Construction of a Hard Direct Digital Signature Scheme

انشاء نظام التوقيع الرقمي المباشر الصلب

Noor Dhia Kadhm Al-Shakarchy
Computer Science Department, Science College, Karbala University

Abstract

The rapid development of internet e-commerce is a new model of business activities; and the spread of electronic government in every organization all that needs to look for signing the documents and reports then verification of this signature in the other side. Digital signature authentication scheme provides secure Communication and reduce transmission costs, because the message is contained in the signature itself and no separate message and signature need be sent again.

This research develops a digital signature scheme to introduce a hard digital signature (double secure signature). This duplicate comes first from applying *RSA* hashing text, and the second from applying hard knapsack to message recovery elliptic curve cryptography *ECC*.

The combination provides secret signature against current attacking mechanisms using public key algorithms and in the other side, the sender can send the signing message directly to receiver without Arbitrated Digital Signature.

الخلاصـة

التطور السريع الحاصل في التجارة الالكترونية واعتماد الحكومة الالكترونية في تعاملات كل المؤسسات ادى الى التوجه للاهتمام بتوقيع الوثائق والتقاريرالكترونياً عند الارسال والتحقق منها واثبات ثوقيتها عند الاستلام. التوقيع الرقمي يوفر الاتصال الامن ويقلل من كلف الارسال و ذلك لبقاء الرسالة نفسها عند التوقيع ولا حاجة لارسال الرسالة مفصولة ثم ارسال التوقيع.

هذا البحث يطور التوقيع الرقمي لانتاج توقيع رقمي صلب (توقيع مزدوج الامنية). هذه الازدواجية تاتي من استخدام طريقة RSA اولاً مع طريقة هجينة من hard knapsack مع elliptic curve cryptography *ECC* .

النظام المقترح يوفر توقيع رقمي مامون بوجه طرق الهجوم على خوارزميات المفتاح المعلن وكذلك امكانية استخدام النظام المقترح في ارسال الرسالة الموقعة مباشرتاً الى المستلم .

1-Introduction:

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. The digital signature is analogous to the handwritten signature. It must have the following properties [1, 2]:

- It must be verifiable by third parties, to resolve disputes.
- Non-repudiation. The signature firmly establishes the identity of the sender. The sender cannot deny having sent the message and the signature (It must verify the author and the date and time of the signature).
- Confidentiality. Secret information shared between sender and receiver; any outsider cannot read the information.

- Message recovery: Upon receipt of the cipher text, the recipient decrypts it and segregates the signature and the message and verifies the authenticity of the sender. Only he will be able to do so because he alone has the necessary tools.
- Authentication. The sender imprints his identity by means of the digital signature, which only the designated receiver can unravel and verify. An anonymous adversary cannot send a malicious message impersonating the genuine sender, because he doesn't have the necessary tools to generate the signature; in other words, It must to authenticate the contents at the time of the signature.

Thus, the digital signature function includes the authentication function. On the basis of these properties; formulate the following requirements for a digital signature [1,16]:

1. The signature must be a bit pattern that depends on the message being signed.
2. The signature must use some information unique to the sender, to prevent both forgery and denial.
3. It must be relatively easy to produce the digital signature.
4. It must be relatively easy to recognize and verify the digital signature.
5. It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
6. It must be practical to retain a copy of the digital signature in storage.

A variety of approaches have been proposed for the digital signature function. These approaches fall into two categories: direct and arbitrated. The direct digital signature [1, 3] involves only the communicating parties (source, destination). It is assumed that the destination knows the public key of the source. A digital signature may be formed by encrypting the entire message with the sender's private key or by encrypting a hash code of the message with the sender's private key. The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.

The problems associated with direct digital signatures can be addressed by using an arbiter. There is a variety of arbitrated signature schemes, they all operate as follows [1] : Every signed message from a sender X to a receiver Y goes first to an arbiter A, who subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to Y with an indication that it has been verified to the satisfaction of the arbiter.

Finally Perfect signature should meet the following three conditions:

1) The signer cannot deny his own signature afterwards.

2) Any other person cannot forge the signature.

3) If the parties on both sides dispute the authenticity of the signature, it can be confirmed its authenticity through verifying the signature in the front of judicial judges.

In this paper we present a new approach of direct digital signature by using multi public key cryptography; that's mean the sender can't deny his or her signature although he/ she purport the key is stolen or attack because it used multi key and it can't attack or stolen all keys in the same time.

2-Related work:

Digital signature authentication scheme provides secure Communication, because the message is contained in the signature itself and no separate message and signature need be sent again. Therefore many researches developed to generate the digital signature scheme with provisional properties. In 1985 Miller [4] and Kobitz [5] introduced the elliptic curve cryptosystem. It provides greater security than integer factorization systems and discrete logarithm

systems, for given key size and bandwidth [4, 6]. Many researches present the digital signature with common system (RSA and AL-GAMAL).
In 1999 Mihir Bellare_ Sara K. Minery [7] describe a digital signature scheme in which the public key is fixed but the secret signing key is updated at regular intervals so as to provide a forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be useful to mitigate the damage caused by key exposure without requiring distribution of keys.
In 2008 Lyubashevsky and Micciancio [8] give a direct construction of digital signatures based on the complexity of approximating the shortest vector in ideal (e.g., cyclic) lattices. The construction is provably secure based on the worst-case hardness of approximating the shortest vector in such lattices within a polynomial factor, and it is also asymptotically efficient: the time complexity of the signing and verification algorithms, as well as key and signature size is almost linear (up to poly-logarithmic factors)in the dimension n of the underlying lattice.
2009 Ramasamy and Prabakar [9] present a digital signature scheme with message recovery based on knapsack based elliptic curve cryptography (ECC) In this scheme, using ECC and then applying the simple knapsack to generates the signature.

2011 Nivethaa, Parthiban [10], presents the implementation of knapsack based Elliptic Curve Cryptography (ECC) for digital signature authentication with message recovery. For any key size, elliptic curve cryptosystem provides greater security when compared to integer factorization and discrete logarithm system. Generally in digital signature, signature (r, s) along with message will be sent to the receiver but in our scheme, signature alone is sent and message will be recovered from (r, s). The strength of knapsack algorithm depends on the selection of the knapsack series.
In this paper we present a new approaches with development of many above research; this proposed approach combining of RSA hashing text with ECC concept and message recovery and used hard knapsack (trapdoor knapsack) to increase the security with reasonable computational cost and to resist against most cryptanalysis. This scheme used two major keys therefore, it can be used with direct digital signature in which the sender can’t deny his signature later in future or claim his\ her key stolen because as far as the first key stolen it can’t second key stolen in the same time. The proposed method has three levels of authenticated encryption. First one is from RSA scheme by using hashing text which present reasonable authentication, the second based on Elliptic Curve signature and third one is applying hard knapsack (trapdoor knapsack) value for the signing message.

3-theoretical side:

3.1 RSA scheme and hashing text:

The RSA scheme can be describe in figure (1) [2]:

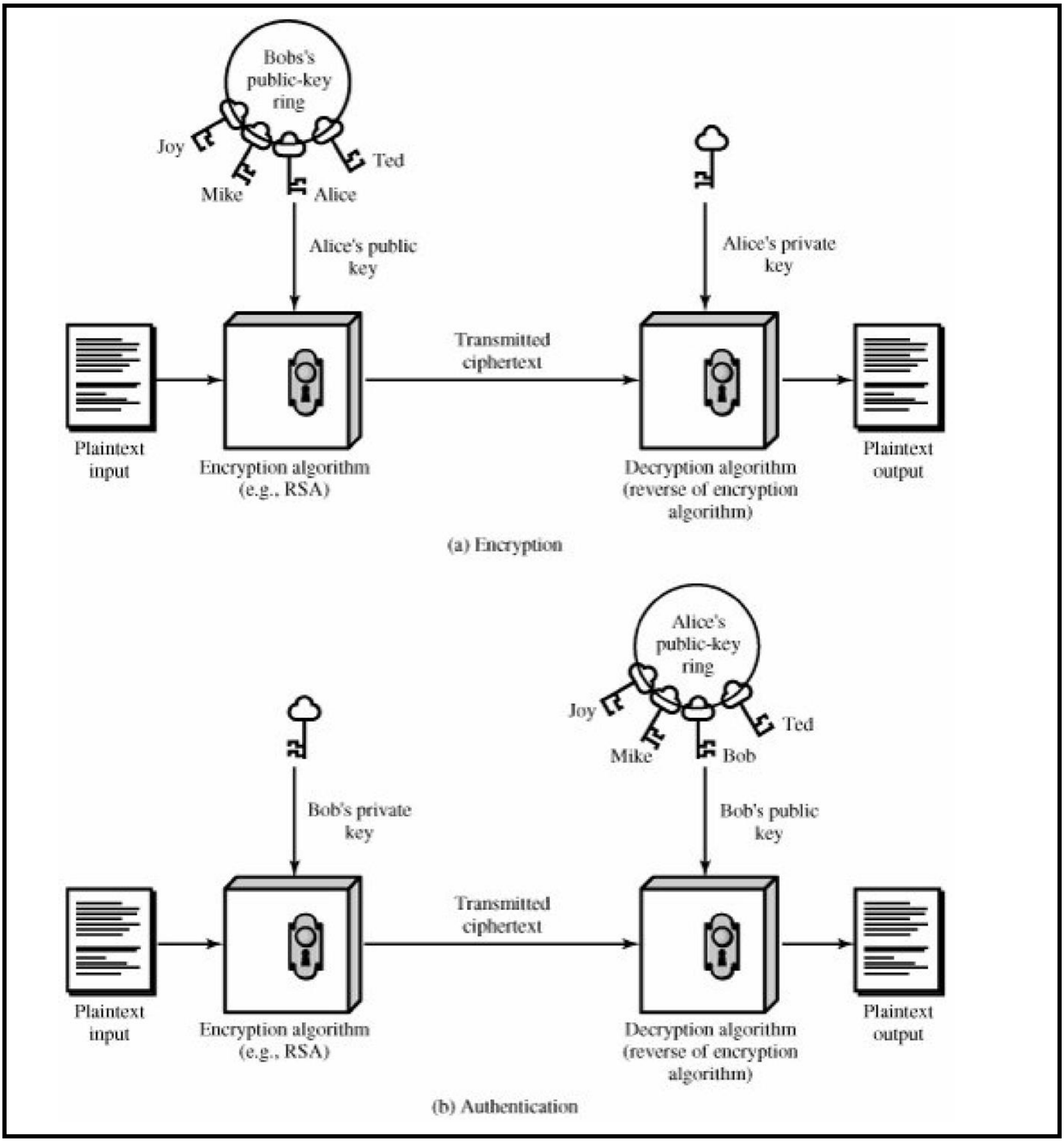

Figure (1) Encryption, authentication process

While hashing function can be definition as a variation on the message authentication code is the one-way hash function [11]. As with the message authentication code, a hash function accepts a variable-size message M as input and produces a fixed-size output, referred to as a hash code H (M) [1]. In another words it can be defined a hash function is a function that maps strings of arbitrary length to strings of fixed length n called the hash length [12].

The security of RSA depends on the following dichotomy [13, 2, 14]:

- Setup. Let p and q be large primes, let N = pq, and let e and c integers.
- Problem. Solve the congruence xe ≡ c (mod N) for x.
- Easy. The person, who knows the values of p and q, can easily solve for x.
- Hard. The intruder, who does not know the values of p and q, cannot easily find x.
- Dichotomy. Thus solving xe ≡ c (mod N) is easy for people possessing certain information, but is apparently hard for everyone else

The Plain RSA Scheme can be describing as [1, 11, 14]:

1. Key Generation: upon input 1n, choose two random primes of length n/2 and compute N = pq.
   Choose e such that gcd(e, φ(N)) = 1.
   Find d such that ed ≡ 1 mod φ (N).
   Output (public key) pk = (e, N) and (secret key) sk = (d, N).
2. Encryption: Given pk = (e, N) and a message m ∈ {1, . . . , N − 1}, compute and output c = x^e mod N .
3. Decryption: Given sk = (d, N) and c,
   Compute m = c^d mod N.

3.2 Message recovery based on elliptic curve cryptography:

Elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible [5]. The size of the elliptic curve determines the difficulty of the problem [5]. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements. For current cryptographic purposes; an elliptic curve is a plane curve which consists of the points satisfying the equation [5, 6, 15]

$$y^2 = x^3 + ax + b,$$

This is the mathematical operations of ECC where 4a3 + 27b2 ≠ 0. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain 'parameter of ECC [6].

3.3 trapdoor knapsack (hard knapsack) [13]:

A trapdoor one-way function is a special type of one-way function with a secret trapdoor. It is easy to compute in one direction, and hard to compute in the other direction But if you know the secret, you can easily compute the function in the other direction. The Trapdoor knapsack (hard knapsack) is more security from simple knapsack because the vector A that is used in encryption process being secret and computing from another vector A' according to some secure parameters u and w.

The vector A' = (a1', a2', … , a_n') is selected such that : $a_i > \sum_{i=1}^{i-1} a_i$'

u is chosen such that (st) : u > $\sum_{i=1}^{n} a_i$'

w is chosen such that : gcd(u, w) = 1

w^{-1} = inv(w,u) [i.e ww^{-1} mod u =1]

A = w * A' mod u: that is a_i = w * a_i' mod u

C = EA [M] = A M where C is ciphertext and M is plaintext message

M = DA [C] = Snap (w^{-1}C mod u, A')

4-The proposed scheme:

The proposed scheme describe in this paper deal with direct digital signature that's mean there is no trusted authority center received the singed message then transmit it to receiver ; the transmission process makes between sender and receiver only without any other side. Therefore the initial phase (preparing the parameters requisites to this system) done by contract between two sides. The main algorithm of proposed scheme consists of three phases:

Phase 1, initial phase: this phase depends on the treaty and contains:

- preparing the keys and parameters of RSA process (such that p and q , private key then compute public key ,this step done in sender side and transmit public key and n to receiver.
- Selects the elliptic curve E: $y^2 = x^3 + ax + b$ defined over Zp where p is a prime. Let G ϵ E (Zp) be a base point of order n which is prime. The sender agreement with receiver identifies E; p; n and G points. The sender chooses a random number x ϵ [1; n - 1] and this value is secret. Then computes y = xG, and sends (y) to receiver.
- Preparing vectors and parameters of hard knapsack process, as discussion in 3.3 above. Then the sender transmits the public parameters (A', w^{-1}, u) to receiver.

Phase 2, the transmission process: this phase includes two parts: The generation phase in sender side and the transmission of the singed message to receiver. The generation part applying in three steps:

a- Compute text hashing h=H (M) then applying RSA scheme E=RSA (h), then added the result E to main message (M'= M+E).
b- Compute s and r according to ECC on message' (M') such that: r = M' + (kG) x mod n, and s = k - H(r) x mod n.
c- Applying trapdoor knapsack and obtained S and R.
R= hard knapsack (r), S= hard knapsack(s).

In transmission parts the singed message (S, R) transmitted to receiver.

Phase3, the verification phase: this phase done in receiver side to verify the signature and recover the main message, when the receiver received the transmitted message = (R, S), he/she applied the original steps:

a- Compute reverse hard knapsack to return the value of r and s; r = simple knapsack (R * W^{-1} mod U, A'), s= simple knapsack (S * W^{-1} mod U, A').
b- Recover and verify the message M with M' = r - (sG +H(r) y) x mod n, M= M' – E.
c- Compute h=decrypt RSA(E) and h= H(M) then compare between two values of h if these values equal then the message is authoritative.

5- The algorithm of suggestion system:

The main form of system determined the user desire to singe or authorize; if the choice is singed then the main steps doing are:

1. Preparing the message we wanted to singed (the system deal with alphabet A..Z, a.. z) By saved it in file.
2. Applying RSA hashing function :
   i) Convert the message to binary from convert every letters to corresponding coding in binary.
   ii) Calculate hash value h using xor function
   iii) Applying RSA algorithm on h value to obtained E
   iv) Add the result E to main message (M'= M+E).
3. Compute s and r according to ECC on message' (M') such that: r = M' + (kG) x mod n, and s = k - H(r)x mod n.
4. Applying trapdoor knapsack and obtained S and R. R= hard knapsack (r), S= hard knapsack(s).
5. The output of this phase is (M, R and S).

If the choice is authorized the send singed message (R, S) the authentication steps doing:

1. Compute reverse hard knapsack to return the value of r and s; r = simple knapsack (R * W-1 mod U, A'), s= simple knapsack (S * W-1 mod U, A').
2. Recover and verify the message M' = r - (sG +H(r) y)x mod n.
3. Compute E from E= M'- M.
4. Compute h=decrypt RSA(E)
5. Applying hashing function by convert the message M to binary then calculate the hash value h= H (M).
6. Compare between two values of h (from 4, 5) if these values equal then the message is authoritative.

6- Conclusion:

The proposed scheme presents a new secret method of direct digital signature (without control center). The main conclusion we can notice in practical part of this system:

1. The message singed verifiable such that the receiver can verify the signature.
2. This method prevent a deny of signature or message from sender (the main problem with direct digital signature) although he/she claim his/ her key stolen because this method used multi key. If the cryptanalyst stolen or broken any key he/she can't forgery the signature because he/she needs to break other keys.
3. The used of combining public key schemes provides high-level security because The used of multi key provide double secure digital signature first from using RSA and the second by using trapdoor knapsack based on elliptic curve cryptosystem. All these schemes have more robustness against most public key attack that's produced multi robustness with combination.
4. The used of message recovery keeps the verification of the signature kind of secret, in another word this method encrypt the message inside the singed process.
5. The proposed system provides a high security with minimum computational costs.

6- References:

[1] William Stallings \ Cryptography and Network Security Principles and Practices, Fourth Edition, Publisher: Prentice Hall, Pub Date: November 16, 2005.

[2] Vincent LeVeque \Introduction to Cryptography”, Manager Science Applications International Corporation (SAIC), Prepared for COMMON Fall, October 1996

[3] Birgit Pfitzmann, Digital Signature Schemes General Framework and Fail-Stop Signatures’, Computer Science, Cryptology, Digital Communication. Springer-Verlag, Heidelberg, August 1996.

[4] V. Miller, \Use of elliptic curves in cryptography", Advances in Cryptology (Crypto'85), LNCS 218, pp. 417-426, 1985.

[5] N. Koblitz, \Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[6] A. Menezes and S. Vanstone, \Elliptic curve systems", Proposed IEEE P1363 Standard, pp. 142, 1995.

[7] Mihir Bellare_ Sara K. Minery\ A Forward-Secure Digital Signature Scheme’,July 13, 1999.

[8] V. Lyubashevsky and D. Micciancio\”Asymptotically Efficient Lattice-Based Digital Signatures”, University of California, San Diego, La Jolla, CA 92093-0404, USA,2008.

[9] R. Rajaram Ramasamy and M. Amutha Prabakar\“ Digital Signature Scheme with Message Recovery Using Knapsack based ECC”, Computer Science and Engineering, Thiagarajar College of Engineering, Thiruparankundram, Madurai, Tamil Nadu, India, 625 015, India, 2009.

[10] Nivethaa Shree, K.; Parthiban, L.\” Knapsack-based Elliptic Curve Cryptography using stern series for digital signature authentication”, Department of Compute Science & Engineering, SSN College of Engineering , Kalavakkam, India, 2011.

[11] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman\ An Introduction to Mathematical Cryptography Mathematics”,Brown University — Fall 2004.

[12] IKrystian Matusiewicz, introduction to cryptographic hash functions’, Centre for Advanced Computing Algorithms and Cryptography, Department of Computing, Macquarie University , 5 October 2007.

[13] Bruce Schneier, John Wiley & Sons\ Introduction to CryptographySummarized from “Applied Cryptography, Protocols, Algorithms, and Source Code in C”, 2nd. Edition, 1995.

[14] R. L. Rivest, A. Shamir, and L. Adleman, \A methodfor obtaining digital signatures and public key cryptosystems," Communications of the ACM, vol. 21, pp. 120-126, 1978.

[15] Neal Koblitz[1] and Victor S. Miller[2],’Elliptic curve cryptography’, Wikipedia, the free encyclopedia, 1985.

[16] Xilong Qu[1] , and Zhongxiao Hao[2]\ A New Approach for Digital Signature Based on Digital Seal “, [1] Department of Computer Science and Technology, Hunan Institute of Engineering, Xiangtan, China , [2] School of information Science & Electrical Engineering, Hebei University of Engineering, Handan, China , 2009.