DOI: 10.21917/ijct.2014.0129

PERFORMANCE ANALYSIS OF DISTINCT SECURED AUTHENTICATION PROTOCOLS USED IN THE RESOURCE CONSTRAINED PLATFORM

S. Prasanna[1] and M. Gobi[2]
[1]*School of Computer Science and Information Technology, Dr. GRD College of Science, India*
E-mail: prasannaraog@yahoo.co.in
[2]*Department of Computer Science, Chikkanna Government Arts College, India*
E-mail: mgobimail@yahoo.com

Abstract
Most of the e-commerce and m-commerce applications in the current e-business world, has adopted asymmetric key cryptography technique in their authentication protocol to provide an efficient authentication of the involved parties. This paper exhibits the performance analysis of distinct authentication protocol which implements the public key cryptography like RSA, ECC and HECC. The comparison is made based on key generation, sign generation and sign verification processes. The results prove that the performance achieved through HECC based authentication protocol is better than the ECC- and RSA based authentication protocols.

Keywords:
Authentication, Asymmetric Key Cryptography, RSA, ECC, HECC, Sign Generation, Sign Verification, Key Generation

1. INTRODUCTION

The significant growth of communication technologies and the massive usage of the Internet have contributed to the development and blooming of m-commerce. On the other hand, now a day, we have seen a huge demand for mobile devices. This seeks for resource constrained platforms have guided to the appearance of smart phones and iphones. Moreover, the needs for migration of e-commerce applications from the conventional desktop to these resource constrained platforms are become mandatory. For example, one might think of buying/selling products through smart phone or browsing pay-per-view news on iPhone, while waiting on the bus stop.

However, being the internet, an open and insecure network, some anxiety has been raised in transmitting sensitive information. The solution lies in using cryptography and secures authentication protocols that guarantee the confidentiality, authentication and integrity of communications [4]. Such protocols, like SSL [13] and SET [12], already exist and are widely used in current e-commerce applications. Most of them are based on RSA public key cryptography. Alternate, two distinct protocols are developed which is exclusively based on Elliptic curve cryptography (ECC) and Hyper-elliptic curve cryptography (HECC), an asymmetric cryptography that performs well in resource constrained platforms and maintain the high security level that one can achieve with the protocols in use today [9][10]. The efficiency and effectiveness of ECC-based direct and indirect authentication protocols are analyzed by Thilagavathi and Rajeswari and they concluded that depends on the application and the environment, the protocol could be utilized to make a secure environment in mobile networks [14]. Fengling Han and Ron van Schyndel proposed an m-identity authentication (MA) protocol based on mobile user's biometric features. M-identity merges mobile device identity into biometrics images [11].

The paper is organized as follows. Section 2 describes the general aspect of the different protocols. In section 3, the implementation and performance analysis of the protocols in J2ME wireless toolkit is provided. Finally, section 4 presents the conclusion.

2. ARCHITECTURE

The authentication protocol must be able to create a secure communication channel between two parties on top of an insecure network, like the internet. It's not difficult to eavesdrop a line or to compromise a router and be able to listen / alter all messages in transit [1]. In order to prevent this, the protocol must ensure the mutual authentication of both parties and the confidentiality and integrity of all the data transmitted through it. Such protocols already exist and have gone through deep analysis, like SSL [13] and TLS [15]. However, they rely heavily on RSA asymmetric cryptography, which causes some anxiety about their performance on resource constrained small devices. In fact, some performance measurement is done for cryptographic functions on one of these devices, the Palm III from 3Com which is shown in the Table.1 [8].

From the Table.1, it is clear that generating RSA keys on the Palm III Pilot is prohibitively expensive and time consuming process. Moreover, RSA signature generation is also very slow and RSA itself is vulnerable [7], which shows a protocol like SSL to become unfeasible. Conversely, different efficient authentication protocols for resource constrained platform have been proposed and implemented [9][10]. Generally, the security level provided by the HECC using 80 bit key size is equivalent to ECC's 160 bit which in turn equivalent to RSA's 1024 bit [2][3][6]. Also, the performance of the digital envelope implemented using HECC is better than the digital envelope implemented using ECC [5], which lead to a simple conclusion: the authentication protocol for resource constrained platforms must be based solely on ECC and HECC separately. The following Fig.1 depicts the general asymmetric authentication protocol over the internet which can be employed using RSA/ECC/HECC.

The idea behind this protocol is simple: in step 1, the mobile starts the protocol by sending its ID (e.g. Serial Number) to the server. In step 2, the server stores the mobile's ID for authentication purpose and generates mobile's private key and public key using any one of the asymmetric cryptographic techniques (RSA/ECC/HECC). These keys (private and public key of the mobile) along with the public

key of the server are sent to the mobile. Notice that the keys travel from the server into the mobile through a secure channel. To send the key to the respective destination, one can even adopt Diffie-Hellman key exchange algorithm. In step 3, the mobile generates a challenge and sends it along with its ID to the server, encrypted with a combination of the server's public key and the mobile's private key.

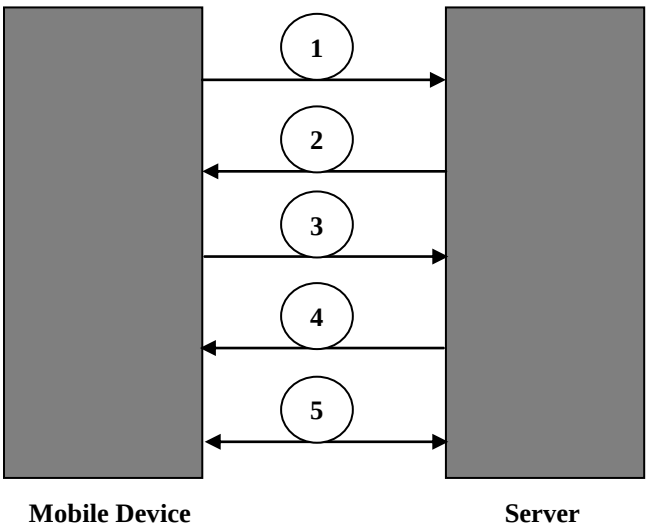

Fig.1. Asymmetric Authentication Protocol over the Internet

The server decrypts the message with mobile's public key and its private key and verifies if this ID matches the ID sent in step 1. This authenticates the client. In step 4, the server sends the challenge received in the previous step plus one and a randomly generated session key and encrypted with a combination of mobile's public key and server's private key. The 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's indeed talking to the right server. Both encryption and decryption process, specified in step 3 and 4 are done using any one of the cryptographic techniques (RSA/ECC/HECC). From now on, in step 5, a secure channel has been created and all data is encrypted with a session key. Notice that a new key is setup for each message to prevent replay attacks.

3. IMPLEMENTATION

The secured authentication protocol using RSA algorithm was implemented in Palm III [8] and the other two secured authentication protocols using ECC and HECC were implemented in J2ME Wireless Toolkit 2.5.1 [9][10]. The details of the Sun Java Wireless Toolkit 2.5.1 can be had from [16] and the toolkit can be downloaded from [17]. With the growing diversity of mobile devices to which the protocol targeted for, its portability was a major concern since the beginning. Therefore it was developed using the J2ME, whose features meet this requirement.

To achieve the high security level required, the ElGamal based Elliptic curve cryptography and Hyper-elliptic curve cryptography, and also MD5 algorithms, were used for the encryption, decryption and digest calculation of the messages exchanged in this protocol. Table.1 shows the performance measurement for the different asymmetric key cryptographic techniques. Fig.2 depicts the pictorial representation of the performance analysis of the key generation, sign generation and sign verification processes by the RSA, ECC and HECC used in the secured authentication protocols.

Table.1. Performance measurement for the different asymmetric 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	165000	5000	640
ECC	160	133000	4200	580
HECC	80	120000	3700	520

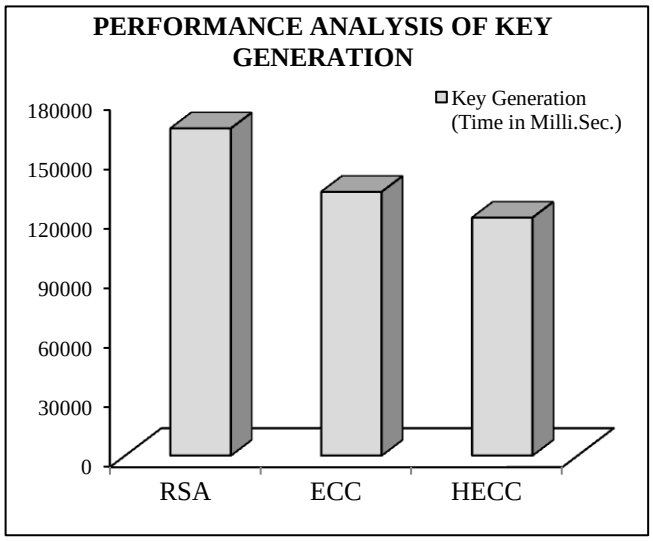

Fig. 2(a)

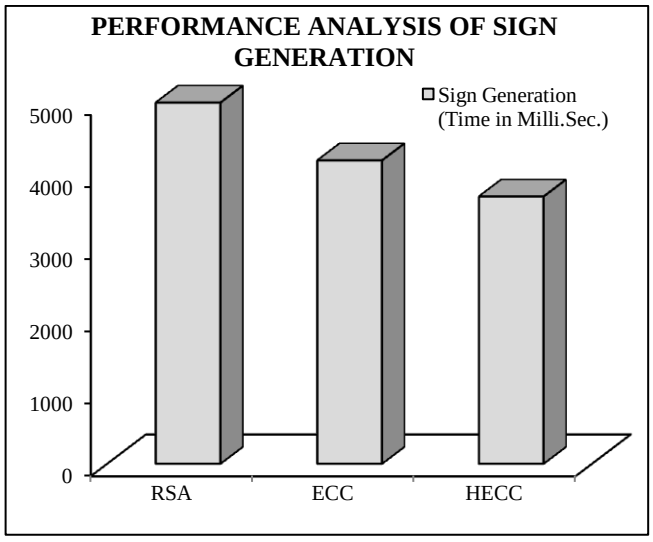

Fig. 2(b)

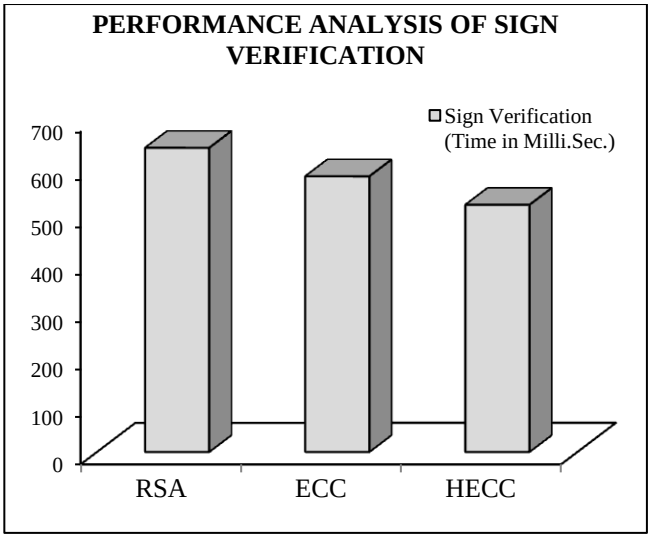

Fig. 2(c)

Fig.2. Performance analysis of the key generation, sign generation and sign verification processes by the RSA, ECC and HECC

From Fig.2, it is clear that the secured authentication protocol using HECC serves better than ECC and RSA in terms of key generation, sign generation and sign verification processes. Moreover, it is already proven that the security level provided by the HECC using 80 bit key size is equivalent to ECC's 160 bit which in turn equivalent to RSA's 1024 bit [2][3][6]. Finally, due to confines in mobile device's computing power, its memory capacity and key sizes used in the algorithm, the secured authentication protocol implemented using HECC algorithm is more appropriate authentication protocol to the resource constrained platforms other than RSA and ECC.

4. CONCLUSION

This analysis shows that it is possible to implement distinct secured authentication protocols using different asymmetric key cryptographic techniques (RSA/ECC/HEC) in resource constrained platforms. This paper concludes that the performance of HECC based secured authentication protocol serves better than RSA and ECC based protocol. Hope this analysis to be a big contribution to the development and widespread acceptance of secured authentication protocol based on HECC in m-commerce.

REFERENCES

[1] CERT Advisory CA-95.01. - IP Spoofing Attacks and Hijacked Terminal Connections,

[2] Xinxin Fan and Guang Gong, "Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations", *14th International Workshop on Selected Areas in Cryptography, Lecture Notes in Computer Science*, Vo1. 4876, pp. 155-172, 2007.

[3] R. Ganesan and K. Vivekanandan, "Performance Analysis of Hyperelliptic Curve Cryptosystems over Finite Field F_p for Genus 2 and 4", *International Journal of Computer Science and Network Security*, Vol. 8, No. 12, pp 415-418, 2008.

[4] R. Ganesan, M. Gobi and V.S. Janakiraman, "Implementation of MD5 Integrity Checking Mechanism for M-Commerce Transactions", *International Journal of Computer Science and Applications*, Vol.1, No.3, pp.194 - 196, 2008.

[5] R. Ganesan, M. Gobi and K. Vivekanandan, "A Novel digital envelope approach for a secure e-commerce channel", *International Journal of Network Security*, Vol. 11, No. 3, pp. 121-127, 2010.

[6] R. Ganesan, M. Gobi and K. Vivekanandan, "Elliptic and Hyperelliptic Curve Cryptography Over Finite Field F_p", *i-Manager's Journal on Software Engineering*, Vol. 3, No. 2, pp. 43-48, 2008.

[7] Imad Khaled Salah, Abdullah Darwish and Saleh Oqeili, "Mathematical attacks on RSA cryptosystem", *Journal of Computer Science*, Vol. 2, No. 8, pp. 665-671, 2006.

[8] Neil Daswany and Dan Boneh, "Experimenting with Electronic Commerce on the PalmPilot", *Proceedings of third International Conference on Financial Cryptography, Lecture Notes in computer Science*, pp. 1-16, 1998.

[9] S. Prasanna, "An Authentication Protocol for Mobile Devices Using Hyperelliptic Curve Cryptography", *ACEEE International Journal on Network Security*, Vol. 2, No. 1, pp. 8-10, 2011.

[10] S. Prasanna, "An Efficient Protocol for Resource Constrained Platforms Using ECC", *International Journal on Computer Science and Engineering*, Vol. 2, No. 1, pp. 89-91, 2009.

[11] Ron van Schyndel and Fengling Han, "M-Identity and Its Authentication Protocol for Secure Mobile Commerce Applications", *Cyberspace Safety and Security, Lecture Notes in Computer Science*, Vol. 7672, pp. 1-10, 2012.

[12] The SET Standard Specification; http://www.setco.org/set_specifications.html. 1999.

[13] O. Alan, Philip Karlton and Paul C. Kocher, "The SSL Protocol Version 3.0(Internet Draft)", Netscape Communications, 1996.

[14] K. Thilagavathi and P.G. Rajeswari, "Efficiency and Effectiveness Analysis over ECC-Based Direct and Indirect Authentication Protocols: An Extensive Comparative Study", *ICTACT Journal on Communication Technology*, Vol. 3, No. 1, pp. 515-524, 2012.

[15] Tim Dierks, "The TLS Protocol Version 1.0(Internet-Draft)", Transport Layer Security Working Group, pp. 1-69, 1997.

[16] http://java.sun.com/javame/reference/apis.jsp

[17] http://java.sun.com/products/sjwtoolkit/download-2_5_1.html