BORANG PENGESAHAN STATUS TESIS^

JUDUL: E-BALLOT USING IDENTITY BASED ENCRYPTION

SESI PENGAJIAN: 2004/2005

Saya KONG PEI ROU
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

   _____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

   _____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

   _____ TIDAK TERHAD

(TANDATANGAN PENULIS)

(TANDATANGAN PENYELIA)

Alamat tetap : 49 Jalan Merak 5 Bandar

Puchong Jaya Puchong 47100 Selangor

SITI RAHAYU SELAMAT
Nama Penyelia

Tarikh : 22 NOV 2005

Tarikh : 22 NOV 2005

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

E-BALLOT USING IDENTITY BASED ENCRYPTION

KONG PEI ROU

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY KOLEJ
UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA

DECLARATION

I hereby declare that this project report entitled

E-BALLOT USING IDENTITY-BASED ENCRYPTION

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT: _____ Date: 22/11/2005

(KONG PEI ROU)

SUPERVISOR: _____ Date: 22 NOV 2005

(PUAN SITI RAHAYU SELAMAT)

DEDICATION

To all who have helped me through the completion of this thesis …

ACKNOWLEDGEMENTS

First and foremost, I would like to show my deepest appreciation to my project supervisor, Pn. Siti Rahayu Selamat, for guiding me through out the process of completing this PSM report. Thanks for the teaching and advising to my previous supervisor Mr. Shekh Faisal Abdul Latip which has given me advice too.

Gratitude is to be expressed to the PSM committee members for providing guidelines and workshop in the aid of producing a report with quality and standards.

Last but not least, I would as well like to thanks my family and my fellow mates for the encouragement and useful thoughts that has been selfishly poured out to me through out the process of producing this report. Without the help from all, the completion of this report will be very much affected.

ABSTRACT

The issue of web-based voting has caused must debates from all party mainly because of its security considerations. A secured web-based voting application should fulfill the following criteria: completeness, soundness, privacy, unreusability, eligibility, fairness, and verifiability. However, most of the current existing application is not able to fulfill those criteria. Therefore, the thesis title "E-Ballot using Identity Based Encryption" is researched and implemented to identity the feasibility of integrating the Identity Based Encryption with the web-based voting application. The Identity Based Encryption is a new scheme to solve the problems which was found on the traditional Public Key Infrastructure. Using Identity Based Encryption, the use of certificates will be eliminated and the cost of infrastructure will be decreased because the maintenance of the certificates database is not necessary anymore. In this thesis, VOTOPIA is taken as a sample current existing web-based voting application that makes use of traditional PKI for analysis purpose. Problem statement is established based on the analysis and requirement for the to-be system is captured. Besides that, an early design of the to-be system is established as well including system architecture, user interfaces design, and logical database design. As in conclusion, the wellness of Identity Based Encryption is to be demonstrated through the completion of this thesis.

ABSTRAK

Isu pengundian melalui web telah menyebabkan terutamanya pendebatan dari pelbagai pihak isu-isu keselamatan yang perlu dipertimbangkan dalam pelaksanaan pengundian ini.Sesebuah aplikasi pengundian web hendaklah memenuhi beberapa kriteria berikut: *completeness, soundness, privacy, unreusability, eligibility, fairness* dan *verifiability*. Bagaimanapun, sebahagian besar daripada applikasi pengundian web yang sedia ada tidak dapat memenuhi kriteria-kriteria yang tersebut di atas. Oleh itu, tesis bertajuk "E-Ballot using Identity-Based Encryption" telah dikaji dan dilaksanakan untuk mengenalpasti kebolehlaksanaan menyatukan *Identity Based Encryption* dalam aplikasi pengundian web. *Identity Based Encryption* merupakan satu skema yang baru untuk menyelesaikan masalah-masalan yang terdapat dalam *Public Key Infrastructure* yang tradisional. Dengan menggunakan *Identity Based Encryption,* pengunaan *certificate* akan dihapuskan dan kos untuk membangunkan infrastuktur akan dikurangkan kerana penyelenggaraan pangkalan data yang digunakan untuk menyimpan *certificate* telahpun tidak lagi diperlukan. Dalam tesis ini, VOTOPIA akan diambil sebagai contoh bagi applikasi pengundian web yang sedia ada dimana ia mengaplikasikan *PKI* untuk kerperluan kajian dan analisis. Pernyataan masalah juga akan dihasilkan berdasarkan analisis dan keperluan untuk sistem yang bakal dibangunkan. Selain itu, satu rekabentuk awal untuk sistem yang bakal dibangunkan juga akan dihasilkan yang antaranya termasuk senibina sistem, rekabentuk antaramuka pegguna dan rekabentuk pangkalan data logikal. Kebaikan *Identity Based Encryption* akan didemonstrasikan dalam tesis ini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Project Background

In modern democratic society, voting is one of the important duties of a citizen. The term voting does not only suggest the public governmental election but it also includes all election under commercial organizations, student councils, board elections, and etc. People was always being discourage to participate because of the aspect of time consuming for presenting themselves to the polling station. Therefore, e-voting which mainly consisted of web-based voting and electronic machine voting is beginning to be widely deployed. However, the controversial issues of deploying the e-voting in a public governmental election has gather much debate from different parties mainly regarding the security and confidential issues of the application. More information will be presented in the Literature Review.

In this Project Sarjana Muda, the research being covered will only serves for the application of non-governmental use. The topic for the Project Sarjana Muda is to implement the concept of Identity Based Encryption in Web-based Voting Application.

Security is the main issues to be considered when developing an application of web-based voting. Voter authentication, voter anonymity, and the ballot integrity and confidentiality were those among the security aspects that comes front in the line. Therefore, identity-based encryption will be researched to be used in providing the security protection in this yet-to-be-developed application.

Identity-Based Encryption is a completely new approach to the problem of encryption. IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the mapping of identities to decryption keys. By using identity as the public key, Identity-Based Encryption (IBE) eliminates the need for certificates and overcomes the hurdles of public key infrastructure. The Public key could be based on commonly known and unique identifiers, such as email addresses, phone number, national identity card number, etc.

It is hoped that through the completion of this Project Sarjana Muda, it can be proved that by using the Identity Based Encryption, authentication and security can be preserved in the web-based voting application.

1.2 Problem Statements

The topic of this project is produced mainly because of the following existing problems of the potential web-based voting application:

a) Completeness (Integrity)

Completeness can be defined as all votes must be counted correctly and accurately [12].In a web-based voting application, a voter could not see the flow of the vote they cast, unlike the traditional paper-ballot scheme where the ballot is put in a locked ballot box. So how does the web-based voting application can provide the confidence to the voter that their vote in indeed being counted and it is counted correctly? How does the voter ensure that their vote is not being tampered in the process of the transmission to the ballot server in a web-based voting application? How can we ensure the integrity of the ballot? This is what that will be researched in this project.

b) Eligibility (Authentication)

Eligibility refers to no one who is not allowed to vote can participate in the voting process [12]. A feasible voting application should ensure only eligible voter is allowed to participate in the voting process. To provide this service, the web-based application needs to authenticate the voter before the vote is being cast. Authentication in the current web-based voting application is often too weak where it only depends on the login id and login password. Unlike a paper-ballot scheme, the authentication is done face-to-face in person. Hence, how can the admin on the other end of the network to authenticate the voter is indeed the eligible voter and not someone else by not only depending on login id and login password which can be easily compromised.

c) Unreusability

Unreusability here means voter can only perform voting once and only once in the voting process [12]. But how does the web-based voting application is going to determine that there is no repeating vote from the same person? The voter could register more than once if the registration method does not provide any means of identifying the person's identity. What unique identity is going to be used in the authentication method to ensure that no repeating user register more than once? If the same person is able to register himself more than once and get different login id, does that means he can vote more than once in the voting process? The problem of eligibility will be discussed in this project.

d) Privacy

Privacy in a voting process would be defined as all votes must be secret, no vote should be able to be link back to the voter, and the vote content is only known by the voter itself and no one else [12].A voter in a web-based voting application must be given the privacy that their vote is indeed confidential and not known to anyone else. No one is supposed to be able to link the vote to the voter. How does a web-based voting application can provide the privacy of the ballot?

1.1 Objectives

The objective of this project is to develop a web-based voting application with appropriate security concerns especially focusing on the voter authentication and ballots security using Identity Based Encryption. The objectives of the application are as following:

a) To proof the concept of Identity Based Encryption and to demonstrate the wellness of Identity Based Encryption by using it to provide completeness, eligibility, unreusability and privacy in web-based voting application.

b) To improve the completeness of a web-based voting application by providing a confirmation SMS to verify the status of the ballot of it is being counted.

c) To computerize and modernize the voting process and therefore boosting voter turnout.

d) To study whether or not Identity Based Encryption can be used as a means to provide digital signature.

1.2 Scope

The project scope is to deliver a secured web-based voting application which can authenticate the voter using Digital Signature via Identity Based Encryption and also encrypt the key of encrypted ballots (block cipher will be used to encrypt the submitted ballot) using the Identity Based Encryption to provide integrity and

confidentiality. This project will only focus on the security aspect of the authentication of the voter and the encryption (privacy) of the ballots. Refer to the project assumption regarding other security issues.

a) Target User Group

- Voters of any non-governmental election
- Organizing committee for any non-governmental election
- Campus election, company election, board election, membership election

b) Modules to be developed

- Voter registration module
- Voting module
- Ballots IBE encryption/Decryption module
- Ballot Server Panel
- PKG (Private Key Generator) Server Panel
- Ballots tabulation module
- Infrared SMS Module
- Database

c) The system will be able to perform the following tasks

- Detection on multiple ballots for same voter
- Ballot casting interface
- Error Handling in ballot casting
- Ballot encryption using Identity Based Encryption

- Ballot decryption using Identity Based Encryption
- Confirmation SMS via infrared
- Key Pair management task
- Tabulation and analysis of ballots from the ballot server

d) Assumption

- The security of the IBE Privet Key will be of the responsibility of the keeper itself and it is assumed that it will be safe with the keeper.

1.3 Project Significance

The issue of web-based voting application has caused much debates from all parties whether opponent or proponent. The security aspect is the reason. Among those security aspects concerned were the integrity and privacy of the ballot and also the voter authentication. Despite these issues, web-based voting is inevitably making its way to this modern community, where everything and anything is making its queue to be computerized and modernize. With this project, it is hoped that the security measures in the prior mentioned aspect can be enhanced with the use of Identity Based Encryption.

Currently, it can be concluded that most of the existing web-based voting application make used of the traditional PKI. The drawback of this approach is the management of the public key and certificates. To manage these large databases of public key and certificates, the cost of infrastructure will be increased, the

maintenance of the database is required where it is often complicated, plus the storage it is required to store the database has to be taken into consideration. However, with the Identity Based Encryption all the above problem is solved as the need of certificates it eliminated. Hence, the question of storing the list of public key and certificates is no more applicable and necessary in the IBE scheme.

Identity Based Encryption is the brand new approach of encryption. It eliminates the use of certificates and it provides the flexibility which other Public Key Encryption could not. Identity Based Encryption is still very new where its implementation is rarely to be seen. Therefore, it would be an achievement if it can be successful integrated into the web-based voting application.

1.4 Expected Output

The expected output of this project will be a web-based voting application, which makes use of Identity Based Encryption to provide completeness, eligibility, unreusability, and privacy.

Identity Based Encryption will be used in this web-based application to eliminate the use of certificates which was being used in the traditional PKI to verify the public keys. It is expected to prove that Identity Based Encryption can be integrated into the web-based voting application as a means of provide cryptographic services. At the same time, by using Identity Based Encryption, the cost of infrastructure will be decreased as the storage and maintenance needed for the certificates and public key database is not necessary in the identity Based Encryption scheme.

The completed output of this project is expected to be able to authenticate the voter using digital signature via Identity Based Encryption. With the implementation of the digital signature, the eligibility of the web-based voting application will be enhanced by not only depending on the login id and login password. By using Identity Based Encryption, the unreusability of the web-based voting application is also provided. This is because the unique identity of the voter for example national identification number will be taken as the identity for verifying it is indeed the repeating person. At the same time, the identity will be the public key and the public key itself is the certificate.

As is overall, the wellness of Identity Based Encryption will be demonstrated in this application.

1.5 Conclusion

The main issues with the development of a web-based voting application revolve around the security risks and measures. Many were worried about the authentication, privacy, and integrity of the application. Most of the debates regarding the web-based voting application focus on the usage on the public governmental election.

Many feels that the current security aspects of the web-based voting application have not reach a standard where it can be entrusted to handle the public governmental election. It is still under the testing phase in the advanced country. Therefore, the scope of this project will focus on non-governmental use.

The objective of this project is to enhance the security measures of the web-based voting application especially on the voter authentication and ballots privacy and integrity by using Identity Based Encryption. Another objective of the project is to present the wellness of Identity Based Encryption comparing to other encryption method. The uniqueness of Identity Based Encryption can provide a lot of functions in the security aspects with more flexibility.

It is hoped that with the completion of this project, the application of web-based voting can be proved as feasible with the help of Identity Based Encryption.