An Elliptic Curve Arithmetic based Private Credentials System that uses Schnorr Blind Signature Scheme

N. Siva Selvan
Assistant Professor
MIT
Manipal, India

R. Vijaya Arjunan
Assistant Professor
Sr. Scale
MIT
Manipal, India

B. Kishore
Assistant Professor
Sr. Scale
MIT
Manipal, India

C. Ganesh Babu
Assistant Professor
MIT
Manipal, India

ABSTRACT

Privacy breach has become a major dispute in online transactions. In such a system, users give their personal information to get the service and that users' personal information may get wide spread across several organizations. Hence, there is a need for privacy protection. Private credentials offer authentication and authorization based on the traits possessed by a user not on the identity of the user. In this paper, we present a private credentials system that uses Schnorr Blind Signature based on elliptic curves. Elliptic curve defined over a prime field is chosen and ECDLP i.e., Elliptic Curve Discrete Logarithm Problem is the basis for the system. The properties of randomness, unlinkability, unforgability are preserved. The performance and storage space requirement of our system are compared with that of the cryptographic techniques that use discrete logarithm.

Keywords

Elliptic Curve Cryptography, Private Credentials, Schnorr Blind Signature

1. INTRODUCTION

In the recent days, there is a drastic increase in the number of users of online services. Users to get the services give their personal information on websites and there is a greater tendency that users' information may get wide spread across several establishments. There is a huge threat for user's privacy.

Firstly, the customary protection scheme i.e., enforcing access control policies based on the known set of identities will not be suitable if the set of potential users of an application go far beyond the community of users local to the system which has the application.

Secondly, maintaining databases of identities will cause applications to lag behind in efficiency. It would clearly be impracticable for an application to have prior knowledge of every individual. It would be difficult for users also to ensure that they have registered themselves with each and every application.

Thus, a more flexible mechanism is needed to allow users to validate that they are permitted to access certain data or services, without any pre-registration. The scheme should be based upon the notion of a user presenting credentials in support of a request. This data is used by the recipient to determine how the requester fits into the application's authorization scheme and so supplies the basis for the access control decision with respect to the request.

An individual could possess several identities corresponding to distinct roles in distinct systems since the credentials supplied with a request generally will not refer to the requester, and each credential which the individual may obtain will refer to him or her in terms of an identity known to the issuing system. Thus private credentials [6] preserve users' privacy. They also satisfy non-repudiation, unforgability.

In this paper we present a private credentials system that uses Schnorr Blind Signature based on ECC. The remainder of the paper is divided into 6 sections. Section 2 discusses Elliptic Curve Cryptography [2]. Section 3 gives an outline of the Existing System. Section 4 states System Overview. Section 5 discusses the Proposed System. Section 6 presents Findings and Discussions. Section 7 concludes the paper with scope for future work.

2. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) was proposed by Victor Miller and Neal Koblitz in 1985. Elliptic curve cryptography [2] [3] is a public-key cryptosystem like RSA, Rabin where every user has a public and a private key. Public Key is used for encryption and Private Key is used for decryption. An elliptic curve [1] is the set of solutions (x, y) to an equation of the form $y^2 = x^3 + Ax + B$, together with an extra point O which is called the point at infinity.

The mathematical operations of ECC are defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Each value of 'a' and 'b' gives a different elliptic curve as shown in Fig 1.

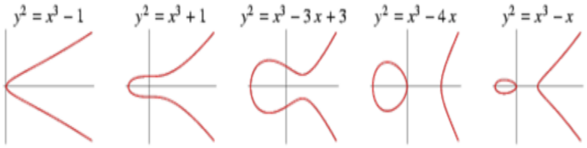


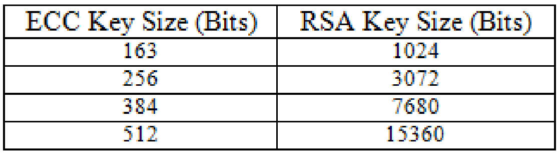
Fig 1 Different Elliptic Curves

For applications to cryptography, we consider finite fields of q elements, which can be written as Fq or GF(q). The former is defined over a prime field and the latter is defined over a binary field. In ECC, public key is computed by multiplying the private key which is a random number with a Generator point G on the curve. The computed public key is again a point on the curve.

The advantage of ECC over RSA is that ECC can provide the same level of security that RSA could provide but with reduced key size. For a 1024 bit RSA key it would take a 163 bit ECC key and other RSA-ECC key size pairs can be referred from table 1. Thus ECC can be used in devices that have limited memory and computational power.

ECC for security relies on the hardness of ECDLP which is called Elliptic Curve Discrete Logarithm Problem [1] [2]. It is relatively easy to compute kP =P+P+ … +P (k times) given a rational point P of prime order q and an arbitrary positive integer k < q, but given P and kP, it is computationally very difficult to recover k.

Table 1 Key Sizes: ECC versus RSA

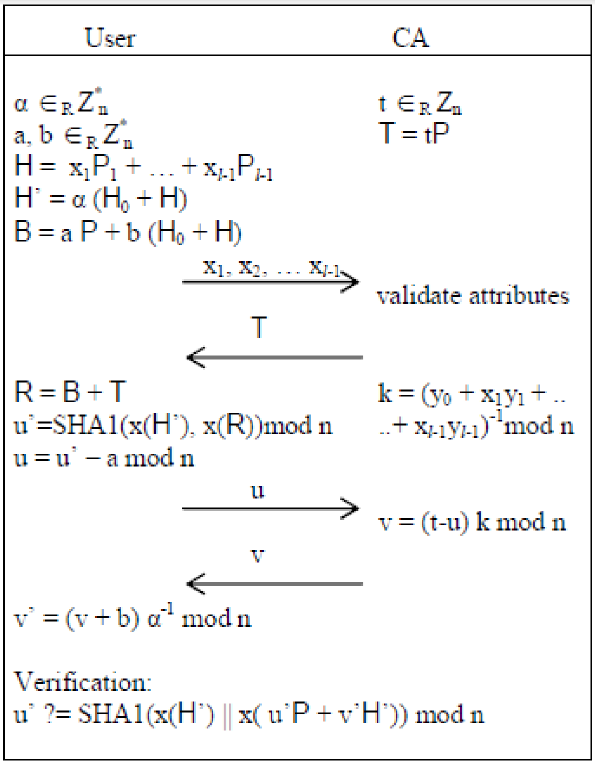


ECC Key Size (Bits)	RSA Key Size (Bits)
163	1024
256	3072
384	7680
512	15360

The ECDLP is analogous to the conventional discrete logarithm problem (DLP) in the multiplicative group of a finite field, and all cryptographic protocols based on the DLP i.e., Diffie-Hellman key exchange, ElGammal signatures. To obtain an effective cryptosystem, the underlying elliptic curve [1] must be carefully chosen. Certain types of curves with known weaknesses must be avoided.

3. EXISTING SYSTEM: CREDENTIAL ISSUE AND CREDENTIAL SHOW PROTOCOL

Existing system uses Restrictive Blind Signature where the Signer gets to see certain parts of the message to be signed. The system uses ECDLREP function which is defined as $f(x_1,x_2,\ldots,x_l)=x_1P_1+x_2P_2+\ldots+x_{l-1}P_{l-1}$ where x_1,x_2 are tuple elements and P_1,P_2 are Generators. Certificate Authority issues private credentials [7] to users and users show them to verifiers. Credential Issue and Credential Show protocols are shown in Fig 2 and 3 respectively.



User | CA

$\alpha \in_R Z^*_n$

$a, b \in_R Z^*_n$

$H = x_1P_1 + \ldots + x_{l-1}P_{l-1}$

$H' = \alpha(H_0 + H)$

$B = aP + b(H_0 + H)$

$t \in_R Z_n$

$T = tP$

$\xrightarrow{x_1,\, x_2,\, \ldots\, x_{l-1}}$ validate attributes

$\xleftarrow{T}$

$R = B + T$

$u' = SHA1(x(H'), x(R)) \bmod n$

$u = u' - a \bmod n$

$k = (y_0 + x_1y_1 + \ldots + x_{l-1}y_{l-1})^{-1} \bmod n$

$\xrightarrow{u}$ $v = (t-u)\,k \bmod n$

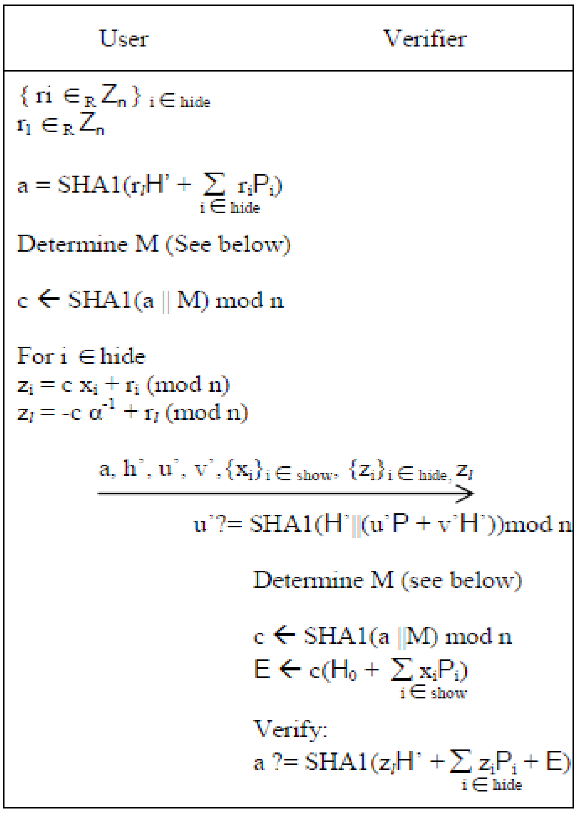
$\xleftarrow{v}$

$v' = (v + b)\,\alpha^{-1} \bmod n$

Verification:

$u' \mathrel{?=} SHA1(x(H') \,||\, x(u'P + v'H')) \bmod n$

Fig 2: Credential Issue Protocol



User | Verifier

$\{ ri \in_R Z_n \}_{i \in hide}$

$r_l \in_R Z_n$

$a = SHA1(r_lH' + \sum_{i \in hide} r_iP_i)$

Determine M (See below)

$c \leftarrow SHA1(a \,||\, M) \bmod n$

For $i \in hide$

$z_i = c\,x_i + r_i \pmod n$

$z_l = -c\,\alpha^{-1} + r_l \pmod n$

$\xrightarrow{a,\, h',\, u',\, v',\, \{x_i\}_{i \in show},\, \{z_i\}_{i \in hide},\, z_l}$

$u' \mathrel{?=} SHA1(H' \,||\, (u'P + v'H')) \bmod n$

Determine M (see below)

$c \leftarrow SHA1(a \,||\, M) \bmod n$

$E \leftarrow c(H_0 + \sum_{i \in show} x_iP_i)$

Verify:

$a \mathrel{?=} SHA1(z_lH' + \sum_{i \in hide} z_iP_i + E)$

Fig 3: Credential Show Protocol

User selects a value ‘α’ which he keeps it confidential and selects attributes $x_1, x_2, x_3 \ldots x_l$. CA issues private credentials [4] if attributes $x_1, x_2, x_3 \ldots x_l$ are valid. The credential comprises H’, u’, v’ which is sent to the verifier for verification.

4. SYSTEM OVERVIEW

Our system uses Schnorr Blind Signature based on ECC [9] where the number of rounds between signer and user is less compared to the existing system. The system uses ECDLREP function defined in Section 3. Throughout the system, the Certificate Authority or Signer issues Private Credentials [6] to users. Users show them to verifiers to get the services. Each Certificate Authority has a public key and a private key. User selects attributes viz., $x_1, x_2, x_3 \ldots x_l$ which he may have to show in showing protocol but keeps the selected random value ‘β’ confidential.

5. PROPOSED SYSTEM UNDER MICROSCOPE

5.1 Credential Issue Protocol

The Credential Issue protocol is shown in Fig 4. It is evident from the figure that between a signer and a user there are 3 steps/rounds. A signer picks 2 points P_1, P_2 on an elliptic curve and 2 random numbers d_1, d_2 which he considers to be secret keys. He then computes Q_1 and Q_2. The Signer selects 2 numbers securely r_1 and r_2, computes U and sends it to the user. User selects β which he maintains secretly and selects attributes $x_1, x_2, \ldots, x_l$. A function of value β together with attributes constitutes the message to be blindly signed by the signer. The Signer calculates Y_1 and Y_2 with the help of e and sends it to user. The user then calculates Y_1’, Y_2’ that form a part of the credential to be sent to the verifier for verification.

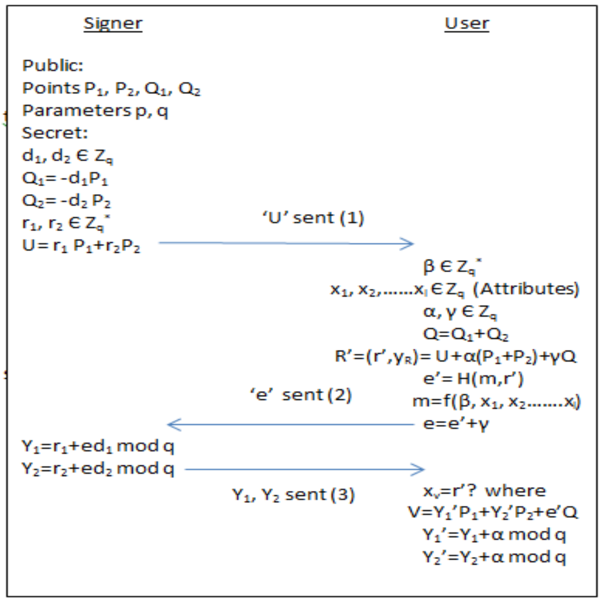

Signer
User
Public:
Points P_1, P_2, Q_1, Q_2
Parameters p, q
Secret:
$d_1, d_2 \in Z_q$
$Q_1 = -d_1P_1$
$Q_2 = -d_2 P_2$
$r_1, r_2 \in Z_q^*$
$U = r_1 P_1 + r_2P_2$
'U' sent (1)
$\beta \in Z_q^*$
$x_1, x_2, \ldots\ldots x_l \in Z_q$ (Attributes)
$\alpha, \gamma \in Z_q$
$Q = Q_1 + Q_2$
$R' = (r', y_R) = U + \alpha(P_1+P_2) + \gamma Q$
$e' = H(m, r')$
'e' sent (2)
$m = f(\beta, x_1, x_2 \ldots\ldots x_l)$
$e = e' + \gamma$
$Y_1 = r_1 + ed_1 \bmod q$
$Y_2 = r_2 + ed_2 \bmod q$
Y_1, Y_2 sent (3)
$x_v = r'$? where
$V = Y_1'P_1 + Y_2'P_2 + e'Q$
$Y_1' = Y_1 + \alpha \bmod q$
$Y_2' = Y_2 + \alpha \bmod q$

Fig 4: Credential Issue Protocol

5.2 Credential Show Protocol

The credential show protocol is shown in Fig 5

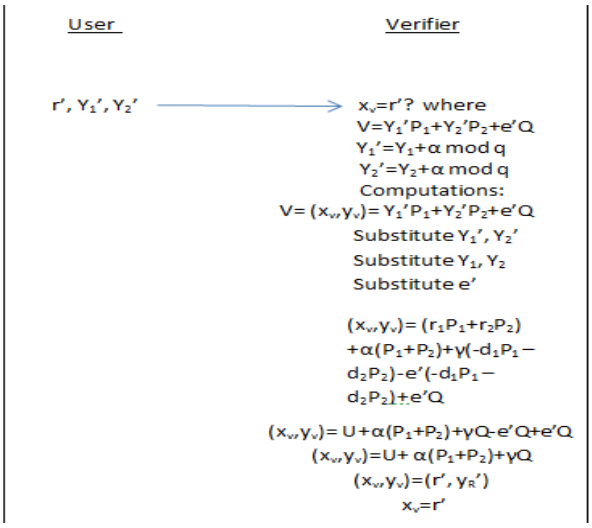

User
Verifier
r', Y_1', Y_2'
$x_v = r'$? where
$V = Y_1'P_1 + Y_2'P_2 + e'Q$
$Y_1' = Y_1 + \alpha \bmod q$
$Y_2' = Y_2 + \alpha \bmod q$
Computations:
$V = (x_v, y_v) = Y_1'P_1 + Y_2'P_2 + e'Q$
Substitute Y_1', Y_2'
Substitute Y_1, Y_2
Substitute e'
$(x_v, y_v) = (r_1P_1 + r_2P_2) + \alpha(P_1+P_2) + \gamma(-d_1P_1 - d_2P_2) - e'(-d_1P_1 - d_2P_2) + e'Q$
$(x_v, y_v) = U + \alpha(P_1+P_2) + \gamma Q - e'Q + e'Q$
$(x_v, y_v) = U + \alpha(P_1+P_2) + \gamma Q$
$(x_v, y_v) = (r', y_R')$
$x_v = r'$

Fig 5: Credential Show Protocol

In the credential show protocol, if the verifier wants to verify that (Y_1', Y_2') is a valid signature he simply does the same verification that user does viz., x_v=r'? Values Y_1', Y_2', r' are sent to the verifier for verification. User must also prove that he knows a DL representation of f(β, x_1,x_2,…..x_l). The role of showing protocol is to convince the verifier that the user possesses a credential and also for the user to show some or none of the attributes but nevertheless β. The computations involved in verification are also shown in Fig 5.

6. FINDINGS AND DISCUSSIONS

Schnorr Blind Signature [8] [9] maintains the unlinkability between issue stage and show stage. Schnorr Blind Signature [9] based on ECC during credential issue stage has less number of rounds than Restrictive Blind Signature based on ECC. Thus there is a considerable improvement in the performance of the system. The storage requirement of our system in terms of bits is 1442 in total where 800 bits are for system parameters, 322 bits are for public key, and 320 are for private key. The performance of our system is measured in terms of 1024-bit modular multiplications. The Statistics show that 58 modular multiplications are needed during signature initialization, 203 and 58 during signing and verification respectively. Systems based on ECC can provide the same level of security that cryptographic techniques that use discrete logarithm can provide with reduced key size.

7. CONCLUSION

In this paper, we have shown that our system is much more efficient than Restrictive Blind Signature Based on ECC. The number of rounds between Signer and User is less in our system. Thus it has improved the overall performance of the system. The system also preserves randomness, unlinkability and unforgability.

As a part of our future work, we plan to increase the efficiency of underlying ECC by finding ways to increase the efficiency of finite field mathematics with research scholars from Department of Mathematics. We also plan to extend the same idea to restrictive partially blind signature scheme which combines both the Schnorr and Chaum-Pedersen signature schemes and compare the results.

8. REFERENCES

[1] Joseph H. Silverman, "The Arithmetic of Elliptic Curves", Graduate Texts of Mathematics, Vol. 106, Springer-Verlag 1986.

[2] Randhir Kumar, Akash Anil, "Implementation of Elliptical Curve Cryptography", International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011.

[3] W. Stallings, "Cryptography and Network Security principles and practice", Published by Prentice Hall, 2006.

[4] A. Glenn, I. Goldberg, F. Legare, A. Stiglic, "A Description of Protocols for Private Credentials", Published by Zero-Knowledge Systems Inc., 2001, pp.1-10.

[5] A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems", Selected Areas in Cryptography, H.Heys and C. Adams, Eds., Springer Verlag, 1999, vol. 1758, Lecture Notes in Computer Science, pp. 184-199.

[6] S. Brands, "Private Credentials", Published by Zero-Knowledge Systems Inc., 2000, pp.1- 25.

[7] Aditi Athavale, Kuldip Singh, Sandeep Sood, "Design of a Private Credentials Scheme Based on Elliptic Curve Cryptography", First International Conference on Computational Intelligence, Communication Systems and Networks, 2009.

[8] D. Chaum, "Blind signatures for untraceable payment", Advances in cryptology, CRYPTO'82, Lect. Notes Computer Science, Published by Springer-Verlag, 1998, pp. 199-203.

[9] M. Chang, I.Chen, I. Wu, Y. Yeh, "Schnorr Blind Signature Based on Elliptic Curves", Asian Journal of Information Technology, Published by Grace Publication Network, 2003, pp.130 -134.

[10] Fuh-Gwo Jeng, Tzer-Long Chen, Tzer-Shyong Chen, "An ECC-Based Blind Signature Scheme", Journal of Networks, Vol. 5 , August 2010.