Personal Authentication Protocol based on ECDLP using Biometric Feature Values

Jayaprakash Kar† and Bansidhar Majhi††

†Department of Information Technology, Al Musanna College of Technology, Sultanate of Oman
††Department of Computer Science & Engineering, National Institute of Technology, Rourkela, INDIA

Summary
This paper proposes a new Biological personal authentication protocol which helps to establish trust by identifying a particular user or system. It is a one-way authentication protocol. Here the biological information, whatever its kind such as fingerprints, iris, retina DNA, tissue and other features which are unique to an individual are embedded into cryptographic keys which consists of both Private and Public keys in Public Key Cryptosystem. Our Protocol is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). Here the entity is generating two numbers for his own private key. If one of the numbers is stolen or modified, the system security can still be guaranteed due to the computational infeasibility of solving Elliptic Curve Discrete Logarithm Problem, unless the other variable is leaked.

Key words:
ECDLP, Biometrics feature values

1. Introduction

Now a day Authentication Protocol is an important application area in Cryptography community. Entity authentication or Personal Authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e. active at, or immediately prior to, the time the evidence is acquired). Distinction is made between weak, strong, and zero-knowledge based authentication. Objectives of identification protocols is from the point of view of the verifier, the outcome of an entity authentication protocol is either acceptance of the claimants identity as authentic (completion with acceptance), or termination without acceptance (rejection). More specifically, it includes the following [4].

- In the case of honest parties A and B, A is able to successfully authenticate itself to B, i.e. B will complete the protocol having accepted A's identity.
- (Transferability) B cannot reuse an identification exchange with A so as to successfully impersonate A to a third party C.
- (Impersonation) the probability is negligible that any party C distinct from A, carrying out the protocol and playing the role of A, can cause B to complete and accept As identity. Here negligible typically means is so small that it is not of practical significance; the precise definition depends on the application.
- The previous points remain true even if: a (poly-nominally) large number of previous authentications between A and B have been observed; the adversary C has participated in previous protocol executions with either or both A and B; and multiple instances of the protocol, possibly initiated by C, may be run simultaneously.

2. Background

In this section we brief overview of Elliptic Curve over finite field, Elliptic Curve Discrete Logarithm Problem and the feature of various Biological Information personal identification data.

2.1 The finite field F_p

Let p be a prime number. The finite field F_p is comprised of the set of integers $0,1,2...p-1$ with the following arithmetic operations [2] [3] [4]:

- Addition: If $a,b \in F_p$ then $a+b=r$, where r is the remainder when $a+b$ is divided by p and $0 \le r \le p-1.$ This is known as addition modulo p.
- Multiplication: If $a,b \in F_p$ then $a.b=s$, where s is the remainder when $a.b$ is divided by p and $0 \le s \le p-1$. This is

Manuscript received June 5, 2009
Manuscript revised June 20, 2009

known as multiplication modulo p.

- Inversion: If a is a non-zero element in F_p, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in F_p$ for which $a.c = 1$.

2.2 Elliptic Curve over F_p

Let $p \geq 3$ be a prime number. Let $a, b \in F_p$ be such that $4a^3 + 27b^2 \neq 0$ in F_p. An elliptic curve $E(F_p)$ over F_p defined by the parameters a and b is the set of all solutions $(x, y), x, y \in E(F_p)$, to the equation $y^2 = x^3 + ax + b$, together with an extra point O, the point at Infinity. The set of points $E(F_p)$ forms an abelian group with the following addition rules [6] [7]:

1. Identity : $P + O = O + P = P$, for all $P \in E(F_p)$
2. Negative: if $P(x, y) \in E(F_p)$ then $(x, y) + (x, -y) = O$, the point $(x, -y)$ is dented as $-P$ called negative of P.
3. Point addition: Let $P(x , y_1), Q(x_2, y_2) \in E(F_p)$ then $P + Q = R \in E(F_p)$ and coordinate (x_3, y_3) of R is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$, Where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$
4. Point doubling : Let $P(x_1, y_1) \in E(F_p)$ where $P \neq -P$ then $2P = (x_3, y_3)$ where $x_3 = (\dfrac{3x_1^{\,2} + a}{2y_1})^2 - 2x_1$ and $y_3 = (\dfrac{3x_1^{\,2} + a}{2y_1})(x_1 - x_3) - y_1$

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_p ,a point $P \in E(F_p)$ of order n, and a point $Q \in (P)$, find the integer $l \in [0, n-1]$ such that $Q = l.P$. The integer l is called discrete logarithm of Q to base P, denoted $l = \log_p Q$ [7].

2.4 The Features of Various Biological Information

Biological information used for biometrics personal identification includes fingerprint, DNA, iris, retina, tissue and other features unique to an individual. More particularly the invention relates to a method of processing biometric features for electronic storage and to facilitate rapid comparison with a present biometric feature. Various types of biometrics features as fingerprint, iris, and retina are used for identification and verification of individuals. The fig-1 shows the features of biological information.

The biometric features are extracted from raw data such as fingerprint images in case of fingerprint, iris images in case of Iris and retinal images for retina based biometrics identification and authentication systems. The extraction of biometric features from the raw data is carried out using feature extraction algorithm. The biometric features contain individualistic characteristics of the biometrics raw data that is used for verification. For example, in case of fingerprint the information on the individual characteristics of the fingerprint image includes, but is not limited to: (i) core points; (ii) ridge join points; and (iii) ridge line ending points The individual characteristics of the features have unique individual properties such as: (i) direction; (ii) angle; and (iii) relativity and other features The above listed properties and the characteristics are applicable for fingerprint. But in case verification using the retina, the characteristics include but are not limited to: (i) optical nerve core; (ii) ecaudate density; and (iii) optical disc-eye ratio As stated for the biometrics types above, the characteristics vary for different types of biometrics and the extraction and recognition of the characteristics are disclosed in prior art documents. The characteristics and their respective properties biometrics are referred in this description as ”biometrics data”. The biometrics data must be able to be stored electronically into a database and also be retrievable when required, for identification and verification.

3. Generate Biometrics Cryptographic Keys

This section describes how to generate the biometrics cryptographic keys, into which biological information is embedded. Also examines how to embed biological information into cryptographic keys. The Cryptographic key consists of Private and Public Key use is Public key cryptosystem. Embedding the biological information into private key means that the same data is automatically embedded into Public key generated in an algorithm defined by the system. After this, the cryptographic key consists of the Private key and the Public keys into which the biological information is embedded are referred as the Biometric Cryptographic keys. Extract the feature points and generate a template as follows:

An algorithm for extracting featuring points from raw biological information to generate the template is vendor-specific. For example, from a finger print pattern, the positional and relational information of branch and end points is acquired as a featuring point to create template. The practical compressed data size of the template ranges from 250 bytes to 500 bytes [9], [10]. Let the template generated from the featuring points be δ .The biometric features include but not limited to fingerprint, DNA, iris, retina, tissue and other features unique to an individual. Since the template δ consists of bit strings written in various format defined on a vendor basis, it can be regarded as a personal identifier showing that the template corresponds uniquely to the genuine person with certain matching probability. To minimize the ambiguity of the template δ as a personal identifier, a fingerprint is taken repeatedly upon initial registration, if the same δ is stored in the client system. When the same δ is generated from two individuals even if their finger prints are repeatedly taken many times, it shows the accuracy limitation of the system. In this case, it is necessary to study a new way, such as combination with other biological information.

We are generating both the Private Key and Public Key as follows:

1 Private Key: Let the template is processed through a hash function either SHA-1 or MD5 i.e. $d_1 = H(\delta)$ and $d_1 \in [1, n]$. and d_2 be another secret key is to be randomly chooses. Where $d_2 \in [1, n]$. Now Private Key is the pair (d_1, d_2) .

2 Public key: Let P and Q are any two points in $E(F_p)$ .The Public key is. $R = d_1.P + d_2.Q$

4. Proposed Personal Authentication Protocol

This section describes about the Authentication Protocol. The Protocol enables the personal identity of the entity while communicating between two parties. The protocol follows the following steps.

Step 1: Mr. A (prover) select the random number r_1 and r_2 where $r_1, r_2 \in [1, n]$ and compute the following equation. Where P and Q are any two points in $E(F_p)$.

$$S = r_1.P + r_2.Q \qquad (1)$$

Mr. A sends the resulting value S to Mr. B (Verifier).

Step 2: Mr. B selects arbitrary random number $e \in [1, n]$ and sends it to Mr. A .

Step 3: Mr. A compute y_1 and y_2 from the following equations:

$$y_1 = r_1 + e.d_1 \bmod p \qquad (2)$$

$$y_2 = r_2 + e.d_2 \bmod p \qquad (3)$$

Mr. A sends the pair (y_1, y_2) to Mr. B .

Step 4: Mr. B checks whether the following equation is satisfied.

$$S = y_1.P + y_2.Q - e.R \qquad (4)$$

The personal identification is successful if satisfied, otherwise unsuccessful.

The above proves that even if the Private key d_1 derived from the biological information is stolen, the system security can still be guaranteed unless the conventional other secret key d_2 is leaked.

Mr. A — Mr. B

Select random numbers r_1 and r_2 from $[1, n]$

Where $r_1, r_2 \in [1, n]$

Compute $S = r_1.P + r_2.Q$

S →

Selects random number $e \in [1, n]$

← e

Compute y_1 and y_2 by the following two equations

$y_1 = r_1 + e.d_1 \bmod p$

$y_2 = r_2 + e.d_2 \bmod p$

And send to Mr. B

(y_1, y_2) →

Checks the personal identity by the following equation

$S = y_1.P + y_2.Q - e.R$

5. Security Analyses

It is assumed that another person Mr. $\tilde{A}$ steals the bio-metric personal ID d_1 of Mr. A and pretends to be Mr. A. Moreover, Mr. A can derived $\tilde{d}_2$ that satisfies the following equation from the stolen d_1 and his own biometric personal ID $\tilde{d}_1$

$$R = d_1.P + d_2.Q = \tilde{d}_1.P + \tilde{d}_2.Q \qquad (5)$$

Mr. $\tilde{A}$ uses his $\tilde{d}_1$ and $\tilde{d}_2$, and compute $\tilde{y}_1$ and $\tilde{y}_2$ as the computation in equation (2) and (3) in Step 3.

$$\tilde{y}_1 = \tilde{r}_1 + e.\tilde{d}_1 \bmod p \qquad (6)$$

$$\tilde{y}_2 = \tilde{r}_2 + e.\tilde{d}_2 \bmod p \qquad (7)$$

Where $\tilde{r}_1$ and $\tilde{r}_2$ have been randomly taken by Mr. $\tilde{A}$ from $[1, n-1]$ who pretend to be Mr. A in step-1 and $e \in [1, n]$, Mr. $\tilde{A}$ sends the resulting $\tilde{y}_1$ and $\tilde{y}_2$ to Mr. B in Step-2 and Mr. $\tilde{A}$ compute the following equation.

$$S = \tilde{r}_1.P + \tilde{r}_2.Q \qquad (8)$$

In Step 4, Mr. B computes the following calculations.

$$\begin{aligned}
&\tilde{y}_1.P + \tilde{y}_2.Q - e.R \\
&= (\tilde{r}_1 + e.\tilde{d}_1).P + (\tilde{r}_2 + e.\tilde{d}_1).Q - e.R \\
&= (\tilde{r}_1 + e.\tilde{d}_1).P + (\tilde{r}_2 + e.\tilde{d}_2).Q \\
&= \tilde{r}_1.P + \tilde{r}_2.Q = S
\end{aligned}$$

Since the equation above holds, the authentication is passed. Accordingly Mr. $\tilde{A}$ can pretend to be Mr. A successfully.

Let us assume that there exist two algorithms ALG and $ECDLP_Q$ for deriving $\tilde{d}_2$ which satisfy equation (5) in polynomial time.
The two algorithms can be defined as follows
ALG is a stochastic algorithm having the input parameter $P, Q, R, d_1, \tilde{d}_1$ to provide $\tilde{d}_2$. More precisely we can describe as

INPUT: Parameters $(P, Q, R, d_1, \tilde{d}_1)$
OUTPUT: $\tilde{d}_2$

$ECDLP_Q$ is a stochastic algorithm having input Q and K to provide w in polynomial time that satisfies $K = w.Q$. More precisely we can describe as

INPUT: Parameters K, Q
OUTPUT: w

Demonstration

It is assumed that the input parameters Q and K of $ECDLP_Q$ are given. A random variable is substituted into β and P is given by $P = \beta.Q$.

Next, $R = d_1.P + K$ and then P, Q, R, d_1 are substituted in ALG which provides $\tilde{d}_2$ that satisfies equation (5) in polynomial time.
Since $d_1.P + w.Q = \tilde{d}_1.P + \tilde{d}_2.Q$, using $P = \beta.Q$ gives the following equation:

$$
\begin{aligned}
R &= d_1.P + K \\
&= d_1.\beta.Q + w.Q \\
&= \tilde{d}_1.\beta.Q + \tilde{d}_2.Q \\
&= d_1.\beta + w = \tilde{d}_1.\beta + \tilde{d}_2 \\
\Rightarrow w &= (\tilde{d}_2 - d_1).\beta + \tilde{d}_2
\end{aligned}
$$

Now the output w of $ECDLP_Q$ is given by

$$w = (\tilde{d}_2 - d_1).\beta + \tilde{d}_2$$

However, $ECDLP_Q$ can not be solved in Polynomial time, which denies the assumption that the Algorithm ALG exist. This proves that there does not exist such algorithm ALG having the input parameters $(P, Q, R, d_1, \tilde{d}_1)$ to compute $\tilde{d}_2$ which satisfies equation - (5).

5.1 Significance of using biometrics feature values

After generating the Private and Public key in which the biological information is embedded are referred to as the biometrics cryptographic keys. Embedding the biological information into cryptographic key has the following advantages [1]:

- Privacy protection of personal information.
- Zero knowledge, which means that no biological information is given directly to an inspector.
- Humanity resulting from embedding biological information into the cryptographic keys.
- Economical system which does not need to built up its own biological database.

6. Security Comparison

The basic question has been answered that how secure ECC is when comparing with RSA or DLP. In 1998, the security of ECC versus RSA/DSA is generally accepted [7]. The key sizes of around 173,210, and 313 bits of ECC has the same level of security with the key sizes of 1024, 2048, and 4096 bits of RSA/DSA.. Therefore, the protocol can use smaller key size while providing the same security in the previous protocols.

7. Conclusion and further research

In this paper, we have presented one-way authentication protocol which is based on ECDLP. So the proposed protocol is most efficient than the others which are based on Integer Factorization Problem (IFP) and Discrete Logarithm Problem (DLP) [1]. Since the best algorithm known for solving the underlying mathematical hard problem (ECDLP) takes fully exponential time [5] [7]. In contrast the sub-exponential algorithms known to solve the underlying problems (IF and DL). This Protocol can be extended to the following Protocols.

- Three way protocol such as Challenge Handshake Authentication Protocol (CHAP).
- Extensible Authentication Protocol (EAP) which is used between a dial-in client and server to determine what authentication protocol will be used.
- Mutual Authentication or two-way Protocol. Such protocols enable the communicating parties to satisfy them self mutually about each other's identity and to exchange the session keys such as Password Authentication (PAP) which is a two way handshake protocol.

References

[1] Yukio. Itakura, Shigeo. Tsujii Proposal on Personal Authentication System in which Biological Information is embedded in Cryptosystem, IACR e-print Archive 2003.

[2] N. Koblitz. A course in Number Theory and Cryptography, 2nd edition Springer-Verlag-1994

[3] K. H Rosen . Elementary Number Theory in Science and Communication, 2nd ed., Springer-Verlag, Berlin,1986.

[4] A. Menezes, P. C Van Oorschot and S. A Vanstone. Handbook of applied cryptography. CRC Press, 1997.

[5] D. Hankerson, A .Menezes and S.Vanstone. Guide to Elliptic Curve Cryptography, Springer Verlag, 2004.

[6] Certicom ECC Challenge. Available at http://www.certicom/index.php

[7] The Elliptic Curve Cryptosystem available at http://www.certicom/index.php.

[8] V. Miller "Uses of elliptic curves in cryptography", Advances in Cryptology CRYPTO'85, Lecture Notes in Computer Science, Volume 218, Springer-Verlag, pages 417-426,1986

[9] NEC solutions: The fingerprint identification system : Secure Engineer. http://www.sw.nec.co.jp/pid/about_pid.html

[10] Oki's product: IRISPASS-WG Gate Control System. http://www.oki.com/jp/SSG/JIS/Prod/iris/iriswg.html

Jayaprakash Kar has completed his M.Sc and M. Phil. in Mathematics from Sambalpur University, M.Tech in Computer Science from Utkal University, and pursuing Ph.D at Utkal University, Bhubaneswar, India. He has 5 years of industry experience in Bharat Earth Movers Limited in EDP department. He has completed 6 years of teaching in Engineering college and IGNOU Study center to MCA and BCA students. Mr. Kar is presently working as a Lecturer at Department of Information Technology, Al Musanna College of Technology, Ministry of manpower, Sultanate of Oman. His research areas are on Cryptography & Network Security, Biometrics and Web Security

Prof. Banshidhar Majhi is currently working as a professor and head of the Department of Computer Science and Engineering at National Institute of Technology, Rourkela, India. He has completed his M.Tech and Ph.D. from Sambalpur University. He has 15 Journal papers and 60 Conference articles to his credit. His research interests include image processing, cryptography and network security, soft computing.