Signcryption

1. Abstract

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 and encryption approach.

This document explains how Signcryption can be implemented. Moreover, it discusses the difference between Signcryption and signature-then-encryption, followed by the advantages and disadvantages of using Signcryption.

2. Introduction

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:

1. Sign it using a Digital Signature (DS) scheme
2. Encrypt the message and the signature using a private key encryption algorithm under randomly chosen message encryption key
3. Encrypt the random message encryption key using the receiver's public key
4. 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?

In 1997, Yuliang Zheng from Monash University in Australia discovered a new cryptography primitive called Signcryption.

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 digital signature followed by encryption.

2.1. Why Signcryption?

- Based on discrete algorithm problem, Signcryption costs 58% less in average computation time and 70% less in message expansion than does signature-then-encryption. [1]
- Using RSA cryptosystem, it costs on average 50% less in computation time and 91% less in message expansion than signature-then-encryption does. [1]

3. Mechanism

Signcryption is a combination of a digital signature algorithm and an encryption algorithm. We take a brief look at these two algorithms in the following sections.

3.1 Shortened Digital Signature Scheme (SDSS proposed by ElGamal)

In the Signcryption scheme we present here, the signature algorithm used is the SDSS scheme proposed by ElGamal [2]. This scheme enables one person to send a digitally signed message to another person and the receiver can verify the authenticity of this message. This scheme uses the private key of the sender to sign the message and the receiver uses the sender's public key to verify the signature.

The parameters involved are: -

m : the message
p : a large prime number
q : a large prime factor of p.
g : an integer with order q modulo p chosen randomly from the range 1,..,p-1
x : a number chosen uniformly at random from the range 1,.......,q-1
x_a: Alice's private key chosen randomly from the range 1,..,p-1
y_a : Alice's public key $y_a = g^{Xa} \bmod p$

- The first step is to compute the component, r, which is essentially a hash of the message m with additional parameters involved.
- Next we compute the component, s, using Alice's private key.

- Next these two components, (r and s) are sent to Bob, along with the message m. On receiving this, Bob uses r, s and Alice's public key to obtain the value k. Then he does a hash of the message using k and verifies that it is equal to r.

  Bob accepts the message only if the hash of m and k gives him the same message, m that he received from Alice. This will ensure that Alice indeed did digitally sign the message

3.2 Public Key Encryption

The other scheme involved in the Signcryption algorithm is public key encryption. The following can broadly sum this up: -

ciphertext = encrypt(plaintext, PK)

plaintext = decrypt (ciphertext, PK^{-1})

Where PK is the public key and PK^{-1} is the private key.

3.3 Signcryption: How it works ?

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 or SPEED. This choice would be made based on the level of security desired by the users.

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).

These are the parameters involved in the Signcryption algorithm: -

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

Alice's keys	x_a: Alice's private key, chosen uniformly at random from [1,…,q-1] y_a: Alice's public key ($y_a = g^{x}{}_{a}$ mod p)
Bob's keys	x_b: Bob's private key, chosen uniformly at random from [1, …,q-1] y_b: Bob's public key ($y_b = g^{x}{}_{b}$ mod p)

3.3.1 Steps involved in Signcrypting a message

- Alice chooses a value x from the large range 1,....,q-1
- She then uses Bob's public key and the value x and computes the hash of it.This will give her a 128-bit string. K = hash (y_bx mod p)
- She 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.
- Next, Alice encrypts the message m using a public key encryption scheme E with the key k_1. This will give her the cipher text c. **c** = E k_1 (m)
- Then, she uses the key k_2 in the one-way keyed hash function KH to get a hash of the message m. This will give her a 128-bit hash, which we will call r. This process uses the SDSS Algorithm. **r** = KH k_2 (m)
- Just like in SDSS, Alice then computes the value of s. She does this using the value of x, her private key x_a, the large prime number q and the value of r. **s** = x / (r + x_a) mod q
- Alice now has three different values, **c**, **r** and **s**. She then has to get these three values to Bob in order to complete the transaction. She can do this in a couple of ways. She can send them all at one time. She can also send them at separately using secure transmission channels, which would increase security. Thus on her part, Signcryption of the message is done.

3.3.2 Steps involved in Unsigncrypting a message

- Bob receives the 3 values that Alice has sent him, **c**, **r** and **s**. He uses the values of r and s, his private key x_b, Alice'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

- Bob then uses the key, k_1, to decrypt the cipher text c, which will give him the message m.

  m = $Dk_1(c)$

- Now Bob 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 Alice. If they match, it means that the message m was indeed signed and sent by Alice, if not Bob will know that the message was either not signed by Alice or was intercepted and modified by an intruder. Thus Bob accepts the message only if $KHk_2(m) = r$.

Features and Security Aspects of Digital Signcryption

4.1 Features

Digital Signcryption strives to do digital signature and public key encryption in one logical step, with a cost less than that required by each of those steps done separately. Let us assume that S is the Signcryption algorithm and U is the Unsigncryption algorithm. The following three aspects define the features of Signcryption: -

Unique unsigncryptability: - A message m of arbitrary length is Signcrypted using the algorithm S. This will give a Signcrypted output c. The receiver can apply Unsigncryption U on c to verify the message m. This Unsigncryption is unique to the message m and the sender. [1]**Security**: - Since Signcryption is a combination of two security schemes, digital signatures as well as public key encryption, it is likely to be more secure and would ensure that the message sent couldn't be forged, the contents of which are confidential and ensures non-repudiation.

Efficiency: - The cost of computation involved when applying the Signcryption and Unsigncryption algorithms as well as the communication overhead is much smaller than with signature-then-encryption schemes.

4.2 Security

Unforgeability: - Bob is in the best position to be able to forge any Signcrypted message from Alice as only he is in possession of his private key, x_b, which is required to directly verify Alice's message. Given the Signcrypted text of c, r and s, Bob can only obtain the message m by decrypting it using his private key x_b. Any changes he then makes to the message m will reflect in the next step of Signcryption, which will ensure that the one-way keyed hash function on the message m, will not match the value r. Thus Bob, the prime candidate for this kind of attack, is prevented from forging Alice's Signcrypted message.

Confidentiality: - Given that an attacker has obtained all three components of the Signcrypted message, c, r and s, he still would not be able to get any partial information of the message m because he would have to also know Bobs private key as well as the two large prime number p and its factorial q, known only to Alice and Bob. This is not feasible, as we know that deriving a factorial from a large prime number is not practical.

5. Possible Applications of Digital Signcryption

Signcryption is still in an incubation state. Currently there is intensive research conducted in this field of study on how to implement Signcryption effectively. The following are some areas where Signcryption would be feasible.

5.1 LM Signcryption and its application in WTLS handshake protocol

The mobile telecommunications business is booming. Tiny digital telephones and sleek pocketsize PDAs (personal digital assistants) are now more than just fashion accessories. The ability to connect to the Internet is a major feature that attracts people to them. It means that mobile communication devices and client mobile devices are now ready to access the Web. This scenario has given rise to a big question in the minds of users, is it secure? Accordingly, operators and manufactures have responded by establishing the WAP (Wireless Application Protocol) forum.

The WAP forum has already developed WTLS (Wireless Transport Layer Security) layer for secured communication in the WAP environment. The primary goal of WTLS is to provide privacy, data integrity and AKA (Authentication and Key Agreement) between communication entities.

Authenticity and confidentiality must be provided by a suitable encryption scheme in case of mobile communication. One way to implement this is to first digitally sign the message and encrypt it. This is commonly known as Signature-then-encryption. The other is vice-versa, called encryption-then-signature.

Currently, the WTLS handshake protocol is used for secure communication through mobile devices. This handshake uses AKA protocol with an end-to-end connection. In handshake message flow, user certificate is sent to the recipient without encryption or another cryptographic scheme. In this scenario an attacker can get the certificate by eavesdropping on the transmission interface and can figure out user information from the certificate. This can provide the attacker with the user's location and activity.

If Signcryption is used to send messages with mobile devices it will rectify this gap by providing stronger security. By the use of Signcryption, bandwidth use can be reduced and computational load can be decreased without compromising on the security of the message.

5.2 Using Signcryption in unforgeable key establishment over ATM Networks

The asynchronous transfer mode (ATM) is a high speed networking technique for public networks capable of supporting many classes of traffic.

It is essentially a packet-switching technique that uses short fixed length packets called cells. Fixed length cells simplify the design of an ATM switch at the high switching speeds involved. The selection of a short fixed length cell reduces the delay. ATM is capable of supporting a wide range of traffic types such as voice, video, image and various data traffic.

In ATM networks data packets are typically 53 bytes. Only 48 bytes out of 53 bytes in an ATM cell can be used for transmitting data, as the remaining 5 bytes are reserved for storing control information. Thus transmitting encryption key materials of more than 384 bits (48 bytes) over an ATM network would require two or more ATM cells. In a fast network such as ATM, if data packets are divided then there could be considerable delay due to packetization, buffering and re-assembling data units.

So, the need of the hour is to design an authenticated key establishment protocol that

- does not rely on a key distribution system,
- has low resource requirements,
- message is as short as possible and
- offers unforgeability and non-repudiation.

In such a scenario, Signcryption or a modified usage of Signcryption can solve the problem by minimizing message size as well as ensuring unforgeability and non-repudiation.

Extensive research is going on in use of Signcryption in key establishment over ATM networks. It is expected that within a few years it will actually be implemented.

6. Advantages and Disadvantages of Digital Signcryption

6.1 Advantages

6.1.1 Low computational cost

Signcryption is an efficient scheme as it does two steps at once during Signcryption and Unsigncryption. When you think of this in terms of one person sending a Signcrypted message to another person using a mobile device, computation cost does not really matter much. Computational power of processors has developed vastly these days, so if you were to consider Signcrypting network traffic between two stations or all of the traffic on a certain network, then computational power as well as savings in bandwidth are major factors.

6.1.2 Higher security

One can argue the fact that whether the bringing together of two security schemes would increase or decrease security. In our group's view, it would only increase security. We base this on the fact that when you combine two security schemes, which by themselves are complex enough to withstand attacks, it can only lead to added security.

Consider the following: -

X: Any Digital Signature Algorithm

Y: Any Encryption Algorithm

X: Total Number of Signature Algorithms known

Y: Total Number of Encryption Algorithms known

Therefore the combination of the schemes X and Y would give you the Signcryption scheme S. **S = X U Y**

If you consider the fact that both X and Y involve complex mathematical functions, it is only logical to assume that S, which is a combination of both X and Y will involve the combination of the complexities of both X and Y and thus be more complex. More the complexity, more the harder it is for cryptanalysis

Another point to be noted here is that X, the digital signature algorithm, can be chosen from a large range of existing digital signature algorithms, X. Similarly the encryption algorithm for Y can be chosen from any encryption algorithm like 3DES, DES, etc from the range Y. Thus the Signcryption algorithm can be implemented using any of the values in X and Y. This would make it very difficult for a cryptanalyst to figure out which implementation was used in the Signcrypting algorithm. Basically he would have **X** x **Y** **>= X** U **Y** i.e. the cryptanalyst would have to decide between the number of total digital signature algorithms times the number of encryption algorithms, which is greater or equal to either the number of X or Y.

6.1.3 Message Recovery

Consider the following scenario: Alice signs and encrypts a message and sends it to Bob. A while later, she wants to use the contents of the message again. To satisfy Alice's requirement, her electronic mail system has to store some data related to the message sent. And depending on cryptographic algorithms used, Alice's electronic mail system may either keep a copy of the signed and encrypted message as evidence of transmission, or

in addition to the above copy, keep a copy of the original message, either in clear or encrypted form.

A cryptographic algorithm or protocol is said to provide a past recovery ability if Alice can recover the message from the signed and encrypted message using only her private key. While both Signcryption and digital signature-then-encryption-with-a-static-key" provide past recovery, digital signature-then-encryption" does not. One may view digital signature-then-encryption" as an information black hole" with respect to Alice the sender: whatsoever Alice drops in the black hole" will never be retrievable to her, unless a separate copy is kept properly.

6.2 Disadvantages

The way Signcryption algorithm works currently, Alice has to use Bob's public key to signcrypt a message. This has a disadvantage when you consider the need to broadcast a Signcrypted text. Imagine a bank needs to send a Signcrypted message to a number of share traders. With the current algorithm, it needs to signcrypt the message with each of its 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.

There is a research going on to solve this by introducing a group key between the bank and the clients that it intends to send Signcrypted text and use that to broadcast Signcrypted messages.

7. Conclusion

Signcryption is a very novel idea that, if implemented in the right way, can be very useful.

In life, it is human nature to try and do two things at once, or to kill two birds in one stone. Humans do this to make shortcuts, save on time and resources. Is this best approach to do things? In terms of computer security, like we explained before, we believe that by combining two complex mathematical functions, you will increase the complexity and in turn increase security. 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.