IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 7 July, 2016

An Investigation on Digital Signatures

Mr. Debasish Hati[1]; Mr. Prasun Kumar Mitra[2]; Mr. Partha Halder[3]

Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]
Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[2]
Technical Assistant, Technique Polytechnic Institute, Hooghly, West Bengal, India[3]
debasishhati2013@gmail.com[1]; mitra.prasun@gmail.com[2]; parthacst@gmail.com[3]

ABSTRACT

Digital signature is a technique that provides security to the data or message .Nowadays, security plays a major role in communication. Security is the degree of resistance to, or protection from harm or viruses that corrupts the system. As there is tremendous increase in the use of internet and various communication channels, the issue of data or message security is arise. In this paper we are going to survey on the digital signature. It is an electronic signature used to authenticate the identity of the sender and it assures that original content of the message or document received by the receiver is unchanged or same. The goal of the paper is to study the various digital signature methods proposed recently to secure the data transmission. The importance of authentication is increasing due to increase of online transactions over the internet. A Digital Signature is one of the authentication mechanisms. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Keywords: Digital signature, Security, Public key, Private key, Message digest, Authentication

1. INTRODUCTION

The Digital signatures and hand-written signatures both rely on the fact that it is very hard to find two people with the same signature. People use public-key cryptography to compute digital signatures by associating something unique with each person. When public-key cryptography is used to encrypt a message, the sender encrypts the message with the public key of the intended recipient. When public-key cryptography is used to calculate a digital signature, the sender encrypts the "digital fingerprint" of the document with his or her own private key. Anyone with access to the public key of the signer may verify the signature. Suppose Alice wants to send a signed document or message to Bob. The first step is generally to apply a hash function to the message, creating what is called a message digest or digital fingerprint. The message digest is usually shorter than the original message. In fact, a hash function takes a message of arbitrary length and shrinks it down to a fixed length. To create a digital signature, one usually signs (encrypts) the message digest. This saves a considerable amount of time, though it does create a slight insecurity (addressed below). Alice sends Bob the encrypted message digest and the message, which she may or may not encrypt. In order for Bob to authenticate the signature he must apply the same hash function as Alice to the message she sent him. He also decrypts the encrypted message digest using Alice's public key and now compares the two. If the two are the same he has successfully authenticated the signature. If the two do not match there are a few possible explanations. Either someone is trying to impersonate Alice, the message itself has been altered since Alice signed it or an error occurred during transmission. For signature verification to be meaningful, the verifier must have confidence that the public key does actually belong to the sender (otherwise an impostor could claim to be the sender, presenting her own public key in place of the real

The documents are commonly authenticated by the signature. Even when the document is signed physically one is authenticating its contents. In the same manner digital signature is a method which is used to authenticate the contents of the electronic documents, which can be used with PDF, e-mail; word processing etc. in this digital ID is required for signing documents. This ID can be obtained from various certification authorities on the web like the VeriSign and Echo Sign. The documents you sign contain the digital signature which is simply a small block of data. It is generated from the digital ID that includes

public key and private key. The signature is applied to the document with the help of private key while the public key is send to the file. Encrypted code is introduced in public key that verifies your identity. There are four classes of digital signature:

Class 0: In this certificate is issued for demonstration.

Class 1: This certificate is issued to the private subscriber. It will confirm that the user name and e-mail address form no duplication within the certifying authorities database.

Class 2: This certificate is issued for both business as well as private use. The task of this certificate is to assure that the information provided by the subscriber will not conflict with the information in well known consumer database.

Class 3: This certificate will be issued to the individuals as well as organizations. As the class 3 certificates is high assurance certificate which is intended for e commerce applications. It should be issued to an individual only on its physical appearance before the certifying authorities.

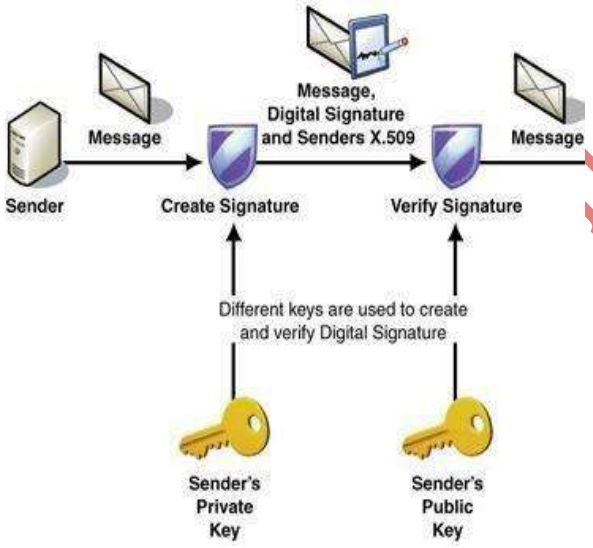

Fig 1: General idea of Digital Signature

In above figure signature generation and signature verification are carried out. For signature generation private key is used and for signature verification public key is used. For message transfer Hash function is used after that message is digested. For signature generation private key is used then signature generation is created. This signature generated is transferred for verification. After verified valid or invalid result is obtained.

There are three algorithms that are used for digital signature generation under the DSS standard.

1) DSA (Digital Signature Algorithm)
2) RSA (Rivest Shamir Adleman)
3) ECDSA (Elliptic Curve Digital Signature Algorithm)

Also hash function is used in the signature generation process, which is used to obtain message digest that is condensed version of the data. This message digest is put in to digital signature algorithm to generate the digitally signed message. In the verification process same hash function is used.

2. DIGITAL SIGNATURE SCHEMES

A. The RSA Signature scheme

The RSA signature scheme [48] is a deterministic digital signature scheme which provides message recovery.
For the RSA public-key encryption scheme the message space M and the cipher text space C are Zn= {0, 1, 2, ... , n-1}.

Key-Generation

In RSA public key cryptosystems each user
1. Generates two large distinct random primes p and q,
2. Computes n = pq and Φ = (p-1)(q-1)
3. Selects a random integer e,1 < e < Φ, such that gcd(e,Φ)= 1
4. Computes the unique integer d,1 < d < Φ, such that ed ≡1 mod Φ

Now the public key of Alice is (n,e) and the private key is d.

Signature Generation

To sign a message m Є M, Alice
1. identifies m with a number ~ m in Zn through a map R :
M → Zn.
2. computes the signature s = ~ m^d mod n.

Verification

To verify the signature of Alice, Bob
1. chooses the public key (e,n) of Alice.
2. computes ~ m = s^e mod n.

Verifies that ~ m Є M' where M' denotes the set of images of R. If it does not hold rejects the signature else recovers the message as m = R^{-1}(~ m).

B. The DSA Signature scheme

The DSA makes use of the following parameters:

1. p = a prime modulus, where 2L-1 < p < 2L for 512 £ L £ 1024 and L a multiple of 64
2. q = a prime divisor of p - 1, where 2159 < q < 2160

3. g = h(p-1)/q mod p, where h is any integer with 1 < h < p - 1 such that h(p-1)/q mod p > 1 (g has order q mod p)
4. x = a randomly or pseudo randomly generated integer with 0 < x < q
5. y = gx mod p
6. k = a randomly or pseudo randomly generated integer with 0 < k < q

The integer's p, q, and g can be public and can be common to a group of users. A user's private and public keys are x and y, respectively. They are normally fixed for a period of time. Parameters x and k are used for signature generation only, and must be kept secret. Parameter k must be regenerated for each signature. Parameters p and q shall be generated as specified in Appendix 2, or using other FIPS approved security methods. Parameters x and k shall be generated as specified in Appendix 3, or using other FIPS approved security methods.

Signature Generation

The signature of a message M is the pair of numbers r and s computed according to the equations below:

r = (gk mod p) mod q and

s = (k-1(SHA-1(M) + xr)) mod q.

In the above, k-1 is the multiplicative inverse of k, mod q; i.e., (k-1 k) mod q = 1 and 0 < k-1 < q. The value of SHA-1(M) is a 160-bit string output by the Secure Hash Algorithm specified in FIPS 180-1. For use in computing s, this string must be converted to an integer. As an option, one may wish to check if r = 0 or s = 0. If either r = 0 or s = 0, a new value of k should be generated and the signature should be recalculated (it is extremely unlikely that r = 0 or s = 0 if signatures are generated properly). The signature is transmitted along with the message to the verifier.

Verification

Prior to verifying the signature in a signed message, p, q and g plus the sender's public key and identity are made available to the verifier in an authenticated manner.

Let M¢, r¢, and s¢ be the received versions of M, r, and s, respectively, and let y be the public key of the signatory. To verify the signature, the verifier first checks to see that 0 < r¢ < q and 0 < s¢ < q; if either condition is violated the signature shall be rejected. If these two conditions are satisfied, the verifier computes
w = (s¢)-1 mod q

u1 = ((SHA-1(M¢))w) mod q

u2 = ((r¢)w) mod q

v = (((g)u1 (y)u2) mod p) mod q.

If v = r¢, then the signature is verified and the verifier can have high confidence that the received message was sent by the party holding the secret key x corresponding to y.

For a proof that v = r¢

when M¢ = M, r¢ = r, and s¢ = s.

If v does not equal r¢, then the message may have been modified, the message may have been incorrectly signed by the signatory, or the message may have been signed by an impostor. The message should be considered invalid.

C. The ELGamal Signature scheme

The ElGamal signature scheme [18] is a signature scheme with appendix. It requires a hash function h : $\{0,1\}^* \rightarrow Z_p$, where p is large prime. In this scheme, system parameters are : p - a large prime number
g - a generator of Z^*_p
h- a secure collision free one-way hash function

xA- a random integer in (1,p-1), it works as secret key of Alice.

yA- where, yA= g^{xA} mod p, works as the public key of Alice.

Signature Generation

To sign a binary message m of arbitrary length, the user Alice selects a random integer
k Є (1,p-1) such that gcd(k,p-1) = 1.
Alice computes r = g^k mod p and k^{-1} mod p-1.
He further computes s = k^{-1}[h(m) - x_{Ar}] mod p - 1. "
Alice's signature for the message m is (r,s,m).

Verification

To verify the signature (r,s,m) Bob
Checks that 1< r < (p-1) to accept a valid commitment r
Computes v1= $yA^r r^s$ mod p. Computes
h(m) and v2= $g^{h(m)}$ mod p.
The signature is valid if and only if v1= v2.

3. RECENTLY IMPLEMENTED TECHNIQUES FOR DIGITAL SIGNATURE

3.1 Method of securely transferring programmable packet using digital signature having access controlled high security verification key:

Programmable network represents a new approach to its network architecture. In programmable network nodes can perform the various calculations with respect to user data. For the calculation purpose users provide their programs to their nodes. So programmable networks are useful to add and provide new services without physical action or hardware modification. Sometimes programmable network raise some security problems. To avoid this problem cryptographic technique is used. At programmable network environment, programmable packet contains programmable codes. Which should perform computations on intermediate node as well as end nodes. So proposed system provides a method of securely transferring programmable packets. By which programmable nodes are verified using digital signature having a high security signing key. This paper also provides a method by which a storage server for verification keys is provided and only authorized programmable nodes verify signature and execute codes.

3.2 New Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem:

This paper gives the solution to the problems such as low work efficiency and weak in delegation authority control. Which were in the existing proxy digital signature scheme. Proxy digital signature scheme means it simulates the function of seal to transfer the digital signing power to another authorized agent. It uses the public key self certified system i.e. only one step is required to complete the process of verification of digital signature. It reduces the storage and computing cost. The proposed self certified proxy digital signature scheme is based on the discrete logarithmic over elliptic curve group. Elliptic curve cryptography is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields.

The proposed scheme is divided into three phase digital signing power delegation phase, the proxy digital signature generation phase and proxy digital signature verification phase. This covers all the operations such as verifying the warrant, verifying the proxy digital signature signed by proxy signer and verifying the certificate of original signer.

3.3 Code – Based Designated Verifier Signature Scheme:

In this paper author introduced a new designated verifier signature scheme, It allows a signer to convince only . The designated verifier the sign message is authentic. Designated verifier signature scheme based on CFS signature and stern identification scheme whose security depends on syndrome decoding problem. The CFS means Courtois, Finiasz and Senderier. This scheme based on difficulty of decoding linear error- correcting codes. In CFS mechanism involves sampling random syndromes. The code-based designated verifier signature scheme proves that the sign message is authenticated. The proposed scheme is first code-based designated verifier signature and it also satisfies unforgeability and distinguish ability which are require for a designated verifier.

3.4 An Improved Digital Signature Scheme with Fault Tolerance in RSA:

In this paper the author proposes a scheme that can efficiently keep confidentially transfer the message and also review a digital signature scheme with fault tolerance based on RSA cryptosystem proposed by Zhang's scheme.

It used for secure data transmission. RSA stand for Ron Rivest , Adi Shamir and Leonard Adleman. In RSA cryptography two keys are used public key and private key. The public key is used for encryption and private key used for decryption purpose. Zhangis scheme has several weaknesses that violate the principle of secure digital signature and it has serious vulnerability. The vulnerability is the cyber security, It defines any type of weakness in computer system itself, in a set of procedures or anything that leaves information security expose to thread. The author meets all the requirements for digital signature and maintains the fault tolerance function in Zhang's scheme.

3.5 Comment on a Digital Signature Scheme with Using Self Certified Public keys :

In this paper the author Tseng et al proposed a digital signature scheme with using self certified public key. The self-certified public keys is one in which both public key and certificate are combined as one piece of information.

The primary of this system is that it reduces the overhead of having a separate public key. With the help of

self certified public key, the verification signature and public key can be carried out in a logic step. Unfortunately, Shao et .al showed that the scheme was insecure and gives an improvement scheme. In this we analyze security of Shao et.al scheme and his attack and show that the attack is not powerful and the improvement scheme cannot resist man-in-middle attack. This attack is very frightful over the internet transactions.

3.6. Importance of cryptography in network security:

This paper gives a broad review of cryptography and digital signature. Cryptography is used to protect the information in digital form and is used to provide the network security. Digital signature provides means for an entity to bind its identity to a piece of information. Digital signature provides authentication, data integrity and non-repudiation. Cryptography protects data from theft or alteration and also used for authentication purpose. In cryptography plaintext is converted to cipher text using key and algorithms. So no one can get plaintext from cipher text without knowing the key for decryption easily. This paper includes various attack methods like known plaintext and cipher text attack , chosen plaintext and chosen cipher text attack etc. cryptography was used to conceal the diplomatic and military secrets from enemy . But it is being used to secure large amount of electronic data that is stored on the corporate networks. Cryptography is means for protecting data while maintaining the privacy of confidential data like financial, personal and medical.

3.7 A secure proxy signature scheme in bilinear group:

Proxy signature is one of the vital aspects of digital signature. Proxy signature scheme is a tuple (key gen, sign, verify, delegate, proxy sign, proxy verify, identify) where the algorithm runs in polynomial time. A proxy signature protocol allows an entity called original signature to delegate signing power to another entity called proxy signer to sign messages on its behalf. Proxy signature is useful to design cryptographic protocols. This paper proposes a new provable secure proxy signature scheme based on Gap Diffie Hellman (GDH) group .GDH is obtained from bilinear pairings. GDH is a group in which problem is easy but Computational Diffie Hellman (CDH) problem is hard. Though there are many other proxy signature schemes the method in this paper is easy and simple and the technique of bilinear map and traditional certificate based signature scheme is being used.

Bilinear map are the tools of pairing based cryptographic groups. The resulting scheme is based on two notations and also security analysis and definition are given. The scheme has low computational cost of signature generation. Hence suitable for low bandwidth environment. Thus the bilinear pairing is presented by using a certificate based scheme and proves its security in the random oracle model.

3.8 A new attack method on digital signature scheme:

This paper describes a new attack method on digital signature scheme. There are some signature schemes which have design defects and can be broken through this method. This method will propose some signature datum (i.e. actual information derived from measurement or research) into identical base datum, and anyone can employ this way to attack and come up with or forge a valid signature. In this the author present four examples and indicates their problems of insecurity or security flaws under the attack based on identical base construction.

B. **Awasthi-Lal signature scheme:** - it is a proxy blind signature scheme.
C. **Duc-Cheon-Kim signature scheme:-** it is a forward security blind signature scheme, which alleviate (make easy) the severe consequences brought by the secret key leak.
D. **Tseng-Jan signature scheme**:- it is an example of group signature and has potential security flaws.
E. **Xue-Cao signature scheme**:- it is also a proxy blind signature scheme. It consists of original signer, proxy signer and signature receiver.

So in this process of designing the signature protocols the security flaws are avoided.

3.9 New Blind Signature Schemes Based on the (Elliptic Curve) Discrete Logarithm Problem:

Blind signature scheme is a kind of digital signature with significant application in anonymous electronic voting and electronic payment. in this the recently introduced blind signature scheme is analyzed and also show that without obtaining the signing key, the attacker can forge a valid signature for any arbitrary message. Dameri in 2012 proposed a new blind signature scheme based on ElGamal signature claimed that their scheme is secure against forgery attack. This scheme is universally forgeable.

Then a new blind signature scheme is proposed based on hardness of discrete logarithm problem and the other which inherits the efficiency of elliptic curve cryptosystem (ECDLP) and is elliptic curved based variant of the proposed system which has lower computational overhead. These schemes are unforgivable, blind and untraceable. Hence they are appropriate candidates to be employed in protocols such as untraceable e-payment or e-voting and this scheme is more efficient one.

4. SECURITY OF DIGITAL SIGNATURE SCHEMES

The concepts of negligible and polynomial functions appear when the security of cryptographic schemes is studied.

Definition (Negligible function): A function f : N →

R+ is negligible in k if, for every c > 0 there exists k0∈ N such that f(k) <1/kc, for all positive integer k ≥ k0. Otherwise, the function f is non-negligible in k.

Definition (Polynomial function): A function g : N →

R+ is polynomial in k if, for every k0∈ N there exists a value c > 0 such that f(k) < kc, for all positive integer k ≥k0.

Roughly speaking, the cryptographic schemes will be defined according to a security parameter k. We will consider such schemes secure if any adversary trying to attack them in polynomial time (in k) has a success probability which is a negligible function of k. On the other hand, we say that an event has overwhelming probability with respect to k if the probability of its complementary is negligible in k. To guarantee that a signature scheme provides authenticity and non-repudiation to digital communications, one must prove in some way that the scheme is secure. That is, only the owner of a secret key should be able to compute valid signatures with respect to the matching public key. Nowadays, a signature scheme is considered secure (or un-forgeable) only if it achieves this level of security.

Definition(Un-forgeability): A signature scheme, with security parameter k, is unforgeable if no adversary which is given the public key and the signatures θ1,...,θs of s messages m1,...,ms adaptively chosen by itself, can produce in polynomial time (in k) and with non-negligible probability (in k) a valid signature θ of some message m, such that (m, θ) ?= (mi, θi), for all i = 1,...,s. Figure 1. gives an idea of what a successful forgery against a signature scheme is:

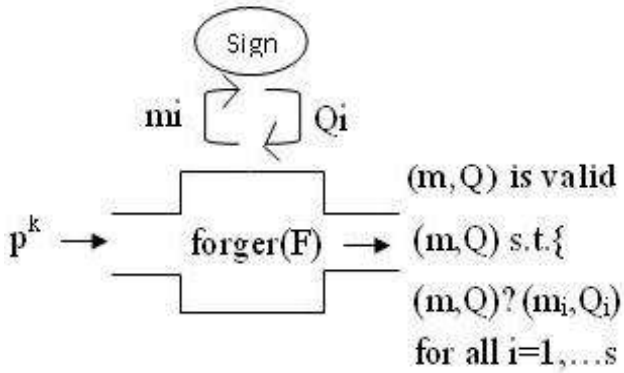

Fig 2: A successful forger against a signature scheme

The usual argument is to reduce the problem of forging a signature to a related computational problem. In other words, assuming the existence of a successful attack against the unforgeability of a scheme, one could solve the related problem. If this problem is assumed to be hard to solve, the reduction implies a contradiction, and one can conclude that the scheme is therefore unforgeable. Proving the unforgeability of a signature scheme in an absolute way, without such a reduction, seems to be a really hard problem. However, constructing such a proof by reduction is not easy at all. The idea is to use the hypothetical existence of a successful adversary to solve an instance of the related computational problem. Roughly speaking, we receive an instance of the problem, and we try to set up the public parameters of the signature scheme in an ingenious way that allows:

- to provide the adversary with valid signatures for messages that it adaptively chooses, when we execute (without knowing the secret key!) the hypothetical successful attack against the signature scheme; and then
- to extract the solution of the problem from the signature forged by the adversary. There exist very few proposals of signature schemes which can be proved secure in this formal (but restrictive) way. However, either the resulting schemes are not very efficient, or the security is based on stronger assumptions, like the Strong RSA Assumption, as it happens in the schemes proposed, or the q-Strong Diffie-Hellman assumption.

COMPARISON OF THE KEY STRENGTHS OF RSA/ DSA AND ECDSA

Use either SI The advantage of elliptic curve over their public key systems such as RSA, DSA etc is the key strength. The following table I summarizes the key

strength of ECDSA based systems in comparison to other public key schemes.

Table I. Comparison of the key strengths of RSA/DSA and ECDSA

RSA/DSA Key length	ECC Key Length for Equivalent Security
1024	160
2048	224
3072	256
7680	384
15360	512

From the table it is very clear that elliptic curves offer a comparable amount of security offered by the other popular public key for a much smaller key strength. This property of ECDSA has made the scheme quite popular of late. As with elliptic curve cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits. By comparison, at a security level of 80 bits, meaning an attacker requires the equivalent of about 2^{80}signature generations to find the private key, the size of a DSA public key is at least 1024 bits, whereas the size of an ECDSA public key would be 160 bits. On the other hand, the signature size is the same for both DSA and ECDSA: $4t$ bits, where t is the security level measured in bits, that is, about 320 bits for a security level of 80 bits.

5. CONCLUSION

In this paper we perused the concept of Cryptography including the various digital signature schemes of system based on the kind of key and a few algorithms such as RSA, DSA and ECDSA. We studied in detail the mathematical foundations of various algorithms for generation of keys and verification of digital signatures and also their security strengths were analyzed.

6. ACKNOWLEDGMENT

We would like to thank our respected Executive Director Prof. S. N. Basu, Administration of Technique Polytechnic Institute, specially respected Chairman (GB) Mr. Tapas Kumar Saha and R&D Cell of this institute for motivating us in this research work. We would also like to thank all the members of Technique Polytechnic Institute for their support and co-operation. We thank all mighty God and our parents for their blessings in our life.

7. REFERENCES

[1]. Julio Lopez and Ricardo Dahab, “An overview of elliptic curve cryptography”, May 2000.

[2]. El-Kassar, A.N., M.Rizk, N.Mirza and Y.Awad,2001.ElGamal public-key cryptosystem in the domain of Gaussian integers.Intl.J.Appl.Math.,7:405-412.

[3]. Haraty, R., O. Otrok and A.N.El-Kassar,2004.A comparative study of ElGamal based cryptographic algorithm. Proc. Sixth Intl. Conf. Enterprise Information Systems (ICEIS 2004),3:79-84.

[4]. Rivest,R.L.,Shamir,A.,and Adleman,L.,” A method of obtaining Digital Signatures and Public key cryptosystems”,Comm.ACM,21,1978.

[5]. Nathanson, Melvyn, B.,Elementary Methods in Number Theory, Springer, 2000.

[6]. William Stallings, Cryptography and Network Security: Principles and practice.Tsinghua press,2002,253-299.

[7]. Rabin, M.O., Probabilistic algorithms. In Algorithms and Complexity, J. F.Traub,Ed., Academic Press,New York,1976,pp.21-40.

[8]. A. Jurisic, A. Menezes, “Elliptic Curves and Cryptography”, 2003,http://www.certicom.com/whitepapers.

[9]. Jindan Zhang1, Xu An Wang2 ,”Yet another way to construct digital signature in the standard model”. Intelligent Networking and Collaborative Systems (INCoS), 2013 IEEE 5th International Conference.

[10]. Jianglang FengJindong Li,”A secure proxy signature scheme in bilinear group. Emerging Intelligent Data and Web Technologies (EIDWT), 2013 IEEE Fourth International Conference.