IMPLEMENTING SIGNCRYPTION ALGORITHM

Laura Savu

Abstract. This paper presents what is the signcryption scheme and shows step-by-step the implementation of the signcryption algorithm. In this paper I provide an overview for the research that has been done so far in signcryption area. Here I also discuss about the extensions for the signcryption scheme and the security in signcryption.

2000 *Mathematics Subject Classification*:54A05, 54B05.

Public key cryptography

Cryptography word comes from the two ancient Greek words: "krypto", which means "hidden" and "grafo", which means "to write". Cryptography meaning is how to make what you write obscure, unintelligible to everyone except whom you want to communicate with. It is believed that the oldest known text on which cryptography has been applied occurred some 4000 years ago in Egypt. The hieroglyphic inscriptions on a tomb were written with a number of unusual symbols to confuse or obscure the meaning of the inscriptions. Since the oldest times until the 1970s the cryptography was based on symmetric encryption.

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt the encrypted data. This method is known as private key or symmetric key cryptography. There are several standard symmetric key algorithms defined: DES, 3DES, AES etc. These standard symmetric algorithms defined are proven to be highly secured and time tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, 'key', to be exchanged between them to

have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key.
Since there may be number of intermediate points between the communicating parties through which the data passes, these keys cannot exchange online in a secured manner. In a large network, where there are hundreds of system connected, offline key exchange seems too difficult and even unrealistic. This is where public key cryptography comes to help. Using public key algorithm a shared secret can be established online between communicating parties without the need for exchanging any secret data. In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online [18].
Here are exemplified applications of public-key cryptography.
RSA is a public key algorithm that is used for Encryption, Signature and Key Agreement. RSA typically uses keys of size 1024 to 2048.
Elliptic curve cryptography (ECC) is relatively new technology compared to other public key cryptography such as RSA. Elliptic key operates on smaller key size. A 160-bit key in ECC is considered to be as secured as a 1024 bit key in RSA. ECC operates on the points in the elliptic curve The above equation of elliptic curve is in real coordinate. To make elliptic curve operation efficient and accurate the elliptic curve can be defined in finite fields. Elliptic curve in two finite fields, prime field and binary field, are defined by standard. In prime field operation the elliptic curve equation is modified as

Key agreement Key agreement is a method in which the device communicating in the network establishes a shared secret between them without exchanging any secret data. In this method the devices that need to establish shared secret between them exchange their public keys. Both the devices on receiving the other device's public key performs key generation operation using its private key to obtain the shared secret.

Encryption Encryption is a process in which the sender encrypts the message in such a way that only the recipient will be able to decrypt/ descramble

the message.

Digital signature Using Digital signature a message can be signed by a device using its private key to ensure authenticity of the message. Any device that has got the access to the public key of the signed device can verify the signature. Thus the device receiving the message can ensure that the message is indeed signed by the intended device and is not modified during the transit. If any the data or signature is modified, the signature verification fails. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. A digital signature scheme typically consists of three algorithms:

1. A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

2. A signing algorithm that, given a message and a private key, produces a signature.

3. A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Elliptic curve Digital Signature Algorithm - ECDSA is a variant of the Digital Signature Algorithm (DSA). For sending a signed message from A to B, both have to agree up on Elliptic Curve domain parameters. Sender A have a key pair consisting of a private key dA (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key QA = dA*G (G is the generator point, an elliptic curve domain parameter).
The Digital Signature Standard is on the base of many current research topics today, like signcryption.

2. Signcryption introduction

In 1997 Yuliang Zheng presented a positive answer to the following question: "is it 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?". This was for the first time, since public-key cryptography has

been invented, that the question is addressed in literature. He discovered a new cryptographic primitive, called 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]. The proposed cryptographic primitive is more efficient for both types of costs involved: computational cost and communication overhead. The computational cost represents how much computational effort has to be invested by the sender and by the receiver of the message. It is determined by counting the number of dominant operations involved. The communication overhead represents the extra bits which are appended to a message in case of a digital signature or encryption based on public key cryptography.
Encryption and digital signature are two fundamental cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. Until signcryption, they have been viewed as important but distinct building blocks of various cryptographic systems. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption, named signature-then-encryption. In many applications, both confidentiality and authenticity are needed together. Such applications include secure email (S/MIME), secure shell (SSH), and secure web browsing (HTTPS). In order to accomplish these two goals, many cryptographic schemes have been created: Schnorr signature-then-ElGamal encryption, DSS-then-ElGamal encryption, RSA signature-then-RSA encryption, Schnorr signature-then-RSA encryption, RSA signature-then-ElGamal encryption.
Any signcryption scheme should have the following properties:

1. Correctness: Any signcryption scheme should be correctly verifiable.

2. Efficiency: The computational costs and communication overheads of a signcryption scheme should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities.

3. Security: A signcryption scheme should simultaneously fulfill the security attributes of an encryption scheme and those of a digital signature. Such additional properties mainly include: Confidentiality, Unforgeability, Integrity, and Non-repudiation. Some signcryption schemes provide further attributes such as Public verifiability and Forward secrecy of message confidentiality while

the others do not provide them.
- Confidentiality means that only the intended recipient of a signcrypted message should be able to read its contents.
-Authenticity, we mean that the recipient of a signcrypted message can verify the sender's identity. It is not possible for an attacker to send a message, claiming to be someone else.
- Non-repudiation means that the sender of a message cannot later deny having sent the message. That is, the recipient of a message can prove to a third party that the sender indeed sent the message. Signature schemes always provide non-repudiation, since anyone can verify a signature using only the sender's public key. Some signcryption scheme can provide non-repudiation and these schemes are called S-verifiable, since the verifier uses only the signature scheme S. The first DSAverifiable signcryption scheme has been introduced by Shin, Lee, and Shim [8].
- Forward secrecy means that an attacker cannot read signcrypted messages, even with access to the sender's private key. The confidentiality of signcrypted messages is protected, even if the sender's private key is compromised.
- Past recovery means that the sender is allowed to use his private key to recover the original message from the cipher-text. Forward secrecy and past recovery are mutually exclusive.

2.1 Shorten Digital Signature Standard

Zheng first scheme is based on the shortened version of the Digital Signature Standard known as SDSS. Shorten Digital Signature Standard parameters are:
p = a large prime number, public to all
q = a large prime factor of p-1, public to all
g = an integer with order q modulo p, in [1,..., p-1], public to all
hash = a one-way hash function
x = a random number from [1, . . . , q-1]
Xa = Alice's private key chosen randomly from [1,. . . , p-1]
The Shortened Digital Signature Standard has two versions: SDSS1 and SDSS2. Alice's signature on a message m is composed of two numbers r and s, where
$s = x/(r + Xa) \bmod q$
in case of SDSS1 and
$s = x/(1 + Xa\ \ r) \bmod q$
in case of SDSS2.
The signature of a message m will be (r, s). In order to verify the signature it is necessary to calculate

When k is obtained the last check can be done:
hash(k, m) = r
The most important characteristic of the presented scheme is that, although mod p is not explicitly contained in the signature (r, s), it can be calculated by the receiver using r, s and the other public parameters.
SDSS1 is more efficient than SDSS2 in signature generation, as the second involves an extra modulo multiplication [2].

2.2 Signcryption Algorithm

A signcryption scheme typically consists of three algorithms:

1. Key Generation (Gen) - generates a pair of keys
2. Signcryption (SC) - is a probabilistic algorithm
3. Unsigncryption (USC) - is a deterministic algorithm.

Signcryption parameters:
p = a large prime number, public to all
q = a large prime factor of p-1, public to all
g = an integer with order q modulo p, in [1,. . . , p-1], public to all
hash = a one-way hash function
KH = a keyed one-way hash function = KHk(m) = hash(k, m)
(E, D) = the algorithms which are used for encryption and decryption of a private key cipher.
Alice sends a message to Bob.
Alice has the pair of keys (Xa, Ya):
Xa = Alice's private key, chosen randomly from [1, .., q-1]
Bob has the pair of keys(Xb, Yb):
Xb = Bob's private key, chosen randomly from [1, .., q-1]
In order to signcrypt a message m to Bob, Alice has to accomplish the following operations:

1. Calculate

Split k in k1 and k2 of appropriate length.

1. Calculate r = KHk2(m) = hash(h2, m)

2. Calculate s = x/(r+Xa) mod q, if SDSS1 is used

Calculate s = x/(1+Xa r) mod q, if SDSS2 is used

1. Calculate c = Ek1(m) = the encryption of the message m with the key k1.

Alice sends to Bob the values (r, s, c).
In order to unsigncrypt a message from Alice, Bob has to accomplish the following operations:

1. Calculate k using r, s, g, p, Ya and Xb

Split k in k1 and k2 of appropriate length.

1. Calculate m using the decryption algorithm

m = Dk1(c).

1. Accept m as a valid message from Alice only if KHk2(m) = r.

Using the two schemes SDSS1 and SDSS2, two signcryption schemes have been created, SCS1 and SCS2, respectively. The two signcryption schemes share the same communication overhead, (|hash(*)|+ |q|). SCS1 involves one less modular multiplication in signcryption then SCS2, both have a similar computational cost for unsigncryption [1].
Applying SDSS1 scheme in the algorithm we obtain the following examples for the signcryption scheme.

p	q	g	X	XA	YA	XB	YB	K
467	233	7	213	127	391	123	13	138
467	233	12	213	127	400	123	22	432
467	233	21	213	127	48	123	141	25
467	233	27	213	127	95	123	448	55
467	233	36	213	127	411	123	59	286
467	233	40	213	127	146	123	68	23
467	233	43	213	127	332	123	411	422
467	233	48	213	127	92	123	38	273
467	233	49	213	127	172	123	169	174
23	11	2	9	3	8	4	16	8
23	11	3	9	3	4	4	12	4
2027	1013	100	219	357	329	158	1316	716
2027	1013	325	219	357	1487	158	878	1473
2027	1013	537	219	357	403	158	599	199
2027	1013	55	219	357	1062	158	1785	1724
2027	1013	71	219	357	1949	158	1644	1028
2027	1013	1001	219	357	1836	158	431	1973
3167	1583	67	246	79	2929	43	1396	1008
3167	1583	25	246	79	498	43	1604	1862
3167	1583	22	246	79	914	43	1189	937
3167	1583	44	246	79	9	43	1641	2592

Changing the value for Alice's private key has an impact only on the Alice's public key.

Changing the value for Bob's private key, his public key will be changed but also the k will have a different value.

Taking fixed values for parameters and different values for the message, the key k remains the same.

When are taken the following fixed parameters:

p	q	g	X	XA	YA	XB	YB	K
467	233	21	213	127	48	123	141	25

and the following values for the massage, then the calculated values for the hash and signature are as follows:

m	r	s
77	385	111
100	119	106
789	458	225
1000	235	45
3579	87	185

Identity based signcryption scheme is rapidly emerging in recent years and the notions of ring signcryption and proxy signcryption have been created.
The introduction of elliptic curve cryptography by Neal Koblitz and Victor Miller independently and simultaneously in the mid-1980s has yielded new public-key algorithms based on the discrete logarithm problem. Although mathematically more complex, elliptic curves provide smaller key sizes and faster operations for equivalent estimated security. Yuliang Zheng also proposed an elliptic curve-based signcryption scheme that saves 58% of computational and 40% of communication costs when it is compared with the traditional elliptic curve-based signature-then-encryption schemes [3]. Zheng original construction is built on a modification of ElGamal signature and carefully exploits randomness reuse to authenticate and encrypt the message more efficiently than simply encrypting the message using ElGamal encryption. In 2000, [17] Steinfeld and Zheng created a scheme which is provably unforgeable assuming the hardness of factoring. This algorithm requires a trusted party to generate system-wide parameters that include an RSA modulus of particular shape.
There are also many other signcryption schemes that are proposed throughout the years, each of them having its own problems and limitations, while they are offering different level of security services and computational costs.

2.3 Signcryption Security

A signcryption scheme is secured if it is able to provide both authenticity and privacy of communicated data. There are two models of security for signcryption: outsider model and insider model. In case of public-key settings, the sender and the receiver do not have the same secret key, but each of them has his/her own secret key. In this situation, it is necessary for the data protection to be kept safety from an outsider but also from an insider, who is a legal user of the system, meaning the sender, the receiver or someone

who knows the sender's secret key or the receiver's secret key. In the strong insider security model, the privacy of the signcryption scheme is based on the security of the public-key encryption scheme and the integrity protection of the signcryption scheme is based on the security of the digital signature scheme.

Non-repudiation should not be part of the definition of signcryption security because it is not necessary in all the applications. Although signcryption allows the receiver to be sure that the message has been delivered by the sender, it does not necessarily enables a third-party to verify this because the verification of the authenticity of the message may involve the receiver's secret key, depending on how the signcryption scheme is built [14]. In 2002 [15] Shin proposed a signcryption scheme that enjoys a secure and efficient non-repudiation procedure, allowing receivers to convince a third party of the origin of the message. In 2005, [16] Malone-Lee suggested a similar technique and proposed a scheme extending Schnorr's signature scheme that was additionally supported by a proof of unforgeability.

Regarding the number of the users involved in the signcryption algorithm, there are two models of signcryption: two-user model and multi-user model. The two-user model contains only the sender and the receiver in this process. In a multi-user network, the algorithm works with identities. In the multi-user context, the signcryption scheme needs to respect the following rules:

1. For encryption it is necessary to include the sender's identity together with the encrypted message.

2. For the digital signature it is necessary to include the receiver's identity together with the signed message.

In the multi-user model the adversary has an extra power, having the ability to access flexible signcryption and unsigncryption oracles which allow him to specify the receiver's and sender's public key, respectively, in addition to the message and signcryptext, respectively. In some applications has been implemented the possibility to place significant constraints on the public keys in such a way that the Certificate Authority ensure that users know the private key associated with their public key.
Evaluating the two-user security of a signcryption scheme is not sufficient for establishing its multi-user security [14].

2.4 Identity Based Cryptography

The idea of identity-based cryptography has been proposed by Shamir in 1984. The main essence of identity-based cryptosystem is to remove the need of certification of the public keys that are required in the conventional public key cryptography setting. The public key of each participant is obtained from his/her public identity, such as email address, IP address combined with a user name, social security number, etc. that can uniquely identify the participant. An ID-based cryptosystem is one in which the public key may be any string or may be derived from any string. This model requires the existence of a trusted authority called Private Key Generator (PKG), whose task is to generate user's private key from their identity information, after a successful identification. The first practical identity-based cryptosystem was that of Boneh and Franklin in 2001[10] that takes advantage of the properties of suitable bilinear maps (the Weil or Tate pairing) over supersingular elliptic curves. The identity-based signcryption scheme with its security model has been introduced first by Malone-Lee. Identity-based signcryption is an adaptation of identity based encryption to the case of signcryption.

3. Ring signcryption

In Asiacrypt 2001, Rivest, Shamir and Tauman firstly addressed and formalized the notion of ring signatures [11]. A ring signature can be considered as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism, and hence, it provides signer's ambiguity. In a ring signature scheme, the information of all possible signers, i.e. ring members, serves as a part of the ring signature for the signed message. A valid ring signature will convince a verifier that the signature is generated by one of member in the ring, without revealing any information about which participant is the actual signer [12].
Ring signcryption is an anonymous signcryption which allows a user to anonymously signcrypt a message on behalf of a set of users including himself. In an ordinary ring signcryption scheme, even if a user of the ring generates a signcryption, he also cannot prove that the signcryption is produced by himself. In 2008, Zhang, Yang, Zhu, and Zhang solve the problem by introducing an identity-based authenticatable ring signcryption scheme (denoted as the ZYZZ scheme). In the ZYZZ scheme, the actual signcrypter can prove that the ciphertext is generated by himself, and the others cannot authenticate it.

In the scheme, a user can anonymously signcrypt a message on behalf of a set of users including himself. ID-based ring signcryption is very useful to protect privacy and authenticity of a collection of users who are connected through an ad hoc network.

4. Proxy signcryption

The concept of proxy signature was first presented by Mambo in 1996 [9]. Proxy signature schemes are useful for secure communication by computing devices lacking the necessary computational power to perform cryptographic computations on an online realtime basis. These devices can use a more powerful trusted proxy server to perform required cryptographic computations on their behalf while maintaining certain checks and balances against misuse or abuse of the trust placed on the proxy agent [7]. Proxy signature schemes have been suggested for use in a number of applications, particularly in distributed computing where delegation of rights is quite common, such as e-cash systems, mobile agents for electronic commerce, mobile communications, grid computing, global distribution networks, and distributed shared object systems.
Many proxy signature schemes have been combined with different encryption methods obtaining proxy signcryption schemes which have a significantly smaller cost, both in terms of cryptographic computation and bandwidth, than the addition of costs for signing and encryption [13].
The basic idea of ID-Based proxy-signcryption schemes is as follows. The original signcrypter sends a specific message with its signature to the proxy signcrypter, who then uses this information to construct a proxy private key. With the proxy private key he can generate proxy signcryption by employing a specified standard ID-Based signcryption scheme. When a proxy signcryption is given, a verifier first computes the proxy public key from some public information, and then checks its validity according to the corresponding standard ID-Based signcryption verification procedure.

ACKNOWLEDGMENT A lot of research has already been done in the field of signcryption. The signcryption schemes that have been discussed here do not represent the entire list, but instead are intended to give an overview of the various research directions which have been explored so far. Research along signcryption lines is open-ended.

References

[1] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). In: CRYPTO'97, LNCS 1294, pp. 165-179. Springer Verlag, 1997.
[2] Whitfield Diffie, Martin Hellman, "New Directions in Cryptography".
[3] Y. Zheng. How to construct efficient signcryption schemes on elliptic curves.
[7] Chandana Gamage, Jussipekka Leiwo and Yuliang Zhengon, "An Eficient Scheme for Secure Message Transmission using ProxySigncryption"
[8] Jun-Bum Shin, Kwangsu Lee, and Kyungah Shim. New DSA-verifiable signcryption schemes. In P.J. Lee and C.H. Lim, editors, Proc. of ICISC '02. Springer-Verlag, 2002.
[9] M.Mambo, K.Usuda and E.Okamoto. "Proxy signature: Delegation of the power to sign messages". IEICE Trans Fundamentals,1996.
[10] D.BonehandM.Franklin, Identity-based encryption from
theWeil Pairing, Crypto'01
[11] R.L. Rivest, A. Shamir and Y. Tauman, How to leak a
secret, Adv in Cryptology-Asiacrypt 2001.
[12] Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang, "Identity-based Ring Signcryption Schemes: Cryptographic Primitives for Preserving Privacy and Authenticity in The Ubiquitous World"
[13] Meng Wang, and Zhijing Liu, "Identity Based Threshold Proxy Signcryption Scheme".
[14] Yuliang Zheng, Alexander W. Dent, Moti Yung, "Practical Signcryption", 2010.
[15] J. Shin, K. Lee and K. Shim, New DSA-Verifiable Signcryption Schemes, Information Security and Cryptology (ICISC 2002).
[16] John Malone-Lee, Signcryption with Non-interactive Non-repudiation, Designs, Codes and Cryptography, October 2005
[17] R. Steinfeld and Y. Zheng, A Signcryption Scheme Based on Integer Factorization, Information Security Workshop (ISW '00), 2000.
[18] Public Key Cryptography, Applications Algorithms and Mathematical Explanations, Anoop MS, Tata Elxsi Ltd, India.

Laura Savu
University of Bucharest
Faculty of Mathematics and Computer Science
Bucharest, Romania email:*laura.savu@microsoft.com*