Signcryption based on Elliptic Curve and its Multi-party Schemes

[Extended Abstract]*

Yiliang Han
Department of Electronic Technology, Engineering College of APF
Xi'an, China
Yilianghan@hotmail.com

Xiaoyuan Yang
Department of Electronic Technology, Engineering College of APF
Xi'an, China
Hanyil@163.com

Yupu Hu
Key Lab on Network and Information Security of Educational Ministry, Xidian University
Xi'an, China
Yphu8969@sohu.com

ABSTRACT

A new signcryption based on elliptic curve cryptosystems that combines ECDSA and PSCE-1 is presented. The signcryption scheme is a publicly verifiable scheme which can be verified by the third party after the specific recipient removes his key information. Analysis shows that the proposed scheme is secure against the adaptive chosen ciphertext attack. The signcryption saves the communication cost at least 1.25 times and enhances computation cost 1.19 times over ECDSA-then-PSCE-1. Compared with other signcryption schemes, such as Y.Zheng's ECSCS, the new signcryption uses a uniform elliptic curve cryptosystem platform instead of four kinds of cryptosystem components: hash function, keyed hash function, symmetric cipher and elliptic curve. While keeping high security and efficiency, the scheme can be implemented in software and hardware at low price because of above advantages. Based on the presented signcryption, a broadcast scheme for multiple recipients and a threshold scheme with Key Distributed Generation for multiple senders are also proposed.

Categories and Subject Descriptors

F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems -*Computations in finite fields, Computations on polynomials*

General Terms

Algorithms, Security, Theory.

Keywords

Signcryption, Elliptic Curve, Threshold Cryptosystem, Distributed Key Generation

1. INTRODUCTION

The traditional approaches that avoid forgery and ensure confidentiality of a message in public key settings can be divided into three classes [5]: *sign-then-encrypt, encrypt-then-sign* and *sign-and-encrypt*. The *encrypt-then-sign* and *sign-and-encrypt* are insecure in some cases. Though *sign-then-encrypt* is an appropriate composition, the high communication cost and computation cost hold its broad using. Signcryption is a novel public key primitive to achieve the combined functionality of authentication and confidentiality in an efficient manner. It is more secure and more efficient than the traditional methods. Y. Zheng proposed the conception of signcryption and the first Discrete-Log based scheme SCS in 1997[1]. The proofs given by [4] showed that the SCS scheme was IND-CCA2 secure. He also gave an Elliptic Curve version of SCS which called ECSCS in 1998[2].

*A full version of this paper is available at http://eprint.iacr.org/2004/142.pdf

InfoSecu04, November 14–16, 2004, Pudong, Shanghai, China.

2. NEW SIGNCRYPTION BASED ON ECC

We propose the first signcryption scheme which is really based on Elliptic Curve Cryptosystem in this section.

2.1 Description of the New Scheme

There is a message m which will be signcrypted and sent to a specific recipient. Alice is a sender. Bob is a specific recipient.

Choosing an elliptic curve $E(Fq)$ on a finite field Fq (q>max (n, s), is a prime number), G is a base point, ord(G)=l. Hence there is a subgroup generated by base point G. Choosing a secret number $s \in Zq$, we can compute $Q=sG$ easily. Computing s via Q and G is an ECDLP which is hard in our scheme. $H(.)$ is a strong one way hash function.

Key Generation: A random number $s_A \in \{1,\ldots,l-1\}$is the private key of Alice. Her public key is a point $P_A = s_A G$. Bob's private key is a random number $s_B \in \{1,\ldots,l-1\}$. His public key is a point $P_B = s_B G$.

Signcryption: Alice will signcrypt the message as following:

Step 1: Chooses $r \in \{1,\ldots,l-1\}$at random.

Step 2: Computes $R=rG=(x_1, y_1)$.

Step 3: Computes $rP_B=(x_2, y_2)$.

Step 4: Computes $y = r^{-1}(H(m)+x_1 s_A) \bmod p$.

Step 5: Computes $e=H(m \| y)$.

Step 6: Computes $c=(m \| e) \oplus x_2$.

The triplet (R, c, y) is the signcryption and will be sent to Bob.

Unsigncryption: Bob verifies the signcryption.

Step1: Computes $s_B R=(x_2', y_2')$.

Step2: Computes $(m' \| e') = c \oplus x_2'$.

Step3: Computes $e' = H(m' \| y)$.Checks if $e \neq e'$, rejects m'.

Step4: Computes y^{-1}.

Step5: Computes $u = y^{-1}H(m')$, $v = y^{-1}x_1$.

Step6: Computes $(x_1', y_1') = uG + vP_A$. Checks if $x_1 \neq x_1'$, rejects m', else return $m = m'$.

The scheme combines ECDSA and PSEC-1[8]. The triplet $(R, H(m), y)$ can be verified publicly as a common ECDSA signature.

2.2 Security of the New Scheme

The security notions of signcryption and the definition of IND-CCA2 security for signcryption were given in [4]. A signcryption scheme is secure if the following conditions are satisfied: *Non-repudiation, Unforgeability* and *Confidentialit.* The following sub-sections are devoted to discussion of the security of the new signcryption scheme. (Omitted)

2.3Efficiency of the New Scheme

The new signcryption enhances the Message Rate 1.25 times and computation efficiency 1.19 times over *Sign-then-Enc* (ECDSA-then-PSEC-1).

3. SCHEME FOR MULTIPLE RECIPIENTS

The new scheme can be used to broadcast a message to multiple users in a secure and authenticated manner. Except the above secure notions, we must prevent a particular recipient form being excluded from the group by a dishonest message originator. A RSA based scheme was given in RFC1421 [9]. Y. Zheng also gave a similar scheme which used his SCS signcryption[3]. Using the signcryption proposed in section 2, we will give a scheme based on elliptic curve for multiple recipients. The description of the scheme in details as following: (Omitted).

4. SCHEME WITH DKG

T.Pedersen proposed the first Distributed Key Generation (DKG) scheme in 1991[6]. R.Gennaro pointed out the scheme is insecure and gave a secure DKG scheme for Discrete-Log Cryptosystems in 1999[7]. We will give an elliptic curve version of the Gennaro's DKG scheme which will be called EC-DKG in the following. Under the assumption that ECDLP is hard, EC-DKG has the equal security as original scheme while is more efficient.

In this section, we will construct a threshold Signcryption protocol with EC-DKG, which is a multi-party secure computation problem. (Omitted)

5. CONCLUSION

The signcryption scheme proposed in this paper uses a uniform elliptic curve cryptosystem computation platform and a set of parameters. Though its computation cost is lightly less than our signcryption, ECSEC's high prices in practice make it not applicable. In other word, an application (software or device) which must contain four kinds of cryptosystem platform can implement ECSCS. Hence the proposed scheme is more feasible than others.

6. REFERENCES

[1] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). In *Advances in Cryptology-CRYPTO'97, LNCS1294*. 1997, 165–179

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

[3] Y. Zheng. Signcryption and Its Applications in Efficient Public Key Solutions.In *Proceedings of 1997 Information Security Workshop (ISW'97), LNCS1397*, Springer-Verlag. 1998,291-312

[4] J.Baek, R.Steinfeld and Y.Zheng. Formal Proofs for the Security of Signcryption. In *LNCS2274* (PKC'02), Springer-Verlag. 2002,80-98

[5] H. Krawczyk. The Order Of Encryption And Authentication For Protecting Communications (Or: How Secure Is SSL?). *In Advances In Cryptology-CRYPTO'01, LNCS2139*, Springer-Verlag. 2001,310-331

[6] T.Pedersen. A threshold cryptosystem without a trusted party. In *Advances in Cryptology-EUROCRYPT'91, LNCS547*. Springer-verlag. 1991, 522-526.

[7] R.Gennaro, S.Jarecki, H. Krawezyk and T. Rabin. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In *Advances in Cryptology-EUROCRYPT'99*. Springer-verlag. 1999,295-310

[8] T. Okamoto, E. Fujisaki H. Morita. PSEC: Provably Secure Elliptic Curve Encryption Scheme. Submission to IEEE P1363a (1998, March), http:// grouper.ieee.org/groups/ 1363/P1363a/contributions/psec.pdf

[9] J. Linn, Privacy enhancement for internet electronic mail: Part I: Message encryption and authentication procedures. RFC 1421 IETF 1993