A Tripartite Signcryption Scheme with Applications to E-Commerce

Yasmine Abouelseoud
Faculty of Engineering,
Alexandria University
Alexandria, Egypt

ABSTRACT

Achieving confidentiality and authentication in e-commerce transactions are among the primary security goals. In this paper, a new cryptographic scheme is proposed which guarantees the authenticity of the customer and ensures the confidentiality of the communications among the bank, the merchant and the customer. The proposed solution is the use of a tripartite signcryption scheme with low computational and communications overhead. A variant of the proposed scheme that enables a firewall to authenticate the origin of the ciphertext without disclosure of the contents of the original plaintext message is also presented.

General Terms

Cryptography, Security.

Keywords

Public key cryptography, Signcryption, E-commerce.

1. INTRODUCTION

The rapid development in communication technologies and the Internet has created new applications such as monetary transactions over the Internet. This prompted the need for efficient security mechanisms to protect those involved in the electronic transaction from each other as well as from outsiders. Among the primary goals of such mechanisms are confidentiality of the communicated data and authenticating the identities of the communicating parties. Confidentiality refers to keeping the communicated information secret to the intended communicants. On the other hand, authentication refers to verifying the identities of all entities involved in a conversation.

In an electronic transaction, there are three entities involved. These are the customer, the merchant and the payment gateway. One of the most widely accepted mobile payment protocols is the Secure Electronic Transaction (SET) protocol. It is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. It defines a framework that enables users to perform financial transactions through existing payment systems over public channels in a much more secure and reliable manner [1].

The traditional method to achieve the aforementioned security goals is to digitally sign a message with the private key of the sender then encrypt the message and the signature with a randomly chosen key using a symmetric cipher. The random key is then encrypted using the public key of the receiver. The encrypted (message + signature) is then sent together with the encrypted symmetric key. The reverse process is run at the receiver's end.

Signcryption is an effective public key cryptographic primitive ensuring both confidentiality and data origin authenticity. It combines the functionalities of a digital signature and encryption in a single logical step. It has been extensively studied by numerous researchers in an attempt to enhance the efficiency and security of the original scheme proposed by Zheng in 1997 [2]. In particular, its extension to the multi-recipient setting has received much attention [3,4].

In this paper, a new tripartite signcryption protocol is proposed and it is demonstrated how it can be applied to efficiently secure electronic transactions.

The rest of the paper is organized as follows. In the following section, the security requirements of a signcryption scheme are summarized. In Section 3, the necessary mathematical tools are reviewed. The proposed tripartite signcryption scheme is presented in Section 4. This is followed by its proof of correctness and performance analysis as well as security analysis in Section 5. In Section 6, the implementation domain is described. Section 7 presents a variant of the proposed scheme that supports public verifiability. The application of the proposed scheme to electronic transactions is investigated in Section 8. Finally, Section 9 concludes the paper.

2. SECURITY REQUIREMENTS OF A SIGNCRYPTION SCHEME

A signcryption scheme should support the following desirable features.

1. Confidentiality: It means that only the intended recipients can recover the plaintext message from the corresponding ciphertext.
2. Unforgeability: No one other than the designated signer can generate valid signatures.
3. Non-repudiation: The sender cannot deny his commitment towards a message he created.
4. Verifiability: Any third party can verify the origin of a message, which is a desirable property to resolve disputes between the sender and receiver.
5. Data Integrity: It refers to verifying that the message contents have not been altered during transmission.

3. MATHEMATICAL BACKGROUND

In this section, the mathematical tools necessary to the understanding of the proposed scheme are reviewed.

3.1 Elliptic Curves

An elliptic curve *E* [5] over a finite field F_p is defined by the Weirestrass equation

$$y^2 = x^3 + ax^2 + bx + c$$

where $a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2 \neq 0$ and $x \in F_p$ with *p* a prime greater than 3.

For efficiency purposes, a point on an elliptic curve is stored in compressed format. In this format, the x-coordinate is only stored along with a single bit indicating whether the positive or negative square root of $x^3 + ax^2 + bx + c$ is the designated y-coordinate.

An elliptic curve *E* over the finite field Z_p should be carefully chosen to avoid specialized attacks such as the MOV-attack and the FR-attack [6,7]. Specifications of safe elliptic curves can be found in [8].

The set of points on an elliptic curve *E* generated by some point *P* together with the point addition operation form an abelian group. The group addition law for elliptic curves over a field of characteristic greater than three is explained below.

Let $P = (x_1, y_1) \in E$, its inverse is defined to be the point $-P = (x_1, -y_1)$, which is the reflection of this point in the x-axis. If $Q = (x_2, y_2) \in E$ and $Q \neq -P$, then the addition operation can be defined as follows in terms of the chord and tangent method.

Case (1): If $P \neq Q$, then the chord $\overline{PQ}$ joining the two points intersects the curve in exactly one more point *R*. By definition, $P + Q = -R$, see Figure 1(a).

Case (2): If $P = Q$, then the tangent line at P intersects the curve at exactly one point denoted as R. By definition, $P + P = 2P = -R$, refer to Figure 1(b).

The coordinates of the point $R = (x_3, y_3)$ can be directly computed according to the following formulae

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{if } P \neq Q \\ \dfrac{3x_1{}^2 + a}{2y_1}, \text{if } P = Q \end{cases}$$

Multiples of a point are calculated using repeated doubling. For example, to compute $101P$, double six times to compute $2P, 4P, 8P, 16P, 32P, 64P$ and then three point additions are needed namely $((P + 4P) + 32P) + 64P = 101P$.

3.2 Bilinear Maps

Bilinear maps have been extensively used in the development of many cryptographic protocols during the last decade. Bilinear maps were used at first to mount cryptanalysis attacks against cryptographic schemes and then they found positive applications in cryptography. Traditional certificate-based- as well as identity-based- key agreement protocols, encryption and signature schemes have been developed in literature based on the use of bilinear pairings. First, Joux was able to construct a three party key exchange protocol based on bilinear pairings [9]. Afterwards, Boneh and Franklin used bilinear pairings to construct the first practical identity-based encryption scheme [10]. Since then, so many cryptographic applications of pairings have been identified that this area of research is sometimes considered a separate line of research called pairing-based cryptography. Symmetric bilinear maps are only considered in what follows.

Consider two groups G_1 (additive) and G_2 (multiplicative). A bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ satisfying the following properties is needed.

- *Bilinearity:* $\forall\ P, Q \in G_1, \forall\ a, b \in F_q{}^*$, it holds that $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, $\hat{e}(P, Q + R) = \hat{e}(P, Q)\ \hat{e}(P, R)$.
- *Non-degeneracy:* For any point $P \in G_1$, it holds that $\hat{e}(P, Q) = 1$ for all $Q \in G_1$ iff $P = O$
- *Computability:* There exists an efficient algorithm to compute $\hat{e}(P, Q), \forall\ P, Q \in G_1$.

The modified Weil pairing and the Tate pairing [11,12] are admissible instantiations of bilinear pairings over super-singular elliptic curves.

The growing preference of using elliptic curves in cryptosystems is due to smaller key sizes being required to achieve the same level of security compared to other schemes that do not employ elliptic curves. Moreover, they present the only known domain where bilinear maps have been defined.

3.3 Hard Computational Problems

The security of the proposed protocol relies on the fact that is infeasible to solve the following computational problems in polynomial time.

The discrete logarithm problem over a finite field F_p can be stated as follows: Given a generator *g* of a subgroup *G* and an element g^a, it is hard to find *a*. The discrete logarithm problem over an elliptic curve can be similarly defined.

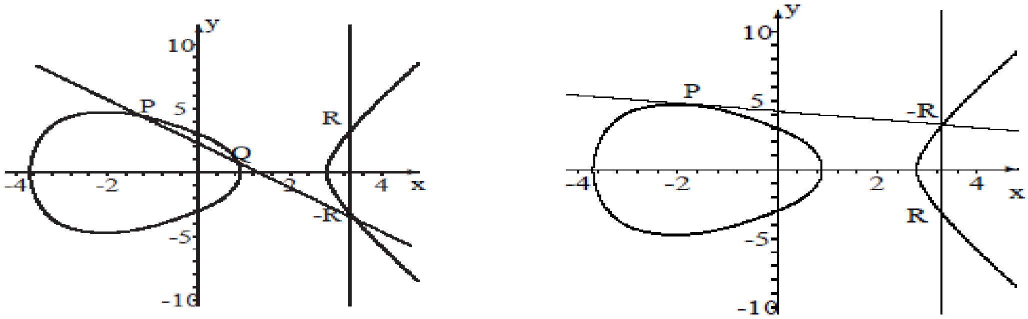
The Diffie-Hellman problem over a finite field can be stated as follows: Given a generator *g* of a subgroup *G* and two elements g^a and g^b, it is hard to compute g^{ba}.

4. THE PROPOSED SCHEME

In this section, the proposed scheme is described. It consists of four phases: the setup phase, the key generation phase, the signcryption phase and the unsigncryption phase.

4.1 Setup Phase

Assume that the three entities A, B and C are registered within the same public key infrastructure (PKI). Moreover, assume that the system-wide public parameters are: $< p, q, E, P, H, \hat{e}, Encryt\,(.,.), Decrypt\,(.,.) >$



1 (a) Addition **1 (b) Doubling**

Fig. 1: Elliptic curve group operation demonstration

where p , q are two large primes such that q divides $p+1$, E is an elliptic curve over Z_p, P is a generator point of a subgroup of points on E of order q; denoted as G_1, $\hat{e}: G_1 \times G_1 \to G_2$ is a symmetric bilinear map such as the modified Tate pairing with G_2 being a finite field extension of Z_p. The $Encrypt\ (.,.)$ function receives two inputs which are the message and the key, respectively. It is a symmetric encryption module. On the other hand, the $Decrypt\ (.,.)$ is the decryption module which takes as input the ciphertext and the key, respectively.

4.2 Key Generation

The private/public key pairs for the three communicating parties are generated as follows. Each member picks a random number x and then computes the corresponding public key as Y = xP. The key pairs for entities A, B and C are given as $(x_a, Y_a = x_a P \bmod p)$, $(x_b, Y_b = x_b P \bmod p)$, and $(x_c, Y_c = x_c P \bmod p)$, respectively.

4.3 Signcryption Phase

Suppose that A wants to send a signed message m, while achieving the confidentiality of the message, to both B and C over a broadcast channel.

1. Choose a random integer x.
2. Compute the key $k = \hat{e}(Y_b, Y_c)^x$
3. Split k into k_1 and k_2.
4. Compute $r = H(m \| k_1) \mod q$
5. Encrypt $c = Encrypt\ (m, k_2)$
6. Compute $s = x\,(r + x_a)^{-1} \mod q$
7. Send (c, r, s) to both entities B and C.

4.4 Unsigncryption Phase

When B receives the cryptogram (c, r, s), it proceeds as follows to retrieve the message m.

1. The key k is recovered as:

$$k = \hat{e}(rP + Y_a\ , Y_c)^{s\, x_b}$$

2. Split k into k_1 and k_2.
3. Decrypt $m = Decrypt\ (c, k_2)$
4. Check whether $r = H(m \| k_1) \mod q$ holds with equality.

Similar steps are carried out by C to retrieve the message. The only difference is in the key recovery step:

$$k = \hat{e}(rP + Y_a\ , Y_b)^{s\, x_c}$$

5. CORRECTNESS, PERFORMANCE AND SECURITY OF THE SCHEME

In this section, the consistency of the proposed scheme is verified and its performance and security properties are examined.

5.1 Proof of Correctness

The correctness of the proposed scheme can be proven through verifying that the key k is correctly recovered by B and C. This is proven for entity B and similar arguments hold for C. The proof is based on the bilinearity property of the map $\hat{e}$.

$$\begin{aligned}
\hat{e}(rP + Y_a\ , Y_c)^{s\, x_b} &= \hat{e}(rP + Y_a\ , Y_c)^{x\,(x_a + r)^{-1}\, x_b} \\
&= \hat{e}((r + x_a)\ P\ , Y_c)^{x\,(x_a + r)^{-1}\, x_b} \\
&= \hat{e}(x_b\ P\ , Y_c)^{x\,(x_a + r)^{-1}\,(x_a + r)} \\
&= \hat{e}(Y_b\ , Y_c)^{x}
\end{aligned}$$

It is clear that the key recovered by B is identical to the key used by A in the signcryption phase and thus the correctness of the remaining steps follows immediately.

5.2 Performance Analysis

For frequently communicating parties, there is no need to compute the only pairing involved in the signcryption phase. It can be pre-computed and stored for later use. This is usually the case in e-commerce. In this case, only one modular exponentiation, one modular inversion, one hashing operation and one encryption operation are needed in the signcryption phase.

On the other hand, in the unsigncryption phase, more computations are involved. One pairing evaluation is needed in addition to one addition operation over an elliptic curve, one scalar point multiplication, one modular exponentiation, one hashing and one decryption operation.

Thus, the proposed scheme is suitable for applications where the sender is a computationally constrained device, while the recipients are more powerful networked devices.

5.3 Security Properties

The security of the proposed protocol relies on the infeasibility of recovering the ephemeral key k using the knowledge of the public key of the sender and those of the recipients, in addition to the data communicated over the public channel.

It is clear that the recovery of the short-term key k by an attacker is somewhat equivalent to solving an instance of the Diffie-Hellman problem. Consequently, confidentiality of the message transmitted is achieved.

Moreover, the signature part is a variant of the DSA and thus unforgeability of the signature follows. Thus, the sender cannot deny being the origin of the message meeting the non-repudiation requirement accordingly.

As for verifiability, the recipient can compute the ephemeral key and forward this key together with the message to any third party in order to verify that the alleged signature has been created by the indicated entity.

Finally, data integrity is verified through the use of a one-way hash function.

6. IMPLEMENTATION

In order to prove the feasibility and ease of implementation of the proposed protocol, the PBC library has been used for the implementation under UBUNTU operating system.

Type A elliptic curves have been used in the sample runs for testing the validity and ensuring the timeliness of the proposed protocol.

Type A pairings (bilinear maps) are symmetric pairings constructed on the elliptic curve [12]

$$y^2 = x^3 + x$$

over the field F_q for some prime q = 3 mod 4. It turns out that

$$\#E(F_q) = q + 1 \quad \text{and} \quad \#E(F_q^{\,2}) = (q + 1)^2$$

thus, the embedding degree is 2, and hence G_2 is a subgroup of $F_q^{\,2}$.

The order a subgroup of points on the above elliptic curve, denoted as ℓ, is some prime factor of $q + 1$. Write

$$q + 1 = \ell \times h$$

For efficiency, ℓ is picked to be a Solinas prime; that is, ℓ has the form of $2^a \pm 2^b \pm 1$ for some integers $0 < b < a$. Also, choose q = -1 mod 12 , so $F_q^{\,2}$ can be implemented as $F_q[i]$ (the field of Gaussian integers, where $i = \sqrt{-1}$). G_1 is a subgroup of points on $E(F_q)$.

7. A VARIANT OF THE SCHEME SUPPORTING PUBLIC VERIFIABILITY

It is sometimes desirable to verify the data origin without the need for any short term or long term keys. This property is referred to as public verifiability. In what follows, a variant of the proposed tripartite signcryption scheme is presented which supports this property.

7.1 Signcryption Phase

Suppose that A wants to send a signed message m to both B and C over a broadcast channel, while achieving the confidentiality of the message as well as public verifiability of the ciphertext origin.

1. Choose a random integer x.
2. Compute the verification key $k_1 = \hat{e}(P\ , P\ )^x$
3. Compute the encryption key $k_2 = \hat{e}(\,Y_b\ , Y_c\ )^x$
4. Compute $r = H(c \,||\, k_1) \mod q$
5. Encrypt $c = Encrypt\ (m, k_2)$
6. Compute $s = x\,(r + x_a)^{-1} \mod q$
7. Send (c, r, s) to both entities B and C.

7.2 Unsigncryption Phase

When B receives the cryptogram (c, r, s), it proceeds as follows to retrieve the message m.

1. Recover the verification key:
$$k_1 = \hat{e}(rP + Y_a\ , P)^s = \hat{e}(rP + Y_a\ , P)^{x\,(r+x_a)^{-1}}$$
$$= \hat{e}((r + x_a)\ P,\ P)^{x\,(r+x_a)^{-1}} = \hat{e}(\ P,\ P)^x$$
2. Check whether $r = H(c \,||\, k_1) \mod q$ holds with equality.
3. The encryption key is recovered as:
$$k_2 = \hat{e}(rP + Y_a\ , Y_c)^{s\ x_b}$$
4. Decrypt $m = Decrypt\ (c, k_2)$.

It is clear that the recovery of the verification key equation does not involve neither short-term nor long-term keys. Moreover, the verification equation involves the ciphertext and not the plaintext message providing better protection for the secrecy of the sent contents even in case of disputes.

8. APPLICATION TO ELECTRONIC TRANSACTIONS

In this section, the SET protocol is reviewed and it is demonstrated how the proposed protocol can be used to reduce the number of rounds needed.

8.1 The SET Protocol

Secure payment systems are critical to the success of E-commerce. As discussed earlier, there are four essential security requirements for safe electronic payments (Authentication, Encryption, Integrity and Non-repudiation). Security protocols adopted in electronic payment systems, such as the SSL (Secure Socket Layer) and the SET protocols, have encryption and authentication mechanisms as key components in them [1,13].

There are four main entities in the original SET protocol; namely,

- The customer (cardholder)
- The merchant (web server)
- The merchant's bank.
- Card issuer (the customer's bank).

In a more restricted model, it is assumed that both the merchant and the customer have accounts in the same bank.

The purpose of the SET protocol is to establish payment transactions that

- provide confidentiality of information;
- ensure the integrity of payment instructions for goods and services; that is, order data;
- authenticate both the cardholder and the merchant.

Before participating in the transaction, all entities must obtain a digital certificate for their public keys from a certifying authority (CA). The protocol involves nine basic steps as described in [1], which are summarized below.

1. The customer browses the website of the merchant and chooses the product.
2. The merchant returns a form containing the list of items along with the total price and the order number. A copy of the digital certificate is also sent for authentication of the merchant.
3. The customer sends its signature of the order information and the payment information along with its digital certificate to the merchant. The digital certificate is to validate the customer's authenticity. The order information confirms that the customer will make the purchase, whereas the payment information is encrypted by the public key of the payment gateway which cannot be read by the merchant.
4. The merchant forwards the payment information to the merchant bank.
5. The merchant bank then forwards the information to the customer bank for authorization and payment.
6. The customer bank confirms authorization to the merchant bank and the merchant bank sends the authorization confirmation to the merchant.
7. The merchant completes the order and sends it to the customer.
8. The merchant captures the transaction from its bank.
9. The customer bank sends a notification to the customer that the payment has been processed.

In an improved model developed in [14], an electronic transaction center (ETC) has been introduced that acts as a regional certifying authority, as an arbitration center resolving disputes and as a payment gateway that ensures transaction data preservation as well as time-stamps transaction.

8.2 Improvement to the SET Protocol

In what follows, it is shown how the proposed tripartite signcryption scheme can be used to achieve secure electronic transactions. The model involving an ETC is assumed. Moreover, it is assumed that a public insecure broadcast channel is available for communication.

The steps of the proposed protocol are summarized below:

1. The customer browses the website of the merchant and chooses the desired items.
2. The merchant uses its private key to sign a form containing the list of items along with the total price and the order number. A copy of the digital certificate ($cert_M$) is also sent for authentication of the merchant.
3. The customer verifies the CA signature for the merchant's public key. It then provides a signature of the invoice sent by the merchant to show its agreement to both the merchant and the ETC. The customer's account information needs to be kept secret so encryption is needed to provide confidentiality. The procedure carried out by the customer is thus given as

a. Choose a random integer *x*.

b. Compute the key $k = \hat{e}(Y_M , Y_{ETC})^x$, where Y_M and Y_{ETC} are the public keys of the merchant and the ETC, respectively.

c. Split *k* into k_1 and k_2 .

d. Prepare the message as follows $Msg = order \,||\, cert_C \,||\, cert_M$ $||\,\text{Encrypt}_{\text{ PK}}(account, Y_{ETC})$

where || denotes the concatenation operator, Encrypt_{PK} denotes public key encryption mechanism and $cert_C$ denotes the digital certificate of the customer's public key.

e. Compute $r = H(Msg \,||\, k_1) \mod q$

f. Encrypt $c = Encrypt\ (Msg, k_2)$

g. Compute $s = x\,(r + x_a)^{-1} \mod q$

h. Send (c, r, s) to both the merchant and the ETC.

4. The ETC uses the proposed tripartite signcryption scheme to send the payment information to both the merchant's bank and the customer's bank to undergo the monetary transfer according to the information received from the customer.

5. If the transaction ends successfully, a notification is sent by the ETC is sent to both the customer and the merchant using the proposed scheme.

9. CONCLUSION

Signcryption is a cryptographic primitive that provides authentication of the message origin and confidentiality of its contents. In this paper, a new tripartite signcryption scheme is proposed and its application to secure electronic transactions is demonstrated. The bank account information of a customer in an electronic transaction must be kept confidential and the identities of the customer, the merchant and the bank must be verified to prevent fraudulent transactions. Thus, signcryption can effectively achieve these security goals. The proposed scheme helps in reducing the number of rounds involved to achieve a secure electronic transaction.

10. REFERENCES

[1] SetCo 1997. Secure Electronic Transaction Specification: Business Description.

[2] Y. Zheng 1997. Digital Signcryption or How to Achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption). Advances in Cryptology, LNCS, Vol. 1294. Springer-Verlag. pp.165–179.

[3] F. Li, Y. Hu and S. Liu 2006. Efficient and Provably Secure Multi-Recipient Signcryption from Bilinear Pairings. In Proceedings of the 2nd Chinese Conference on Trusted Computing and Information Security (CTCIS’06), China.

[4] S. Duan and Z. Cao 2006. Efficient and Provably Secure Multi-receiver Identity-Based Signcryption. L. Batten and R. Safavi-Naini (Eds.), ACISP 2006. Springer-Verlag. LNCS 4058, pp. 195-206.

[5] J. H. Silverman 1986. The Arithmetic of Elliptic Curves. GTM 106. Springer-Verlag.

[6] A. Menezes, T. Okamoto and S. Vanstone 1993. Reducing Elliptic Curve Logarithm to Logarithms in a Finite Field. IEEE Transactions on Information Theory, vol. 39, pp. 1639-1646.

[7] G. Frey and H. Ruck 1994. A Remark Concerning *m*-divisibility and the Discrete Logarithm Problem in the Divisor Class Group of Curves. Mathematics of Computation. Vol. 62, pp. 865-874.

[8] Standards for Efficient Cryptography 2000, SEC 2: Recommended Elliptic Curves Domain Parameters, Certicom Research, Version 1.0.

[9] A. Joux 2002. The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems. In Proceedings of the Fifth Algorithmic Number Theory Symposium. LNCS. Springer-Verlag.

[10] D. Boneh and M. Franklin 2001. Identity Based Encryption from the Weil Pairing, In Advances in Cryptology- CRYPTO 2001, LNCS 2139. Springer.

[11] V. Miller 2004. The Weil Pairing and Its Efficient Calculation. Journal of Cryptology, vol. 17(4), pp. 235-262.

[12] B. Lynn 2007. On the Implementation of Pairing-Based Cryptosystems, PhD thesis, Stanford University.

[13] H. L. McKinley 2003. SSL and TLS: A Beginner's Guide. SANS Institute.

[14] Z. Boping , and S. Shiyu 2009. An Improved SET Protocol. Proceedings of the 2009 International Symposium on Information Processing (ISIP’09). Huangshan, P. R. China. pp. 267-272