Elliptic Curve based Signature Method to Control Fake Paper based Certificates

SGK Murthy, MV Ramana Murthy, A Chandrasekhara Sarma

Abstract–**Cryptography plays vital role in many electronic applications. Information confidentiality, authentication and integrity are desirable features for electronic transactions and these features are achieved by using a proper combination of symmetric and asymmetric cryptographic techniques. In order to ensure information authenticity, digital signatures are the equivalent part for normal signatures. It is well known that with the help of digital signature, forgery of digital information can be identified and it is widely used in e-commerce and banking applications. As Elliptic curve based digital signatures are stronger and require less size, in this paper a method is presented to detect fake paper based documents with ECC based digital signatures, which in turn control fraudulent practices related to paper based certificates.**

Index Terms- **Authentication, Digital signatures, Public key Cryptography**

I. INTRODUCTION

As technology is advancing, creation of fake paper-based documents becomes easier. Forgery is a crime in which some one falsifies something with the intent to deceive. There are different kinds of forgeries, which are treated as criminal under law. There are number of sites available on Internet to issue fake degree certificates. It is a growing trade world wide in counterfeit university degree certificates and academic transcripts, which in turn creates a potential damage to the universities in national as well as international level. An audit in may 2004 showed that around 463 employees in the federal government had the fake academic degrees [6]. In order to control fraudulent practices, predominantly university degree certificates, organizations issuing certificates with holograms containing security features. Some of the organizations verify the authenticity of the certificates over phone also. However different mechanisms exist to identify fake certificates, the verification process is time consuming and not reliable as generated fake certificates are similar to original certificates. It is well known that digital signatures are more reliable and stronger to normal signatures for authentication. As E-commerce applications adopted digital signature based mechanisms to ensure integrity and authentication for electronic transactions, the same concept can be extended to paper based certificates also. In this paper a method is proposed that utilizes the combination of hashing and signing techniques to control fake university degree certificates. As the objective is strong signatures that occupy minimal space on the certificate, Elliptic curve Digital signatures are considered for the proposed scheme. A brief description is given in the following sections about public key cryptography and Elliptic curve Digital signature scheme that is applied to paper based certificates.

II. PUBLIC KEY CRYPTOGRAPHY

Cryptography is a branch of cryptology, deals with the design of the algorithms for encryption and decryption to ensure secrecy and authentication of information. There are two kinds of crypto systems, symmetric and asymmetric. In symmetric crypto systems same key is used for encryption and decryption process. In asymmetric crypto systems a key pair called public and private keys used for encryption and decryption process, so that information is encrypted with a public key can be decrypted with corresponding inverse key (private key) only. Asymmetric crypto systems are called public key crypto systems. On the other way, information encrypted with a private key can be decrypted with corresponding inverse key called public key. This concept raised information authentication with digital signatures.

A digital signature is a term used for marking or signing an electronic document by a process meant to be analogous to paper signatures, but which makes use of a technology known as public-key cryptography. In other words, it's a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender and ensures that the document has not been altered in any way, since the sender has signed it[1].

III. ELLIPTIC CURVE BASED DIGITAL SIGNATURES

Whitfield Diffe and Martin Helman introduced the concept of asymmetric cryptography to solve the key distribution problem in 1976. Same concept is used for the creation of digital signatures. All asymmetric key crypto systems are based on certain hard problems that can’t be solved in polynomial time. These hard problems are used to create one-way trapdoor functions. RSA, DSA (Digital

Manuscript received May 9,2010

SGK Murthy is with the Defence Research and Development Laboratory,Hyderabad,INDIA,Phone:91-40-24151654,e-mail: sgk_murthy@yahoo.com
MV Ramana Murthy is with the Department of Mathematics,Osmania university, Hyderabad ,INDIA,e-mail:mv_rm50@gmail.com
A Chandrasekhara Sarma is with the Department of Information Technology ,ATRI, Hyderabad,INDIA,e-mail:candidsoft@yahoo.com

signature algorithm), ECC (Elliptic curve cryptography) are popular asymmetric crypto algorithms used for digital signatures to ensure information authentication.

Elliptic curve cryptography (ECC) is an asymmetric cryptographic technique uses 160 bits key (or more) for encryption/decryption operations. ECC derives its strength from elliptic curve discrete logarithm problem[2]. When compared to other cryptographic hard problems (i.e. factorization and discrete logarithms on a finite groups), elliptic curve discrete logarithm provides more cryptographic strength. In ECC, encryption/decryption operations are based on two operations called scalar multiplication and addition of two points on the elliptic curve[3]. Required operations to create and generate a digital signature with the help of hashing are discussed in detail in the following section.

(a) Hashing Techniques

Hash functions take an arbitrarily long piece of plaintext and compute a fixed length hash value. Computing a message digest from a piece of plain text is much faster than encryption of same text, with the asymmetric crypto algorithms. By using message digest, speed of the signature generation and verification process is increased[5]. Hashing techniques are frequently used for message integrity and for the creation and verification of digital signatures. MD5 (Message Digest Algorithm) and SHA (Secure Hashing Algorithm) are two popular hashing algorithms used in security applications. In this Paper SHA-I algorithm is considered as, it generates 160 bits hash value.

(b) ECDSA Signature Generation

To sign an information m, an entity A with the domain parameters D = (q, a, b, G, n) and associated key pair (Q, d) [4]. Where d and Q represents public and private keys. a, b represents the coefficients of the elliptic curve. G is a point on the curve. n is the order of the elliptic curve ($y^2 = x^3 + ax + b \bmod (n)$).

1. Select a random integer k, where 1 <= k <= n-1.
2. Compute kG = (x1,y1) and convert x1 to an integer x1bar.
3. Compute r = x1 mod n, if r = 0 go to step 1.
4. Compute k^{-1} mod n.
5. Compute SHA-1(m) and convert this bit string to an integer e.
6. Compute s= $k^{-1}(e + dr)$ mod n. if s=0 then go to step 1.
7. A’s signature to the message m is (r,s).

(c) ECDSA Signature Verification

To verify A’s signature (r,s) on m, B obtains a required copy of A’s domain parameters D = (q,a,b,G,n) and associated public key Q.

1. Verify that r and s are integers in the interval [1,n-1].
2. Compute SHA-1 (m) and convert this bit string to an integer e.
3. Compute w = s^{-1} mod n.
4. Compute u1 = ew mod n and u2 = rw mod n.
5. Compute X = u1G + u2Q.
6. If X = 0, then reject the signature. Other wise convert the x-co-ordinate x1 of X to an integer x1bar, and compute v = x1bar mod n.
7. Accept the signature if and only if v =r.

IV. CREATION AND VERIFICATION OF THE PAPER BASED CERTIFICATES WITH SIGNATURE.

In this section a method is described to generate/verify the signature pertaining to the information. It is assumed that the certificate issuing authority, obtained digital certificates from proper channel, and the public key of the issuing authority is available to all concerned.

Creation of Signature on the issuing Certificate

1. The variable unique information pertaining to the candidate, to whom certificate is issued, (ex Unique no, Reg no, first name, middle name, last name, Father’s name, year of passing and obtained marks) has to be considered as an input **m**.
2. **m** is hashed with the Secure Hashing algorithm (SHA-I) to create a hash value **md**.
3. Hash value **md** is encrypted using the private key of the issuing authority, and the encrypted value (**ds**) is considered as digital signature.
4. **ds** is converted into a barcode **BC** and printed along with the information required on the certificate.

The following block diagram (Fig-1) explains the creation of signature on the certificate

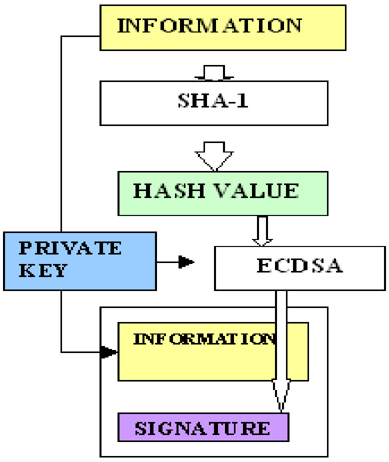
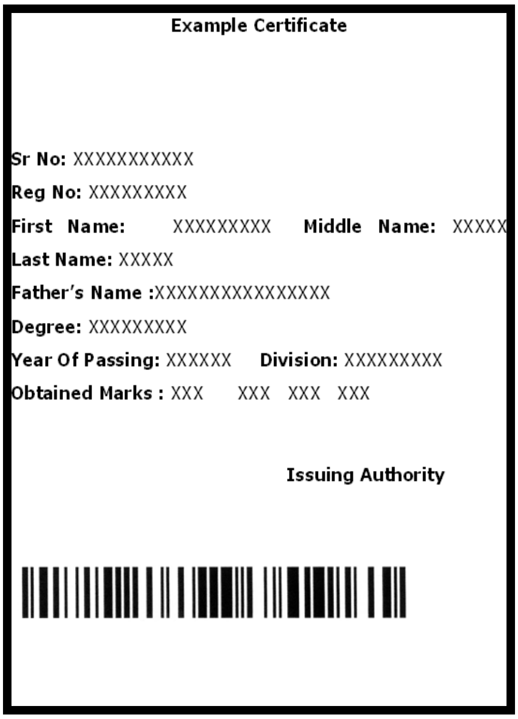


Fig –1 :-Creation of a signature

The following diagram (Fig-2) describes the model of the certificate.



Example Certificate

Sr No: XXXXXXXXXXX

Reg No: XXXXXXXXX

First Name: XXXXXXXXX **Middle Name:** XXXXX

Last Name: XXXXX

Father's Name :XXXXXXXXXXXXXXXX

Degree: XXXXXXXXX

Year Of Passing: XXXXXX **Division:** XXXXXXXXX

Obtained Marks : XXX XXX XXX XXX

Issuing Authority

Fig –2 :- Model of the certificate

Verification of the certificate

1. The variable information pertaining to the candidate mentioned in the above procedure is considered as input **m.**
2. **m** is hashed with the secure hashing algorithm (SHA-I) to create Hash value **md1**
3. Bar code **BC,** available on the certificate is converted into ASCII code **ds** and it is decrypted with the public key of the issuing authority, which gives a value **md2**.
4. Compare the values **md1** and **md2**. Certificate is treated fake if **md1** does not match with **md2** other wise it is original.

The following diagram (Fig –3) describes verification of signature

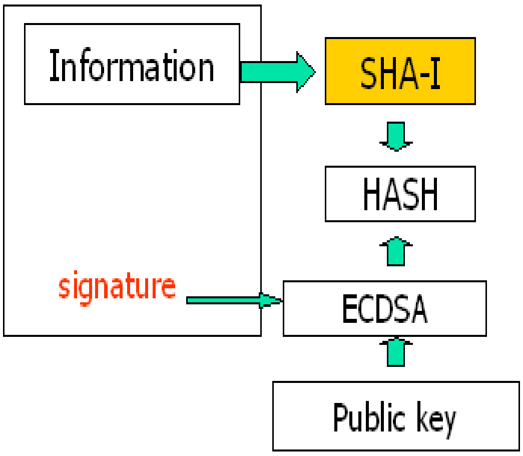


Fig -3:-Verification of signature

V. CONCLUSION

In this paper, issues related to fake university certificates and different mechanisms to ensure authenticity of the certificates are discussed. In order to control fake certificates, a method is proposed by utilizing digital signatures. As RSA related signatures demand more space, Elliptic curve based signatures are considered for this method. The combination of Elliptic curve and SHA-I algorithm provides strong cryptographic strength and optimizes the computational speed as well as space. As the proposed method is based on the strength of the elliptic curve discrete logarithm problem; it is not vulnerable for crypt analysis attacks, which are readily available.

References

[1] Schneier, B, Applied Cryptography, John Wiley, New York

[2] Stallings, W, Cryptography and Network Security: principles and practice,2nd ed (Indian Ed) , Prentice hall

[3] The Elliptic curve cryptosystem, A Certicom white paper, Certicom Corp, Canada

[4] Don Johnson et al, The elliptic curve digital signature algorithm, Certicom Research, Canada

[5] Andrew S Tanenbaum, Computer Networks, Third edition, Prentice-hall inc, New Delhi, India, 1999

[6] Chris Chew, Fake university Degree Scam, HotScams.com, April 2007