Design for Enhanced Security and Convenience of E-Voting Scheme

Pin-Chang, Su Yui-Chong, Yeh*

***Abstract*—The popularity of Internet has altered the traditional way of life and behavioral patterns. Indeed, while the Internet has brought great convenience, it has also highlighted numerous issues for network security. Many countries are committed to the development of e-voting, which would help societies reduce the amount of resources allocated for traditional elections. However, most literatures exploring the signature mechanisms of electronic elections only address research and technology pertaining to the single voting scheme and single blind signature mechanism. Further, these electoral processes typically exploit only blind signature rather than encryption. In the case where multiple votes are cast simultaneously by a single voter, thereby requiring various ballots to be signed electronically, both the processing speed of the server as well as the security of the ballots would be greatly compromised. This study thus examines the mechanism that would accord a more efficient and secure design for the e-voting system, which would also take into account the immediacy of proxy voting as well as the need to ensure voters' anonymity. This research focuses on the implementation of the Elliptic Curve Cryptosystem and its capacity to generate computations rapidly as its foundation. The properties of blind signature and proxy signature in proxy blind signature are engaged to facilitate the signcyrption of multiple ballots simultaneously. It further harnessed the avalanche effect in the design of encryption to increase the difficulty of deciphering ciphertext. In all, these designs, which enhance the overall efficiency and security of the e-voting system, would be applicable to an e-voting mechanism that features multiple and varied polls in the future.**

Keywords: Elliptic Curve Cryptosystem, E-Voting, Multi-Document Signcryption, Proxy Blind Signature

I. INTRODUCTION

The rapid development of the Internet and e-commerce have accorded greater convenience and flow of information at great speed, as well as increased opportunities for profits for among business enterprises. For instance, in traditional transactional processes, both sellers and buyers engage face-to-face interaction to ensure smooth and safe exchange of goods and services for the right fees. However, business models in the age of the Internet have transcended theses barriers and restrictions, and have indeed rendered face-to-face transactions obsolete. Indeed, third-party payments, online shopping and other novel trading patterns have emerged and are integrated rapidly into the modern way of living, thereby allowing consumers to enjoy the convenience of shopping while remaining in the comforts of their homes, as well as creating significant global opportunities and profits for businesses. Amid the convenience accorded by the Internet, security concerns have also surfaced, especially with the advent of big data analytics. How to discern information safely and effectively amidst the enormous huge amount of data available marks a pressing concern. With Taiwan's nine-in-one local elections due at the end of 2014 where voters are expected to cast their ballots on the very same day, it is timely to examine the application of the concept of multi-document to the field of e-voting. Many countries have adopted the practice of e-voting amid the popularization of the Internet. In 2007, Estonia held the world's first electronic parliamentary election. Yet the contents of the poll must be adequately encrypted so as to prevent parties with vested interests from deliberately back-tracing the poll to the voter, which would otherwise result in the loss of any credibility for e-voting. Further, how could one prove that the data of the voter as entered into the electronic system is authentic rather than deliberately forged? The digital signcryption mechanism is thus adopted to address these inadequacies and concerns.

Digital signatures can be used to assure the identity of parties involved in an event. However, how to encrypt the information entered by the actor while ensuring the actor's signature is registered and transmitted instantaneously represents yet another challenge. Numerous researchers worldwide have conducted various studies on developing digital signatures and encryption techniques to ensure secure e-voting and mobile commerce. In 1982, Chaum [1] first introduced the blind signature concept, which enables signature requestors to obtain signatures from signers without information disclosure. Moreover the concept of proxy signature was proposed by Mambo et al. [2] in 1996. In a proxy signature scheme, an original signer delegates his signing capability to a person named the proxy signer, who can signs the message or document on behalf of the original signer. Proxy blind signature was first proposed by Lin and Jan [3] in 2000. It combines the concept of the proxy signature and the blind signature. In 2002, by applying Schnorr blind signature, Tan et al. [4] proposed a new proxy blind signature schemes based on DLP and ECDLP.

Manuscript received October 21, 2014.

P. C. Su is with the Department of Information Management, National Defense University, Taiwan, R.O.C (e-mail: spc.cg@msa.hinet.net).

Y. C. Yeh* is with the Department of Information Management, National Defense University, Taiwan, R.O.C (corresponding author to provide phone: 0982049221; e-mail: leo99988@yahoo.com.tw).

Later, Lal and Awasthi [5] pointed out that Tan et al.'s proxy blind signature schemes suffer from a kind of forgery attack due to the signature receiver in 2003. Compared with Tan et al.'s schemes, Lal and Awasthi further proposed a more efficient and secure proxy blind signature scheme to overcome the pointed out drawback in Tan et al.'s schemes. However, Sun and Hsieh [6] show that Tan et al.'s schemes do not satisfy the unforgeability and unlinkability properties in 2004. In addition, they also point out that Lal and Awasthi's scheme does not possess the unlinkability property either. But they did not give an improved scheme to overcome the insecurity. Afterwards, Wang and Wang [7] proposed a proxy blind signature scheme based on ECDLP in 2005. However, Yang and Yu [8] proved that Wang and Wang's scheme did not meet the security properties and proposed an improved proxy blind signature scheme in 2008. In 2011, Pradhan-Mohapatra [9] and Alghazzawi et al. [10] also proposed new proxy blind signatures based on ECDLP. Later, Wang and Liao [11] show that their schemes are insecure against linkability attacks and proposed a enhanced construction on ECDLP-based proxy blind signature scheme in 2014. In 1997, Zheng [12] first proposed the signcryption concept, merges traditional digital signature and public key encryption into one step so that computational complexity and communication costs are greatly reduced.

With scholars' continuous efforts to research and improve in this area, e-voting via the Internet could be expected to materialize in the future, thereby maximizing the benefits and minimizing the limitations of e-voting [13, 14]. Based on these advancements, voters can cast ballots online regardless of their location, which saves voters time and trips to and from designated voting venues and offers immense convenience in elections. However, most literatures only considered the single voting mechanism. They also failed to take into account any encryption mechanism for the ballots. As such, this study incorporates the design of permutation and avalanche effect from multi-document signcryption algorithm to strength system security. In the case of Taiwan's nine-in-one local elections due at the end of 2014, each voter may need to cast three or more ballots to select different categories of electoral candidates. Depending on the voter turn-out, a ten-thousand strong electorate would generate tens of thousands of ballots. As such, the multi-document proxy blind signcryption mechanism is more appropriate for the multi-election system as it reduces the excessive attempts at signcryption per vote, thus facilitating efficient execution and operation of the multi-election system. These would, in turn, reduce the amount of resources which societies spend on elections. Also, the ballot encryption mechanism would offer more protection and security to the e-voting system. This study contains the following sections: Section 2 presents a literature review, Section 3 shows the design of the multi-document proxy blind signcryption scheme for e-voting, Section 4 provides the security analysis, and Section 5 offers a conclusion.

II. LITERATURE REVIEW

Proxy Blind Signature based on ECDLP

In 2002, by applying Schnorr blind signature, Tan et al. proposed a new proxy blind signature schemes based on DLP and ECDLP. We only review Tan et al.'s proxy blind signature based on ECDLP calculus architecture has three stages:

(1) Proxy Delegation Stage: The original signer computes $R_o = k_o \cdot B, r_o = x(R_o)$ and $s_o = x_o r_o + k_o \bmod q$, where k_o is a random number. Next, original signer sends (r_o, R_o, s_o) to the proxy signer in a secure manner. Proxy signer accepts (r_o, R_o, s_o) if the equation $R_o = s_o \cdot B - r_o \cdot Y_o$ does hold. Finally, the proxy signer computes the proxy secret key $s_{pr} = s_o + x_p \bmod q$.

(2) Blind Signing Stage: The proxy signer computes $T = k \cdot B$, where *k* is a random number and sends it to the asker. Asker computes $L = T + b \cdot B + (-a - b) \cdot Y_p - a \cdot R_o - (ar_o) \cdot Y_o$, $r = x(L),\ e = h(r \parallel m) \bmod q$, $U = (-e + b) \cdot R_o + (-e + b) r_o \cdot Y_o - e \cdot Y_o$, $e' = e - a - b \bmod q$ where *a* and *b* are random numbers. Next, asker sends e' to proxy signer. Proxy signer then computes $s' = e' s_{pr} + k \bmod q$ and return s' to asker. Upon receiving s', asker computes $s = s' + b \bmod q$. The signature of message *m* is (m, U, s, e).

(3) Verification Stage: The recipient of signature can verify the proxy blind signature by checking whether $e =? h\left(x\left(s \cdot B - e \cdot Y_p + e \cdot Y_o + U\right) \parallel m\right)$ holds.

III. PROPOSED SCHEME

This study proposed a multi-document proxy blind signcryption scheme based on elliptic curve cryptosystems that is applicable for signature verification in multi-ballot elections. The research examines the design of an e-voting scheme that allows for the multiple ballots from one voter to be signed and encrypted simultaneously. Similarly, this mechanism could be applied to the field of medicine, particularly to Electronic Medical Records (EMR). The diagnostic medical advice, medication records, medical imaging and other information for multiple EMR could be blinded and encrypted at one go, then it would be signed by the medical practitioner with legal effect. Together with the concept of proxy blind signature mechanism, this improved mechanism reduces the amount of processing time significantly by removing excess procedures, thereby enhancing the operations efficiency.

Flowchart and Architecture of the Overall System and Parameters

The overall flowchart of the system is depicted in Fig. 1.

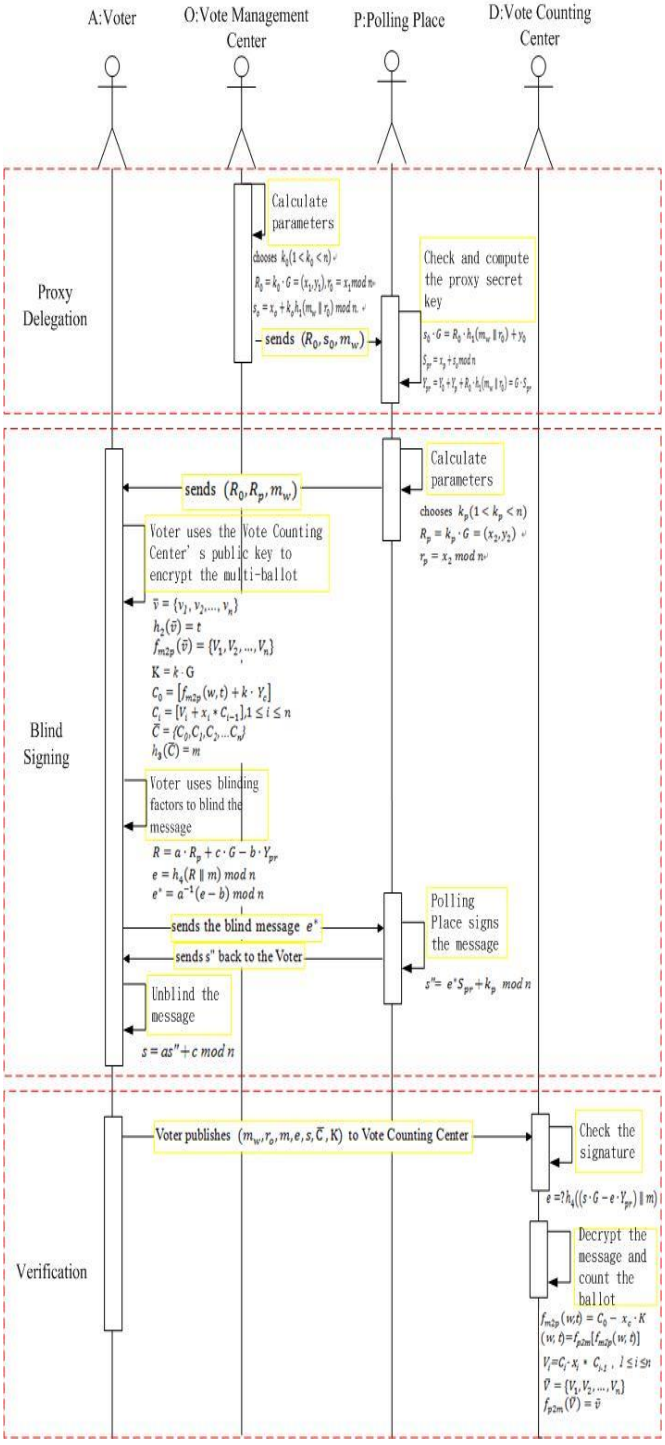

Fig. 1. Operational flow of the system

The notations of our multi-document proxy blind signcryption scheme are introduced in Table I.

TABLE I
DESCRIPTION OF NOTATIONS USED IN THE SYSTEM

Item	Notation	Description
1	$E(F_q)$	An elliptic curve within a finite field F_q
2	G	Base point of the elliptic curve
3	N	Order of the base point of the elliptic curve
4	q	A prime number: $q > 2^{160}$
5	Y_O, Y_p, Y_c	Public keys of Vote Management Center O, Polling Place P, and Vote Counting Center C
6	x_O, x_p, x_c	Private keys selected by Vote Management Center O, Polling Place P, and Vote Counting Center C
7	$h_1(\ )$	Hash function (value transposition)
8	$h_2(\ )$	Hash function (plaintext-sequence transposition)
9	$h_3(\ )$	Hash function (ciphertext point-sequence transposition)
10	$h_4(\ )$	Hash function (point transposition)
11	$f_{m2p}(\ )$	Function that transforms a message into points on an elliptic curve
12	$f_{p2m}(\ )$	Function that transforms points on an elliptic curve into a message
13	*	Shift operations
14	V	Plaintext ballot
15	C	Ciphertext ballot
16	w	Knapsack values 0 and 1 in plaintext
17	t	Plaintext sequence hash value
18	m	The digest to be signed
19	m_w	Proxy warrant
20	k	Randomly selected value of Voter A

TABLE II
COMPARISON OF SECURITY MECHANISMS OF THE PROPOSED SCHEME AND VARIOUS PROXY BLIND SIGNATURE-BASED SYSTEMS

Security \ Algorithm	Tan et al.'s scheme (2002)	Alghazzawi et al.'s scheme (2011)	Wang and Liao's scheme (2014)	Our scheme
Verifiability	V	V	V	V
Non-repudiation	V	V	V	V
Anonymity	V	V	V	V
Unforgeability	X	V	V	V
Confidentiality	X	X	X	V
Integrity	△	△	△	V
Unlinkability	X	X	V	V
Distinguishability	V	V	V	V
Identifiability	V	V	V	V
Prevention of misuse	X	V	V	V

Note: Our scheme contains the property of multi-document signcryption

IV. SECURITY ANALYSIS

The security of the proposed multi-document proxy blind signcryption scheme is based on elliptic curve discrete logarithm problem and one-way hash function.

In this section, we show that our scheme satisfies the requirements of confidentiality, integrity and other aspects of information security management required by ISO organizations [15, 16]. Meanwhile, we satisfies all properties of proxy blind signature, such as verifiability, non-repudiation, anonymity, unforgeability, unlinkability, distinguishability, identifiability, prevention of misuse.

Table II presents a summary comparison of various security mechanisms for proxy blind signature-based systems. In the table, Symbols: V, △ and X that mean the degree of supporting the component of requirements by each corresponding scheme: support, partially support and no support, respectively.

V. CONCLUSION

At Taiwan's inaugural nine-in-one local elections due at the end of 2014, each voter is expected to cast three or more of the votes. If the technology of e-voting could be applied in this case, coupled with the incorporation of the concept of multi-document proxy blind signcryption as elaborated in this study, the amount of electoral funds and social resources allocated to the elections would be reduced considerably. Indeed, the mechanism featured in this study harnesses the concept of blind signature to protect the identity of the voter; the concept of proxy signature to allow for instant data transmission; the concept of multi-document signcryption to improve the inadequacies of the traditional one-ballot-per-election signcryption method. The combination of the above concepts would shorten the procedural flows, reduce the cost of the computing server significantly, as well as ensure the encryption design would improve the safety of electronic elections by preventing the votes from being intercepted and the contents of the ballots revealed to unauthorized parties. The above security analysis bears testament to the security accorded by the system proposed by this study, which exceeds the level of security featured in the various systems proposed by previous scholars. As such, this system proposed in this study would better facilitate the promotion and actualization of e-voting while ensuring both efficiency and security.

REFERENCES

[1] D. Chaum, "Blind signatures for untraceable payments," In Proceedings of Advances in Cryptology—CRYPTO, 1982, pp. 199-203.

[2] M. Mambo, K. Usuda, E. Okamoto, "Proxy signatures for delegating sign operation," In: Proceeding of the 3rd ACM conference on computer and communications security (CCS96), 1996, pp. 48-57.

[3] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," Proc. of Int Conference on Chinese Language Computing, 2000, pp. 273-277.

[4] Z. Tan, Z. Liu, C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, vol. 21, 2002, pp. 212-217.

[5] S. Lal and A. K. Awasthi, "Proxy Blind Signature Scheme" to appear in Journal of Information Science and Engineering, vol. 2, 2003, pp. 5-11.

[6] H. M. Sun, B. T. Hsieh, S. M. Tseng, "On the security of some proxy blind signature schemes," The Journal of Systems and Software, 2005, pp. 297-302.

[7] H. Y. Wang and R. C. Wang, "A proxy blind signature scheme based on ECDLP," Chinese Journal of Electronics, vol. 14, 2005, pp. 281-284.

[8] X. Yang and Z. Yu, "Security Analysis of a proxy blind signature scheme based on ECDLP," in Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), 2008, pp. 1-4.

[9] S. Pradhan and R. K. Mohapatra, "Proxy blind signature scheme based on ECDLP," International Journal of Engineering Science & Technology, vol. 3, 2011, pp. 73-79.

[10] D. M. Alghazzawi, T. M. Salim, S. H. Hasan, "A new proxy blind signature scheme based on ECDLP,"IJCSI International Journal of Computer Science Issues, vol. 8, no. 1, 2011, pp. 73-79.

[11] C. H. Wang and M. Z. Liao, "Security analysis and enhanced construction on ECDLP-based proxy blind signature scheme," International Journal of e-Education, e-Business, e-Management and e-Learning, vol. 4, no. 1, 2014, pp. 47-51.

[12] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," Advances in Cryptology-Crypto 97, 1997, pp. 165-179.
[13] S. Delaune, S. Kremer, M. Ryan, "Coercion-resistance and receipt-freeness in electronic voting,"19th IEEE Computer Security Foundations Workshop (CSFW), 2006, pp. 28–39.
[14] C. I. Fan and W. K. Chen, "An Efficient Blind Signature Scheme for Information Hiding,"International Journal of Electronic Commerce, vol. 6, no. 1, 2008, pp. 93-100.
[15] ISO, 2005, Information technology-Security techniques-Code of practice for information security management, ISO/IEC 17799.
[16] ISO, 2008, Information technology-Security techniques-Key management-Part 3: Mechanisms using asymmetric techniques, ISO/IEC 11770-3.
[17] R. C. Wang, "A Web Metering Scheme for Fair Advertisement Transactions," International Journal of Security and its Applications , vol. 2, no. 4, 2008, pp. 49-55.