A Multicasting Scheme Based on Signcryption for Dynamic Groups

Sanjeev Agnihotri[1] and Uma Kumari[2]

[1] Department of Information Technology, Modi Institute of Technology
Kota, Rajasthan, India

[2] Department of Computer Science and Information Technology, Shekhawati Engineering College,
Sikar, Rajasthan, India

Email: sanjiv_agnihotri@rediffmail.com

Abstract

A cryptographic primitive is termed as “signcryption" which simultaneously fulfills both the functions of digital signature and public key encryption in a logically single step and with cost significantly smaller than that required by signature-then-encryption as proved by Zheng[1]. Signcryption satisfies unforgeability and it focuses on point-to-point communication . In this algorithm a new signcryption scheme has been proposed for multiple broadcasters and for multiple recipients in distributed environments by creating a new hierarchical tree for every broadcaster having scalability and containment features. This is achieved by the use of routers connected to various stages which will perform the proxy encryption work. At any stage any of the routers may perform the filtering work as it can act as filter and can perform whether incoming packet is for connected subtree. The beauty of this algorithm is that there can be any number of users connected to the routers. The users may be added or deleted time to time we can use untrusted parties as intermediatery routers which won’t get any idea of what is broadcasted.

Keywords: *Signcryption, Multiple broadcast, Filter, containment, proxy encryption, rekeying, asymmetric cryptography.*

1. Introduction

To avoid forgery and ensure confidentiality to the contents of a letter, for centuries it has been a common practice for the originator of the letter to “sign” his or her name on it and then seal it in an envelope, before handing it over to a deliverer. Then a two-step process “public key cryptography” discovered nearly three decades ago which has revolutionized the way for people to conduct secure and authenticated communications. It became possible for people who have never met before to communicate with one another in a secure and authenticated way over an open and insecure network such as Internet. In doing so, the same two-step approach has been followed. Before a message is sent out, the sender of the message would sign it using a digital signature scheme and then encrypt the message (and the signature) using a private key encryption algorithm under a randomly chosen message encryption key. The random message encryption

key would then be encrypted using the recipient's public key. We call this two-step approach "signature-then-encryption".

Signature generation and encryption consume machine cycles and also introduce "expanded" bits to an original message. A comparable amount of computation time is generally required for signature verification and decryption. Hence the cost of a cryptographic operation on a message is typically measured in the message expansion rate and the computational time invested by both the sender and the recipient. With the standard signature-then-encryption approach, the cost for delivering a message in a secure and authenticated way is essentially the sum of the cost for digital signature and that for encryption.

It is possible to transfer a message of arbitrary length in a secure and authenticated way with an expense less than that required by signature-then-encryption. A new cryptographic primitive is termed as "**signcryption**" which simultaneously fulfills both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly smaller than that required by signature-then-encryption [1,9]. For size of public moduli = 512 bits, signcryption costs 58% less in average computation time and 70% less in message expansion than does signature-then-encryption it is based on the discrete logarithm problem[7], which is based on the difficulty in factorization of large numbers . A comparison of performance and cost involved using Zheng signcryption scheme is compared to well known sign-then-encrypt scheme like RSA, DSS combined with Elgamal , Schnorr signature then Elgamal encryption as mentioned in [1]. Thus, signcryption is the best option for digitally signing the message.

Signcryption techniques generally has a signcrypting algorithm S at the sender end and a unsigncrypting U algorithm at the receiver end has following characteristics :

1)Unique unsigncryptability --Given a message m of arbitrary length, the algorithm S signcrypts m and outputs a signcrypted text C. On input C, the algorithm U unsigncrypts C and recovers the original message at the receiver end.

2)Security -- (S, U) fulfills both the properties of a secure encryption scheme and those of a secure digital signature scheme at the same time. Any of the attacker can not find out the message until the private key of receiver is known and the receiver is sure that whatever is message she is getting as a result of U is unforged and signed by an authentic person.

3)Efficiency – Signcryption is economical in terms of computational time i.e., computational time involved both in signcryption and unsigncryption, and the communication overhead or adding redundant bits to prove authenticity of the message is much smaller smaller than that required by signature-then-encryption scheme as proved by Zheng in [1,9].

2. Related Works

The signcryption scheme first proposed by Zheng [1] was not having non repudiation using public verification later schemes provide these by bits sent on un-secure channel. Besides this, Zheng scheme did not provided any method for broadcasting of data to selective users. Broadcast encryption scheme allow a multiple broadcasting channels and each may have zero or any number of receivers. In [3] we have a multiple broadcaster signcryption scheme discussed it is like Pay-TV channel where a broad caster is sending data to multiple users. It has a public

verifiability facility but has following shortcomings. **Firstly**, this scheme does not have the capability to scale i.e., receivers can not be added or deleted. There is no provision of rekeying once the session got started it has to adhere to a set of keys . So, it is more vulnerable to be broken. **Secondly**, the message which is broadcasted is $(C,S,w_2,P_0,P_1....P_t)$ where t is the number of receivers, the greatest disadvantage associated here is a large chunk has been broadcasted which might be greater than the message itself if number of users are large. **Thirdly**, when the message approaches at the receiver it has to apply a formula and it has to multiply all of these $(P_0,P_1....P_t)$ which might incur in a great loss of computation power. Because of all these shortcomings it might happen that whole purpose of including signcryption in multiple broadcasts will be lost. In [4] We have a signcryption scheme which is having low cost and public verifiability ensure confidentiality again it is not covering multiple broadcasts it covers only point to point communications. In [5] We have a scalable multicast security and dynamic recipient groups which works fine when the topic of concern is only communication / broadcasts , JOIN and LEAVE security , containment, scalability. Here we can't obtain authenticity and unforgeability, which is required when a signed confidential document is to be broadcasted to a set of members.

3. Proposed Solution

The proposed scheme "A Multicasting scheme based on Signcryption for dynamic groups" some set of broadcasters are there and we have some users, the broadcasters provide the services to selected users logically in a group. We may assume that there are n authentic broadcasters {B1,B2..Bn}, and receivers are {U1,..Um}.

3.1 Hierarchical tree

A hierarchical tree is made by each broadcaster having intermediatery router(s) and users come at leaves of the tree. As shown in fig-1. Stage1 router(s) are directly connected to broadcaster the routers perform some conversion work.

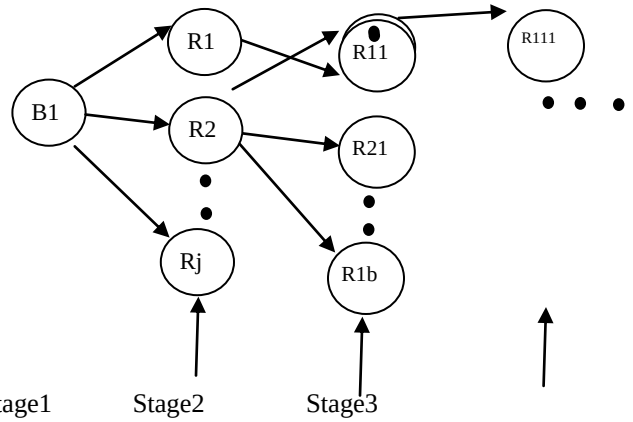

Fig 1 : Hierarchical tree illustrating broadcaster B1 and routers at various stages

Above naming conventions are used throughout this paper the users are directly connected thru routers at different stages. For illustration we have a broadcasting hierarchical tree for B1, each broadcaster has its own hierarchical tree the users in different hierarchical trees can be shared. Each router has a corresponding set of users as shown in fig-2. Any number of routers may be connected to any stage router as shown in fig-2, the nomenclature used for users connected to router(R1) is $\{U_{11}..U_{1c}\}$

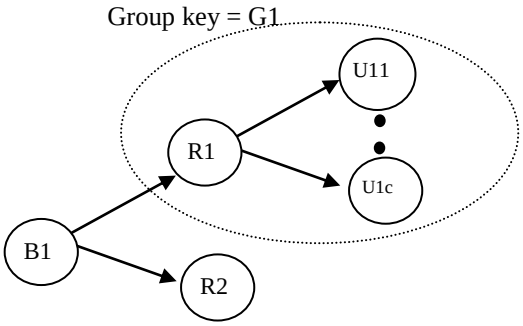

Fig 2 : Illustrating group and group key

3.2. Key terms

Trusted Authority (TA) : Sets up hierarchical tree for each broadcaster, tree consist up of routers and users.

Broadcaster (B) : A station interested in sending some digital document which is digitally signed by the broadcaster , this document is to be sent to selective users. Each user is able to verify that the document it has received is unforged and authentic.

Users (U) : Nodes which are interested in receiving the digitally signed document each user is a member of any one group only, however same node may be members of different groups but all groups must be from different hierarchical trees for different broadcasters.

Stage : The various levels in any hierarchical tree

Router (R) : Nodes which are responsible for doing some processing like doing filtering work so as to allow the packet to its respective sub tree and routing work i.e., receive incoming traffic do some conversion and send it to all outgoing lines, we assume that routers perform their work sincerely.

Scalability : The extra work incurred in processing of each action in terms of number of group members i.e., users like adding and removing users.

Containment : A security action applied in one group does not affect other subgroups.

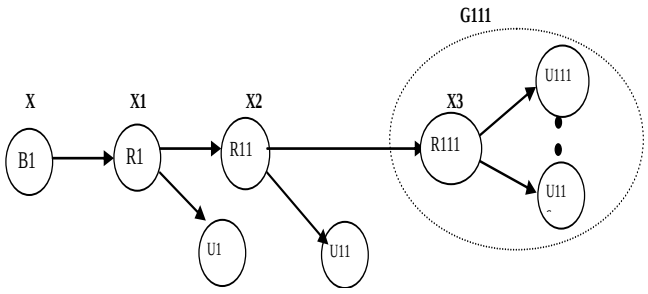

Fig 3 : Illustrating broadcaster B1, Router R1 , R11, R111 at stages 1,2,3 respectively

TA is a controlling authority which decides the structure of hierarchical tree, TA also provide the set up that which Bi, ($1 \leq i \leq n$) may have the corresponding set of routers and users and which routers come at which stages as in fig-1 and which users are connected to which stages as in fig-2. Once hierarchical tree for each broadcaster has been generated (say B1) 6 phases are there to do complete operation.

3.3. Phases

3.3.1. Setup phase

In this the T "Trusted third Party" sets up the hierarchical tree for each broadcaster (B1 for instance) as follows

- Decides number of routers at various stages and also provide preliminary structure as to which users are connected to which routers later insertion and deletion are dealt by the routers and broadcasters (B1 for instance) by using rekeying

Each *broadcaster*(B1 for instance) decides

- X a large number which is distributed to routers at various stages. let there are **s** stages then $X=\sum X_i$ where $1 \leq i \leq s$
- All X_i are distributed such that X_i is known only to i^{th} stage routers for this a secure communication mechanism may be used
- B1 has to ensure that each user U connected to router at stage i must know the X_i sums of the next (s-i) stages .

Each *router* at t^{th} stage

- Accepts incoming packet and checks whether it is destined to the corresponding sub tree in filtering phase.
- group key which is only known to the users connected to this router e.g., G111 in fig -3.

The variables, hash, keyed one way hash, encryption / decryption all set up in this phase for the tree rooted at B1

Variable / Function	Description
P	a large prime of length at least 512 bits
Q	a large prime factor of (p-1)
G	integer in the interval [1..p-1] with order q modulo p
hash(.)	is a one way hash which maps arbitrary long inputs into a string of length 256 bits for this any hash algorithm like SHA can be used
E(.)	is a symmetric encryption algorithm like AES
D(.)	is a compatible symmetric decryption algorithm

3.3.2. Key generation phase

- Each broadcaster chooses his private key X_{Bi} in the interval [1..q-1] and computes the corresponding public key as $Y_{Bi}=g^{(XBi)} \bmod p$, for all $1 \leq i \leq n$
- $X \in Z^*_p$ generated by B1 and is divided into s values such that $X= X_1+X_2+..+X_s$, all X_i are kept secret by B1 and each router of i stage will get X_i and is kept secret by the routers of that stage and so on.
- A random number **r** is generated by B1 and is kept secret by B1 itself.
- A symmetric key i.e., Group key which a random number G (e.g., G11 in fig-2) generated by each router R (e.g., R1, R11, R111 in fig-3 and R1,R2 in fig-2) and kept secret by respective router and known to all the users connected to it.

3.3.3. Signcryption phase

To encrypt a message **m** the broadcaster performs following steps

1. Choose a number '**r**' randomly in range [1..(q-1)]
2. Compute $\beta= Y_{B1}{}^r.g^{Xr} \bmod p$
3. Compute $k1=Hash(Y_{B1}{}^r \bmod p)$
4. Compute $k2=(g^r \bmod p)$
5. Compute $C = E_{k1}(m)$
6. Compute $R = Hash(C\| K2)$
7. $S = [r - X_B . R]$
8. Broadcast (C || R || S , β, k2)

3.3.4. Filtering Phase

1. The ciphertext (C || R || S , β, k2) is accepted on its incoming line before being transmitted to the next level routers or to the users.
2. Routers perform check on partial cipher text as

- Compute ϵ = hash(C || k2)
- On completing above step verify that
  $K2=(g^S . Y_{B1}{}^R) \bmod p$

If this equation holds then the cipher text (C || R || S , β, k2) is correct and the router forwards this to the corresponding subtree.

3.3.5. Routing phase

Routers (intermediatery nodes in the hierarchical tree) and users which are at leaves perform the conversion work. We assume some trust on the routers as they pass the incoming broadcasted traffic do some processing and broadcast it to all outgoing lines may be to the users or to the next stage routers which are directly connected to it. Processing done by routers is as follows

1) Accept (C || R || S , β, k2) on its incoming line
2) Let the router is stage i router then it must be having a portion of X i.e., Xi (which is known to all the routers of this stage this is devised at the time of set up of tree by TA(trusted authority)then it will perform

- Accept the incoming message from stage i-1 router ie, (C || R || S , β_{i-1}, k2) where $\beta_{i-1=} Y_{B1}{}^r.g^{(X-(X1+X2..+X_{i-1}))r} \bmod p$
- Router will perform

$$\beta_i = \beta_{i-1} / (g^r)^{X_i} \bmod p$$
$$= Y_{B1}{}^r.g^{(X-(X1+X2..+X_{i-1}))r} \bmod p$$
$$= \frac{Y_{B1}{}^r.g^{(X-(X1+X2..+X_{i-1}+X_i))r}}{(g^r)^{X_i} \bmod p} \bmod p$$

- Then i^{th} stage router broadcast message (C || R || S , β_i, k2) to stage i+1 routers and to broadcast E_G((C || R || S, β_i, k2)) to all the users connected to stage i routers as these users are supposed to decrypt the message and they have to prove that they are authentic users by D_G((C || R || S , β_i, k2))

3.3.6. Unsigncryption phase

This is done by the users connected to the routers at any stage ranging from 1 to s where s is maximum stage. Processing done by users is as follows :

CASE 1. Consider that a user(s) is(are) connected to first stage router say R1 which is directly connected to B1

1) Accept E_G (C || R || S , β_1, k2) , perform D_G (C || R || S , β_1, k2) on its incoming line where $\beta_{1=} Y_{B1}{}^r.g^{(X-X1)r} \bmod p$
2) At time of set up of tree it has been specified that user connected to stage 1 must have X2+X3+..+Xs the user will perform

R' = Hash(C || k2)
K2' = Hash(($g^S . Y_{B1}{}^{R'}$)mod p)
If R = R' and K2 = K2' then compute

$$k1 = \frac{Y_{B1}{}^R.g^{(X-X1)r} \bmod p}{(g^r)^{X2+X3+..+Xs} \bmod p} \bmod p$$
$$= Y_{B1}{}^R.g^{(X-X)r} \bmod p$$

$= Y_{B1}^{R} \bmod p$

where $X = X1+X2..+Xs$

3) $m = D_{k1}(C)$

CASE 2. Consider that a user(s) is(are) connected to i^{th} stage router

1) Accept $E_G (C \| R \| S , \beta_i, k2)$, perform $D_G (C \| R \| S , \beta_i, k2)$ on its incoming line where $\beta_{i=} Y_{B1}^{r}.g^{(X-X1-..-Xi)r} \bmod p$
2) At time of set up of tree it has been specified that user connected to stage i must have $X_{i+1}+..+Xs$ the user will perform

$R' = Hash(C \| k2)$

$K2' = Hash((g^{S} . Y_{B1}^{R'}) \bmod p)$

If $R = R'$ and $K2 = K2'$ then compute

$$k1 = \frac{Y_{B1}^{R}. .g^{(X-X1-..-Xi)r}}{(g^{r})^{X_{i+1}+..+Xs}} \bmod p$$

$= Y_{B1}^{R}.g^{(X-X)r} \bmod p$

$= Y_{B1}^{R} \bmod p$

where $X = X1+X2..+Xs$

3) $m = D_{k1}(C)$

CASE 3. Consider that a user(s) is(are) connected to last stage router i.e., at stage = s

1) Accept $E_G (C \| R \| S , \beta_s, k2)$, perform $D_G (C \| R \| S , \beta_s, k2)$ on its incoming line where $\beta_{s=} Y_{B1}^{r}.g^{(X-X1-..-Xs)r} \bmod p = (Y_{B1})^{r} \bmod p$
2) At time of set up of tree it has been specified that user connected to stage i must have 0 as part for x the user will perform

$R' = Hash(C \| k2)$

$K2' = Hash((g^{S} . Y_{B1}^{R'}) \bmod p)$

If $R = R'$ and $K2 = K2'$ then compute

$k1 = Y_{B1}^{R}.g^{(X-X)r} \bmod p$

$= Y_{B1}^{R} \bmod p$

3) $m = D_{k1}(C)$

4. Analysis of Proposed Solution

4.1 Privacy in broadcasting

Only users who are attached to respective routers at various stages can decrypt the original message.

4.2 Incorporating dynamic JOIN / LEAVE

Users in various groups can join or leave dynamically any user who joins router **R** at stage i, then only the group key (G_1 as in fig-2 and G_{111} as in fig-3) has to be modified. For illustration if a user joins the group of router R111 then in order to work properly it must have two values say Group key and $X_{(i+1)}+..+X_s$. Both these keys are obtained as follows

- New joining user decides a private- public key pair (X_U, Y_U).
- Router generates G_i new and sends G by $\mathbf{E}_{YU}$ (G_i)
- Broadcaster B1 sends $X_{(i+1)}$+..+X_s by $\mathbf{E}_{YU}(X_{(i+1)}+..+X_s)$

When a user leaves the group then only rekeying is done by the router and sent to all the currently active users by encrypting newly generated key using their public keys. The left user can't interfere in future as she is not having new G_i.

4.3 Scalability

This achieves scalability as some extra work incurred in processing of join or leave action in terms of number of group members i.e., users. But this does not scale when routers join or leave, at that time complete restructuring of hierarchical tree is to be done.

4.4 Containment

Proposed algorithm has containment property as it won't create any impact on any other group when users JOIN / LEAVE.

4.5 Fixed size message

Only fixed size message is broadcasted to next stage routers and to users of same stage.

4.6 Filtering at intermediatery nodes

Filtering can be used at the routers to enhance the performance of the Multiple Broadcasting system.

5. Conclusion & Future work

In this paper we presented a multiple broadcasting signcryption scheme which allows multiple broadcasters to send signed data to selected set of users authorized by Trusted Authority (TA). Security of proposed scheme is intractability of DLP and reversing one-way hash function. This F-MBSS provided a public cipher text authenticity and enables the gateway to the sub system connected to it (routers or users) without knowing the contents of the message. The transmitted text can be easily verified by the users connected at any stage. The stages are static i.e., the number of levels consisting of routers in the proposed tree is fixed but the users are dynamic i.e., they may be added or removed . This won't affect other routers or users residing in other groups.

This concept may be extended in various dimensions like, firstly we have confined to fixed message sizes we can extend it to variable sized messages. Secondly, intermediatry routers are used to do some processing, but the channel may break if routers malfunction. Here we can include the possibility of selecting alternate path if router stops working / malfunction. Thirdly, we have considered only textual data we can think of extending the same concept to visual images.

References

[01]. Y. Zheng, "Digital Signcryption or How to Acheive Cost (Signature and Encryption) << Cost(Signature) + Cost(Encryption)," Advances in Cryptography, Proc. of CRYPT'97, LNCS 1294, Springer-Verlag, pp 165-179, 1997.

[02]. Yumei Cai and Jiwen Zeng "A method of identifying cheaters in secret sharing schemes based on signcryption," IEEE 2008, pp 1-4, 2008.

[03]. H. Elkamchouchi, M. Nasr, Roayat Ismail, "A new efficient multiple broadcasters signctyption scheme (MBSS) for secure distributed networks," Fifth International Conference on Networking and Services 2009 , IEEE, pp 204-209, 2009.

[04]. Fahad Ahmed, Dr. Faisal Bashir, Dr. Asif Masood, " A publicly verifiable low cost signcryption scheme ensuring confidentiality," Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010 , IEEE pp 232-235, 2010.

[05]. Refik Molva and Alain Pannetrat, "Scalable Multicast Security with dynamic recipient groups," ACM Transactions on Information and System Security, Vol. 3, No. 3, August 2000, ACM, pp 136-160, 2000.

[06]. Yun-Peng Chiu, Chin-Laung Lei and Chun-Ying Huang, "Secure Multicast using proxy encryption," Seventh International Conference on Information and Communications Security,2005, IEEE , Beijing, December 10-13, 2005.

[07]. William Stallings, Cryptography and network security principles and paradigms, Pearson Education, ISBN 81-7808-902-5, 2003.

[08]. Atul Kahate, Cryptography and network security, Tata McGraw-Hill, ISBN 0-07-049483-5, 2004.