**International Journal of Electrical and Electronics Research** ISSN 2348-6988 (online)
Vol. 3, Issue 4, pp: (209-214), Month: October - December 2015, Available at: www.researchpublish.com

# Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography

[1]Aditya B Kakde, [2]Dr. D. V. Rojatkar

[1]B.E. student, Electronics and Telecommunication dept. Government College of Engineering, Chandrapur, India
[2]Supervisor, HOD of Electronics and Telecommunication dept. Government College of Engineering, Chandrapur, India

***Abstract:*** **The overall use of mobile devices has made it possible to develop mobile e voting system as a complement to the existing e voting system. However, due to limited on board resource, it is difficult to achieve both efficiency and security strength for mobile voting system. traditional solution is to use symmetric encryption algorithms or hybrid symmetric and asymmetric algorithms at the expense of weaker security strength. In our proposed mobile voting scheme, the users votes are secured by using the elliptic curve cryptography (ECC) algorithm Finally, the election server administrator will sort the final result by success in reading the received encrypted information using RSA private key. Actually, this Electric-Voting protocol is more wasting time and energy than others E-Voting protocols since the voter can vote from his/her own personal computer (PC) without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed protocol.**

***Keywords:*** **E-Voting, Cryptography, RSA, System Access Control, and Public-Key.**

## 1. INTRODUCTION

For more than twenty year, electronic voting has been implemented. Despite its argument for and against [1], it is investigated in the real environment, either in a small or large scale, such as in Estonian public election [2]. On the other hand, mobile phones have been widely used around the world whose number of subscribers has reached over 4 billions worldwide [3]. Its popularity, flexibility and portability have inspired people to use it in various functions, not only as a voice exchanging tool, but also as a polling machine .This mobile voting (m-voting) system provides a more convenient means of e-voting. In general, e-voting systems must meet the principles and requirements for an election which include [4, 5]: Confidential Anonymity Integrity Due to its resource limitation, mobile voting has more challenges than the common electric-voting systems in term of performance and security. While some requirements have been presented in other research problems such as in [6], we will focus on the cryptographic performance issue. In our mobile voting scheme, the data transferred from mobile devices to the voting administrator is secured by elliptic curve cryptography as it has more advantages than other public key cryptographies, in term of key size, for instance. Those factors are useful to meet the mobile devices computing performance, the confidentiality, integrity In Egyptian E-Voting protocol [2], the authors established an Electronic Voting System in Egypt (EVSE) scheme. This scheme is impliment to fit in the environment and the conditions of Egypt, trying to remove problems in the old system, conventional system. This system offers a certain degree of elastisity and convenience to the voter to ensure a maximum dedication in the democratic process. If the voter is registered for voting in a particular constituency, e.g. ALX but works in another, e.g. Agouza, then she/he can vote in the Agouza polling station near his/her work place. However, she/he will only have access to the Ballot Server of ALX to participate in the local election of her/his constituency (refer to Figure 1).

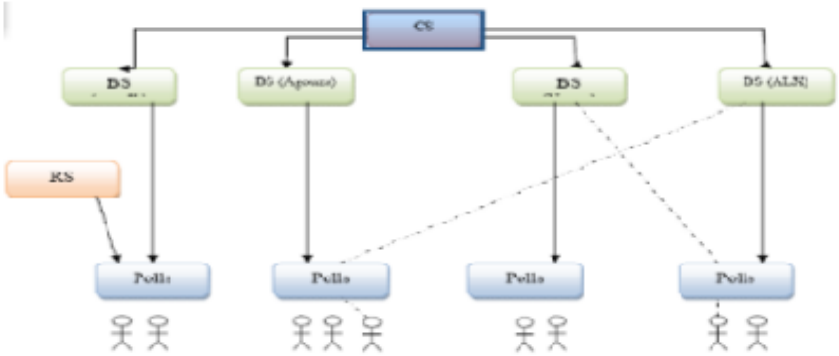



Figure 1. Egyptian E-Voting system hierarchal [2]

## 2. INFORMATION SECURITY AND CRYPTOGRAPHY

Information security is the process which present all measure taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of destruction, use, disclosure, implementation or disruption. Additionally, information security and Cryptography share the common services of protecting the confidentiality, integrity and availability of the information disagree data form (electronic document, printed document) [4].

### 2.1 Cryptography:

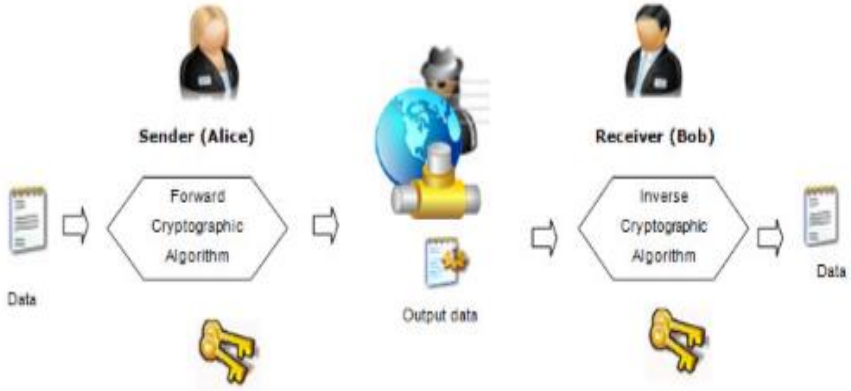



Figure 2. Cryptographic scheme

Cryptography [4] is one of the most essential fields in computer information security. It is a method of sending private information and data through open network communication. However, cryptography provides many services such as: confidentiality, authentication, integrity, non-repudiation, and accessibility.

Cryptography provides the information security for other necessary applications such as in encryption, message digests, zero-knowlegde proof of identity, key-sharing and digital signatures.

The length and capacity of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. They must be save from unauthorized users and must be available when they are needed.

Cryptography also contributes to Computer Science, particularly, in the techniques used in computer and network security for access control and information confidentiality [5]. Cryptography is also used in many advantage encountered in each day life such as: Electronic Voting, computer passwords, ATM cards, and electronic commerce. Generally, Cryptography may be classified into two main categories [4, 6]:

1. Asymmetric/ two key/ public-key: Ciphering and deciphering using a couple of keys.

2. Symmetric/ one key/ secret-key: Ciphering and deciphering using the same key (or without key – in the case of Hash function).

***2.1.1 Secret-Key (Symmetric) Algorithms:***

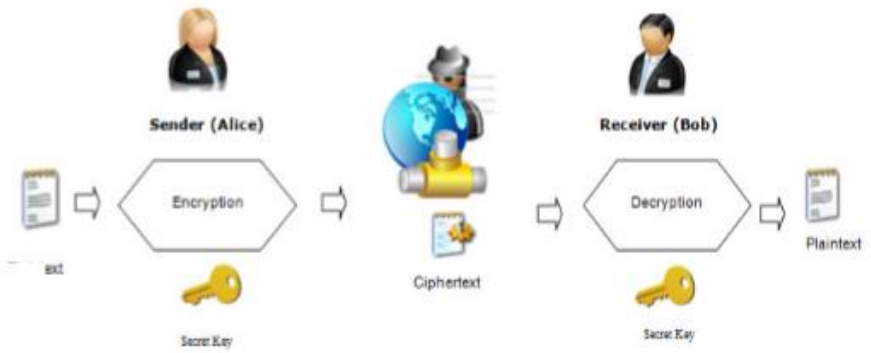



Figure 3. Secret-key cryptographic scheme

Secret-key (refer to Figure 3) is also known as one-key, or single-key algorithm. Secret-key is an encryption offer consisting sets of encryption and decryption algorithms. The plaintext is encrypted by key e and the cipher text is decrypted by key d, where e is the encryption key and d is the decryption key. In secret-key scheme, key d must be equal to key e as shown by Figure 3. The Data Encryption Standard (DES) [7] is an example of the secret-key offer. ds the acknowledgment to the user In this scheme, steps (a), (b), (d) and (e) include the use of mobile component which the most attention is submit to the step (e) that mobile component perform encryption to the data. This encryption process is analyzed in section 4.2. The other steps: (c), (f - l) are carried out in non-resource-constrained devices, so the security and to performance may not be a big problem. Decryption can only be done by counter 1 or counter 2 since those two methods are the only one who has the official key. Finally, the whole result will be 1 2 m'= m' = m'. The counter 1 is not able to modify the result (m) without acknowledgment from the counter 2, since the counter 2 is alsocatch the same data and vice versa. Therefore, the confidentiality and integrity of the data maintainence According to the trustworthy entities scheme [12], the users anonymity is also keep. This is because the administrator only knows the users identity but not the vote. On the other hand, the counter 1 and counter 2 works on the vote without user identity in it. Moreover, the counters also unable keep the users identity data because it is only available for the administrator. In addition, it may also use the homomorphism property of the EC-ElGamal encryption offer [18, 19] to kept the anonym. To increment the security process, the encryption scheme

***2.1.2 Public-Key (Asymmetric) Algorithms:***

In public key algorithms (refer to Figure 4), there is a couple of keys, one of which is known to the public and used to encrypt the plaintext to be transfer to the receiver who owns the corresponding decryption key, known as the private key.

Every asymmetric-key cryptosystem is based on a mathematical problem that is in some sense hard to solve. These problems are called "difficult problems" and are divided in two major parts according to the Cryptography dividation [8], as P (Polynomial) and NP (Non-deterministic polynomial). The problem is t to be assume difficult problem if the problem can be solved in polynomial time, while a problem is considered to be an NP difficult mathematical problem if the validity of a proposed answer can be checked only in polynomial time.

Basically, the three major types of mathematical difficult problem that had been successfully being used in Cryptography are tells in the following subsections of this part. These problems are [4, 8]:

• The Integer Factorization Problem (IFP) • the Discrete Logarithm Problem (DLP) • the Elliptic Curve Discrete Logarithm Problem (ECDLP).

## 3. THE PROPOSED PUBLIC-KEY CRYPTOGRAPHIC E-VOTING PROTOCOL

As mentioned earlier, many previous studies on E-Voting method have been done and focused on facilitating the E-Voting method. These methods are suffering from various weaknesses such as voters' exhaustion, the required hardware cost, and the mandatory polling places.

In this study, the proposed method is based on the analysis of the different factors that play amajor role in the previous E-Voting methods. Therefore the proposed protocol is slow down the voters' exhaustion since the voters can vote by using her/his own PC and the required time to add and analyze the last results. However, the proposed protocol is based on RSA public-key encryption protocol. Whereby, the RSA is used to guarantee information it is accessible only to authorized entities and is inaccessible to others. As well RSA is used also to guarantee information remains unchanged from the source entity to the destination entity.

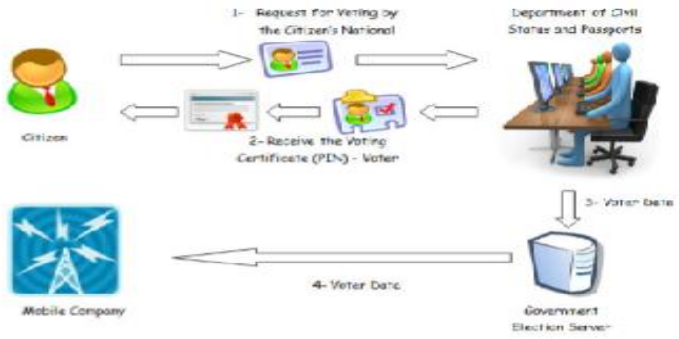
Generally, the proposed method tells three steps for electronic voting system by using the assymetric-key E-Voting protocol (refer to Figures 6-9). These steps are: the system access control process that is to authenticate the voter on the election server, the voting process, and collecting data process.

### I. System Access Control Process:

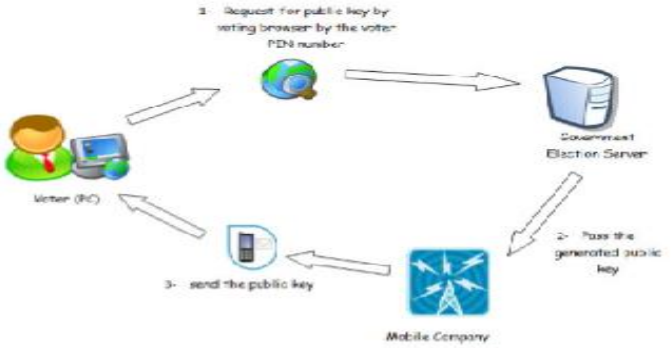
As mentioned earlier, system access control process is one of the cryptographic services, which is used to authenticate the voter in the government election server. This process is the first step in the proposed E-Voting system that prepares the voter to be authorized in the advanced E-Voting process. Therefore, the system access control involves Identification phase and Authentication phase.

### 1. Identification phase (Registration):

In this phase, the Department of Civil Status and Passports plays the main role, whereby it verifies that the citizen can vote legally. As illustrated in Figure 6 Step 1, the citizen should visit the Department of Civil Status and Passports to verify his/her information to get the election right. Once the citizen registered in the Department of Civil Status and Passports, the following three steps should have been done. As shown in Figure 6 Step 2, the citizen becomes certified voter. In Figure 6 Steps 3 and 4, the voter data will be saved in the specified election server and then passed to mobile Phone Company for advance process.




**2. Authentication Phase (Immediately Before Voting)**



As we have mentioned, the factors that required to conducting the E-Voting process are the software and hardware related factors. In this phase, the voter can access the voting process simply by using his/her personal computer (refer to Figure 4).

Moreover, the whole Voting process is clarified in Figure 7 from the beginning to the end. The voter login to the E-Voting website by using his/her national_ID and PIN numbers as shown in Figure 4. Once the voter signed to the election website (Refer to Figure 5 Step 1), the election severwill generate a computed RSA public-key (refer to Figure 5). This public key will be then directpassed by mobile company as a short mobile message (sms) to the voter (Refer to Figure 4 Steps 3and 4). Note that, the receiving of the public key indicates that the voters are ready for voting process immediately.

## 4. CONCLUSION

Encryption of data transferred between two parties in a mobile environment is a critical part in keeping data security, especially for its confidentiality and integrity. However, achieving high security level by demanding high computing cost is not the solution. In this paper, we have proposed to use ECC for directly encrypting data in a specified size in the mobile devices. Encryption in a mobile device itself is slightly difference from other machines since it needs to consider its resource limitation. The time of 15 seconds for encryption using ECDH-256 and AES-128 may not be acceptable in the mobile environment. Considering that performance is a critical issue, we believe that directly encrypting the specified data size as in the table will increase performance without reducing the security level. By using the latter method, which is ECC-256 bit, it just needs about 3 seconds. ECC256 bit itself may be considered too high to use in one or two times encryption application.

## ACKNOWLEDGMENT

We show our deep gratitude towards our supervisor Dr. D. V. Rojatkar who has supported and mentored us throughout our work in a righteous way

## REFERENCES

[1] C. Karlof, N. Sastry, and D. Wagner, (2005), “Cryptographic voting protocols: A Systems perspective”, 14th USENIX Security Symposium, pp. 33-49.

[2] M. Abo-Rizka, and H. Ghounaim, (2007) ” A Novel in E-voting in Egypt”, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.11.

[3] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

[4] A. Pardos, A. Encinas , S. White , A. del Rey and G. Sánchez, (2007), “A Simple Protocol for Yes-No Electronic Voting”, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.7.

[5] Menezes, A., P. Van Oorschot, and S. Vanstone, (1996), Handbook of Applied Cryptography, CRC Press, pp.4-15, 516.

[6] I. Branovic, R. Giorgi, E. Martinelli, (2003) “Memory Performance of Public-Key Cryptography Methods in Mobile Environments”, ACM SIGARCH Workshop on Memory performance: Dealing with Applications, systems and architecture (MEDEA-03), New Orleans, LA, USA, pp. 24-31.

[7] M. Alia and A. Samsudin, (2007), “A New Public-Key Cryptosystem Based on Mandelbrot and Julia Fractal Sets”, Asian Journal of Information Technology, AJIT, 6(5), pp. 567-575.

[8] National Bureau of Standards (1977) Data Encryption Standard. FIPS-Pub.46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

[9] RSA Laboratories, (2007) “What is a Hard Problem. RSA the Security Division of EMC”. [9] W. Diffie, and M. E. Hellman, (1976), “New Directions in Cryptography”, IEEE Transactions on Information Theory, IT-22, pp. 644-654.

[10] R. A. Rivest, A. Shamir, and L. Adleman, (1978), “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, 21(2), pp.120-126.

[11] T. ElGamal, (1985) "A Public-Key Cryptosystem and a Signature Scheme Based on Discret Logarithms", IEEE Transactions on Information Theory, IT-31(4), pp. 469–472.

[12] N. Koblitz, (1987)"Elliptic Curve Cryptosystems", Mathematics of Computation, pp. 203–209.

[13] R. Lehtinen, (2006), "Computer Security Basics", 2nd Edition, O'Reilly, ISBN-10: 0-596-00669-1.

[14] I. Branovic, R. Giorgi, and E. Martinelli, "A workload characterization of elliptic curve cryptography methods in embedded environments," ACM SIGARCH Computer Architecture News, vol. 32, pp. 27-34, 2004.

[15] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," Proc. IEEE Symposium on Security and Privacy, IEEE, 2004, pp. 27-40.

[16] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, "Are your votes really counted?: testing the security of real-world electronic voting systems," Proc. the 2008 international symposium on Software testing and analysis, Seattle, Washington, USA, ACM, 2008.

[17] J. Light and D. David, "An efficient security algorithm in mobile computing for resource constrained mobile devices," Proc. the 4th ACM symposium on QoS and security for wireless and mobile networks, Vancouver, Canada, ACM, 2008.

[18] C. Fontaine and F. Galand, "A Survey of Homomorphic Encryption for Nonspecialists," EURASIP Journal on Information Security, 2007.

[19] J.-M. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A secure and resilient WSN roadside architecture for intelligent transport systems," Proc. the first ACM conference on Wireless network security, Alexandria, Virginia, USA, 2008, pp. 161-171.

[20] Bouncy Castle, "Lightweight API," [on-line] accessed on March 15, 2009 from http://www.bouncycastle.org/, The Legion of the Bouncy Castle, 2008.

[21] S. Han, E. Chang, W.-q. Liu, V. Potdar, and J. Wang, "A new encryption algorithm over elliptic curve," in INDIN 2005: 3rd International Conference on Industrial Informatics, Frontier Technologies for the Future of Industry and Business, T. Dillon, X. Yu, and E. Chang, Eds. Perth, WA: IEEE, 2005.

[22] NIST, "Advanced Encryption Standard Algorithm Validation List," [on-line] accessed on April 15, 2009 from http://csrc.nist.gov/, Computer Security Division, National Institute of Standards and Technology (NIST), 2009.

[23] F. Han, J. Hu, X. Yu, Y. Feng, and J. Zhou, "A novel hybrid crypto-biometric authentication scheme for ATM based banking applications," Proc. IAPR International Conference on Biometrics Published at Lecture Notes in Computer Science vol. 3832, Hong Kong China, 2006.

[24] F. Han, J. Hu, L. He and Y. Wang, "Generation of reliable PINs from fingerprints", Proc. Security Symposium IEEE International Conference on Communication (ICC), Glasgow, Scotland, June, 2007.

[25] Y. Wang, J. Hu, K. Xi and B.V.K. Vijaya Kumar, "Investigating correlation-based fingerprint authentication schemes for mobile devices using the J2ME technology. Proc. IEEE Workshop on Automatic Identification Advanced Technologies, AutoID 2007. Alghero, Italy, 7-8 June 2007.

[26] J. Hu, D. Gingrich A. Sentosa, "A k-nearest neighbor approach for user authentication through biometric keystroke dynamics," Proc. IEEE ICC Conference, Beijing, China, 19-23 May, 2008.