Improving Efficiency of Basic Encryption and Authentication Technique using Elliptic Curve with Parameterized Hash Algorithm

Usha Chauhan
M.E 4th sem (IT),
Department of Computer Science
Medicaps Institute of Technology and Management, Indore

Mohsin Sheikh
Assistant Professor,
Department of Computer Science
Medicaps Institute of Technology. and Management, Indore

Prateek Nahar
Assistant Professor,
Department of Computer Science
Lord Krishna College of Technology, Indore

ABSTRACT
In present era, mostly data sends via the internet for sharing, so the reliability on data is decreased. To maintain reliability, several kinds of security and authentication is mechanisms needed, less security increase the liability of attacks on data. Digital Signature of the data is a solution to this security problem which provides the reliability, authenticity and accuracy. Most basic algorithm for security and authentication is RSA, DSA, ECDSA algorithms which uses the different key of different sizes. This paper presents elliptic curve algorithm to encrypt the data and use parameterized hash algorithm to authenticate the data.

Keywords
RSA, ECDSA, Hash Functions, PHAL, Digital Time Stamping.

1. INTRODUCTION
Cryptography is the branch of cryptology dealing with the design of algorithms for encryption and decryption to provide the authenticity and secrecy of information. Different types of active and passive attacks are introduced which growing less security happen on application level or network level. To protect a user's identity from being read or modify (Data integrity), we need security. For a message which is signed and encrypted, the message is signed once and the signature is verified by each recipient. The symmetric key used to encrypt the message is encrypted with each recipient's public key by the sender, and each recipient must decrypt his encrypted copy of the symmetric key. Some factors like flexible, security of digital signature algorithm and speed problem of signing and verifying in digital signature must be considered an important issue. In practical application, security is often influenced by machines' operating speed. And transmitting speed is a big bottleneck especially in network environment. So, operation should be simplified and also ensure safety. There are data protections schemes are used to transmitting data across the network. These schemes take more time to efficiently provide the security.

2. DIGITAL SIGNATURE SCHEMES
In past several decades public-key systems provide authentication via secret-key systems requires the sharing of some secret & required trust of a third party. Public-key systems provide a method for digital signatures. There are three main methods: RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm). Every method has a different key size that can be change to give higher security. The attack on each public-key cryptosystem computes an amount of permutations and iterations determined by a security parameter which is related to the key size [4].

2.1 RSA
In 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman invented RSA which is a public-key cryptosystem used encryption and authentication. RSA has become popular as it is the most widely used public-key cryptosystem. RSA take two large primes, p and q, and find their product n = pq. Both the sender and the receiver must know the value of n. choose a number, e, less than n and co-prime to (p-1) (q-1), and find its inverse, d, mod (p-1) (q-1). The sender knows the value of e, and only the receiver knows the value of d. Then find e.d = 1 mod (p-1) (q-1); e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is d. The factors p and q must be kept secret, or destroyed. The RSA security will depend on the length of the keys used. RSA uses 512 bits length key. If we use 384 bits key can be broken much easier than a 512 bits, then the amount of possible combinations grow substantially [1].

2.2 DSA
The DSA was proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) and was specified in a U.S. Government Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS).The Digital Signature Algorithm (DSA) is public key techniques which developed by ElGamal and Schnorr, is based on the problem of discrete logarithms. The DSA techniques based on computing exponentiation modulo which is a large prime number p. The key size length is length of prime i.e. 512 or 1024 bits. The size of exponents used for exponentiation is an important security parameter for DSA. For DSA, the exponent size is fixed at 160 bits. The General Number Field Sieve is the best attack known to break the size of DSA algorithm [2].

2.3 ECDSA
ECDSA was first proposed in 1992 by Scott Vanstone in response to NIST's (National Institute of Standards and Technology) [3]. Then it was accepted in as an ISO (International Standards Organization) standard (ISO 14888-3), accepted in 1999 as an ANSI (American National Standards Institute) standard (ANSI X9.62). In elliptic curve cryptography, the public key size say to be needed for ECDSA is about twice the size of the security level, in bits and the signature size is the same for both DSA and ECDSA: 4* bits needed security level. The elliptic curve cryptography use elliptic curves to give the high security to data because it's hard to compute curve

calculations. The variables and coefficients of curve are involved into a finite field. The ECDSA techniques based on computing exponentiation modulo a large prime number (GF (p)) or over binary polynomials (GF(2m)). The key size is the size of the prime number or binary polynomials in bits in between 160 to 200 bits. The security of ECDSA refers to the size of multipliers used and it's always smaller than the key size. According to the difficulty of elliptic curve discrete logarithm, it is hard to explain the password. Authentication information keeps dynamic, so replay attack can be prevented effectively.

2.4 Key Generation

ECDSA follow some different steps [7]. An entity A's key pair is associated with a particular set of EC domain parameters D= (q, FR, a, b, G, n, h). E is an elliptic curve defined over Fq , and P is a point of prime order n in E(Fq), q is a prime. Each entity A does the following:

1. Select a random integer d in the interval (1, n- 1).
2. Compute Q = dP.
3. A's public key is Q, A's private key is d.

(a) Signature Generation

To sign a message m, an entity A with domain parameters D= (q,FR, a, b, G, n, h) does the following:

1. Select a random or pseudorandom integer k in the interval (1, n-1).
2. Compute k*P =x1, y1 and r= x1 mod n (where x1 is regarded as an integer between 0 and q-1). If r= 0 then go back to step 1.
3 . Compute k-1mod n.
4. Compute s= k-1 {h (m)+dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1.
5. The signature for the message m is the pair of integers (r, s).

(b) Signature Verification

To verify A's signature (r, s) on m, B obtains an authenticated copy of A's domain parameters D = (q, FR, a, b, G, n, h) and public key Q and do the following:

1. Verify that r and s are integers in the interval (1, n-1).
2. Compute w = s-1mod n and h (m).
3. Compute u1 = h(m)w mod n and u2 = r*w mod n.
4. Compute u1P + u2Q =(x0, y0) and v= x0 mod n.
5. Accept the signature if and only if v = r.

3. DIFFERENT DIGITAL SIGNATURE SCHEMES

We can find the comparison of the most operations as signing and signature verification. The RSA algorithm is slow for the process of signing and much faster for signature verification [2].

Table 1.1-Comparision of different digital signature schemes

Schemes	Sign	Verify	Key Generation	Parameter Generation
RSA-1024 (e=3)	4.3	0.6	1100	none
DSA-1024	7	27	7	6500
ECDCA-168(over GF (p))	5	19	7	Large(research area)

The DSA algorithm and ECDSA algorithm can be compare over GF(*p*). Elliptic curves over (GF (2*m*)) appear to be slower than those over (GF (*p*)).

4. HASHING FUNCTIONS

The Hashing functions are used to compress the length of message to a fixed size, usually for following signature by a digital signature algorithm**.** The hash function should be computationally infeasible given a message and its hash value to compute another message with the same hash value. It should to be unaffected finding any 2 messages with the same hash value, perhaps by iterating through minor permutations of 2 messages (birthday attacks). MD2 is the oldest, produces a 128-bit hash value, and is regarded as slower as and less secure than MD4 and MD5. MD4 produces a 128-bit hash of the message, using bit operations on 32-bit operands for fast implementation. MD5 was designed as a strengthened version, using four rounds, a little more complex than in MD4.

4.1 SHA (Secure Hash Algorithm)

SHA has very recently been subject to modification following NIST identification of some concerns, the exact nature of which is not public, current version is regarded as secure. SHA is extended variation of MD5 [5]. It produces 160-bit hash values. SHA consists of following elements:

a. Pad message length must a multiple of 512 bits.
b. Initialize the 5-word (160-bit) buffer.
c. Process the message in 16-word (512-bit) chunks,

Using 4 rounds of 20 bit operations each on the chun & buffer.

4.2 PHAL

PHAL is a hash algorithm designed as to improve the weaknesses of MD/SHA hash functions. Due to the proposed attacks motivates to design of a new hash functions where few elements of hash function are parameterized. This algorithm gives more secure and more flexible because of its iterative structure [5].

PHAL consists of two mechanisms: new iteration schema and dedicated compression function. For PHAL hash algorithm parameterwas the number of rounds. The design goals of this hash algorithm are as follows:

It shall support a maximum message length of at least 264–1 bits. Its iteration structure should be parameterized and resistant against known attack against the MD-type structure and for high performance and security.

Its compression function should be resistant against known attack. Algorithm must provide message digests of 224, 256, 384 and 512 bits.

5. DIGITAL TIME STAMPING

The time stamping is used to calculate the time that took by user to complete the process. The digital time stamping certified the particular record at the particular time and shows the digital document when introduced and changed by the user.

The digital time stamping system raise the integrity of the digital signature system by supporting two features with it. One is, a digital time stamping systems do not rely on keys, or any other secret information. So, time-stamping system cannot be affected by the disclosure of a key. Second, digital time-stamping certificates can be renewed so as to remain valid indefinitely.

6. PROPOSED APPROACH

The digital signature scheme used in this paper ensures the high security by using the combination of symmetric and asymmetric cryptography. The ECDSA provides more security and less computation time. The Elliptic curve cryptography is an

important branch of public key cryptography based on the elliptic curve and finite fields. In this scheme we use 3-DES algorithm for the document encryption and to send secret key (symmetric key) and for digital signature we use ECDSA algorithm. To measure the time during process we apply digital time stamping. Hash Function is used to generate the hash values. During the all process we assume that sender public key (Ka2) and receiver public key (Kb2) both known the public keys of each other. But the private keys of both sender (Ka1) and receiver (Kb1) are private to each. The transmitting process in the scheme is shown by the dotted line. The steps in this scheme are as follows:

1.First of all, the electronic document which transmitting is send to PHAL function to generate the PHAL value of the document which is compare with the ECDSA signature verifying process. Then ECDSA use the private key (Ka1) of sender to sign the PHAL value and digital time-stamp. At the same time, electronic document is encrypted by 3-DES that produces cipher text.

At the same time, the secret key will be encrypted using public key (Kb2) of receiver by ECDSA. Then generate the cipher block (a small dark rectangular in the right hand of **Fig.1.2.).** The cipher text and digital signature are sending from sender to receiver as shown in **Fig 1.2.**

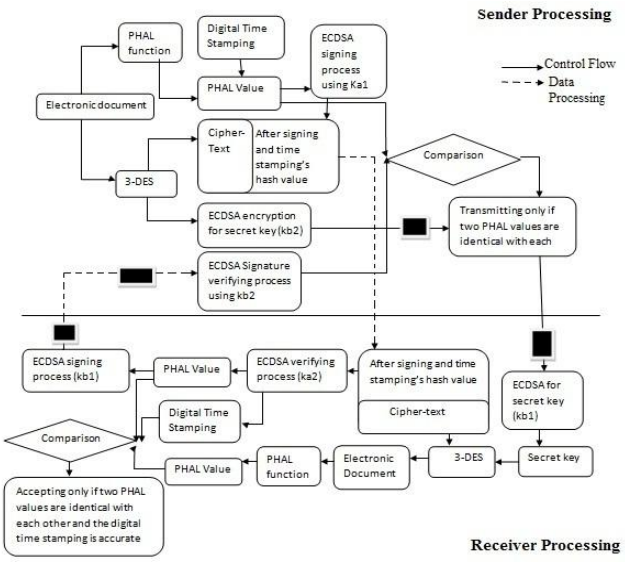

Fig 1.2-A new scheme for digital signature

1. At the receiver end the cipher text and digital signature are abstracted. The digital signature is verifying by sender public key Ka2. It produces PHAL value and digital time-stamp. To verify digital signature and sending secret key from sender to receiver, PHAL value will be signed by ECDSA by receiver private key Kb1and then transmit feedback to the sender.

2. The sender verifies the digital signature using receiver private key (kb1) after receiving from receiver. It is shown asa small dark rectangular in the left hand of figure 1.2. Then the sender can get a PHAL value which must be compared with the step 1's PHAL value. And if the two PHAL values are identical with each other then the cipher block in first stepof the scheme will be transmitted to receiver.

3. Then the cipher text is decrypted by ECDSA using receiver private key (Kb1). After decrypting the cipher block, receiver must obtain a secret key which used for decrypting the cipher block using 3-DES. Then the document obtained to receiver.

4. The document obtained from previous step should be processed by PHAL function that produces PHAL value. The receiver can accept the document only if both PHAL values (one of sender and second of receiver) are identical and digital time-stamp is accurate by comparing these PHAL valuesand at the same time check to the digital time-stamp obtained from step 2.

The security of this scheme provides several properties such as confidentiality, integrity, and authenticity, anti-denial and anti-replacement attack have implemented successfully in this scheme of digital signature. Specifically, anti-denial is implemented in step 2 and step 3; anti-replacement attack [8] is implemented in step 2 and step 5.

7. CONCLUSION

Digital signature scheme applies in specific environment of electronic government. This scheme solves some secure problems in electronic document such as not enough trust between sender and receiver and so on. In a word emphasis is placed on how to combine security with efficiency in electronic government. But the secure problems that can be solved thoroughly also need to consider other factors like the security and credibility of both network and relating hardware or strengthen the management of operating personnel.

8. ACKNOWLEDGMENTS

We would like to thanks my Project Guide Asst Prof- Mr . Mohsin Sheikh and additional support to Asst Prof. Mr. Vijay Verma , Dr. Sanjay Thakur and Dr. R.P Mahajan for giving good guideline.

9. REFERENCES

[1] Zhu Na and GuoXi Xiao 2008. The Application of a Scheme of Digital Signature in Electronic Government

[2] Lawrence E. Bassham III March 2004. The Digital Signature Algorithm Validation System (DSAVS).National Institute of Standards and Technology Information Technology Laboratory Computer Security Division

[3] Wei Haiping and Jia Chuanying 2007. The Study of Password Authentication System Based on Elliptic Curve Cryptosystem Navigation college, Dalian Maritime University Dalian,Liaoning 116026,China Liaoning Shihua University Fushun,Liaoning 113001,China IEEE.

[4] Michael J. Wiener 1998. Performance comparision of public key cryptosystems" Entrust Technologies,canada, RSA Laboratories Vol. 4,No. 1,1998.

[5] P.Rodwald and J.Stokłosa, *PHAL-256 - Parameterized Hash Algorithm.* Proceedings of the Fourth International Conference onInformation Assurance and Security, IEEE Computer Society Press, Naples, Italy, 2008.

[6] Stuart Haber, Burt Kaliski and Scott Stornetta .How do digital timestamps support digital signatures, *CryptoBytes*, Vol.1, No. 3, RSA Laboratories, 1995, pp. 14-15.

[7] Johnson, D.B , Menezes and A.J 2007. Elliptic Curve DSA (ECDSA): An Enhanced DSA. Scientific Commons.

[8] Zhenfeng zhang and Dengguo feng, Key Replacement attack on a certificateless signature scheme, State Key laboratory of information security, chinese academy of science,Beijing.