Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy

Elsayed Mohamed and Hassan Elkamchouchi
Alexandria University, Alexandria, Egypt

Summary
This paper presents a comprehensive signcryption scheme based on elliptic curves. In addition to the message confidentiality, non-repudiation and unforgeability, the proposed scheme achieves forward secrecy and encrypted message authentication needed by firewalls. A judge can resolve disputes by directly verifying the sender's signature on signcrypted messages without help from the sender and without decrypting the message. Firewalls can securely filter signcrypted messages passing through them without having to do full unsigncryption to verify the sender's identity. If the sender's long-term key is compromised, the previous messages signcrypted with that key remain confidential. Elliptic curves are used for their security, key size and bandwidth advantages. The proposed scheme combines these security properties with savings in computational complexity and bandwidth overhead.

Key words:
Elliptic Curve, Signcryption, Forward Secrecy, Encrypted Message Authentication

1. Introduction

To guarantee unforegeability, integrity and confidentiality of communications, the traditional method 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 with the encrypted symmetric key. The opposite process is run at the receiver. This scheme is known as signature-then-encryption. An alternative scheme called signcryption was proposed by Zheng to simultaneously sign and encrypt messages in a single logical step with a computational cost significantly lower than that required by the traditional signature-then-encryption approach [1].

Zheng's scheme was based on the discrete logarithm problem (DLP). Zheng and Imai proposed another signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) that achieved similar functionality [2]. Both schemes lacked forward secrecy, public verifiability and encrypted message authentication. Gamage, Leiwo and Zheng proposed a scheme that enabled firewalls to authenticate encrypted messages without having to decrypt them [3]. Gamage-Leiwo-Zheng scheme was based on DLP signcryption and lacked forward secrecy. Bao and Deng proposed a signcryption scheme with signature verifiable by the public key of the recipient [4]. Bao-Deng scheme was based on DLP. It lacked forward secrecy and encrypted message authentication as the message had to be sent to a third-party together with r and s to settle a dispute. LI Xiang-xue, CHEN Ke-fei and LI Shi-qun analyzed Zheng-Imai scheme and showed that it lacked forward secrecy and public verifiability [5]. To overcome these two weaknesses in Zheng-Imai scheme, LI-CHEN-LI proposed two signcryption variants based on ECDLP; one with only public verifiability and another with only forward secrecy. Each scheme had only one of the desired properties and both lacked encrypted message authentication. In 2006, LEI Feiyu, CHEN Wen and CHEN Kefei modified Zheng and Bao-Deng schemes to add the public verifiability property [6]. Their schemes were based on DLP and the quadratic residue problem but lacked forward secrecy and encrypted message authentication.

In this paper, a new signcryption scheme is proposed based on ECDLP. In addition to confidentiality, unforegeability and non-repudiation, the proposed scheme provides forward secrecy, public verifiability and encrypted message authentication.

2. Zheng-Imai Elliptic Curve Signcryption Scheme

Two signcryption schemes were given in [2] and named ECSCS1 and ECSCS2. They were based on shortened variants of the elliptic curve DSS (SECDSS1 and SECDSS2) presented in [1]. Only ECSCS1 is described here. The case is similar for the other ECSCS2.
Alice has a message m to send to Bob. Alice signcrypts m as follows so that the effect is similar to signature then encryption.

Public Parameters:
C: an elliptic curve over $GF(p^h)$, either with $p \geq 2^{150}$ and $h = 1$ or $p = 2$ and $h \geq 150$.
q: a large prime whose size is approximately $|p^h|$.
G: a point with order q, chosen randomly from the points on C.
hash: a one-way hash function whose output has, say, at least 128 bits.
KH: a keyed one-way hash function.

E, D: the encryption and decryption algorithms of a private key cipher.

***Alice's keys*:**
v_a: Alice's private key, chosen uniformly at random from [1, …, q - 1].
P_a: Alice's public key ($P_a = v_aG$, a point on C).

***Bob's keys*:**
v_b: Bob's private key, chosen uniformly at random from [1, …, q - 1].
P_b: Bob's public key ($P_b = v_bG$, a point on C).

Signcryption of m by Alice the sender:
$v \varepsilon_R [1, \ldots, q-1]$
$(k_1, k_2) = hash(vP_b)$
$c = E_{k_1}(m)$
$r = KH_{k_2}(m)$
$s = v / (r + v_a) \bmod q$
Send c, r, s to Bob

Unsigncryption of c, r, s by Bob the recipient:
$u = sv_b \bmod q$
$(k_1, k_2) = hash(uPa + urG)$
$m = D_{k_1}(c)$
Accept m only if $KH_{k_2}(m) = r$

3. Proposed Scheme

The new scheme has the same public parameters and the same keys for Alice and Bob as Zheng-Imai. It works as follows.

Signcryption of m by Alice the sender:
$v \varepsilon_R [1, \ldots, q-1]$
$k_1 = hash(vG)$
$k_2 = hash(vP_b)$
$c = E_{k_2}(m)$
$r = hash(c, k_1)$
$s = v / (r + v_a) \bmod q$
$R = rG$
Send c, R, s to Bob

Unsigncryption of c, R, s by Bob the recipient:
$k_1 = hash(s(R + P_a))$
$r = hash(c, k_1)$
$k_2 = hash(v_bs(R + P_a))$
$m = D_{k_2}(c)$
Accept c only if $rG = R$

Verification of c, R, s by a firewall or a judge:

$k_1 = hash(s(R + P_a))$
$r = hash(c, k_1)$
Accept c only if $rG = R$

4. Analysis

4.1 Proof

To prove the verification condition:

$sR + sP_a = vrG / (r + v_a) + vP_a / (r + v_a)$

$= (vrG + vP_a) / (r + v_a)$

$= vG (r + v_a) / (r + v_a)$

$= vG$

Thus: $hash(sR + sP_a) = hash(vG) = hash(k_1)$

Computing k_1 allows the verification of the signcrypted text.

To prove the decryption step:

$sv_b(R + P_a) = v_b(sR + sP_a)$

$= v_b\, vG$

$= vP_b$

Thus: $hash(sv_b(R + P_a)) = hash(vP_b) = hash(k_2)$

Computing k_2 allows the decryption of the message using $m = D_{k_2}(c)$

4.2 Security

The security properties of the proposed scheme are described as follows.

1) Unforgeability: It is computationally infeasible to forge a valid signcrypted text (c, R, s) and claim that it is coming from Alice without having Alice's private key v_a.
2) Non-repudiation: If the sender Alice denies that she sent the signcrypted text (c, R, s), any third party can run the verification procedure above to check that the message came from Alice.
3) Public verifiability: Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or published directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide a proof.
4) Confidentiality: Confidentiality is achieved by encryption. To decrypt the ciphertext, an adversary needs to have Bob's private key (v_b).
5) Forward secrecy: An adversary that obtains va will not be able to decrypt past messages. Previously recorded

values of (c, R, s) that were obtained before the compromise cannot be decrypted because the adversary that has v_a will need to calculate r to decrypt. Calculating r requires solving the ECDLP on R, which is a computationally difficult.

6) Encrypted message authentication: The proposed scheme enables a third party to check the authenticity of the signcrypted text (c, R, s) without having to reveal the plaintext m to the third party. This property enables firewalls on computer networks to filter traffic and forward encrypted messages coming from certain senders without decrypting the message. This provides speed to the filtering process as the firewalls do not need to do full unsigncryption to authenticate senders. It also provides additional confidentiality in settling disputes by allowing any trusted/untrusted judge to verify messages without revealing the sent message m to the judge.

4.3 Saving in Computational Complexity

It is assumed that the elliptic curve point operations are the most expensive computations in terms of the time consumed in them. In the proposed scheme, signcryption requires three point multiplications, unsigncryption requires two point multiplications and one point addition, and verification requires one point multiplication and one point addition. The traditional signature-then-encryption based on SECDSS1 followed by ElGamal elliptic curve encryption requires three point multiplications with one point additions for signature-encryption and three point multiplications with two point additions for verification-decryption. This makes the proposed scheme faster than signature-then-encryption in both signcryption and unsigncryption. The Zheng-Imai scheme requires one point multiplication for signcryption and two point multiplications with one point addition for unsigncryption. Thus, the proposed scheme is slower than Zheng-Imai in signcryption but has the same number of point operations in unsigncryption. The additional two point multiplications in the signcryption procedure of the proposed scheme, compared to Zheng-Imai, are justified by their value in offering the public verifiability and forward secrecy properties.

4.4 Saving in Communication Overhead

Communication overhead calculations are based on the following assumptions:

a) $|hash(.)| = |KH(.)| = |q|/2$

b) $|q| \approx |p^h|$

c) Point compression is used

d) ElGamal elliptic curve encryption is over the same curve C and has the same base point G. Note: ElGamal elliptic curve encryption outputs two points on the curve [7].

The communication overhead of SECDSS1 followed by ElGamal elliptic curve encryption is $(|hash(.)| + |q|) + 2(|q| + 1) = |hash(.)| + 3|q| = 3.5|q|$ assuming that $|q| >> 1$. The communication overhead of the proposed scheme is $|q| + (|q| + 1) = 2|q| + 1 \approx 2|q|$ assuming that $|q| >> 1$. Thus, bandwidth saving can be calculated as:

Saving = $(3.5|q| - 2|q|)/ 3.5|q| = 43\%$

This saving is higher than the one calculated in Zheng-Imai paper, which is 40%.

5. Conclusion

This paper presents an improved signcryption scheme that achieves the highly desired features in e-commerce and secure network applications. It utilizes elliptic curves for their high security and small key size. In addition, the new scheme achieves public verifiability, forward secrecy and encrypted message authentication. Previous researches have achieved only part of these properties in a discrete logarithm setting. The new scheme enables network firewalls to authenticate message source without having to decrypt messages. The scheme's forward secrecy property ensures that past messages remain confidential even if the sender's long-term private key is compromised. Public verifiability is especially useful in e-commerce environments as it enables the trading partners to settle disputes through any trusted or untrusted judge without interacting with the judge in a zero-knowledge proof communication and without revealing any secret information.

The new scheme achieves these security properties with a saving in computation cost compared to the traditional signature-then-encryption scheme, which makes the new scheme more appropriate for environments with limited computing power. It also achieves a bandwidth saving of 43%.

References

[1] Y. Zheng, “Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)”, Advances in Cryptology - Crypto’97, LNCS 1294, Springer-Verlag, 1997, pp. 165–179.

[2] Y. Zheng, H. Imai, “How to construct efficient signcryption schemes on elliptic curves”, Information Processing Letters 68 (1998) 227–233.

[3] C. Gamage, J. Leiwo, Y. Zheng, “Encrypted message authentication by firewalls”, Proceedings of 1999

International Workshop on Practice and Theory in Public Key Cryptography (PKC'99), LNCS 1560, Springer-Verlag, 1999, pp. 69–81.

[4] F. Bao, R.H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceedings of PKC'98, LNCS 1431, Springer-Verlag, 1998, pp. 55–59.

[5] LI Xiang-xue, CHEN Ke-fei, LI Shi-qun, "Cryptanalysis and improvement of signcryption schemes on elliptic curves", Wuhan University Journal of Natural Sciences, Vol. 10, No. 1, 2005, 231-234.

[6] LEI Feiyu, CHEN Wen, CHEN Kefei, "A generic solution to realize public verifiability of signcryption", Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.

[7] Lawrence C. Washington, "Elliptic Curves: Number Theory and Cryptography", CRC Press, 2003.