Signature-then-encryption towards

A new paradigm of security

Prof. Pooja Kadam

Assistant Professor
Department of MCA,
Bharti Vidyapeeth's Institute of Management & Information Technology,
C.B.D. Belapur, Navi Mumbai, India

Prof. Divya PremChandran

Assistant Professor
Department of MCA,
Bharti Vidyapeeth's Institute of Management & Information Technology,
C.B.D. Belapur, Navi Mumbai, India

ABSTRACT

In traditional approach Signature-then-Encryption used to secure the message. It was a two step process where sender had to sign the message first and then encrypt it. Here we introduce "Signcryption", which fulfills both the functions of digital signature and public key encryption in a logical single step. The emergence of Signcryption has huge potential for assuring secure and authenticated transaction in computer networks. Signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption. Traditional method in cryptography is Hybrid encryption can be employed instead of simple encryption, and a single session-key reused for several encryptions to achieve better and overall efficiency across many signature-encryptions than a Signcryption scheme but the session-key reuse causes the system to loose security under even the relatively weak CPA model. This is the reason why a random session key is used for each message in a hybrid encryption scheme but for a given level of security (i.e., a given model, say CPA) a Signcryption scheme should be more efficient than any simple signature-hybrid encryption combination.

KEYWORDS

Authentication, Digital Signature, Encryption, Key Distribution, Secure Message Delivery-Storage, Public Key Cryptography, Security, Signcryption, Group Key.

I. INTRODUCTION

In order to send a confidential letter in a way that it cannot be forged, it is a common practice for the sender of the letter to sign it, put in an envelope and then seal it before handing it over to be delivered. Discovering Pubic key cryptography has made communication between people who have never met before over an open and insecure network, in a secure and authenticated way possible. To avoid forgery and ensure confidentiality of the contents of a letter, for centuries it has been a common practice for the originator of the letter to sign his /her name on it and then seal it in an envelope, before handing it over to a deliverer. This two-step process is

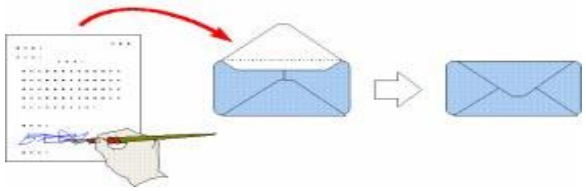

Figure1: Traditional "Signature-Then-Seal"

Public key cryptography has revolutionized the way people used to conduct secure and authenticated communications. It is now 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. Namely 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 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".

II. LITERATURE SURVEY

Traditional encryption techniques are the earliest methods of encryption and have been around for centuries. The main component of any traditional encryption technique was the alphabet.

Historians believe that the first case of cryptography was in ancient China where the written language itself was used as an encryption technique. The first documented use of cryptography, however, dates back to

1900 BC in Egypt, where inscriptions were found that contained, not a different set of hieroglyphs, but a system of partial nonstandard hieroglyphs.

The most famous traditional encryption method is probably the Caesar Cipher, developed by Julius between 50 and 60 BC. The Caesar Cipher worked on the principle of substitution, where each letter in the alphabet is substituted for another letter.

Modern encryption techniques

Modern encryption techniques are specifically designed for use on computers and no longer concern the written alphabet. The focus is on the use of binary bits. The cryptography is an important characteristic of modern encryption techniques.

Symmetrical Encryption

Also known as secret-key encryption, symmetrical cryptosystems require the sender and receiver to have the same secret key. This single key is required for both the encryption and decryption of the message. A classic among the symmetric ciphers is the Data Encryption Standard known as DES. DES was developed in the 1970s and got the official approval of NIST (The United States National Institute of Standards and Technology) in 1977. DES uses substitution and permutation to scramble the bits of a message. Today DES is considered to be a weak encryption method since it was compromised by a machine built by the Electronic Frontier Foundation in 1998.

While DES is still used frequently in governmental and military operations, it will soon be replaced with AES (Advanced Encryption Standard). The main problem with symmetrical encryption is that if the key is lost, or stolen, the entire transmission can be compromised since the interceptors can immediately decrypt the message with the one key. This leads to another problem which is the distribution of keys. A key must either be communicated in a face-to-face manner, or must be delivered through a very trusted courier. Both methods are inconvenient to both parties as well as putting the method at risk.

Asymmetrical encryption

Asymmetrical encryption methods, also referred to as Public Key encryption systems, were developed in 1976 by Whitefield Diffie and Martin Hellman. The principle of public key encryption is that parties, the sender as well as the receiver, have a pair of keys. The one key does not have to be kept secret and is called the public key. The two different keys held by the parties have different uses – one is used for encryption and the other for decryption. The encryption key is the public key, while the decryption key is the "private" key. The private key must be kept secret. The public and the private key are mathematically related so that anything encrypted with the one can be decrypted with the other. The sender takes the receiver's key, which is publicly available on a website for instance, and encrypts a message. He then sends it to the receiver who will only be able to decrypt the message with his private key. The main advantage of this method is that the sender and receiver do not have to exchange keys at any time.

III. PROBLEM DEFENITION

In order to send a confidential letter in a way that it cannot be forged, it has been a common practice for the sender of the letter to sign it, put it in an envelope and then seal it before handing it over to be delivered.

Discovering Public key cryptography has made communication between people who have never met before over an open and insecure network, in a secure and authenticated way possible. Before sending a message, the sender has to do the following:

- Sign it using a Digital Signature (DS) scheme
- Encrypt the message and the signature using a private key encryption algorithm under randomly chosen message encryption key
- Encrypt the random message encryption key using the receiver's public key
- Send the message following steps 1 to 3.

This approach is knows as signature-then-encryption. The main disadvantage of this approach is that, digitally signing a message and then encrypting it, consumes more machine cycles and bloats the message by introducing extended bits to it. Hence, decrypting and verifying the message at the receiver's end, a lot of computational power is used up. Thus you can say that the cost of delivering a message using signing-then-encryption is in effect the sum of the costs of both digital signatures and public key encryption.

Is it possible to send a message of arbitrary length with cost less than that required by signature-then-encryption?

Here we propose Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional signature followed by encryption.

IV. OBJECTIVES

Considering problem definition we framed following objectives.

(1) Signcryption provides confidentiality and authenticity.
(2) Signcryption schemes are more efficient, in terms of computational complexity and/or communication overhead, than the sequential composition of signature and encryption schemes.

Parameters public to all	**p** – a large prime number **q** – a large prime factor of p-1 **g** – an integer with order q modulo p chosen randomly from [1,…,p-1] **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
Sender's keys	$\mathbf{x_a}$ – Alice's private key, chosen uniformly at random from [1,…,q-1] $\mathbf{y_a}$ – Alice's public key ($y_a = gx_a \bmod p$)
Receiver's keys	$\mathbf{x_b}$ – Bob's private key, chosen uniformly at random from [1,…,q-1] $\mathbf{y_b}$ – Bob's public key ($y_b = gx_b \bmod p$)

(3) Some Signcryption schemes allow expensive cryptographic operation to be parallelized rather than that we should go with SDSS (Shortened Digital Signature Scheme) proposed by Elgamal scheme.
(4) Signcryption schemes can provide clear benefits over the traditional sequential composition of encryption and signature schemes.
(5) In Signcryption cost significantly lower than that required by the traditional "signature and encryption" approach.
(6) It is more secure because any two complex security schemes can be combined.

V. SCOPE

Already there are so many research has been done in the field of Signcryption, it is impossible to cover the entire field here. The Signcryption schemes which are presented here do not constitute exhaustive list, but we are intended to give overview and to propose the multiple receivers by introducing the concept of group key on which so many researches are going on. Broadcasting Signcrypted message is redundant in terms of bandwidth consumption and computational resource usage. Hence we are proposing the group
key concept for multiple receivers.

SIGNCRYPTION

Signcryption can be defined as a combination of two schemes; one of digital signatures and the other of public key encryption. One can implement Signcryption by using ElGamal's shortened digital signature scheme, Schnorr's signature scheme or any other digital signature schemes in conjunction with a public key encryption scheme like DES, 3DES. This choice would be made based on the level of security desired by the users.

Signcryption consist of pair of algorithm (S, U) Where S is called as Signcryption algorithm and U is called as Unsigncryption algorithm. Give a message M of arbitrary length, the algorithm S signcrypt M and output a signcrypt text C. On input C, the algorithm U unsincrypt C and recover the original message M. Here we present the implementation of Signcryption using ElGamal's shortened signature scheme and a public key encryption algorithm denoted by E and D (Encryption and Decryption algorithms).

SIGNCRYPTING A MESSAGE

These are the parameters involved in the signcryption algorithm

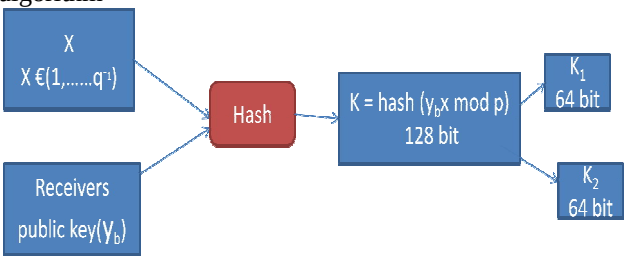

Figure 2.1 Signcryption - generating k1 and k2

1. Sender chooses a value x from the large range 1,…,q-1
2. Sender then uses Receiver's public key and the value x and computes the hash of it.
3. This will give a 128-bit string. K = hash (y_bx mod p)
4. Then splits this 128-bit value K into two 64-bit halves. We can name them as k_1 and k_2 and refer to them as the key pair.

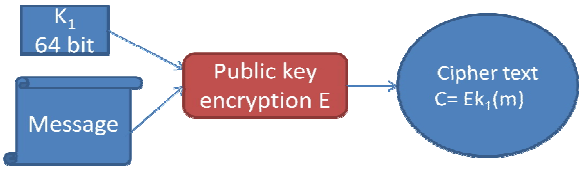

Figure 2.2 Signcryption - generating components c

Next, Sender encrypts the message m using a public key encryption scheme E with the key k_1.
This will give the cipher text c. **c** = E k_1 (m).

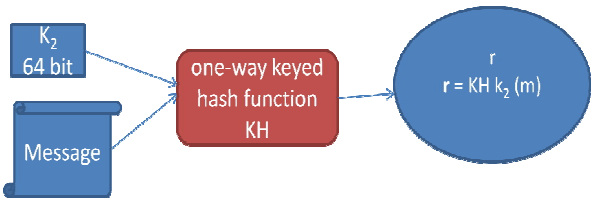

Figure 2.3 Signcryption - generating components r

Then, sender uses the key k_2 in the one-way keyed hash function KH to get a hash of the message m. This will give a 128-bit hash, which we will call r. This process uses the SDSS Algorithm. **r** = KH k_2 (m)

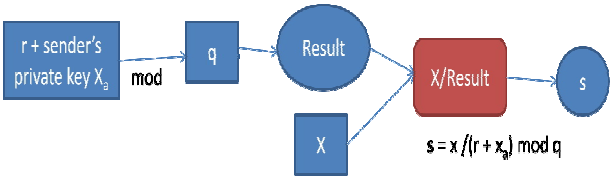

Figure 2.4 Signcryption - generating components s

Just like in SDSS, sender then computes the value of s. Sender does this using her private key x_a, the large prime number q and the value of r. **s** = x /(r + x_a) mod q

Sender now has three different values; **c**, **r** and **s**. Sender has to send these three values to receiver in order to complete the transaction. Sender can do this in a couple of ways send them all at one time or send it separately using secure transmission channels, which would increase security. Thus on sender part, Signcryption of the message is done.

UNSIGNCRYPTING A MESSAGE

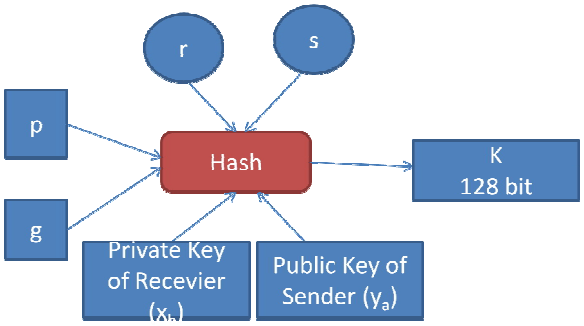

Figure 2.5 Unsigncryption - generating component k

Receiver receives the 3 values that sender has sent him, **c**, **r** and **s**. He uses the values of r and s, his private key x_b, sender's public key y_a and p and g to compute a hash which would give him 128-bit result. K = hash ((y_a * g^r)^s X x_b mod p). This 128-bit hash result is then split into two 64-bit halves which would give him a key pair (k_1,k_2). This key pair would be identical to the key pair that was generated while Signcrypting the message.

Now, Receiver then uses the key k_1, to decrypt the cipher text c, which will give him the message m. **m** = Dk_1(c)

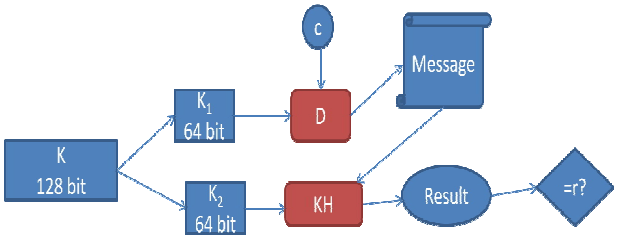

Figure 2.5 Unsigncryption – obtaining the message m and verification of the message m

Now Receiver does a one-way keyed hash function on m using the key k_2 and
compares the result with the value r he received from Sender. If they match, it
means that the message m was indeed signed by sender, if not receiver will

know that the message was either not signed by sender or was intercepted and
modified by an intruder. Thus Receiver accepts the message only if $KHk_2(m) = r$.

DISADVANTAGE OF SIGNCRYPTION

The way Signcryption algorithm works currently, Sender has to use Receiver's public key to Signcrypt a message. This has a disadvantage when you consider the need to broadcasta Signcrypted text. Imagine an ISP needs to send a Signcrypted message to number ofdistributors. With the current algorithm, it needs to Signcrypt the message with each of it's intended recipient's public keys and send them separately to each one of them. This approach is redundant in terms of bandwidth consumption and computational resource usage.

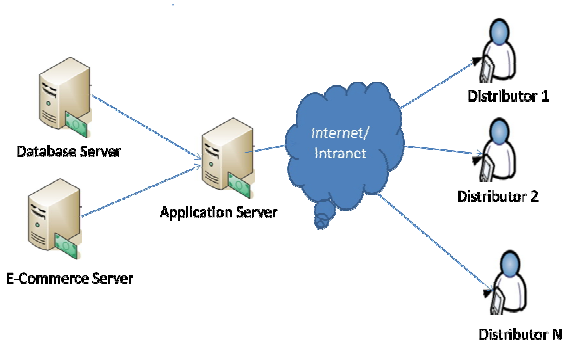

Figure 3 One-to-Many transmission

To solve this here we propose the concept of a group key between the ISP and the distributors, that it intends to send Signcrypted text and use that to broadcast
Signcrypted messages.

HOW GROUP KEY WILL WORK?

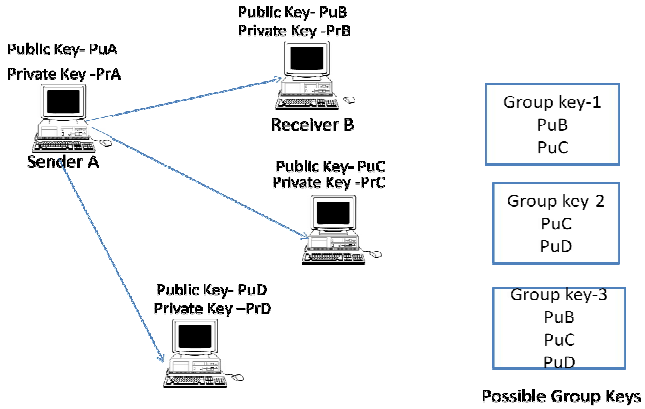

Figure 4 Model of Group Key

Here we propose that group key generation algorithm should be there through which we use public key of intended receivers to produce group key. In above figure Groupkey1 will send the data to B, C receivers, Groupkey2 will send the data to C, D receivers where as Groupkey3 will send the data to B, C, D receivers. Group key should be generated with combination of intended receiver's public key.

VI. CONCLUSION

Signcrytion is in incipient state. Signcryption or a modified usage of Signcryption can solve the problem by minimizing message size as well as ensuring unforgeability and nonrepudiation. Reasearch on Signcrytion are going on in fields like mobile computing and in banking sector.
Signcryption still has a long way to go before it can be implemented effectively and research is still going on in various parts of the world to try to come up with a much more effective way of implementing this.

REFERENCES

[1] Formal Proofs for the Security of Signcryption
- Joonsang Baek, Ron Steinfeld, Yuliang Zheng
- [http://coitweb.uncc.edu/~yzheng/publications/files/BaekSteifeldZheng-fsps-joc-bsz-261206.pdf]

[2] Identity-Based Signcryption
- John Malone Lee
- [http://eprint.iacr.org/2002/098.pdf]

[3] Signcryption scheme for Identity-based Cryptosystems
- Divya Nalla, K.C.Reddy
- [http://eprint.iacr.org/2003/044.pdf]

[4] Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes
- Yuliang Zheng
- [http://grouper.ieee.org/groups/1363/StudyGroup/contributions/signcr.pdf]

[5] Digital Signcryption or How to Achieve Cost(Signature&Encryption)<<Cost(Signature)Cost (Signature)+Cost (Encryption)
- Yuliang Zheng
- [http://www.signcryption.org/publications/pdffiles/yz-c97-fnl-rvs.pdf]

[6] Signcryption (Short Survey)
- Yevgeniy Dodis∗
- [http://www.cs.nyu.edu/~dodis/ps/signcrypt-survey.pdf]