A multi-recipient signcryption scheme for secure and authenticated group communications

Hassan Elkamchouchi and Yasmine Abouelseoud
Electrical Eng. Dept., Faculty of Eng., Alexandria University, Alexandria, Egypt
Email address: yasmine.abouelseoud@gmail.com*

In this paper, a new multi-recipient signcryption scheme is presented. The proposed scheme achieves considerable reductions in the computational overhead as well as bandwidth requirements compared to re-signcrypting the message for each recipient individually. In the proposed scheme, the message is signcrypted only once using a random session key and a receivers' information part is appended to the ciphertext that enables each receiver to retrieve the message, if he is an authorized user. The receivers' information part consists of a polynomial chosen such that the embedded session key is only recoverable by the intended set of recipients. The consistency of the scheme is validated. Further enhancements in bandwidth requirements are achieved through employing elliptic curves over finite fields. The scheme is actually a protocol for secure group communications that achieves both message confidentiality and data origin authenticity. One important aspect of the proposed scheme is that it may be considered as a general framework useful in the conversion of any single recipient signcryption scheme based on discrete logarithms into a multi-recipient one.

هذا البحث يعرض طريقة جديدة للإمضاء و التشفير المدمج لعدة مستقبلين. الطريقة المقترحة تحقق تخفيض ملحوظ في المتطلبات الحسابية و كذلك حيز الإرسال مقارنة بإعادة الإمضاء و التشفير لكل مستقبل على حدة. في الطريقة المقترحة يتم الإمضاء و التشفير مرة واحدة فقط و يتم إلحاق جزء خاص ببيانات المستقبلين مع الرسالة المشفرة حتى يتمكن كل مستقبل من استرداد الرسالة. الجزء الخاص ببيانات المستقبلين يتكون من كثيرة حدود مختارة بحيث يتمكن المستقبلين فقط من استرداد مفتاح التشفير الكامن فيها. تم التحقق من صحة الطريقة. تم تحقيق تخفيض أكبر في حيز الإرسال عن طريق استخدام المنحنيات الناقصية. الطريقة المقترحة تمثل بروتوكول للاتصال الآمن و الموثق بين أعضاء مجموعة معينة. أحد الملامح الهامة للطريقة المقترحة أنها تعتبر طريقة عامة لتحويل طرق الإمضاء والتشفير المدمج المعتمدة على اللوغاريتم المتقطع لمستقبل واحد إلى طرق لعدة مستقبلين.

Keywords: Cryptography, Signcryption, Multi-recipients, Secure group communications, Authentication

1. Introduction

In practice, broadcasting a message to multiple users in a secure and authenticated manner is an important facility for a group of people who are jointly working on the same project to communicate with one another. Several cryptographic primitives and constructions have been proposed in the last decade to tackle the challenging problem of managing secure group communications. In this scenario, a message is broadcast through a multi-cast channel, such that all recipients receive an identical copy of a broadcast message. Major concerns with broadcasting to multiple recipients include confidentiality, unforgeability, data origin authenticity, non-repudiation and consistency of a message. *Confidentiality* is keeping information secret from all other than those who are authorized to see it. *Data origin authentication* is the assurance that the communicating party is the one that it claims to be. *Non-repudiation* is preventing the denial of previous commitments or actions. *Consistency* refers to the fact that all recipients recover an identical message from their copies of a broadcast message. Signcryption [1] is a public key cryptographic primitive that provides both message confidentiality and unforgeability simultaneously, but at lower computational and communication overhead compared to the traditional sign-then-encrypt paradigm. Recently, Zheng et al. developed a formal

security proof model for signcryption schemes [2].

In order to adapt a signcryption scheme to be suited for multiple recipients, one basic idea proposed in literature is to use two types of keys: the first type is a *message encryption key* k_m and the second type is a *recipient specific key* [3]. The message is encrypted using k_m and k_m is signcrypted to each receiver individually.

In this paper, a new multi-recipient signcryption scheme for secure and authenticated group communications is presented. The scheme achieves both message confidentiality and authenticity at low communications and computational costs compared to re-signcrypting the message for each receiver independently as well as the scheme in [3]. Moreover, the scheme is adapted to work over elliptic curves over finite fields to further reduce the bandwidth requirements.

2. Signcryption

Secure and authenticated message delivery is one of the major aims of computer and communication security research. The standard method to achieve this aim is a digital signature followed by encryption. However, Zheng in [1] introduced the concept of signcryption which achieves the same goals but at a significantly lower cost. He proposed a scheme based on a shortened variant of ElGamal digital signature scheme [4].

The system-wide public parameters [1] include p (a large prime) and q (a large prime factor of $p-1$), a random integer g in the set $\{1,2,\cdots,p-1\}$ with order q modulo p, i.e. q is the smallest integer satisfying that $g^q \equiv 1 \bmod p$, as well as a one-way keyed hash function $KH_k(.)$. In addition, a symmetric key (block cipher) scheme [5] is agreed upon, for instance the Data Encryption Standard (DES) [6]. In what follows E_k and D_k stand for the processes of encryption and decryption, respectively. Each member in the system has a secret key x from the set $\{1,2,\cdots,q-1\}$ and a public key $y = g^x$.

Assume that Alice has a private/public key pair (x_a, y_a) and Bob has (x_b, y_b) as his private/public key pair.

For Alice to signcrypt a message m for Bob, she carries out the following procedure.

- *Signcryption by Alice (the sender)*

1. Pick x randomly from the set $\{1,2,\cdots,q-1\}$ and let $k = y_b{}^x \bmod p$.
2. Split k into k_1 and k_2 of appropriate length.
3. $r = KH_{k_1}(m) \bmod q$
4. $s = x(r + x_a)^{-1} \bmod q$
5. $c = E_{k_2}(m)$
6. Send to Bob the signcrypted text (c,r,s)

On receiving (c, r, s), Bob unsigncrypts it using the following procedure.

- *Unsigncryption by Bob (the recipient)*

1. Recover k, where $k = (g^r y_a)^{s\, x_b} \bmod p$
2. Split k into k_1 and k_2 .
3. $m = D_{k_2}(c)$
4. Accept m as a valid message originated from Alice only if $KH_{k_1}(m)$ is identical to r.

Further developments of the original scheme, including signcryption schemes on elliptic curves over finite fields, have been proposed in the literature [7-8].

One basic idea in signcryption for multiple recipients involves the use of two types of keys: the first type is a *message encryption key* k_m and the second type is a *recipient specific key* k_R. The idea proposed by Zheng [3] is to signcrypt k_m under each of the recipients specific keys and encrypt the message once under k_m. Other techniques for multi-recipient signcryption include multiple encryption with signature sharing [9] and the scheme recently proposed by Li et al. [10] which is based on bilinear pairings [11] over elliptic curves. However, the computational cost of bilinear pairings is generally greater than that associated with multiplications and exponentiations.

3. Proposed secure group communications protocol

The proposed group communications protocol consists of the following five procedures. The protocol involves a trusted Group Manager (GM) who sets up the system and interactively manages addition of new members to the group.

- *System setup:* The group manager selects the system-wide public parameters [12]. To setup the system the group manager computes the following values.
- Two large primes p and q such that $q \mid p-1$, i.e. q divides $p-1$.
- A cyclic group $G = <g>$ of order q, usually taken to be a subgroup of Z_p^*, in which computing discrete logarithms is infeasible [13]. The set associated with the group G may be $\{1,2,\cdots,q\}$.
- A secret master key d is chosen at random from the set Z_q^*.

The GM publishes the public parameters of the system $params =< p,q,G,g >$ and keeps his administration key $SK =< d >$ a secret.

- *Join:* This is an interactive protocol between the new group member u and the group manager. The new member u selects her secret key x_u, computes $y_u = g^{x_u} \bmod p$ and sends her membership key to the group manager who in turn sends her the membership certificate $v_u = (y_u)^d \bmod p$. The membership certificate is kept a secret while y_u is used as a public key for the member u. The distinction of the membership certificate from the private key of the member is intended to prevent a malicious group manager from impersonating any of the group members.
- *Session key establishment:* The main contribution in this paper is in this module. The session key is made recoverable to the intended set of recipients as well as the sender through a specially designed polynomial given below. Other mechanisms for broadcasting a secret session key have been proposed in literature, for instance the scheme suggested in [14]. However, the scheme in [14] involves polynomial interpolation to recover the session key which is more expensive than the procedure proposed below. Furthermore, the scheme in [15] for conference key distribution is based on multiple exponentiations by end users whose computational capabilities may be limited. On the other hand, in the proposed module end users perform polynomial evaluation which may be efficiently carried out by means of Horner's method.

The session key establishment module is an interactive protocol between the GM and the sender Alice. Both sides should abide by the following steps.

1. Alice sends a broadcast request to the group manager indicating the set of desired recipients.
2. The GM prepares the following polynomial

$$f(\xi) = [(\xi - v_a)(\xi - v_{i_1})\cdots(\xi - v_{i_N}) \times (\xi - w_1)\cdots(\xi - w_{N^*})] + k_m$$

where v_{i_j} are membership certificates of desired recipients, v_a is the sender's certificate and w_i are random elements not equal to any membership certificate given to any system user. The purpose of adding those random elements is to hide the number of recipients as well as raise the degree of the polynomial to ensure the hardness of its factorization. The randomization process adds security to the scheme. k_m is a randomly chosen integer belonging to the set $\{1,2,\cdots,q-1\}$.

It is clear that the intended set of recipients can easily recover the message encryption key k_m by substituting their membership certificates into the polynomial $f(\xi)$, simply $k_m = f(v_{i_j})$. Similarly, the sender could recover k_m as $k_m = f((v_a)$.

3. The GM broadcasts the coefficients of the polynomial $f(\xi)$ after reducing them modulo q.

- *Signcryption:* The sender Alice having a private/public key pair (x_a, y_a), then signcrypts the message m using the key k_m as follows:

a. Recover $k_m = f(v_a)$

b. Pick x randomly from the set $\{1,2,\cdots,q-1\}$ and let $k=(g^x)^{k_m} \bmod p$.
c. Split k into k_1 and k_2 of appropriate length.
d. $r=KH_{k_1}(m) \bmod q$
e. $s=x(r+x_a)^{-1} \bmod q$
f. $c=E_{k_2}(m)$
g. Broadcast the signcrypted text (c, r, s)

- *Unsigncrypt:* Any member of the set of desired recipients whose certificate is v_{i_j} can follow the steps given below to retrieve the message.

a. Recover $k_m=f(v_{i_j})$
b. Recover k, where $k=(g^r y_a)^{s\,k_m} \bmod p$
c. Split k into k_1 and k_2.
d. $m=D_{k_2}(c)$
e. Accept m as a valid message originated from Alice only if $KH_{k_1}(m)$ is identical to r.

The following figure summarizes the proposed protocol.

4. Consistency of proposed protocol

The consistency of the proposed protocol may be validated through verifying that the key k is correctly recovered in the unsigncryption phase. This is easily seen by the following argument.

$$(g^r y_a)^{s\,k_m}=(g^r g^{x_a})^{s\,k_m}=(g^{r+x_a})^{s\,k_m}$$
$$=(g^{r+x_a})^{x(r+x_a)^{-1}k_m}=g^{x\,k_m}=k$$

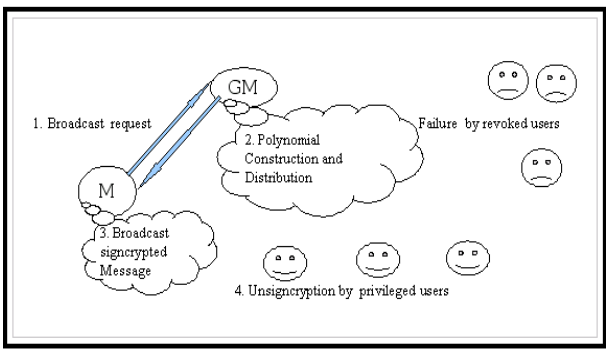

Fig.1. Summary of the proposed group communications protocol basic steps.

Hence, any intended recipient can retrieve the original message m correctly.

5. Performance evaluation

Using the approach proposed by Zheng [3] of signcrypting the message encryption key k_m for each of the N recipients requires $3N|q|$ communication overhead, where $|q|$ denotes the number of bits used to represent the integer q. In our proposed protocol, the message overhead is reduced to $(N+3)|q|$ which is the overhead associated with broadcasting the polynomial $f(\xi)$ and the signature pair (r,s). Thus, the bandwidth requirements are reduced by a factor of $1/3$. On the other hand, in the scheme due to Boyen [9], the communications overhead is $2N$. Generally, $|q|$ is in the order of 256 bits and the number of recipients may be thousands and even millions in some applications. For, the communications overhead of the proposed scheme is 2.56Mb compared to 7.68Mb. The reductions are significant and this is more clear in case of multi-media data transfer, where the message is broken down into a large number of packets each being treated as a separate message requiring authentication and protection on its own.

As for the computational overhead, instead of requiring O(N) exponentiations, which is an expensive operation, O(N) inversion and multiplication operations to signcrypt the message per user, O(N) multiplications are required for the construction of the polynomial and its evaluation using Horner's method [16]. The message is signcrypted only once saving a lot of computational work.

The security of the proposed multi-recipient scheme rests on the hardness of the factorization of polynomials. The proposed scheme is of value for large groups of recipients and hence the polynomial constructed would be of high enough degree to prevent its factorization.

It is noteworthy that the proposed scheme includes a trusted third party, namely the group manager. This does not hinder its

functionality as in many applications, there is inherently a group leader who is naturally trustworthy.

In order for the scheme to support non-repudiation, the identity of the sender may be appended to the message [2]. The fourth step of the signcryption phase is modified to be as follows:

$bind = y_a || y_1 || y_2 || \cdots || y_N, r = KH k_1(m, bind)$, where y_a is the public key of the sender, y_i's stand for the public keys of the recipients, and || denotes the concatenation operator.

6. The proposed scheme over elliptic curves

In this section, multi-recipient signcryption over elliptic curves over finite fields is considered. It is well-known that elliptic curves based schemes achieve the same level of security compared to schemes which do not employ elliptic curves but using keys of smaller size [17]. In this case, $|q|$ is in the order of 150 bits instead of 256 bits when working with Z_p.

An elliptic curve is defined by the equation

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

where $D = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2 \neq 0$ and $x \in F_p$ for some finite field F_p. One of the popular elliptic curves used in cryptography is given by $y^2 = x^3 + 1$ over F_p, where p is a prime satisfying $p \equiv 2 \mod 3$ and $p = lq - 1$, where q is also a prime. In what follows, let E be the elliptic curve defined by the equation above over F_p and let G be the subgroup of points on E of order q.

An adaptation of the proposed scheme in case of elliptic curves is given below.

- *System setup:* GM selects the system-wide public parameters.
- Two large primes p and q such that $p = lq - 1$.
- E an elliptic curve over Z_p.
- G =<P> a subgroup of points on E of order q.
- A secret master key d is chosen at random from the set Z_q^*.

The GM publishes the public parameters of the system $params =< p, q, G, P >$ and keeps his administration key $SK =< d >$ a secret.

- *Join:* This is an interactive protocol between the new group member u and the group manager. The new member u selects her secret key $x_u \in Z_q^*$, computes $y_u = x_u P$ (a multiple of the generator point P) and sends her membership key to the group manager who in turn sends her the membership certificate $v_u = dy_u = dx_u P$. The membership certificate is kept a secret while y_u is used as a public key for the member u. It is noteworthy that the discrete logarithm problem over elliptic curves is even harder than over Z_p, i.e. given xP it is computationally infeasible to compute x.
- *Session key establishment:* This module remains unchanged except that the x-coordinate of the point v_i is involved in the polynomial construction, thus the y-coordinate is ignored which is common practice as it contains a single bit of information. The GM prepares the following polynomial

$$f(\xi) = (\xi - v_{a,x})(\xi - v_{i_1,x}) \cdots (\xi - v_{i_{N,x}}) \times (\xi - w_1) \cdots (\xi - w_{N^*}) + k_m$$

where $v_{i_j,x}$ are the x-coordinates of the membership certificates of desired recipients, $v_{a,x}$ is the sender's certificate and w_i are random elements not equal to any membership certificate x-coordinate given to any system user. k_m is a randomly chosen integer belonging to the set $\{1, 2, \cdots, q-1\}$.

The GM then broadcasts the coefficients of the polynomial $f(\xi)$ after reducing them modulo q.

- *Signcryption:* The sender Alice having a private/public key pair (x_a, y_a), then signcrypts the message m using the key k_m as follows:

a. Recover $k_m = f(v_{a,x})$

b. Pick x randomly from the set $\{1,2,\cdots,q-1\}$ and let $k = hash(xk_mP)$, here again only the x-coordinate of the point xk_mP is involved in the hashing operation.
c. Split k into k_1 and k_2 of appropriate length.
d. $r = KH_{k_1}(m, bind) \bmod q$
e. $s = x(r + x_a)^{-1} \bmod q$
f. $c = E_{k_2}(m)$
g. Broadcast the signcrypted text (c, r, s)

- *Unsigncrypt:* Any member of the set of desired recipients whose certificate is v_{i_j} can follow the steps given below to retrieve the message.

a. Recover $k_m = f(v_{i_j}, x)$
b. Set $u = s\,k_m \bmod q$ and recover k as $k = hash(uy_a + urP)$
c. Split k into k_1 and k_2 .
d. $m = D_{k_2}(c)$
e. Accept m as a valid message originated from Alice only if $KH_{k_1}(m, bind)$ is identical to r.

The key recovery process of the proposed scheme is validated by the following arguments.

$$\begin{aligned} hash(uy_a + urP) &= hash(s\,k_m x_a P + s\,k_m rP) \\ &= hash([s\,k_m(x_a + r)]P) \\ &= hash([x(r + x_a)^{-1}(x_a + r)\,k_m]P) \\ &= hash(xk_mP) = k \end{aligned}$$

7. The proposed scheme as a framework for multi-recipient signcryption

The proposed scheme may be viewed as a general framework to construct a multi-recipient version of a single user signcryption scheme based on discrete logarithms over finite fields. The message encryption key km replaces the single recipient key in the signcryption phase. As shown above, only the intended set of recipients can recover k_m from the polynomial $f(\xi)$.

For instance, consider the signcryption scheme based on Schnorr's signature [18-19] which may be extended to the multi-user case as follows.

Signcryption by a member Alice

1. Recover $k_m = f(v_a)$
2. Pick x randomly and let $k = (g^x)^{k_m} \bmod p$
3. Split k into k_1 and k_2 of appropriate length.
4. $r = KH_{k_1}(m \,||\, y_a \,||\, y_1 \,||\cdots||\, y_N) \bmod q$
5. $s = x - rx_a \bmod q$
6. $c = E_{k_2}(m)$
7. Broadcast the signcrypted text (c, r, s)

On receiving (c, r, s), any of the set of intended recipients unsigncrypts it using the following procedure.

Unsigncryption by any other Group Member Bob

1. Recover $k_m = f(v_b)$
2. Recover k, where $k = (g^s y_a{}^r)^{k_m} \bmod p$
3. Split k into k_1 and k_2.
4. $m = D_{k_2}(c)$
5. Accept m as a valid message originated from Alice only $KH_{k_1}(m \,||\, y_a \,||\, y_1 \,||\cdots||\, y_N)$ if is identical to r.

The key recovery process is validated as follows.

$$(g^s y_a{}^r)^{k_m} = (g^{x - r x_a} g^{x_a r})^{k_m} = g^{x\,k_m} = k$$

The advantage of using Schnorr's signature scheme is that it saves the computation of an inverse compared to the original scheme by Zheng.

8. Real life applications

Broadcasting a message to multiple users in a secure and authenticated manner is an important facility for a group of people who are jointly working on the same project to communicate with one another. Consider, the manager of a large enterprise who needs to securely communicate with his employees. He needs to share his opinions and experience with them to achieve the best profit possible. Moreover, various employees need to communicate with one another, with the manager naturally being able to monitor all such communications. Information leakage to other competitors means failure on the market.

Further applications include virtual conferences [20]. Typical scenarios include on-

line meetings of corporate executives or committees, town-hall type meetings, interactive lectures and classes, and multi-party video games. In a virtual conference, sender authenticity is the most crucial security concern. With multi-media data over limited bandwidth channels, the reductions offered by the proposed scheme are essential.

The proposed protocol achieves the requirements of such systems in a straightforward manner making it an appealing choice in these systems as well as other systems having similar requirements.

9. Conclusions

A new secure and authenticated group communications protocol based on multi-recipient signcryption has been proposed. The scheme reduces both the communications overhead and the computational costs required compared to re-signcrypting the message encryption key per user. The scheme allows secure communication and data origin authentication in large groups. The scheme has been adapted to the elliptic curves setting to further reduce the bandwidth requirements. The scheme is actually a framework that could be employed to construct other efficient multi-recipient signcryption schemes, for instance a multi-recipient signcryption scheme based on Schnorr's signature is offered as an example.

References

[1] Y. Zheng, Digital Signcryption or How to Achieve Cost (Signature and enCryption) << Cost (Signature) + Cost(Encryption), In Advances in Cryptology CRYPTO' 97, Vol. 1294 of LNCS, pp. 165-179, Springer-Verlag (1997).

[2] J. Baek, R. Steinfeld and Y. Zheng, Formal Proofs for the Security of Signcryption, In Proceedings of PKC'02, Springer LNCS 2274 (2002).

[3] Y. Zheng, Signcryption and its Applications in Efficient Public Key Solutions, In Proceedings of ISW'97, pp. 291-312 (1998).

[4] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory IT-31 (1985).

[5] A.P. Menezes, Van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press (1996).

[6] National Bureau of Standards: Data Encryption Standard. FIPS PUUB 46 U.S. Department of Commerce, January (1977).

[7] Y. Zheng and H. Imai, "Efficient Signcryption Schemes on Elliptic Curves," In Proceedings of IFIP SEC'98, Chapman and Hall, Vienna (1998).

[8] J. Malone-Lee, Signcryption with Non-Repudiation, Technical Report CSTR-02-004, Department of Computer Science, University of Bristol, June (2002).

[9] X. Boyen, "Multipurpose Identity-Based Signcryption: A Swiss Army Knife for Identity-Based Cryptography", In Advances in Cryptology, CRYPTO, LNCS 2729 (2003).

[10] F. Li, Y. Hu and S. Liu, "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 (2006).

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing, In Advances in Cryptology", ASIACRYPT, LNCS 2248 (2001).

[12] J. Camenisch and M. Stadler, "Efficient Group Signature Schemes for Large Groups," LNCS No. 1294, pp. 410-424 (1997).

[13] K. Rosen, "Elementary Number Theory and Its Applications," Addison-Wesley Publishing Company (1984).

[14] S. Berkovits, "How to Broadcast a Secret, In Advances in Cryptology", EUROCRYPT'91, LNCS 547 (1991).

[15] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System", In Advances in Cryptology -- EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 275-286 (1995).

[16] J. Gathen and J. Gerhard, "Modern Computer Algebra", Cambridge University Press (1999).

[17] Niven, H. Zuckerman and H. Montgomery, An Introduction to the Theory of Numbers, John Wiley and Sons, Inc., 5th Edition (1990).
[18] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and Sons, New York (1993).
[19] C. Schnorr, "Efficient Signature Generation for Smart Cards", Journal of Cryptology, Vol. 4 (3), pp. 239-252 (1991).
[20] R. Canetti et al., "Multi-cast Security: A Taxonomy and Some Efficient Constructions", In Proceedings of INFOCOM'99, Vol. 2, pp. 708-716, New York, NY, March (1999).

Received August 14, 2007
Accepted March 19, 2008