A NOVEL ELLIPTIC CURVE BASED MULTI-KEY ENCRYPTION METHOD FOR MULTICASTING SINGLE CONTENT WITH ACCESS CONTROL

TMKK Jinasena[1], RGN Meegama[2], and RB Marasinghe[3]
[1,2]Department of Computer Science, University of Sri Jayewardenepura,
[3]Department of Medical Education and Health, University of Sri Jayewardenepura,
[1]kasunkosala@yahoo.com

Abstract- The most remarkable invention in the history of cryptography is the invention of public key encryption in the 1970s. It enables users to have a single encryption on a pair of two unique keys. As a result, the way of delivering many security services has changed drastically. Moreover, it introduced new features such as non-repudiation to the cryptographic world. However, in this paper, we present a novel elliptic curve based multi key encryption method to facilitate a single encryption for multiple users where the resulting encrypted content can be multicast to them with access control. Initially, we establish an elliptic curve based public key infrastructure to cover the whole user space. Then the sender can select multiple recipients using their public keys with the desired access levels and generate a unique polynomial for that using the Lagrange polynomial interpolation. Next, the content is encrypted using the generated polynomial and multicast it to the recipients. Finally, the recipient can use their private key together with the polynomial to decrypt the received content. Encryption is robust because the elliptic curve cryptography is stronger than the present RSA encryption. Moreover, it is more suitable for mobile devices due to small key sizes. However, the cryptographic libraries have to be improved and optimized in order to make it practical. Further, the applications like email clients, media players, document viewers have to be enhanced to integrate this cryptographic mechanism as an add-on.

Keywords- Elliptic Curve, Multi-key Encryption, Access Control

I. INTRODUCTION

Encryption plays an important role in computer security. With the modern human civilization going back to well over 4000 years, a significant improvement has happened with the use of computing devices for cryptography in the 20th century. With the invention of public key cryptography in 1970's, a set of new dimensions have been added to the field of computer security resulting in significant variation in the way of delivering authentication, integrity verification, key distribution, non-repudiation, digital certificates, etc. With the advent of mobile technology in the recent decade, people meet each other virtually to accomplish their personal and professional tasks. When conducting such virtual meetings over public networks such as mobile and internet, people need to have a robust and secure mechanism that ensures privacy. It has always been a challenge to enforce access control on digital contents especially in a dynamic multi user environment where fixed roles do not exist. However, an encryption method that can open using multi keys separately has not been found yet. In this paper, we present such an encryption method based on existing elliptic curve encryption which will allow users to multicast the same content to multiple users with a single encryption. In this scenario, each recipient has the capability to decrypt the message using his/her private key if permission to access the key has already been granted. Moreover, it will be a robust, fool-proof technology that can be used in devices such as mobile phones that utilizes less computing power.

Another advantage of the technique is its ability to encrypt large contents such as medical images efficiently. (Abdalla, Shavitt & Wool 2000; Armstrong 2006; Ausanka-Crues 2001; Edge & O' Donnell 2016; Godwin 2004; Hazarika 2012; Yao, Lee & Nam 2009; Dahlman 2014).

II. BACKGROUND

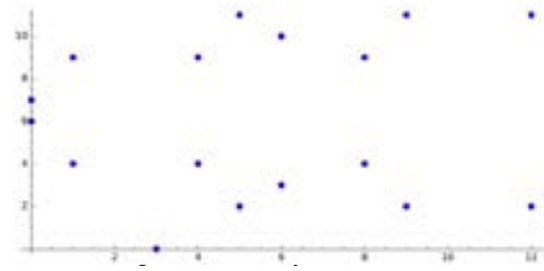
The application of this research is to facilitate medical image encryption in a peer-to-peer real-time mobile collaborative discussion sessions over public accessible mobile networks. Certain mobile apps such as OsiriX, Mobile MIM, etc. allow people to share medical images via public networks. In the recent past, experiments have been carried out to investigate about the privacy and security of sensitive medical data transmitted through unsecured public networks. Moreover, some have used public key cryptography to provide security services such as authentication, integrity verification, non-repudiation, key sharing, etc. Contents were sharing using client server architecture rather than peer-to-peer architecture. Though some of the applications provide role base access control, none of the applications provides multi-key access control mechanisms as present in this research. Further, this research presents the design and implementation of peer-to-peer real-time communication over public mobile networks. (Zhang 2011; Xiaoqin & al 2012; Patel & Bansode 2012).

A. Digital Rights Management

Digital rights management (DRM) is the field where it forces access control policies such as view, save, edit, delete, and distribute digital contents such as eBooks, audio& video songs, films, computer games, cable and satellite televisions, and software CD & DVDs on its users. Though it is not universally accepted, it is necessary to have such a mechanism to protect copy rights as we do with other physical materials. Otherwise it would be difficult for digital content providers to generate revenue from their digital properties as they expect. Thus, digital content providers such as Microsoft, Son, Apple, etc. have tried various techniques over the years and could not be found a strong standard method. Microsoft has tried ten versions of Microsoft Media DRM before 2005 and failed all within a few months. However, the Sony has used an Elliptic curve based DRM to protect SonyPlay Station 3. But it was also cracked within short time due to an issue of its random number generator. Moreover, iTune is enforcing access control on their digital music files. Thus, it limits the number of songs a user can play. (Armstrong 2006; Hazarika 2012; Yao, Lee & Nam 2009; Zhang 2011; Perlman & al 2010).

B. Finite Fields and Elliptic Curves

Numerical computations may contain some round-off errors due to its limitations in floating point representations. However, in cryptography it is not possible to have such errors. As a result, finite fields have been used for most of the cryptographic works. On the other hand, the raising computing power has threatened the existing RSA public key cryptosystems. Therefore, in this research, the novel elliptic curve cryptosystem based on elliptic curve discrete logarithm problem is used. Figure 1 shows the elements of finite field in (Dawahdeh & al 2015; Goo & Lee 2015; Jager & al 2015; Goo & Lee 2015; Joye 2016; Soleymani & al 2013; Boruah & Saikia 2014; Yang & al 2012).



C. Android, Sponge Castel Library and OpenSSL

Android is the most popular mobile platform among the Sri Lankan people today. It is based on Java and Java provides a partially developed cryptographic library for its users. However, the in-built libraries in Java are not sufficient for cryptographic works described in this research. Therefore, a Java based, open source cryptographic library called Sponge Castel has been used to do the cryptographic works within the Android application. Apart from that, a free and open source cryptographic library called OpenSSL has been used to do the other cryptographic works describe in this research. It is mainly used for key generation, signing, verification, and digital certificate management (Bernstein & al 2012; Gozalvez 2015; Zhou & al 2007; Pancholi & Patel 2016; McIntosh 2015).

D. Polynomial Interpolation

Polynomial interpolation is used to find the polynomial that goes through a set of selected points on a space. Though there are several methods to find the interpolated polynomial of a given set of points, the resulting polynomial will not be the same for all the methods (Liu & al 2016; Krishna & al 2016; Perlman & al 2010). Moreover, the Lagrange interpolation takes linear time to find coefficients whereas the Newton interpolation takes quadratic time to do the same. Thus, the Lagrange method for polynomial interpolation is theoretically efficient than the other methods. Moreover, it is a simple algorithm and can be implemented easily. However, in practice, it is not the most efficient algorithm due to its large number of floating point calculations. Besides, researchers have found methods to interpolate a given set of points without passing through specific points if needed. Equation 1 shows the Lagrange interpolation method.

$$p(x) = L_1(x)y_1 + L_2(x)y_2 + \cdots L_N(x)y_N$$

$$L_k(x) = \frac{(x-x_1)(x-x_2)\ldots(x-x_{N-1})(x-x_N)}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{N-1})(x_k-x_N)}$$

Except;

$(x = x_k)$ *in the numerator and* $(x_k = x_k)$ *in the denominator*

Equation 1. Lagrange polynomial interpolation method

III. METHODOLOGY

First, the architecture of the system was designed. It consists of three main components namely mobile application, servers, and security infrastructure. The mobile application is mainly responsible for applying secure mechanism for access control on digital data and facilitating peer-to-peer video conferencing. Severs are used to store medical images and establish peer-to-peer communications. Finally, the security infrastructure defines the customized public key infrastructure and the proposed access key algorithm.

A. Collaborative Mobile Application

First, by considering the most popular platform of the users, Android has been chosen as the development language of the mobile application. Then a mobile application with collaborative tools was developed to share medical images over the public mobile network. Tools such as real-time video conferencing, interactive whiteboard for real-time collaborative drawings, viewing, zooming, and rotating medical images were developed to facilitate collaborative discussions.

B. File and Application Servers

Medical images were stored in a remote server. L2TP VPN was configured in order to so that the Android Mobile users are allowed to connect to the server over VPN connections and access images securely.

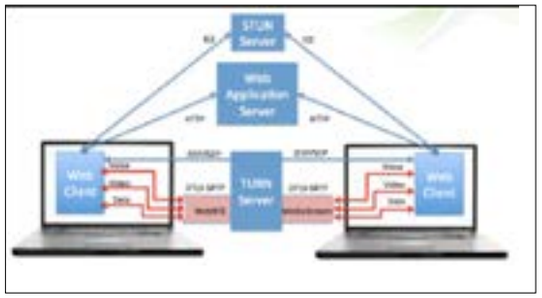


Figure 3. WebRTC server communications
Source: https://bincoder.com/category/webrtc/

Peep-to-peer communications cannot be directly achieved over the public mobile networks due to their local IP addresses. However, if two parties can share their public IP address, then they can communicate with each other directly and securely by opening a VPN tunnel between them. Thus, a third party the WebRTC server has been used to establish the VPN tunnel between peers. Thereafter, peers can do real-time video conferencing and content sharing securely over the public mobile network. Figure 3 shows how the STUN and TURN servers help to establish a real time peer-to-peer communication between peers.

C. Public Key Infrastructure

This method uses the customized public key infrastructure. It is based on the novel elliptic curve cryptography instead of the present RSA encryption. Thus, it is robust and future proof. However, since it is new, not many tools have developed for it yet. Moreover, most of the stakeholders do not have much technical exposure. Therefore, they cannot use command line well. Thus, a Java based GUI tool was developed to manage digital certificates and its associated operations such as generating keys, generating certificate requests, signing certificates and documents, verifying certificates and documents, renewal and etc. Certificate authority hierarchy was established and the certificates were issued to all the stakeholders. However, the libraries are not optimized. Thus, the efficiency of the algorithms cannot be achieved as expected.

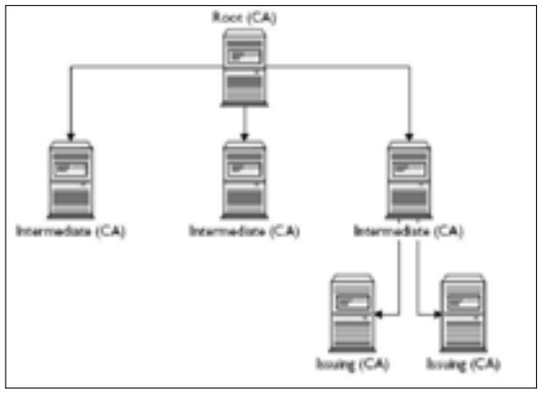


Figure 2. Public key infrastructure
Source: http://www.vce-download.net/study-guide/comptia-networkplus-11.6-remote-access-procedures2.html

D. The Proposed Multi-key Access Control Mechanism

The proposed multi-key encryption algorithm is consisting of four main steps as follows.

1) **Curve Parameters and Modulo Arithmetic:** Once an elliptic curve is chosen, the curve parameters will be extracted and elliptic curve arithmetic will be implemented. Next, the modulo arithmetic operations will be implemented for the chosen number. Moreover, a new user defined data type will be used to handle big integers.

2) **Public Keys and Polynomial Generation:** When a digital content is multicast, it's authorized users and their access levels will be chosen. Their elliptic curve public keys will be extracted from their digital certificates and interpolated polynomial will be generated using the Lagrange interpolation method. $P(x) = ax^3 + bx^2 + cx + d \ mod \ p$ shown in the Equation 2. Figure 4 shows an interpolated polynomial using Lagrange interpolation method.

Equation 2. Generic format of the polynomial

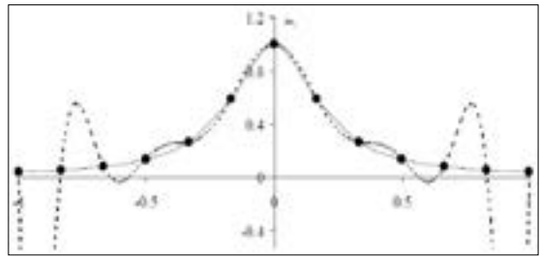


Figure 4. Interpolated polynomial
Source: https://melissacabral.wordpress.com/ 2009/11/29/ lagrange-interpolating-polynomial-2/

3) **Secret Session Key Generation and Encryption:** The generated Lagrange interpolated polynomial will be used to generate a temporary secret session key. This key will be used to encrypt the content that wanted to be multicast using the AES symmetric key algorithm. Thus, it becomes more efficient and robust.

4) **Regenerate the Secret Session Key and Decryption:** Recipients will be used their private key and the received polynomial to regenerate the session key that used to encrypt the content. Thereafter, the obtained AES symmetric is used to decrypt the content and view it the mobile application. Because the content is decrypted with the mobile application, the end users will not be able to access the original content and reuse it as they wish.

IV. RESULTS AND DISCUSSION

A mobile application has been developed for real-time secure video conferencing and medical image sharing. Figure 5 shows a screenshot of the video conferencing app.

Theoretically, a successful multi-key encryption mechanism has been developed. However, due to lack

Figure 5. Video conferencing app

of well-established libraries and standards, the proposed secure mechanism could not be tested practically. For example, a basic computation such as addition should support addition of very large integers, elliptic curve group addition, and modulo arithmetic within a mobile device. However, it is based on the solid mathematical concepts and future proof technologies. These missing libraries will be developed in the future. Thus, there is a high probability of being used it in the near future.

V. CONCLUSION

The necessity of digital rights managements, historical attempts of DRM and their failures have been presented. The challenges of implementing access control in a multi user domain have been identified and emphasized. The proposed secure algorithm will be able to provide multi-key encryption mechanism to enable the access control in a multi user environment. The technical limitations and lack of supporting libraries have been identified and published for the benefit of future researches and the field. Further the end user applications such as email clients, media players, document and image viewers, etc. have to be enhanced in the future to support this secure mechanism as an add-on. However, a theoretical model of a successful, novel, future proof and robust access control mechanism has been invented and presented in this research.

REFERENCES

Abdalla, M, Shavitt, Y & Wool, A 2000, 'Key management for restricted multicast using broadcast encryption', *Networking, IEEE/ACM Transactions on*, vol 8, no. 4, pp. 443-454.

Armstrong, TK 2006, 'Digital rights management and the process of fair use', *Harvard Journal of Law & Technology*, vol 20, p. 49.

Ausanka-Crues, R 2001, 'Methods for access control: Advances and limitations', *Harvey Mudd College*, vol 301.

Bernstein, DJ & al, E 2012, 'High-speed high-security signatures', *Journal of Cryptographic Engineering*, vol 2, no. 2, pp. 77-89.

Boruah, D & Saikia, M 2014, 'Implementation of ElGamal Elliptic Curve Cryptography over prime field using C', *Information Communication and Embedded Systems (ICICES)*, 2014 International Conference on.

Dahlman, EAMGAPSAEA 2014, '5G wireless access: requirements and realization', *IEEE Communications Magazine*, vol 12, no. 52, pp. 42--47.

Dawahdeh, ZE & al, E 2015, 'Modified ElGamal Elliptic Curve Cryptosystem using Hexadecimal Representation', *Indian Journal of Science and Technology*, vol 8, no. 15.

Edge, C & O' Donnell, D 2016, 'Introduction to Cryptography', in *Enterprise Mac Security*, Springer.

Godwin, M 2004, 'What Every Citizen Should Know About DRM', *Public Knowledge New America Foundation, Washington*.

Goo, E-H & Lee, S-D 2015, 'Reconfigurable real number field elliptic curve cryptography to improve the security', *Journal of Computer Virology and Hacking Techniques*, vol 11, no. 3, pp. 123-128.

Gozalvez, J 2015, '5G Tests and Demonstrations [Mobile Radio]', *Vehicular Technology Magazine, IEEE*, vol 10, no. 2, pp. 16--25.

Hazarika, SS 2012, 'Digital Rights Management: A Restrictive Rather than a Defensive Mechanism and the Survival of the 'Fair Use' Doctrine', *Available at SSRN 2180305*.

Jager, T & al, E 2015, 'Practical invalid curve attacks on TLS-ECDH', *Computer Security--ESORICS 2015*, pp. 407-425.

Joye, M 2016, 'Secure ElGamal-Type Cryptosystems Without Message Encoding', *in The New Codebreakers,* Springer.

Krishna, CV & al, E 2016, 'Design Implementation of Composite Field S-Box using AES 256 Algorithm', *International Journal of Emerging Engineering Research and Technology (IJEERT)*, vol 3, no. 12, pp. 43-51.

Liu, X & al, E 2016, 'A Secure Medical Information Management System for Wireless Body Area Networks', *KSII Transactions on Internet & Information Systems*, vol 10, no. 1.

McIntosh, C 2015, 'Cyber-security: Who will provide protection?', *Computer Fraud & Security,* vol 2015, no. 12, pp. 19-20.

Pancholi, VR & Patel, BP 2016, 'Enhancement of Cloud Computing Security with Secure Data Storage using AES', *International Journal for Innovative Research in Science and Technology*, vol 2, no. 9, pp. 18-21.

Patel, JR & Bansode, RS 2012, 'Hybrid Security Algorithms for Data Transmission using AES-DES', *International Journal of Applied Information Systems (IJAIS)*, vol 2, no. 2, pp. 15-21.

Perlman, R & al, E 2010, 'Privacy-preserving DRM', *Proceedings of the 9th Symposium on Identity and Trust on the Internet*, ACM.

Soleymani, A & al, E 2013, 'A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field', *Journal of Image and Graphics,* vol 1, no. 1.

Xiaoqin, L & al, E 2012, 'Application of the Advanced Encryption Standard and DM642 in the image transmission system', *Computer Science Education (ICCSE), 2012 7th International Conference on*.

Yang, CAO & al, E 2012, 'One ECDH key agreement scheme with authentication based on ECDLP', *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, vol 1, no. 24.

Yao, J, Lee, S & Nam, S 2009, 'Privacy preserving DRM solution with content classification and superdistribution', *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, IEEE.*

Zhang, X 2011, 'A survey of digital rights management technologies', *last modified: Nov*, vol 28, pp. 1-10.

Zhou, Y & al, E 2007, 'Access control in wireless sensor networks', *Ad Hoc Networks*, vol 5, no. 1, pp. 3-13.