International Journal of Computer and Communication Technology

Volume 5 | Issue 1 Article 6

January 2014

A Secure Short Signature Scheme Based upon Biometric Security

Mousumi Parida
Department of Computer Science & Engineering National Institute of Technology, Rourkela Orissa-769008, India,, mousumiparida87@gmail.com

Sujata Mohanty
Department of Computer Science & Engineering National Institute of Technology, Rourkela Orissa-769008, India,, sujata.nitrkl@gmail.com

A Secure Short Signature Scheme Based upon Biometric Security

Mousumi Parida *, Sujata Mohanty
Department of Computer Science & Engineering
National Institute of Technology, Rourkela
Orissa-769008, India, 2010
mousumiparida87@gmail.com*, sujata.nitrkl@gmail.com

Abstract— This paper presents a short signature scheme whose security is based upon two computationally hard problems, namely, discrete logarithm problem (DLP) and Integer factorization problem (IFP). In this scheme, biometric feature values of the signer are used to compute biometric cryptographic key, which is further used in signature generation. As biometric data is unique to a person, the signature cannot be forged. Also the length of the signature is short, which helps to reduce communication overhead. The verification cost of the proposed scheme is low, thus applicable in real life scenarios, such as e-voting, e-cash and e-commerce.

Keywords— digital signature, biometric cryptographic key, entropy, fractal transform.

I. INTRODUCTION

Biometrics security is becoming an important part of information security. Biometric data of an individual can never be changed. Biometric data is derived from physical or behavioural traits which exhibit the properties like universality, distinctiveness, permanence, collectability. So we can say biometric is a foundation of trust and cryptography is the projection of trust. Cryptography uses secret keys. Secret keys are generated using some algorithm which generates random numbers. But the numbers generated are never random, they are pseudorandom, means at some point they are repeated. So we need to approach a method of getting secret key absolutely random. Moreover it will be highly advantageous if we can bind an individual with the key generated for him for his data encryption. Passwords are prone to be obscured. To alleviate this problem we can introduce biometric authentication instead of password authentication. After using the biometric input as a means to authenticate we can use the same input for the generation of biometric key also, which can be used for cryptography.

Biometric cryptography uses biometric features to encrypt the information. There are a number of traits which can be used for key generation like fingerprint, palm print, iris, face, voice etc. As fingerprint is the most easily collectable and most commonly used biometric we can consider fingerprint as the input to our authentication and key generation system. Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits per pixel has 300x400x8 = 960,000 bits of information. Of course, this information is highly redundant. One can ask a question: Is it possible to consistently extract a relatively small number of bits, say 128, out of these 960,000 bits? Or, is it possible to bind a 128-bit key to the biometric information so that the key could be consistently regenerated? While the answer to the first question is problematic, the second question has given rise to the new area of research, called Biometric Encryption (BE). Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric so that neither the key nor the biometric can be retrieved from the stored template.

In this paper, we present a digital signature scheme, which is based on the work of Shao [1], in which biometrics data of the signer are used to generate signature. The signature length is small, which helps to reduce communication complexity. The scheme is secure as its security lies in the complexity of solving two computationally hard problems, namely, discrete logarithm problem and integer factorization problem. As biometric data of the signer are embedded in the signature, it is almost impossible to get secret parameters of the signature from the public data. The biometric cryptographic key generation of this scheme is based upon Liu et al.'s scheme [2].The proposed scheme is proved to be resistant against active attacks, such as, forgery attacks, plaintext only attack.

The rest of the paper is organised as follows. Section 2 describes the proposed signature scheme. Discussion of the proposed scheme is done in Section 3. We prove the correctness and do the security analysis of the proposed scheme. Finally we conclude in Section 4.

II. RELATED WORK

Our work is inspired by a number of previous works related to cryptographic key generation from biometrics and cancelable biometrics. A brief review of some of the works is given below:

A irrevocable cryptography key generation scheme from cancellable fingerprint template, which performs in an efficient manner was projected by N.Lalithamani et al [6].The scheme employs the minutiae points in the cancelable fingerprint template formation and cryptographic key generation.The approach initially extracts the minutiae points from the fingerprint images and transforms the extracted minutiae points in order to obtain deformed points. Subsequently, the acquired deformed minutiae points are employed to obtain the cancelable fingerprint templates which were then utilized to generate the irrevocable cryptographic key.

The concept of cancelable biometrics was proposed by Andrew B. J. Teoh et al. [7] to express biometric templates that can be cancelled and restored with the addition of another independent authentication factor. A kind of cancelable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The quantized random projection collection on basis of the Johnson-Lindenstrauss Lemma was employed to accomplish the mathematical foundation of BioHash. Depending upon this model, they have explained the characteristics of BioHash in pattern recognition in addition to security view points and provided some methods to resolve the stolen-token problem.

A.T. Beng Jin and Tee Conniea [8] have proposed the Cancelable biometrics in order to describe biometric templates that can possibly be canceled and replaced. A kind of cancellable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The chief disadvantage of BioHash was its immense deprivation in performance when the legitimate token is stolen and is utilized by the pretender to claim as the legitimate user. A modified probabilistic neural network was utilized by them as a classifier to address the aforesaid issue.

Anna Squicciarini et al.[9] employed techniques from vector-space model to generate cryptographic biometric keys. Each element of the characteristic vector is weighted with respect to the importance of that characteristic. Here classification of a fingerprint is based on the pattern type which can be precisely one of five classes, namely, whorl, right loop, left loop, arch, and tented arch. Since this classification is based not on exact minutiae points but instead on certain invariant characteristics of a fingerprint depending on the properties of the fingerprint as a whole, two such sets of characteristics of a particular fingerprint would be almost the same.

I. PROPOSED SECURE SHORT SIGNATURE SCHEME

The proposed short signature scheme is based on discrete logarithm and takes biometric string generated from fingerprint as input. This scheme has two parties, namely, signer and verifier. The signature scheme has the following three phases: biometric cryptographic key generation, signature generation and signature verification.

A. Biometric Cryptography Key Generation

The steps of generating biometric cryptographic key are given as below:

- A binarized fingerprint image is taken as input. Zero padding done to make it both 4 and 8 divisible.
- An array sub entropy H is created and will store the entropy of each 4*4 sub matrix. The array parent entropy PH is created taking 8*8 windows.
- Now we have two 2D Arrays H and PH. Number of elements in H is 4 times PH. Each element of PH is matched with 4 elements of H. The matched elements are kept in an array. Now we get a (row/8) *(col/8) 2D array of matched entropies.
- The 16 pixels from which the array element (entropy) is formed is found out and replaced in place of the array element. Now we get a matrix of ((row/8) *(col/8) *16)) pixels. This matrix is converted to binary string. The sub block size can be increased so as to adapt to the public key's size required.

A. Signature Generations

Let p and q be large primes with q|(p-1). Also let $G_{g,p}=\{g_0,g_1....g_{q-1}\}$ be a prime order q subgroup of the multiplicative group $Z^*_{p,}$ where g is a generator with prime order q. Let H be the hash function SHA-1. For notational convenience, we will omit the "(mod p)" and "(mod q)" markers. The notation $a \xleftarrow{R} S$ means that a is picked randomly from a set S. We now describe the proposed signature scheme in full detail.

- The key generation algorithm Gen:
  Picks a random $x \xleftarrow{R} Z^*_q$ as the private key. The corresponding public key is

$$y = g^x. \quad (1)$$

- The signing algorithm Sign:
  The inputs are private key x, public key y, a message m, and the biometric data we have generated in the first phase is ä. Then a random $k \xleftarrow{R} Z^*_q$ is picked. The SHA-1 hash function is applied and the digest f is computed.

$$f = H(m, ä). \quad (2)$$

Then the value of r, h and s are computed

$$r = g^k f. \quad (3)$$

$$h = H(m, r). \quad (4)$$

$$s = k - x. \quad (5)$$

The signature of the message m is

$$ó = (h, s). \quad (6)$$

C. Signature Verification

The verification algorithm Ver: The inputs are the public key y, message m, biometric data ä and the signature ó. Computes f, r× and h×. If h = h×, Ver outputs valid, otherwise it outputs invalid.

$$f = H(m, ä). \quad (3)$$

$$r× = y\, g^s f. \quad (4)$$

$$h× = H(m, r×). \quad (5)$$

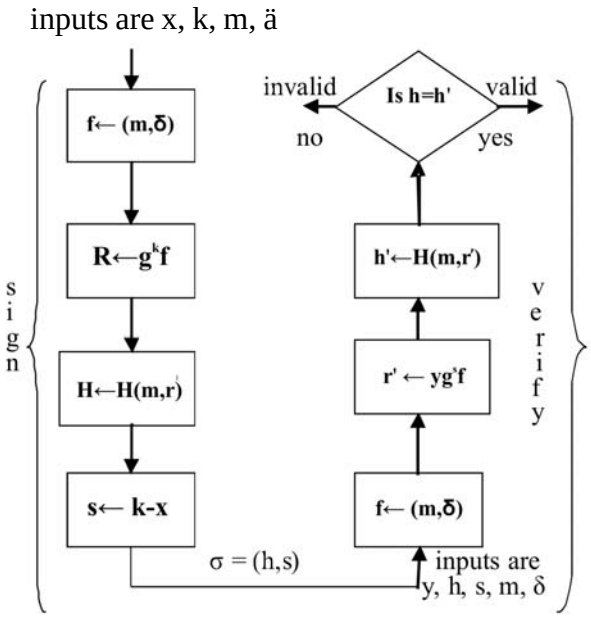

Fig 1. Proposed short signature scheme based on biometric security.

I. DISCUSSION

A. Security Analysis of Biometric Key Generation

Here we describe two possible attacks to the biometric data generation scheme and identify ways of preventing it.

- It is possible for an attacker to obtain a copy of the signer's biometric data. Then he can send the data as his own to KGC and acquire the corresponding private key as the same as the signer's. That is, the attacker has obtained the private key of the signer and could imitated signer to sign some contracts or documents. To prevent this attack, we suggest that in key generating stage, user must have provided his biometric data on the spot in KGC with a trusted witness in presence. Then KGC turns the biometric data into public key string using compression algorithm proposed in this scheme, assures that the public key is unique in the system and issues the public/ private key pairs to user in a secure way.

If biometric data such as fingerprints of an attacker is extremely similar with the signer's, attacker could come to see the verifier with a contract signed by signer and claim that he is the very one who had signed the contract. To prove it, he could provide his

- fingerprints data on the spot. It is very difficult for verifier to distinguish the two extremely similar fingerprints image. So, the verifier maybe has

trusted the attacker. To prevent this attack, contract can be signed in the presence of a trusted witness. If there is a legal dispute over whether a contract had been signed or not by a user later, the witness could come to assert which one is the genuine signer. Alternatively, signers also can utilize a digital certificate obtained from a trusted certificate authority. The digital certificate will contain the public key and some other information such as social security number about the signer.

A. Security Analysis and Correctness of proposed scheme

1) Correctness: The correctness of the verification method used by verifier to check the validity of signature is as follows: h will be equal to h× when r = r×. We have:

$$r = g^k f. \qquad \text{from (3)}$$

$$g^k f = g^{s+x} f. \qquad \text{from (5)}$$

$$g^{s+x} f = y\, g^s f. \qquad \text{from (1)}$$

$y\, g^s f. = r\times$. Thus proved

2) Security Analysis of Proposed Scheme: We describe the security of our proposed scheme with the following Lemmas:

Lemma 1: If the adversary has access to plaintext m and r× then also it cannot forge the signature ó.

Proof: It is computationally almost impossible to solve discrete logarithm problem. Suppose an adversary A has access to plaintext m and r× it is infeasible to find s, h from the multivariant congruence:

$$H(m, yg^s f) = h \qquad (10)$$

Lemma 2: The proposed scheme can withstand forgery attack.

Proof: If an intruder has access to plaintext m and key she cannot find r because of the embedding of biometric data in hash function. Intruder may follow the following steps to forge signature. Let ä× be an assumed binary string by eve. Then eve computes f× = H(m, ä×). Then it computes r× = g^k f×, h× = H(m, r×) and s = k - x. Then eve sends the dummy signature pair s and h× to be verified. Verifier verifies with the following steps: It finds out f = H(m, ä×) then computes r = y g^s f , y g^s f ‘“ r×. Thus h ‘“ h×. Verifier discards the signature.

V. IMPLEMENTATION OF PROPOSED SCHEME

We generate biometric key in Matlab. We have taken a standard fingerprint image which is of dimensions 364*256(91 KB).Then we binarize the grey image.We have used 64*64 window size for finding subentropy array and 128*128 window size for finding parent entropy array. We have increased window size so as to adapt to our key size required. We did 20 bits zero padding to row so that it is divisible by our taken window sizes. We found the subentropy array which was of size 6*4 and the parent entropy array which was of size 3*2. Applying the matching algorithm to the parententropy array and subentropy array we find the most matched entropy array which was of size 3*2. Then each element of that array which is a entropy value is replaced with the 64 bits(pixel values) from which it was calculated. Finally we get the key which is of size 2*3*64 that is 384 bits. The input image is shown in fig 2 and the key generated in fig 3. We then implement the proposed secure short signature scheme using JCE(java cryptography extension) which takes less computation time than the SSDL algorithm as it has two exponential computation and three multiplications as compared to three exponential computation and four multiplications in SSDL algorithm.

Fig 2. fingerprint image for input to biometric key generation

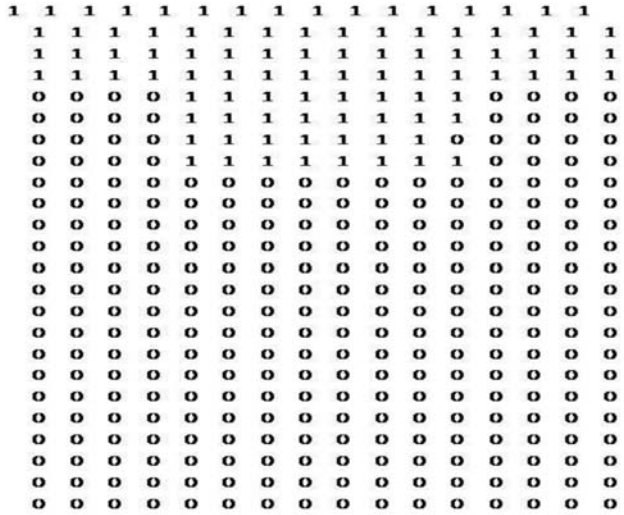

Fig 3 output biometric key

I. CONCLUSION

We have described an improved short signature scheme which is existentially unforgeable. The main advantage of this scheme is that it reduces both the length of the signature and computation done in verification significantly. Level of security is also preserved. To guarantee security we can use SHA-256 or SHA-512 hash functions. In this scheme it is also not possible to recover the private key by solving the related discrete logarithm problem.Thus in our scheme, it is more visible and convenient for the verifier to finish a verification. The verification cost of the proposed scheme is low, thus applicable in real life scenarios, such as e-voting, e-cash and e-commerce.

REFERENCE

[1] Z. Shao, "A provably secure short signature scheme based on discrete logarithm", Information Sciences 177, 2007, pp. 5432-5440.

[2] X. Liu, Q. Miao, D. Li, "A New Special Biometric Identity Based Signature Scheme", International journal of Security and its Applications, vol. 2, 2008.

[3] S. Pankanti, S. Prabhakar and A. K. Jain, "On the individuality of fingerprints", IEEE Transaction on PAMI, vol. 24, No. 8, 2002, pp. 1010-1025.

[4] A.Cavoukian, A.Stoianov, "Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy", Academy of Information and Management Sciences Journal, vol. 7, no 2, March 2007.

[5] L. Leong, Edward J., "Password Pitfalls and Dynamic Biometrics: Towards a Multi-Layer User Authentication approach for electronicbusiness", Academy of Information and Management Science Journal, vol. 7, no. 2, 2004.

[6] Lalithamani, K.P. Soman , "Irrevocable Cryptographic Key Generation from Cancellable Fingerprint Templates: An Enhanced and Effective Scheme", European Journal of Scientific Research ISSN 1450-216X Vol.31 No.3,pp.372-387N,2009.

[7] Teoh AB, Yuang CT., "Cancellable biometrics realization with multispace random projections.", IEEE Trans Syst., vol:37, no:5, pp:1096-106, 2007.

[8] Andrew Teoh Beng Jin, Tee Conniea, "Remarks on Bio-Hashing based cancellable biometrics in verification system", Neurocomputing, Vol: 69, no: 16-18, Pages 2461-2464, 2006.

[9] Anna Squicciarini, Elisa Bertino, Abhilasha BhargavSpantze "Privacy Preserving Multi-Factor Authentication with Biometrics",Association for Computing Machinery, November 3, 2006.