Cryptographic Method of Protecting Educational Certificates From Forgery Using DSS

[1]Nashwan Ahmed Al-Majmar, [2]Ayedh Abdul-Aziz Mohsen
[1,2]Dept. of Math's and Computers, Faculty of Science, Ibb university, Yemen

Abstract
Protecting educational certificates from forgery in a modern society is a very important issue.That protection can be provided by using information cryptographic authentication methods based on digital signature schemes.The present paper suggests a system to issue such documents in a way that provide high security and this can be done through using two or more digital signatures based on different and difficult mathematical problems.

Keywords
Digital Signature Scheme (DSS), Digital Signature (DS), Information Authentication, Information Verification, Public Key Infrastructure (PKI).

I. Introduction

One of the actual and sensitive issues in the modern society is getting illegal certificates and diplomas on education by the people who are not enrolled in universities. This issue is related to the nature of criminal activities structure, performing the for gery of these documents. In this paper we propose a system that uses cryptographic protection methods for issuing and verifying the authenticity of documents, practically the application of this method solves the problem referred to previously and does not require significant costs.

II. System Description

The proposed system can be explained simply on the basis of existence of the used and wide information infrastructure (internet) and the presence of used broadly DS. The proposed method for the validation of diplomas and certificates is based on using a centralized database where reserved digital certificates for documents issued by educational institutions. These digital certificates contain signatures of these educational institution as shown in fig. 1.

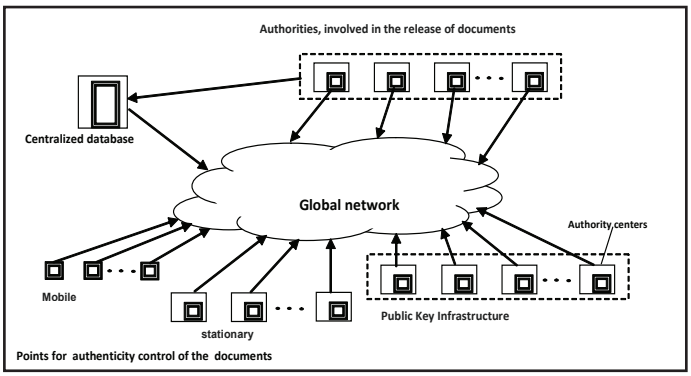

Fig. 1: Architecture of Automated System ForSupporting Cryptographic Protection Technology of the Documents Against Forgery

Each educational document related to digital certificate containing the readable automatically following information:

1. First and last name of the student
2. Name of educational institution
3. Issuing date of the document
4. Number of document
5. Specialization
6. Public key and DS of educational institution

Such documents' issuing system has increased resistance against attacks related to falsifying documents. This resistance linked to using cryptographic protection technology against forgery and applying two DS schemes, based ontwo different and difficult computational problems i.e. discrete logarithm and factorization. The possibility of applying DSS of the second typeis due to the resultof development of DS algorithms based on complexity of factorization problem that provide reducing signature's up to 320 bits [1]. Personalized thanks to the small size of DS has the possibility to sign a master image, associated with the document and its content by several different authorities involved in the release of this document. This provides a high security to the system against insiders.

The presence of several authorities, legalizing release of the document, will significantly reduce the probability of participation of the people who are authorized to carry out the legalization of documents, in the process of illegal documents' registration. This is due to a remarkable decrease of the probability that potential internal adversaries will receive simultaneously authority to issue documents. Therefore, in the considered technology requires the presence of two or more digital signatures of controlled message. On the basis of constructing of this system has a technical solution involving the use of a digital signature to bind a specific form of the document with a specific data contained in the document. Thus, we propose the use of paper with stable random microscopic inclusions and the presence of mass production of portable and stationary scanners with sufficient resolution. It also assumes that on the form of document to apply a special mark on which the scanner automatically determines the location of the site is scanned to identify the unique digital image of the form, in which is made an educational certificate document.

The practical impossibility of forgery is linked to the formation of DS to the message, which is formedas an union ofa digital image of a particular form with the specific content of the document through the series and number of the document. Taking into consideration the possibility of acceding to such information and biometric information about the owner of the document. As a result, it is possible to verify the authenticity of the document by digital signature, which uses the public key of one, two or more authorities, confirming by its digital signatures the legitimacy issue of this particular instance of the document and its authenticity.

It's supposed to use existing and practically applied PKI for the sake of the distribution of public keys related to the digital legal certificates of the documents on education. Public keys can be obtained from the centralized database via the Internet or from a public key directory distributed by certifying centers.In the case of the developed system obtaining public keys of authorities that certify the authenticity of documents, and checking their

authenticity is not a problem, since relying party requires only a few public keys that are valid for quite a long time and are used to verify a large number of documents.

DS is applied to the document in one or two places in a document given that provides a constant presence of the signature in the document. When checking the authenticity of the document, should be scanned the digital image of the document, should be read the information content of this document, form control message and verify the authenticity of a digital signature to this control message. Because that DS physically must be presented on the document, then the crucial issue is to reduce the total size of all DS captured on document in the form of machine-readable tags, this is achieved by using algorithms DS generating signatures with minimal size.

Document's Authentication Procedure Includes

1. Scanning digital image of document.
2. Formation controlled dataset.
3. Verifying the validity of all signature, using public keys of authorities, confirming the authenticity of the educational certificate.

Modern scanning devices are quite reliable, miniature and reasonably priced, so the proposed technology to protect documents from material counterfeiting is promising formass application.

III. Generation and Verification Algorithms of Digital Signatures

Persistence of modern DS schemes based on the complexity of solving a difficult computational problem, however, there is a sufficiently small probability that theoretical advances will reduce the security of a digital signature below the critical level.In order to reduce this probability, we have suggested DS schemes, the disclosure of which requires the simultaneous solution of two or more difficult mathematical problems of various types.In this case, the probability of compromise DS drastically reduced because it is equal to the product of the probabilities of developing more effective ways to solve each of the difficult mathematical problems, such as:

probability (solution of difficult problem of type 1) $\approx 10^{-9}$
probability (solution of difficult problem of type 2) $\approx 10^{-9}$
probability(simultaneous solution of difficult problems of the 1st and 2nd type)$\approx 10^{-18}$

As mentioned earlier regarding automated system for supporting technology of cryptographic protection of documents against forgery is supposed to provide confirmation of the validity of the document by two or more authorities, involved in the issuance of documents. Therefore it's interesting to use two or more different algorithms DS based on various difficult mathematical problems. However, Currently there is a limited number of such problems on which can be provided high resistance and relatively small size of DS (320-640 bits).

The simplest solution for diagramming DS, hack which requires the simultaneous solution of two different difficult computational problems is to construct DS schemes, which are based on"mechanical" combination of two different DS schemes, i.e generation of signature as a combination of two independent signatures. This means that a user's digital signature to some document consists of two independent parts, generated by independent algorithms. DS is considered true if each of individual digital signature is genuine. The most interesting mathematical problems for this application are the integer factorization problem of a special type and the discrete logarithm problem in a finite group of large prime order.

A. DSSBased On Factorization Problem

As DS scheme, based on the complexity of the factorization problem, it is proposed to use the following scheme represented by the following algorithms of generation and authentication of the digital signature having small size.

(i). Generation Algorithm of the System Parameters

1. The public key is a pair of numbers n and $y = \alpha^x \bmod n$, where x – is a secret key, n – is a 1024-bit number that = p * q where | p |= | q | = 512-bit
2. α - is a number referring to simple indicator γ'on modulo p and simultaneous referring to simple indicator γ''on moduloq, where γ' and γ''– 80-bit primes.
3. Generate a random number k, such that GCD $(k,\gamma'\gamma'') = 1$ and $1 < k < \gamma'\gamma''$

(ii). Generation Algorithm of Signature to the Message M

1. Generate a random number k, such that GCD $(k,\gamma'\gamma'') = 1$ and $1 < k < \gamma'\gamma''$, where γ' and γ'' are some 80-bit primes.
2. Calculate the value of $r = \alpha^k \bmod n$.
3. To the message m joined the number r to form a message M = m||r, and compute the hash function of the value M: E = h (M)
4. Calculate the value of s: $s = k - xE \bmod \gamma'\gamma''$

The public key is (n , y ,α) and the digital signature is a pair of numbers (s, E).

(iii). Verification Algorithm of Signature (S, E)

1. Calculate the value of r′: $r' = \alpha^s y^E \bmod n$.
2. To the message M joined the number r'to form a messageM' =M||r', and compute the hash function of the value M′: E′ = H (M′).
3. Compare the values EandE′, i.e. if E = E′, then the signature is considered genuine.

This scheme is based on the complexity of the factorization problem as a basic problem. In fact, the secret key can be calculated by solving the discrete logarithm on modulon, i.e. solving the equation of calculating the public keyy = $\alpha^x \bmod n$, wherex – is the unknown quantity. However, the complexity of computing discrete logarithms on composite modulo is not lower complexity of module factorization [1-2].

B. DSS Based on Discrete Logarithm Problem

As another type of algorithm, supplementing 1st type algorithms can be used the following scheme of Schnorr C. P. [3].

(i). Generation Algorithm of the System Parameters

1. Choose primes p, γ, such that γ| (p - 1); |p| $\approx$ 1024, |γ| $\approx$ 160
2. Choosean element $\alpha \in Z_p^*$ of orderq, i.e. $\alpha^\gamma = 1 \bmod p$
3. Choosea cryptographic has h function H
4. Generate random number x such that $1 < x < \gamma$
5. Calculate $y = \alpha^x \bmod p$
6. Private key is x, and the public key is (p, γ, α, y)

(ii). Generation Algorithm of Signature to the Message m

1. Generate a randomnumberk such that 1< k < q
2. Calculate thevalue of r = α^k mod p
3. To the message m joined the number r to form a message M = m||r, and compute the hash function of the value M: E = h (M)
4. Calculate the value of s: s = k + xE (mod q) the digital signature is a pair of numbers (s, E).

(iii). Verification Algorithm of Signature (s, E):

1. Calculate the value of r′: $R' = \alpha^S y^{-E} \bmod p$
2. To the message m joined the number r'to form a message M′ = m||R', and compute the hash function of the value M′: E′ = h (M′).
3. Performs a comparison of E and E′, if E = E′, then the signature is considered genuine.

We will show that the system is cryptographic, if the pair (m, (s,E)) is a true pair of "message-signature":

$$R' = \alpha^S y^{-E} \bmod p = \alpha^{k+xE}\alpha^{-xE} = \alpha^k = R \bmod p$$

As in ElGamal scheme [4] the parameter k, acting the role of a one-timesecret key must be selected using simple random selection method and used only once.

IV. Conclusion

Thus, the suggested system that involves the proposed cryptographic methods, on the basis of their used different DSS makes the forgery of documents impossible. By using this technology, the possibility of criminal groups and elements in their malicious activity are considerably reduced, which in general will favor the rule of law in the society.

References

[1] Berezin A. N., Moldovyan N. A., Shcherbakov V. A., "Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems", Computer Science Journal of Moldova, Vol. 21, No. 2(62), pp. 280-290, 2013.

[2] Menezes, A.J.,"Handbook of Applied Cryptography [Текст]", A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone. – CRC Press, Boca Raton, FL, 1997.- 780 p.

[3] Schnorr, C.P.,"Efficient signature generation by smart cards [Текст]", C.P. Schnorr. – J. Cryptology, Vol. 4, pp. 161-174, 1991.

[4] ElGamal, T.,"A public key cryptosystem and a signature scheme based on discrete logarithms [Текст]", T. ElGamal. – IEEE Transactions on Information Theory, Vol. 31, No. 4. pp. 469-472, 1985.

Nashwan Ahmed Al-Majmar received his B.S. degree in Computer Systems Engineering and Informatics, in 2003, the M.S. degree in Computer Systems Engineering and Informatics, in 2006 from Saint-Petersburg Electro-technical University "LETI", Saint-Petersburg, Russia, and the Ph.D. degree in methods and systems of information protection and security from Saint-Petersburg State University of Information Technologies, Mechanics and Optics, Saint-Petersburg, Russia, in 2010. He is an assistant professor with Department of Mathematics and computer science, Ibb University, Ibb city, Yemen since 2010 and with IT Department, University of science and technology "UST", Yemen. He is a Head of IT Department at University of science and technology "UST", Ibb branch, Yemen since 2011. His research interests include "information protection and security" and "software development".

Ayedh Abdulaziz Mohsen received his B.S. degree in engineering and technology from Saint Petersburg Electro-technical University" LETI", Saint Petersburg, Russian Federation, in 2006, the M.S. degree in engineering and technology from Saint Petersburg Electro-technical University "LETI", Saint Petersburg, Russian Federation, in 2008, and the Ph.D. degree in Technical Sciences from Saint Petersburg Electro-technical University " LETI", Saint Petersburg, Russian Federation, in 2011. He is an assistant professor in Department of Math's and Computer, Faculty of Science, Ibb University, Yemen and Department of information technology, Faculty of Computer and information technology, University of Science and technology "UST", Yemen. His research interests include Computer Aided Design (CAD), web application design and data mining through web.