications such as EFT protocol in which more than two participants involved is that only the intended recipient can verify the message. A modified signcryption scheme was proposed in [1] by Bao and Deng to overcome this limitation. But it has the increased computational cost while still preserving the transmission cost savings achieved by the original scheme. Two disadvantages of this modified signcryption scheme are :

- The signature verification-only mode of operation can be used only after the original recipient has recovered the plaintext message.
- The plaintext message must be forwarded to a third party for signature verification and the message confidentiality can be lost.

In [4], Camage, Leiwo and Zheng modified Bao and Deng's scheme to carry out signature verification without accessing the plaintext for preserving confidentiality of the original message without altering sign-then-encrypt paradigm. But in this scheme, whereas any verifier can verify the signature, only one person to unsigncrypt signcrypted message can obtain the whole plaintext message.

Therefore, these all schemes could not be applied directly for EFT protocol which transaction consists of partial information for each participant that requires confidentiality about his own information even against other protocol participants.

2.1 Zheng's Scheme

Task: Alice has a message to send to Bob. Alice signcrypts it so that the effect is similar to signature-then-encryption.

Public Parameters :
p : a large prime
q : a large prime factor of $p-1$
g : an element of Z_p^* of order q
$hash$: a one-way hash function
KH : a keyed one-way hash function
(E, D) : the encryption and decryption algorithms of a symmetric key cipher
Alice's key :
$x_a \in Z_q^*$: Alice's private key, $y_a = g^{x_a} \bmod p$: Alice's public key
Bob's Keys :
$x_b \in Z_q^*$: Bob's private key, $y_b = g^{x_b} \bmod p$: Bob's public key

Signcrypting : Alice randomly chooses $x \in Z_q^*$ then sets
$(k_1, k_2) = hash({y_b}^x \bmod p)$
$c = E_{k_1}(m)$
$r = KH_{k_2}(m)$
$s = x/(r + x_a) \bmod q$.
Alice sends (c, r, s) to Bob.

Unsigncrypting : Bob computes
$(k_1, k_2) = hash((y_a g^r)^{s x_b} \bmod p)$,
$m = D_{k_1}(c)$ to recover the plaintext message, and then checks whether $KH_{k_2}(m) = r$ for signature verification. In unsigncrypting process, it is straightforward to see that x_b is involved for signature verification.

2.2 Bao and Deng's Scheme

Signcrypting : Alice randomly chooses $x \in Z_q^*$ then sets
$k_1 = hash({y_b}^x \bmod p)$
$k = hash(g^x \bmod p)$
$c = E_{k_1}(m)$
$r = KH_k(m)$
$s = x/(r + x_a) \bmod q$.
Alice sends (c, r, s) to Bob.

Unsigncrypting : Bob computes
$t_1 = (y_a g^r)^s \bmod p$
$t_2 = {t_1}^{x_b} \bmod p$
$k_1 = hash(t_2)$
$k = hash(t_1)$,
$m = D_{k_1}(c)$ to obtain the plaintext message, then checks whether $KH_k(m) = r$ for signature verification.

Later when necessary, Bob may forward (m, r, s) to others, who can be convinced that it came originally from Alice by verifying $k = hash((y_a g^r)^s \bmod p)$ and $r = KH_k(m)$.
In this signature verification, verifiers require to get the plaintext message.

2.3 Gamage, Leiwo and Zheng's Signcryption for Third-Party Verification

Signcrypting : Alice randomly chooses $x \in Z_q^*$ then sets
$k = hash({y_b}^x \bmod p)$
$y = g^x \bmod p$
$c = E_k(m)$
$r = hash(y, c)$
$s = x/(r + x_a) \bmod q$.
Alice sends (c, r, s) to Bob.

Unsigncrypting : Bob will compute from (c, r, s)
$y = (y_a g^r)^s \bmod p$
$k = hash(y^{x_b} \bmod p)$,
$m = D_k(c)$ to obtain the plaintext message.
Bob accepts signature if and only if $hash(y, c) = r$.

For partial unsigncryption with signature verification-only, any verifier will compute from (c, r, s) and $y = (y_a g^r)^s \bmod p$.
Any verifier accepts signature if and only if $hash(y, c) = r$.
This signature verification does not require access to the plaintext message.

3 Domain-verifiable Signcryption Scheme

Within domain of protocol participants, each participant wants to be maintained his own message included in transaction secretly even against any other participants. Also, all participants require to authenticate the transaction that consists of participants secret partial information. We construct the Domain-verifiable signcryption scheme that satisfys these requirements. Each participant can decrypt just his own message and all participants can verify the whole transaction. This scheme could be applied to EFT protocol as well as any other protocols like SET protocol that need to be kept participant's partial information secret and to be authenticated total message by all participants simultaneously.

3.1 Scheme for Domain Verification

For consistency, we use the same notations as in Zheng's scheme except recipients' key.

Recipient B_i's Keys within domain of n participants ($i \in \{1, \ldots, n\}$)
$x_{b_i} \in Z_q^*$: B_i's private key
$y_{b_i} = g^{x_{b_i}} \bmod p$: B_i's public key

Signcrypting : Alice randomly chooses $x \in Z_q^*$ then sets
$k_1 = hash({y_{b_1}}^x \bmod p), k_2 = hash({y_{b_2}}^x \bmod p), \ldots, k_n = hash({y_{b_n}}^x \bmod p)$
$k = hash(g^x \bmod p)$
$c_1 = E_{k_1}(m_1), c_2 = E_{k_2}(m_2), \ldots, c_n = E_{k_n}(m_n)$
$r_1 = KH_k(m_1||c_2||\cdots||c_n), r_2 = KH_k(c_1||m_2||\cdots||c_n), \ldots,$
$r_n = KH_k(c_1||c_2||\cdots||m_n)$
$s = x/(r_1 r_2 \cdots r_n + x_a) \bmod q$.
Alice sends $(c_1, c_2, \ldots, c_n, r_1, r_2, \ldots, r_n, s)$ to B_n.

Unsigncrypting : Recipient B_i computes
$t = (y_a g^{r_1 r_2 \cdots r_n})^s \bmod p$
$t_i = t^{x_{b_i}} \bmod p$
$k = hash(t)$
$k_i = hash(t_i)$,
$m_i = D_{k_i}(c_i)$ to obtain B_i's own plaintext message, then checks whether $KH_k(c_1||\cdots||m_i||\cdots||c_n) = r_i$ for signature verification.

Later when necessary, B_i may forward $(c_1, c_2, \ldots, c_n, r_1, r_2, \ldots, r_n, s)$ to any other participants, who want to decrypt his own message and can be convinced that it came originally from Alice by executing through this unsigncrypting.

3.2 Performance and Security

We should consider a situation where Domain-verifiable signcryption scheme must be used. If we use Zheng's scheme, TTP must be involved to divide message into partial messages for each participant and signcrypt the partial message for the corresponding participant[10]. But our Domain-verifiable signcryption scheme does not need TTP. While considering only exponentiation cost as the computational cost and n participants, Domain-verifiable signcryption requires $n + 1$ modulo exponentiations for signcryption and $3n$ modulo exponentiations for unsigncryption. In the general case of n participants more than 2 or 3 participants are involved, the communication bandwidth of our scheme is not lower than that of the Zheng's scheme, since the whole transaction message for n participants must be always transferred.

It can be done only within domain of protocol participants to unsigncrypt message, since a participant B_i having his own secret key x_{b_i} within a domain can obtain partial information m_i and the only person who gets m_i can try to check if $KH_k(c_1||\cdots||m_i||\cdots||c_n) = r_i$ for signature verification. Any other persons that have not secret x_{b_i} will not be able to take part in unsigncryption.

In [4], they not only provide the formal proof based on the random oracle model about the security argument about the computation of two values, ${y_b}^x \bmod p$ and $g^x \bmod p$ using the same secret x, but also show the pseudo-independence of two computed values as an adequate guarantee of security for the signature scheme. Namely, if a signer chooses the integer x uniformly and randomly, then two values are (pseudo) independent as both g and $y_b = g^{x_b} \bmod p$ are generators in Z_p^* of order q which is a prime. This ensures that the signature verification and partial recovery of bits does not leak information that can be used in an attack on breaking message confidentiality or signature forgery. We can consider to apply this method to our scheme. According to this security analysis, if a signer chooses the integer x uniformly and randomly, then $n+1$ values such as ${y_{b_1}}^x \bmod p, \ldots, {y_{b_n}}^x \bmod p$ and $g^x \bmod p$ in Domain-verifiable signcryption are (pseudo) independent as $g, y_{b_1} = g^{x_{b_1}} \bmod p, \ldots, y_{b_n} = g^{x_{b_n}} \bmod p$ are generators Z_p^* of order q which is a prime. This guarantees that Domain-verifiable signcryption scheme has message confidentiality and signature unforgeability.

4 EFT Protocol Based on Domain-verifiable Signcryption

EFT is considered to be any transfer of funds, other than a transaction by check, draft, or similar paper instrument, that is initiated through an electronic terminal, telephone, computer or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account. In the inter-bank EFT protocol, withdrawal accounts and deposit accounts are placed in different banks. A client should request EFT transaction to the bank that has business relations with him. The bank that receives the request draws the corresponding money from the requester's account and asks the deposit bank to deposit the same amount of money to recipient's account. The withdrawal bank that receives the result of deposit from a deposit bank informs the client who requests the EFT transaction of the final result of the funds transfer [2].

The message that clients send to the withdrawal bank will be constituted of client's information such as his own account number and PIN (Personal Identification Number), and recipient's information such as deposit bank name, deposit account number and amount of money to be transferred, *etc.* This message has to be encrypted and signed for privacy and integrity. In detail, client's information is encrypted for withdrawal bank and recipient's information is encrypted for deposit bank. Also the transaction for EFT protocol has to be authenticated by both withdrawal and deposit banks.

To use signcryption scheme at the inter-bank EFT protocol, we need TTP when using Zheng's scheme. But when using Domain-verifiable signcryption, we don't need TTP as shown in Fig. 1.

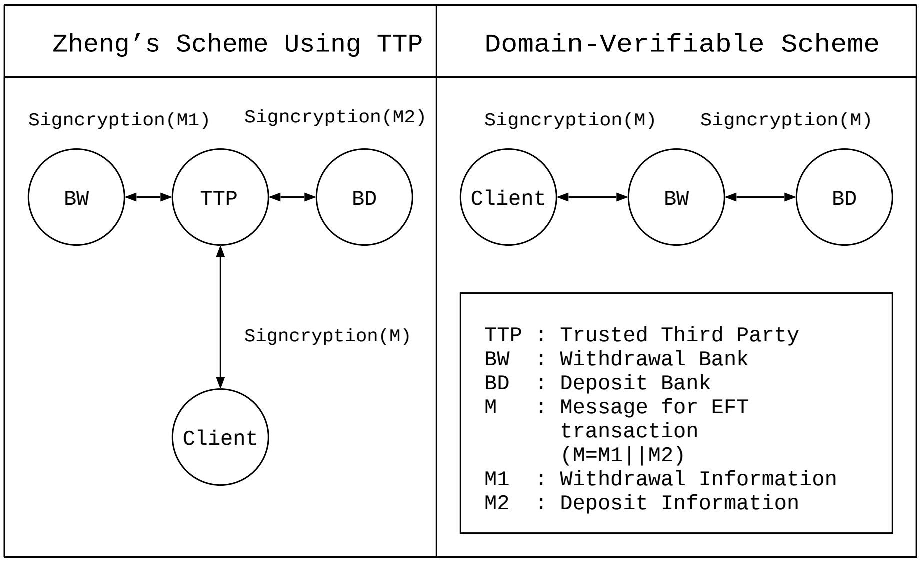

Fig. 1. EFT protocol using the signcryption schemes

4.1 Inter-bank EFT Protocol

We use the following notations to describe this protocol.

Participants and Tools
Client : A
Withdrawal Bank : BW
Deposit Bank : BD
$Signcrypt_A(\bullet)$: Domain-verifiable signcryption by client A including signature-only mode[9]
$Unsigncrypt_A(\bullet)$: Domain-verifiable unsigncryption by client A
$Sign_A(\bullet)$: signature-only mode of signcryption by client A
$||$: message concatenation
$hash(\bullet)$: hash algorithm

Preparation
Creation of funds transfer information : $M = M_1||M_2||COM$

- M_1 : Client A's information such as withdrawal account number and PIN, encrypted for withdrawal bank
- M_2 : Deposit information such as deposit bank and deposit account number, encrypted for deposit bank
- COM : Common data for EFT such as amount of money to be transferred, date, sequence number and recipient's name, *etc.* This data should be maintained as plaintext for the transaction processing.

Transfer Protocol

1. Client A generates $SM = (c_1, c_2, COM, r_1, r_2, s)$ where $c_1 = E_{k_1}(M_1), c_2 = E_{k_2}(M_2), r_1 = KH_k(M_1||c_2||COM), r_2 = KH_k(c_1||M_2||COM)$ and $s = x/(r_1 r_2 + x_A) \bmod q$ through $Signcrypt_A(M)$ and then A sends SM to the withdrawal Bank, BW.
2. BW processes $Unsigncrypt_A(SM)$ to decrypt his own message M_1 from c_1 and verifies SM.
3. After BW checks whether if the request is replayed by date and sequence number in the message, BW draws money from A's account in M_1 and sends SM to deposit bank BD.
4. BD processes $Unsigncrypt_A(SM)$ to decrypt his own message M_2 from c_2 and verifies SM.
5. After BD checks whether if the request is replayed by date and sequence number in the plaintext COM, BD deposits money to the corresponding account using the decrypted M_2.
6. BD generates $r = Sign_{BD}(SM||\text{Result of Deposit})$ and then sends (Result of Deposit, r) to the BW.
7. BW does the necessary job according to the result of deposit that received from BD and generates $\hat{r} = Sign_{BW}(\text{Result of Transfer})$. And then BW sends (Result of Transfer, $\hat{r}$) to client A.
8. Client A can use the received (Result of Transfer, $\hat{r}$) as receipt for counterpart of transfer.

4.2 Security Consideration

The security of the inter-bank EFT protocol based on Domain-verifiable signcryption is summarized as below.

- Confidentiality : An adversary cannot recover the message M that transferred between a client and the banks because that message is encrypted for the corresponding bank before the transmission. Specially PIN in M_1, client's secret information for making withdrawal is not compromised by any others except only withdrawal bank.
- Authentication and Integrity : To send a fund transfer message, a client must sign on that message using his own private key. The banks that received a fund transfer message can authenticate the client who sends that message using the private key for the client. Also the banks can determine the integrity of the received message, since that message is signed by the client.
- Non-repudiation : A client's signature on the fund transfer message for a transaction can be used for the evidence[5, 8] of an user's request for EFT.
- Replay attack : If an adversary tries to replay the protocol, the bank can detect the message replayed by checking whether if the date and sequence number in the message are duplicated with the message that already has received.

- Usage as receipt : The result of a transfer along with signature from the bank can be used as a receipt for the result of funds transfer to the recipient. The recipient can verify the receipt that received from requester of funds transfer using the bank's public key.

5 Concluding Remarks

We proposed Domain-verifiable signcryption scheme applicable to the situation that only predetermined n participants can decrypt and verify within a domain. This scheme is useful when each participant can decrypt his own message that is partial information of the whole transaction message and all participants can verify the whole transaction message.

As an example application, we designed inter-bank EFT protocol based on the Domain-verifiable signcyption scheme. We found that this inter-bank EFT protocol is so efficient that it can be used at the real world. The detailed designs of multi-level hierarchical key distribution or SET protocol based on our Domain-verifiable signcryption need further research.

Acknowledgments

The authors would like to express great thanks to Pil Joong Lee, Kunsoo Park and Sangjae Moon for their useful discussions on our manuscript.

References

1. F.Bao and R.H.Deng, "A signcryption scheme with signature directly verifiable by public key,"Proc. of PKC'98, LNCS, Vol. 1431, Springer-Verlag, pp. 55-59, 1998.
2. Electronic Funds Transfer Act (EFTA), 15 U.S.C. Sec. 1693.
3. T.ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms,"IEEE Transactions on Information Theory, IT-31(4):469-472, 1985.
4. C.Gamage, J.Leiwo, and Y.Zheng, "Encrypted message authentication by firewalls,"Proc. of PKC'99, LNCS, Vol. 1560, Springer-Verlag, pp. 69-81, 1999.
5. K. Kim, S. Park, and J. Baek, "Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol,"Proc. of 1999 ICPP Workshops on Security(IWSEC), pp. 140-145, IEEE Computer Society, Sep. 21-22, 1999
6. C.P. Schnorr, "Efficient identification and signature for smart cards,"Advances in Cryptology- CRYPTO '89, LNCS 435, Springer-Verlag, pp. 239-251,1989.
7. Visa International and MasterCard International, Secure Electronic Transaction(SET) Specification book 1:Business Description, May 1997.
8. J. Zhou and D.Gollmann, "Observation on non-repudiation,"Advances in Cryptology- ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp. 133-144, 1996.
9. Y. Zheng, "Digital signcryption or how to achieve cost(signature and encryption) $<<$ cost(signature)+cost(encryption),"Advances Cryptology-CRYPTO'97, LNCS 1294, Springer- Verlag, pp. 165-179, 1997.
10. Y. Zheng, "Signcryption and its application in efficient public key solutions,"Proc. of Information Security Workshop(ISW'97), LNCS, Vol. 1396, Springer-Verlag, pp. 291-312, 1998.