

A Novel Secured Authentication Protocol for Mobile Banking

S. Prasanna^{1*} and M. Gobi²

¹Department of Computer Science and Applications, Prof Dhanapalan College of Arts and Science, Kelambakkam, Chennai - 603103, Tamil Nadu, India; sprasannaganesan@gmail.com

²Department of Computer Science, Chikkanna Government Arts College, Tiruppur - 641602, Tamil Nadu, India; mgobimail@yahoo.com

Abstract

Objective: In the modern era, smart phones and iPhones are the most dominating gadgets among human beings. The tremendous number of mobile users along with the omnipresent nature of mobile devices has created an immense market for mobile commerce. But, for that m-commerce to be recognized to 100%, users have to believe the security measures of m-commerce generally and m-payment especially. In other words, the growth of wireless networks and massive usage of mobile devices have increased the concerns about performance and security of mobile payment systems. The two critical and challenging features of any payment protocol are security and privacy. **Method:** This paper proposes a novel secured authentication protocol for mobile banking which would overcome the two critical features of any mobile payment transactions. This proposed protocol combines both asymmetric and symmetric key cryptographic techniques. **Findings:** Compared to few existing authentication protocols based on either ECC or RSA, the proposed authentication protocol over resource-constrained mobile devices serves better in terms of privacy, security and computation. **Novelty:** This paper proposes a novel secured authentication protocol which combines both asymmetric and symmetric key cryptographic techniques (HECC and AES).

Keywords: Authentication, ECC, HECC, Privacy, RSA, Security

1. Introduction

Now days, higher end mobile devices, such as smart phones, and iPhones are becoming the foremost gadgets among the end users. The immense number of mobile users along with the ever present nature of mobile devices has created a huge market for mobile commerce. It has been estimated that the market share of smartphone revenue has attained 85.1% between November 2013 and November 2014¹. But, for the market to be realized to 100%, users have to trust the security measures of m-commerce in general and m-payment in particular. Security and privacy are the two critical and challenging features of any payment protocol. One of the survey pointed out that nearly one third of survey respondents reported that using mobile was “somewhat riskier” than standard web commerce². Therefore, the main focus of this paper is to propose a novel secured authentication proto-

col for mobile devices through which any authenticated mobile user can do any mobile banking transactions in a secured manner. This proposed protocol combines both asymmetric and symmetric key cryptographic techniques. The rest of the paper is organized as follows: Section 2 describes the related work, the hyperelliptic curve cryptographic algorithm which is adopted in the proposed protocol is highlighted in the Section 3, Section 4 explains the proposed novel secured authentication protocol for mobile banking, the implementation results and analysis are shown in the Section 5 and finally Section 6 enlighten the conclusion of this paper.

2. Related Work

The advancement in technology have increased the necessity of m-commerce applications for business transactions,

*Author for correspondence

which resulted in need of mutual authentication protocol to ensure non-repudiation and confidentiality between involved parties. A mutual authentication protocol is necessary to resist the attacks when a malicious user pretends as an authorized one and attempt to duplicate, modify, insert or delete the data during transmission. Many researchers have contributed towards the design and development of the authentication protocols. Zuowen has proposed an enhanced and secured three-party encrypted key exchange protocol (3SPAKE) for mobile commerce environments³. A secured authentication protocol for mobile transactions without adopting public key cryptosystem is proposed by⁴. In⁵ have introduced m-identity in an m-commerce transaction, which includes both identities of a user and his/her bound mobile device. A hybrid authentication protocol based on elliptic curve cryptography is designed by⁶. In⁷ has developed an authentication protocol in mobile RFID environment which effectively achieves forward security with preventing replay, eavesdropping, and counterfeit tag attacks. In⁸ has proposed a real time authentication system for RFID applications. To ensure authentication, digital signature is also being used in the authentication protocol. Most of the authentication protocol adopt RSA algorithm for the encryption and decryption of either the secret key or the information to be transferred in its digital signature scheme. The familiar secured authentication protocols like Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) which are the most dominant protocols widely used in the e-commerce/m-commerce applications, are based on the RSA asymmetric key cryptographic technique only⁹. The security of RSA is based on the incapability to proficiently factor a large composite number. RSA will no longer be secured, if any such integer factoring algorithm is discovered¹⁰. Since the integer factoring algorithm is in RSA, an alternative asymmetric key algorithm can be adopted. So, this research paper is mainly focusing on designing a novel secured authentication protocol for mobile banking using hyperelliptic curve cryptographic technique.

3. Hyperelliptic Curve (HEC)

In this section, the hyperelliptic curve cryptographic technique which is used for securing mobile ID and symmetric key technique for transmitting the mobile banking transactions is described. HECC is a cryptographic technique based on hyperelliptic curves of genus 2, 3 and

so on. The following sub sections describe the overview of hyperelliptic curve and ElGamal based hyperelliptic curve cryptographic algorithms. Details about various mathematical operations which are performed on these hyperelliptic curves can be had from¹²⁻¹⁶.

3.1 Hyperelliptic Curve Cryptographic Algorithms

Discrete Logarithm Problem for the hyperelliptic curve cryptographic technique is described as follows:

“Let F_q be a finite field with q elements. Given 2 divisors, D_1 and D_2 in the Jacobian, determine $m \in Z$, such that $D_2 = mD_1$ ”.

The step by step procedures for ElGamal based hyperelliptic curve encryption and decryption algorithms are shown below¹⁷.

3.1.1 Encryption / Decryption Algorithms

To encrypt and send a message to receiver (R), Sender (S) accomplishes the following procedure.

- $r \in_r N$ (r - random positive prime number)
- $I \leftarrow [r]D$ (D - Divisor of the HEC & I is represented as $(u(x), v(x))$)
- $P_k \leftarrow [r]P_R$ (P_R : $(u(x), v(x))$ is receiver's (R's) public key)
- $C_m \leftarrow \{ I, E_m + P_k \}$ (C_m - Cipher Text to be sent)

The decryption algorithm works as follows: To decrypt C_m , R extracts 'I' from C_m then multiply with (a_B) and subtract the result from the second coordinate. This can be written as follows,

$$Em + rPR - aR (I) = Em + rPR - aR (rD) = Em + kPR - r(aR D) = Em + rPR - rPR = Em$$

In the above process, 'S' has masked the message E_m by adding rP_R to it. Except 'S', the content of r is not known to anyone. Even though P_R is a public key, the mask rP_R can not be identified by anyone except S. If any attacker wants to confiscate/modify message, the attacker would have to identify k from the given D and $[r]D$ i.e., I , which is assumed very hard.

4. Proposed Secured Authentication Protocol for Mobile Banking

Figure 1 shows the proposed novel secured authentication protocol for mobile banking. This proposed protocol

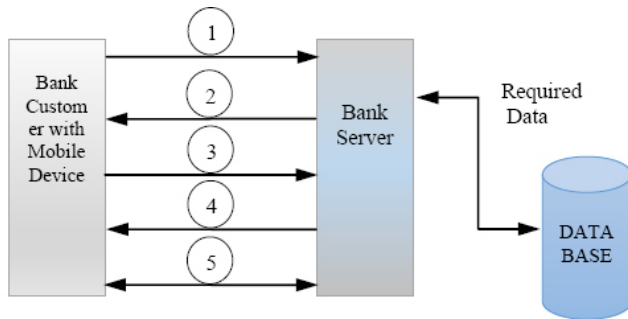


Figure 1. Novel secured authentication protocol for mobile banking.

ensures the secured authentication for the mobile banking as follows:

In step 1, the authentication process is initiated by the bank customer with his mobile device by sending his mobile's Serial Number (SN) to the bank server. In step 2, the bank server stores the mobile's SN for the purpose of authentication and generates the mobile's private key and public key using genus 2 hyperelliptic curve cryptography over prime field F_p . The private and public key of the mobile along with the public key of the bank server are delivered to the respective bank customer's mobile. A secured key exchange protocol can be used for sending the key to the respective destination. In step 3, the customer's mobile creates a challenge and transmits the encrypted version of the challenge and its SN to the bank server using the combination of the bank server's public key and the mobile's private key. The bank server decrypts the message with mobile's public key and private key and checks if this SN matches the SN sent in Step 1. This authenticates the mobile client. In Step 4, the bank server sends a randomly generated session key and the encrypted version of the challenge received in the previous step to the mobile using the combination of mobile's public key and bank server's private key. The respective bank customer's mobile then decrypts this message with server's public key and its private key and verifies the challenge. If it matches the one that was sent in Step 3, then the mobile can trust that it is communicating to the right bank server. The genus 2 hyperelliptic curve cryptography over finite field is used for both encryption and decryption process specified in Step 3 and 4. Now onwards, in Step 5, mobile client and the bank server can be communicated using a secure channel and all mobile payment data is encrypted with a session key using any standard symmetric key algorithm. Note that a new key

is setup for each mobile payment transmission to prevent replay attack.

5. Implementation Results and Analysis

The proposed secured authentication protocol is implemented using Sun Java Wireless Toolkit 2.5.2, Apache Tomcat Server 6.0 and SQL Server 2000. The details of the Sun Java Wireless Toolkit can be had from¹⁸. The Table 1 shows the comparative analysis of key generation, sign generation and sign verification processes performed by RSA, ECC and HECC respectively.

From Table 1, it is realized that the secured authentication protocol which is designed using HECC performs better than ECC and RSA in terms of key generation, sign generation and sign verification processes. Moreover, it is proven that 80 bit key size for HECC is enough to achieve the same level of security instead of by 160 bit key size for ECC and by 1024 bit key size for RSA^{12,14,15}. Through this secured authentication protocol, confidentiality is ensured by the following ways:

- Secured authentication process by encrypting the mobile ID and the challenge generated by the mobile user (Step 3 in Figure 1) and by encrypting the challenge received by the server and the session key generated by the server (Step 4 in Figure 1).
- By creating a secure channel between two parties after successful completion of authentication process and all mobile payment data is encrypted by the session key using any symmetric key algorithm like AES.

5.1 Security Analysis

In this section, the security of the proposed secured authentication protocol using HECC is discussed. This proposed

Table 1. Comparative analysis of key generation, sign generation, and sign verification processes

Public-key cryptographic techniques	Key Length (bits)	Key Generation (Time in Milli.Sec.)	Sign Generation (Time in Milli.Sec.)	Sign Verification (Time in Milli.Sec.)
RSA	512	160000	4500	600
ECC	160	131000	4000	500
HECC	80	115000	3500	400

protocol will be considered to be secured authentication protocol, if it satisfies the following properties.

5.1.1 Replay attack

Replay attack means capturing the data in passive manner and its consequent retransmission to ensure unauthorized effect. This proposed protocol protects replay attack as it depends upon new key values. In this protocol, after completion of each mobile payment transmission session between authenticated parties, a new session key will be generated for another mobile payment session, so that replay attack is not possible.

5.1.2 Man in the Middle Attack

This attack is an active attack. In this protocol, no sensitive information about the secret key is known to others during the secured authentication process. If an attacker W intercepts the message packet containing $(I, E_m + P_k)$, W then receives $E_m + P_k$ and I from S . However, this means that W must calculate 'r' to break $E_m + P_k$ but W cannot compute the value of 'r'. This problem is called Discrete Logarithm Problem (DLP). So, W will not be able to compute 'r'. Thus this protocol avoids man-in-the-middle attack.

5.1.3 Small Subgroup Attack

Through Chinese remaindering algorithm, intruder could easily identify the secret scalar modulo of all the primes and compute large part of secret if curve H has adequate prime factors. For observing this, first see that $[l]D = 0$ and computing $[h]D$ for $h = c/pi$, for all prime divisors pi of c and checking that the result is not 0^{19} .

5.1.4 Known Key Attack

In this proposed protocol, both users generate new 'r' value in every encryption process, and also, the secret key is generated with every new session. Further important aspect of this protocol is that the 'r' value is computed independently on both sides. Thus the proposed protocol is secured against known key attacks, provided that the hyperelliptic curve discrete logarithm problem is intractable.

6. Conclusion

This proposed protocol using hyperelliptic curve cryptographic technique is well suited for secured

authentication protocol for mobile banking as the key size used in HECC (genus 2) is smaller than the key size used in ECC and RSA. As HECC (genus 2) of 80-bit operand lengths provide same security level with ECC of 160-bit, in our view, HECC is more suitable for implementing the proposed secured authentication protocol over resource constrained platforms. It is seen that the proposed secured authentication protocol using HECC is efficient as the timings of key generation, signature generation/verification compares favorably with the timings of ECC and RSA. Moreover, the proposed protocol guaranteed confidentiality and security which are the critical and key challenging features of any payment protocol. Finally, the proposed protocol is secured from the replay attack, man in the middle attack, sub group attack and known key attack.

7. References

1. Available from: http://share.brandingbrand.com/Branding-Brand_Mobile-Commerce-Index_November-2014.pdf
2. Available from: <http://www.pymnts.com/in-depth/2014/merchants-mobile-commerce-is-riskier-than-ecommerce/Mobile-Payments-and-Fraud-Survey-2014>
3. Tan Z. An enhanced three-party authentication key exchange protocol for mobile commerce environments. *Journal of Communications*. 2010 May; 5(5).
4. Lee J-S, Chang Y-F, Chang C-C. Secure authentication protocols for mobile commerce transactions. *International Journal of Innovative Computing, Information and Control*. 2008 Sep; 4(9).
5. Han F, van Schyndel R, M-identity and its authentication protocol for secure mobile commerce applications. *Cyberspace Safety and Security. Lecture Notes in Computer Science*. 2012; 7672:1-10.
6. Bensari M, Bilami A. A new hybrid authentication protocol to secure data communications in mobile networks. *Modeling Approaches and Algorithms for Advanced Computer Applications Studies in Computational Intelligence*. 2013; 488:195-204.
7. Sandhya M, Rangaswamy TR. A forward secured authentication protocol for mobile RFID systems. *International Journal of Information Technology and Knowledge Management*. 2011 Jul-Dec; 4(2):549-53.
8. Kumari S. Real time authentication system for RFID applications. *Indian Journal of Science and Technology*. 2014 Mar; 7(S3).
9. Shedid SM, Kout M. Modified SET protocol for mobile payment: An empirical analysis. *IEEE 2nd International Conference on Software Technology and Engineering (ICSTE)*; San Juan, PR. 2010 Oct 3-5. p. 350-5.

10. Ambedkar BR, Bedi SS. A new factorization method to factorize rsa public key encryption. IJCSI. 2011 Nov; 8(6).
11. Menezes AJ, Wu YH, Zuccherato RJ. An elementary introduction to hyper elliptic curves. Technical Report CORR 96-19, Ontario, Canada: University of Waterloo; 1996 Nov.
12. Duquesne S, Lange T. Arithmetic of Hyper elliptic curves. Handbook of Elliptic and Hyper Elliptic Curve Cryptography. Cohen H, Frey G, editors. Florida: Chapman and Hall/CRC, Taylor and Francis Group; 2006.
13. Fan X, Gong G. Efficient explicit formulae for genus 2 hyperelliptic curves over prime fields and their implementations. Waterloo, Ontario, Canada: Department of Electrical and Computer Engineering, University of Waterloo. Available from: www.cacr.math.uwaterloo.ca/techreports/2007/cacr2007-01.pdf
14. Ganesan R, Vivekanandan K. Performance analysis of hyperelliptic curve cryptosystems over finite field \mathbb{F}_p for genus 2 and 4. IJCSNS. 2008 Dec; 8(12):415–8. ISSN: 1738-7906.
15. Ganesan R, Gobi M, Vivekanandan. Elliptic and hyperelliptic curve cryptography over finite field \mathbb{F}_p , i-Manager's. Journal on Software Engineering. 2008 Oct-Dec; 3(2):43–8. ISSN: 0973-5151.
16. Lange T. Efficient arithmetic on genus 2 hyper-elliptic curves over finite fields via explicit formulae. Cryptology ePrint Archive: Report 2002/121; 2002.
17. Ganesan R, Gobi M, Vivekanandan K. A novel digital envelope approach for a secure e-commerce channel. International Journal of Network Security. 2010; 11(3):121–7.
18. Available from: <http://www.oracle.com/technetwork/java/download-135801.html>
19. Cohen H, Frey G. Handbook of elliptic and hyperelliptic curve cryptography. Chapman and Hall/CRC Press; 2006.