Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

A Survey on Encryption Algorithms and Protocols in Smart Card for User Centric Ownership Model

Harsha B R
MTech CNE
Dept. of Computer Science
R.V.C.E Bangalore

Dr. N.K. Srinath
Prof. and Dean
Dept. of Computer Science
R.V.C.E Bangalore

Abstract— User Centric Ownership Model (UCOM) enables the smart card users to install/delete application they prefer in their smart card. UCOM provides smart card users to have any number of applications installed on their smart cards. Though UCOM provides flexibility for the smart card users, it lacks centralized authority. UCOM creates major problem if the user has more than one application installed in his/her smart card. Smart card may contain applications from the provider that may interrupt the proper working of the neighbor applications. Smart card user may hack his way to a known aboutapplication through a smart card simulator. Thus, there is no security for an application in the smart card for UCOM model. This survey paper includes background and motivation about the available encryption algorithms for smart cards such as RSA, ECC, AES, DES, T-DES, ECDSA and the smart card protocols which can be used to overcome the problem of security for the applications in smart card for UCOM model.

KEYWORDS— UCOM, RSA, ECC, AES, DES, T-DES, ECDSA, SMART CARD PROTOCOLS

I. INTRODUCTION

Smart card with multiple applications enables application form different application provider to co-exist in the single smart card [1]. Issuer Centric Ownership Model (ICOM) refers to control and ownership of the smart card by the card issuer (single application per smart card). User Centric Ownership Model (UCOM) refers to the control and ownership of the smart card delegated to the smart card user which supports multiple application to be installed on a smart card [2]. The security of a smart card in UCOM is not guaranteed as the control lies with the smart card user who can be a trustable user or a malicious user. User Centric Smart Card Framework (UCF) gives a secure relationship among the entities involved in UCOM in order to support delegation of the ownership to smart card user [2].

Smart card is known to be a secure computing device [1]. The most challenging aspect in smart card communication is to provide security for the smart card applications. Security in case of Issuer Centric Ownership model is managed by a centralized authority. But this concept of centralized authority never exists in UCOM. It is this reason which gives way for reliable and efficient cryptographic algorithms [1] and secure channel protocols for multi-application smart cards [4]. Smart card in general may be any chip which is capable of executing and storing application securely [2] examples of which include Universal Integrated Circuit Card, Embedded Secure element, Secure Memory Card [5, 6] used in NFC [7] enabled mobile phones.

In this paper, section two deals with the discussion on all available encryption algorithms which can be used in the smart card communication to make it secure one. It also includes the discussion among RSA-ECC, RSA Digital Signature Algorithm-ECC Digital Signature Algorithm, DES,T-DES and AES with respect to their execution time, encryption time, decryption time, signature generation and signature verification. Section three deals with the need of the secure channel protocol in smart card communication, the design requirement of the protocol and the list of all available secure channel protocols.

II. ENCRYPTION ALGORITHMS

The algorithms developed over years to solve cryptographic applications is time exponential [8, 9] and is based on integer factorization [10]. If security is the need for smart card, then cryptography will remain the best solution [10]. It's this encryption which makes smart card secure from cryptanalysis. Using cryptography to provide security in constrained environment (Example: smart card) where there is issue with the bandwidth, computation and memory remains the major challenge [10]. Confidentiality, Data Integrity, Authentication and Non-repudiation are the main objectives of cryptography in smart card. "Long term key in cryptographic algorithms always promises the security"[11]. The most important progress in the cryptography system forsmart card is the introduction of electronic signature.

Encryption algorithms in smart card can be classified as

1. Public Key
2. Private Key
3. Hash Function

Public Key Algorithms can be further classified as Asymmetric (RSA and ECC) and Digital Signatures (RSA Digital and ECDSA). Private Key or Symmetric algorithms include AES, DES and T-DES. Hash Functions include SHA-1 and SHA-2.

a) Asymmetric Algorithms- RSA, ECC

Zhang Peng and Jia Jian Fang in 2010 gave the comparison of RSA and ECC public key cryptosystems based on their key sizes with respect to the corresponding security level [12]. Table 1 follows the comparison made by Zhang Peng and Jia Jian Fang. In the comparison, initial key size for RSA is considered to be 1024 bits. This is because RSA is believed to provide high security for key size more than 1024 bits. It can be observed from the table that, the key sizes that RSA uses for the corresponding security level is very high when compared to that of ECC. Thus, the computational power, memory and bandwidth required in case of RSA implementation in smart card is more when compared to ECC implementation. ECC compensates for the limitations in smart card hardware as it doesn't require any additional hardware [10]. Since the key generated in ECC is very short, faster information transfer rate can be achieved.

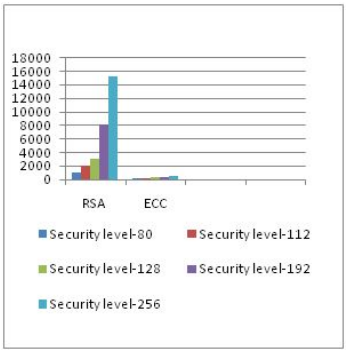

Figure 1 Key Size comparison for RSA and ECC

b) Digital Signature Algorithms- RSA, ECDSA

Digital Signature process includes signature generation and signature verification [13]. The comparison of Encryption in ECC and RSA made by Abdurahmonov Tursun in 2010 can be put forth as in Figure 2 and Figure 3 [14]. From Figure 2 and Figure 3 it can be observed that, ECC takes less time for encryption whereas RSA takes less time in decryption. Signature generation is fast in ECC whereas signature verification is fast in RSA.

Table 1 shows the results of RSA and ECDSA signature comparison made by Robshaw and Yin in 1997 in RSA laboratory [14]. Table 2 shows the results of RSAand ECDSA signature comparison made by Weiner [14]. Table 3 shows the results of RSA and ECDSA signature comparison made by V.Gupta, S.Gupta and D.Stebila [14]. T. Abdurahmonov and Helmi Mohammed Hussain after comparing RSA and ECDSA digital signature suggested that, ECDSA is more efficient Digital Signature Algorithm to be used in smart card [15].

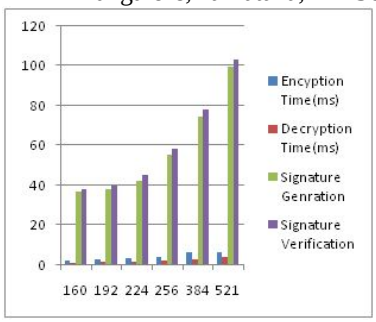

Figure 2 ECC Computation

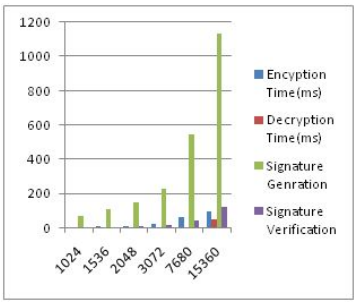

Figure 3 RSA Computation

Table 1 Comparison of Signature Generation and Verification

Public Key Algorithm	Key-size	Signature Generation	Signature Verification
RSA	1024	7 times Slow	6 times Fast
ECDSA	160	Fast	Slow

Table 2 Comparison of Signature Generation and Verification

Public Key Algorithm	Key-size	Signature Generation	Signature Verification
RSA	1024	8 times Slow	30 times Fast
ECDSA	168	Fast	Slow

Table 3 Comparison of Signature Generation and Verification

Public Key Algorithm	Key-size	Signature Generation	Signature Verification
RSA	1024	5 times Slow	8 times Fast
ECDSA	163	Fast	Slow

c) Symmetric Algorithms- DES, T-DES, AES

The comparison among the symmetric algorithms can be done as follows

i. An advantage of AES is that it is difficult to attack when compared to DES / T-DES. But it's slower in computation than DES / T-DES
ii. DES is easy to attack than T-DES / AES. DES is simpler than AES and faster than T-DES
iii. T-DES overcomes all the problems of DES and makes the process secure against hacking. T-DES computation is slower than DES.

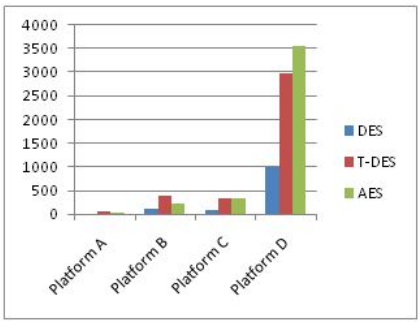

Figure 4 Execution Time Comparisons for Symmetric algorithms

Figure 4 gives the comparison of execution time of DES, T-DES and AES in seconds on different platforms [14] and modes (ECB- Electronic Code Book, CFB- Cipher feedback).
Platform A – ECB mode on P-II 266 MHZ machine
Platform B – ECB mode on P-4 2.4 GHZ machine
Platform C–CFB mode on PENTIUM-IL266 MHZ machine
Platform D – CFB mode on P-4 2.4 GHZ machine [14]

III.SMART CARD PROTOCOLS

Protocol may be defined as the set of rules that govern the communication between the communicating entities. GlobalPlatform (now OpenPlatform) card specification [16] provides necessary functionality such as secure storage of keys, key management and so on which are essential for a smart card protocol. GlobalPlatform architecture is been coupled with Java card [17] technology to provide portability to other smart card platforms [18, 19]. Smart card communication can be secured by authenticating the communicating entities (card and the off-card entity) and establishing session keys to preserve the integrity and confidentiality of the communication. Public key cryptography is used to establish a secure channel. Cryptographic protocols designed for smart cards must consider the limitations of the smart card. If protocols designed follow large number of messages to be exchanged between the communication entities, this will in turn results in communication and processing overheads [20].

UCOM provides the flexibility to have multiple applications being installed in the smart card. Secure channel can be used by the application provider to lease the application to the smart card user in UCOM and also during the entity authentication or key exchange between the communicating entities. The application provider leases the application based on the Application Lease Policy (ALP) [21]. The multiple applications may need to communicate with the off-card entity simultaneously. This communication can be provided by establishing logical channels (as in Figure 5) between an application and off-card entity which is specific to one application only. As per the Global Platform Card specification, the maximum number of logical channels allowed is 4, ie at any instance only 4 applications can communicate with the off-card entity. Security to such logical channel communication is ensured through Secure Channel Protocol [22].

Every Logical Channel communication [22, 23] provides an illusion as if the communication happens with a separate smart card. GlobalPlatform security domains are the on-card representatives of the card issuer or an application provider in the UCOM [24].Secure channel protocols are established in order to communicate with the off-card entity in secure manner. Every security domain is associated with a secure channel protocol (SCP) (as in Figure 6).

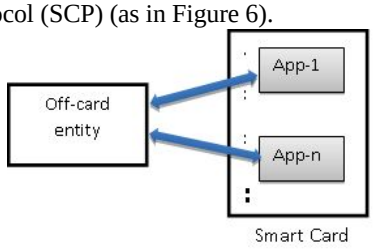

Figure 5 Logical Channel Communication

Whenever an application uses the security domain for the communication with the off-card entity, it uses the secure channel protocol for the communication. Secure Channel Protocol [24] ensures security for the communication between the on-card entity (Issuer Security Domain/Application Security Domain) and off-card entity through the corresponding logical channel. Secure channel protocol are used in situation when there is need for card content management.

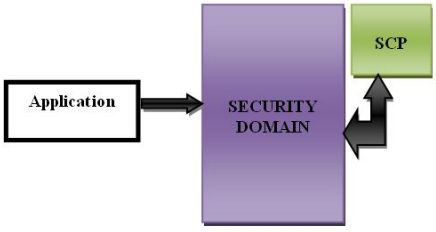

Figure 6 Security Domain and Secure Channel Protocol (SCP)

Secure Channel is a trusted channel which is cryptographically bounded to the current communicating states of the two

communicating entities [25]. A secure channel protocol (SCP) should address the following requirement,

i. SCP should assure that the service provider is communicating with a genuine smart card platform and not the simulator [26]
ii. SCP must ensure that the smart card security and operational environment is certified by a reputed third party evaluation [26]

Following are the list of currently available Secure (trusted) Channel Protocols,

i. Station to Station (STS) protocol [27]
ii. Aziz-Siffie (AD) protocol [28]
iii. ASPeCT protocol [29]
iv. Just Fast Keying (JSF) protocol [30]
v. Trusted TLS protocol (T2LS) [25]
vi. GlobalPlatform
    a. SCP01 [31] – deprecated
    b. SCP02 [31] – based on T-DES
    c. SCP10 [31] – based on Asymmetric key cryptosystem
    d. SCP81 [32] – based on SSL/TLS
    e. SCP80 [33] – for mobile telecom industry
vii. Markantonakis-Mayes (MM) protocol [34]
viii. Sirett-Mayes (SM) protocol [35]
ix. Preserving Secure and Trusted Channel Protocol (P-SCTP) [36]
x. Secure and Trusted Channel Protocol (SCTP) [26]

IV.CONCLUSION

a) Conclusion on Encryption Algorithms

ECC algorithm is more efficient and well suitable for smart card which has constrained environment. This is because, ECC key size is very less when compared to that of RSA which makes ECC faster in computation and well suitable for smart card which has limitation in memory, bandwidth and computation power. In some situation RSA algorithm is used in smart card and not ECC. This is when the key size used for the RSA is very small for which same level of security is provided by ECC algorithm even.

b) Conclusion on Digital Signature Algorithms

In conclusion to the comparison made between RSA and ECDSA digital signature algorithm in section two of this paper, even though RSA is faster than ECDSA in signature verification, ECDSA is considered the efficient digital signature algorithm for smart cards because of the negligible difference in situations where RSA is faster than ECDSA.

c) Conclusion on Symmetric Algorithms

AES has more advantages over DES / T-DES. Choosing a symmetric algorithm for encryption solely depends on the requirement of the system. If security is more concerned than speed, then AES is the right choice, if speed is more concerned than security, then DES / T-DES is the right choice.

d) Conclusion on Secure Channel Protocols

This paper aims at demonstrating the importance of Secure Channel Protocol in smart card communication especially in UCOM where there is more chances of tampering smart card application or the keys exchanged between the two communicating entities in the smart card communication.

V.FUTURE WORK

In this paper, we did the survey on the available encryption algorithms and protocols for smart card which would help the smart card to perform secure communication in User Centric Ownership Model (UCOM). This survey can be a motivation and helpful for making the smart card communication more secure and efficient tamper resistant device.

REFERENCES

[1] "Smart Card Operating Systems: Past, Present and Future," in the 5th NORDU/USENIX Conference, 2003.
[2] Akram, Raja Naeem, Konstantinos Markantonakis, and Keith Mayes. "A Paradigm Shift in Smart Card Ownership Model." In Computational Science and Its Applications (ICCSA), 2010 International Conference on, pp. 191-200. IEEE, 2010.
[3] "Mobile NFC Services," GSM Association, White Paper Version 1.0, 2007. [Online]. Available: http://www.gsmworld.com/documents/nfc_ services_0207.pdf
[4] Markantonakis, Konstantinos, and Keith Mayes. "A Secure Channel protocol for multi-application smart cards based on public key cryptography." InCommunications and Multimedia Security, pp. 79-95. Springer US, 2005.
[5] "The GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging," GlobalPlatform, White Paper, April 2009. [Online]. Available: http://www.globalplatform.org/documents/GlobalPlatform_NFC_Mobile_White_Paper.pdf
[6] "Contactless and Flash Memory Cards Combine," Card Technology Today, vol. 16, no. 11-12, pp. 6 – 7, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/B6W6X-4DTSP0M-C/2/0a2637d89dbed6d40be388ff9b37945b
[7] "Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications," White Paper, November 2006. [Online] Available: www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf
[8] Alfred J. Menezes, "Elliptic curve public key cryptosystem", Auburn University, Kluwer AcademicPublishers, Dordrech, London, 1993.

[9] V. Miller, "Uses of Elliptic Curve in Cryptography", Advances in Cryptography, Proceedings of Crypto'85, Lecture Notes on Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.

[10] Jena, Debasish, Saroj Kumar Panigrahy, Pradip Kumar Biswal, and Sanjay Kumar Jena. "A novel protocol for smart card using ECDLP." In Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on, pp. 838-843. IEEE, 2008.

[11] Rankl, Wolfgang, and Wolfgang Effing. Smart card handbook. John Wiley & Sons, 2010.

[12] Peng, Zhang, and Jia Jian Fang. "Comparing and implementation of public key cryptography algorithms on smart card." In Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 12, pp. V12-508. IEEE, 2010.

[13] T. Abdurahmonov, Y. E Thiam, M. H. Helmi, "Improving smart card security using Elliptic Curve Cryptography over prime field," IEEE Xplore. January 28, 2011, Pp.169-173

[14] Savari, Maryam, and Mohammad Montazerolzohour. "All about encryption in smart card." In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pp. 54-59. IEEE, 2012.

[15] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." In Information and communication technologies, 2005. ICICT 2005. First international conference on, pp. 84-89. IEEE, 2005.

[16] Global Platform. "Open Platform Card Specification", Version 2.1. June 2001. http://www.globalplatform.org.

[17] Javasoft. "Java Card Platform Specifications", Version 2.2, September 2002. http://java.sun.com/products/javacard/specs.html

[18]Microsoft "Windows for Smart Card". http://www.microsoft.com/HWDEV/TECH/input/smartcard/

[19] MAOSCO. "MULTOS Reference Manual Ver 1.2". http://www.multos.com/

[20] K. Markantonakis. "Is the Performance of the Cryptographic Functions the Real Bottleneck?", IFIP TC11 16th International Conference on Information Security (IFIP/SEC'01), June 11-13, 2001, Paris, France, In "Trusted Information: The New Decade Challenge" , Kluwer Academic Publishers , ISBN 0-7923-7389-8, pages 77-92.

[21] "Application Management Framework in User Centric Smart Card Ownership Model," in The 10th InternationalWorkshop on Information Security Applications (WISA09), ser. LNCS, H. Y. YOUM and M. Yung, Eds., vol. 5932/2009. Busan, Korea: Springer, August 2009, pp. 20–35.

[22] Akram, Raja Naeem, Konstantinos Markantonakis, and Keith Mayes. "A Secure and Trusted Channel Protocol for the User Centric Smart Card Ownership Model." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 336-345. IEEE, 2013

[23] Oracle Documentation on Java Card™ Technology (dated March 6th 2015)

[24] GlobalPlatform Card Specification Version 2.2.1 January 2011

[25] Y. Gasmi, A.-R. Sadeghi, P. Stewin, M. Unger, and N. Asokan, "Beyond Secure Channels," in STC '07: Proceedingsof the 2007 ACM workshop on Scalable trustedcomputing. NY, USA: ACM, 2007, pp. 30–40.

[26] Akram, Raja Naeem, Konstantinos Markantonakis, and Keith Mayes. "A Secure and Trusted Channel Protocol for the User Centric Smart Card Ownership Model." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 336-345. IEEE, 2013.

[27] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," Des. CodesCryptography, vol. 2, pp. 107–125, June 1992.

[28] A. Aziz and W. Diffie, "Privacy And Authentication For Wireless Local Area Networks," IEEE Personal Communications, vol. 1, pp. 25–31, First Quarter 1994.

[29] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in Computer Security ˚U ESORICS98, ser. LNCS, J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, Eds. Springer, 1998, vol. 1485, pp. 277– 293, 10.1007/BFb0055870.

[30] W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold, "Just fast keying: Key agreement in a hostile internet," ACM Trans. Inf. Syst. Secur., vol. 7, pp. 242–273, May 2004.

[31] GlobalPlatform: GlobalPlatform Card Specification,Version 2.2,, Online, GlobalPlatform Specification, March 2006.

[32] Remote Application Management over HTTP, Online, GlobalPlatform Specification, September 2006.

[33] "Smart Cards; Secured Packet Structure for UICC based Applications (Release 6)," ETSI, France, Tech. Rep. ETSI TS 102 225 (V6.8.0), April 2006.

[34] K. Markantonakis and K. Mayes, "A Secure Channel Protocol for Multi-application Smart Cards based on Public Key Cryptography," in CMS 2004 - Eight IFIP TC-6-11 Conference onCommunications and Multimedia Security, D. Chadwick and B. Prennel, Eds. Springer, Sep 2004, pp. 79–96.

[35] W. G. Sirett, J. A. MacDonald, K. Mayes, and C. Markantonakis, "Design, Installation and Execution of a Security Agent for Mobile Stations," in Smart Card Research andAdvanced Applications (CARDIS), ser. LNCS, J. Domingo- Ferrer, J. Posegga, and D. Schreckling, Eds., vol. 3928. Spain: Springer, April 2006, pp. 1–15.

[36] R. N. Akram, K. Markantonakis, and K. Mayes, "A Privacy Preserving Application Acquisition Protocol," in 11th IEEEInternational Conference on Trust, Security and Privacyin Computing and Communications (IEEE TrustCom-12), F. G. M. Geyong Min, Ed. Liverpool, United Kingdom: IEEE Computer Society, June 2012.

