UNIVERSITI PUTRA MALAYSIA

A MODIFIED GROUP AUTHENTICATION SCHEME FOR MACHINE TYPE COMMUNICATION IN LTE/LTE-A NETWORKS

HAQI KHALID ISMAIL

FSKTM 2018 75

A MODIFIED GROUP AUTHENTICATION SCHEME FOR MACHINE TYPE COMMUNICATION IN LTE/LTE-A NETWORKS

By

HAQI KHALID ISMAIL

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

September 2018

COPYRIGHT

DEDICATIONS

To all of my loved one!!

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

A MODIFIED GROUP AUTHENTICATION SCHEME FOR MACHINE TYPE COMMUNICATION IN LTE/LTE-A NETWORKS

By

HAQI KHALID ISMAIL

September 2018

Chairman : **Kweh Yeah Lun**
Faculty : **Computer Science and Information Technology**

Machine-Type Communication (MTC), as one of the essential advancements of wireless communication, has become a new business development in mobile communication. Meeting the necessities of control usage of devices and mass implement transmission is a key issue in the implementation of MTC in the Long Term Evolution/Long Term Evolution Advanced systems. Likewise, an authentication scheme is the most important piece of the system as MTC is one of the procedures that suffers under group authorization requests. The emphasis of this research is on MTC of group authentication scheme in an LTE/LTE-A network that is based on a pairing-based cryptography in order to obtain a highly efficient scheme that lessens signalling congestion. In this research, an authentication scheme has been modified to enhance the performance of group authentication in an LTE/LTE-A network. High signalling congestion occurs during the verification phase since every MTC device needs to go through a full authentication process. The computation of the relevance cryptographic operations such as pairing, hashing, multiplication and XOR operations consumes time especially when a large group of MTC devices requests access to the LTE/LTE-A network simultaneously. Then, the Home Subscriber Server (HSS) verifies every request message, generates group pairing and even calculates the system keys (both private and public). Thus, an accumulation of a big number of MTC devices in a simultaneous authentication process is the main factor that causes signalling congestion as the computation requires time to authenticate the LTE/LTE-A network. Therefore, this research proposes a modified group authentication scheme for MTC in an LTE/LTE-A network in order to reduce signalling and computational overheads. The proposed method adopts two efficient algorithms, namely, the Encapsulated Double and Add algorithms which depend on the Tate Pairing form by the bilinear pairing cryptography. In the improved group authentication scheme, which has been modified, the dominance

of the signalling/computational overhead time is acknowledged. The derived results indicate that the proposed approach has successfully lessened congestion problems up to 40 % in terms of computation and up to 30 % in terms of signalling overhead. In addition, the MTC devices can verify and complete a simple exchange AKA with the network. The two performance metrics used in the study are signalling overhead and computation overhead.

Abstrak tesis yang dikemukakan kepada kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan ijazah Sarjana Sains

Skim Pengesahan Kumpulan Terubah Suai Komunikasi Jenis Mesin dalam Rangkaian LTE/ LTE A

Oleh

HAQI KHALID ISMAIL

September 2018

Pengerusi : **Kweh Yeah Lun**
Fakulti : **Sains Komputer dan Teknologi Maklumat**

Komunikasi Jenis Mesin (MTC) sebagai salah satu kemajuan penting komunikasi tanpa wayar telah berkembang menjadi suatu perniagaan baru dalam komunikasi mudah alih. Memenuhi keperluan penggunaan kawalan peranti dan melaksanakan transmisi besar-besaran merupakan isu utama dalam pelaksanaan MTC dalam sistem Evolusi Jangka Panjang/ Lanjutan Evolusi Jangka Panjang. Selain itu, skema pengesahan juga adalah bahagian penting sistem ini kerana MTC merupakan salah satu prosedur yang terlibat dalam permintaan pengesahan kumpulan. Penyelidikan ini memberi penekanan pada skema pengesahan kumpulan MTC dalam rangkaian LTE / LTE-A yang berdasarkan pada kriptografi berasaskan pasangan untuk mendapatkan skema yang berefisien tinggi, yang mengurangkan kesesakan pengisyaratan. Dalam kajian ini, skema pengesahan telah diubah suai bagi meningkatkan prestasi pengesahan kumpulan dalam rangkaian LTE/ LTE-A. Kesesakan isyarat yang tinggi berlaku dalam fasa penentusahan kerana setiap peranti MTC perlu melalui proses pengesahan penuh. Penghitungan kerelevanan operasi kriptografi seperti berpasangan, pencincangan, pendaraban dan operasi XOR memerlukan masa lama terutama apabila sekumpulan besar peranti MTC memohon akses ke rangkaian LTE / LTE-A secara serentak. Seterusnya, Pelayan Pelanggan Rumah (HSS) menentusahkan setiap mesej permintaan, menjana pasangan kumpulan dan juga mengira kekunci sistem (untuk kedua-dua peribadi dan awam). Akibatnya, pengumpulan sejumlah besar peranti MTC dalam proses pengesahan serentak menjadi faktor utama yang menyebabkan kesesakan isyarat kerana pengiraan memerlukan masa untuk menentusahkan rangkaian LTE / LTE-A. Oleh itu, kajian ini mencadangkan skema pengesahan kumpulan yang terubah suai untuk MTC dalam rangkaian LTE / LTE-A bagi mengurangkan overhed pengisyaratan dan pengiraan. Kaedah yang dicadangkan menggunakan dua algoritma yang cekap, iaitu, algoritma Kembar Terkapsul dan algoritma Tambah

yang bergantung pada Pasangan Tate yang dibentuk oleh kriptografi pasangan biliner. Dalam skema pengesahan kumpulan yang ditambah baik, dan yang telah diubah suai, kuasa pengisyaratan / masa overhed pengiraan diambil kira. Keputusan yang diperoleh menunjukkan bahawa pendekatan yang dicadangkan telah berjaya mengurangkan masalah kesesakan sehingga 40% dari segi pengiraan dan sehingga 30% dari segi overhed pengisyaratan. Selain itu, peranti MTC dapat menentusahkan dan melengkapkan pertukaran AKA mudah dengan rangkaian. Kedua-dua metrik prestasi yang digunakan dalam kajian ini adalah overhed pengisyaratan dan overhead perhitungan.

ACKNOWLEDGEMENTS

First, all thanks, praises, and gratitude to the omnipotent Allah, who has favored me with the valuable bounties during my life and has given me the physical and mental power that empowered me to be what I am, I would like to express my deep gratitude after God almighty in the accomplishment of this thesis to my supervisor Dr. Kweh Yeah Lun for his time, encouragement, exceptional support, guidance, and fruitful discussion. Big thanks to my thesis committee supervisors Prof. Mohamed Othman, and Dr. Idawaty Ahmad for their effort to review my work and provide me with their comments. Finally, I would eternally thankful to my parents for their encouragement, help and for their psychological and material support during these two years. I would like to dedicate this success to my dear parents who provided me moral and material support during this period without them, I would not be here today. My God offers wellbeing and bliss to all of them.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.The members of the Supervisory Committee were as follows:

Kweh Yeah Lun, Ph.D
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Mohamed Othman, Ph.D
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Idawaty Ahmad, Ph.D
Senior lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH YUNUS , Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work;
- Quotations, illustrations and citations have been duly referenced;
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- Intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- Written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature:_____ Date:_____

Name and Matric No: Haqi Khalid Ismail, GS44266

Declaration by Members of Supervisory Committee

This is to confirm that:

- The research conducted and the writing of this thesis was under our supervision;
- Supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of Supervisory Committee
Kweh Yeah Lun

Signature: _____
Name of Member of Supervisory Committee
Mohamed Othman

Signature: _____
Name of Member of Supervisory Committee
Idawaty Ahmad**.**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

LTE	Long Term Evolution
LTE-A	Long Term Evolution advanced
MTC devices	Machine Type Communication Devices
M2M	Machine To Machine
eNB	Evolved Node B
MME	Mobile Management Entity
S-GW	Serving Gateway
HSS	Home Subscriber Server
P-GW	Packet Data network Gateway
UE's	User Equipment's
3GPP	Third Generation Partnership Project
DPG	Dynamic Peer Group
AKE	Authentication Key Exchange
MS's	Mobile Stations
HN	Home Network
SN	Serving Network
AKA	Authentication Key Agreement
G-AKA	Group Authentication Key Agreement
mGAP	Mobile Group authentication Protocol
HD	Home Domain
ABAKA	Anonymous Batch Authentication Key Agreement
DGB-AKA	Dynamic Group Based Authentication Key Agreement
ECDH	Elliptic Curve Diffie-Hellman
SEGR	Secure and Efficient Group
DGB-AKA	Dynamic Group-Based Authentication Key Agreement
LGTH	Lightweight Group Authentication Protocol
OBU's	On-board Units
ECPP	Efficient Conditional Privacy-Preservation
BS	Base Station
RSU's	Roadside Units
DoS	Denial of Service
M-AKA	Mutual Authentication and Group Key Agreement
DDH-Based	DDH-Based Group Key Agreement
GKA-MDDC	Group Key Agreement Protocol-Mobile Devices in Different Cells
AEP-MC	Authenticated Encryption Protocol- Mobile Communication
M-GAP	Mobile Group Authentication Protocol
ECPP	Efficient Conditional Privacy Preservation Protocol
CAA-MTC	Congestion Avoidance Algorithm-Machine Type Communication
AB-AKA	Anonymous Batch Authenticated and Key Agreement
EGBHA	Efficient Group-Based Handover Authentication
EHAPP	Efficient Handover authentication with privacy preservation
DGBAKA	Group Based Authentication and Key Agreement
EG-AKA	EAP-Based Group Authentication and Key Agreement

MTC-AKA	Machine Type Communication Authentication and Key Agreement
SEGR	Secure and Efficient Group Roaming
GAHAP	Group-based Anonymity Handover Authentication Protocol
UGHA	Uniform Group-based Handover Authentication
GBAAM	Group-Based Access Authentication for MTC
SEAP	Secure and Efficient Authentication Protocol
UE	User Equipment
IMS	IP Multimedia System
IMSI	International Mobile Subscriber Identity

CHAPTER 1

INTRODUCTION

This chapter outlines the group authentication protocols of Machine- Type Communication in LTE/LTE-A networks to provide an understanding of the concept of the work and to determine the requirements that enable the system to provide better performance. This chapter describes the motivation of the framework in Section 1.1. Section 1.2 states the problem statements, followed by Section 1.3 which lists the thesis research questions. The objectives of this work are stated in Section 1.4. Section 1.5 presents the scope of the present thesis, followed by Section 1.6, which summarizes the main contributions of the thesis. Finally, Section 1.7 outlines the organization of the thesis.

1.1 Background

Nowadays, among of the various techniques in applications communication networks with numerous utilizations, one of the most important techniques is the Machine-Type Communication in LTE/LTE-A networks. Machine-Type Communication (MTC) has excellent efficiency in applications and networks that have a big effect on the system, also known as (M2M) Machine-To-Machine (Alam et al. (2014); Lai et al. (2015)). Also, MTC has driven extensive scale constant system applications according to its small authority, small cost and no human obtrusion, which lead to automatic metres, monitoring and smart homes Lai et al. (2015). Additionally, MTC devices are widely applied in manufacturing and factories for the Third-Generation-Partnership Project (3GPP) because they are consistent with this platform Lai et al. (2013). To support MTC, 3GPP administrator needs to oblige by its system to sustain a substantial number of MTC devices, which can over-burden system assets and present congestion in the system at both the information and control planes (Lai et al., 2013). Generally, authentication signalling congestion problems become prevalent in the MTC technique, especially when the set of MTC devices needs to be admitted to the network simultaneously under the traditional authentication protocol (e.g., EPS-AKA). As a result, this causes the authentication protocol to face significant signalling overhead (Lai et al., 2013). However, there are a few schemes more vulnerable to network access delay and signalling overhead in a set of communications as each full authentication procedure must incorporate an MTC device with a home authentication server (Lai et al., 2014). UGHA or Uniform Group-based Handover Authentication is offered for several MTC devices using the signature and total (AMAC) strategies, making it suitable for all mobility platforms in LTE/LTE-A in 3GPP

standard (Sun et al., 2016). Figure 1.1 demonstrates the MTC Engineering of the LTE/LTE-A systems. This model joins Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Evolved Packet Core (EPC) and the extant radio framework. Also, a greater part of Machine-Type Communication devices and base stations, also referred to as eNodeBs (eNBs) contained in the E-UTRAN, the shared MTC, are prepared to connect with each and with every eNB. Mobile Management Entity (MME), Home Subscriber Server (HSS), Serving Gateway and (P-GW) Packet Data Network Gateway are all included in EPC. For the most part, the network sends signalling traffic and client data utilising MME and S-GW. The reservation data about MTC devices are included in HSS while HSS produces authentication vectors to help MME verify MTC devices (Fu et al., 2016). The reason is that each device must perform a full AKA authentication system with home confirmation servers so that verification signalling in the network will increase. Meanwhile, the overload of home authentication servers will increase as the authentication vectors are produced (Lai et al., 2013). As mentioned above, the group authentication protocol is important to internet usage as attacks, and threats to the network system may cause impairment in the protocol. This may become the main reason for signalling issues. An extensive number of MTC devices getting to the system at the same time will bring about a serious authentication signal bottleneck (Lai et al., 2013).

With a wide variety of possible applications, numerous model discussions and associations have created and improved the present advances to empower the MTC applications. Specifically, the third Generation Partnership Project (3GPP) is winding up plainly and progressively dynamic with a few things characterised on MTC, particularly for Long Term Evolution (LTE/LTE-A) networks (Cao et al., 2015a). Recent years have seen a colossal development of mobile client populace and interactive media benefit, which are followed by a serious over-burden issue in cell networks. Device to-Device (D2D) communication has been proposed as a promising information offloading arrangement and range productivity upgrade strategy because of its inalienable attributes, e.g. enhancing asset usage, upgrading client's overhead, amplifying battery lifetime etc. (Bresson et al., 2001). The reason for the MTC innovation is to empower machinery and equipment networking and communication capacity which is the primary method for the Internet of Things (IoT). The authentication signalling problems are due to requests of a large number of MTC devices in light of the fact that each MTCD needs an autonomous comprehensive access authentication process with the centre system, which may bring about genuine signals bottleneck in the centre system (Fu et al., 2016).

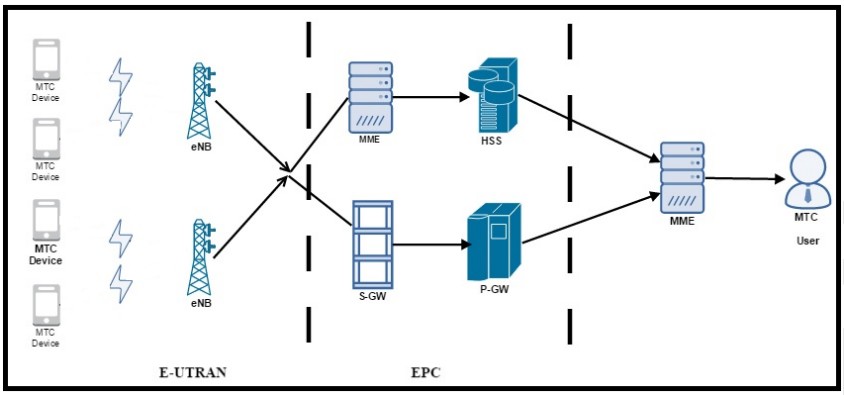

Figure 1.1: The model of Machine Type Communication in an LTE/LTE-A network.

1.2 Research Problem

In recent years, several works have focused on group authentication protocol for the MTC devices over the Long term evolution networks to provide simultaneous authentication of group devices. In spite of the optimized schemes of MTC communication, there are several problems concerning MTC devices accessing cellular networks. One of the problems is signalling overhead used in Machine Type Communications to achieve synchronization and resolve contention can be much larger than the size of actual user data packet. More challenges is the network congestion, including signalling congestion, the congestion takes place when a large number of devices are attached to a single e-NodeB. As described in Fu et al. (2016), the number of MTC devices within a cell can be significantly large, e.g., thousands of devices accessing a single base and simultaneously. The system will suffer from severe congestion if these devices try to transmit to e-NodeB within a short period of time. In Fu et al. (2016), it discussed that Machine Type communication related signalling congestion and overhead can be caused by:

- A large number of MTC with low-power consumption requirements simultaneously requests access to the LTE/LTE-A networks, each MTC device needs an independent complete access authentication process with core network.
- High computational overhead caused while verifying every group of MTC devices before gets authentication access with network.

The verification of each group may cause high computation when the density of the authentication requests increases, and this requires an execution of a mass

of bilinear pairing operation and primitive cryptographic operations. However, exploiting the bilinear pairing to verify the MTC devices at the first phase of the scheme in accuracy if been used for example in [Fu's scheme] can be largely effect on the network. Because every group of MTC devices have to wait for a full verification process and the computation of the authentication requirements. Therefore MTC devices have to wait for a completed calculation of the parameters values at the first phase of the authentication scheme.

1.3 Research Questions

This thesis proposes an enhancement to the MTC devices group authentication protocol over LTE/LTE-A networks by reducing the computation overhead and achieving less signalling congestion. The proposed scheme attempted to answer the following questions:

- Do Encapsulate Double and Add lines algorithms modify MTC group authentication protocol?
- Does the proposed scheme reduce the computation of the primitive's cryptographic operation and minimise signalling overhead?

1.4 Research Objective

The objective of this research is as follow:

- To propose a modified group authentication scheme for Machine Type Communication in LTE networks, aiming to reduce the signaling and computational overhead.

1.5 Research Scope

This research focuses on group authentication protocol of MTC over LTE/LTE-A net- works which consists of two phases: the initialisation phase and the mutual authentication phase. The main concern of this research is the initialisation phase where enhancement is made by modifying the core function in the initialisation phase to improve the group authentication protocol properties (signalling and computation overhead) and by making the Machine-Type Communication over LTE/LTE-A networks prove to be efficient with a signalling congestion avoidance that is comparable to the signal overhead caused

by the two factors i.e. signalling and computation overhead of the previous schemes. Currently, most of the authentication protocols are using the cryptographic methods to guarantee signaling congestion avoidance. The proposed scheme is classified as a symmetric key cryptography. The proposed modified scheme adopts one of the bilinear map types which is the enhanced Tate pairing over the Jacobian coordinates to improve the group authentication protocol in order to obtain less signalling congestion. The study combined the different performance metrics and parameters that need to be considered when improving the group authentication protocol of MTC over LTE/LTE-A networks. Group authentication protocols, their constraints, applicability, assumptions and enhancement issues related to MTC authentication cryptographic protocols have been recently proposed as seen in a number of surveys.

1.6 Research Contribution

The major contribution of this study is an improvement to the group authentication scheme of Machine-Type Communication over LTE/LTE-A networks. In the proposed approach, the core function of the MTC authentication scheme is modified. By using the double-and-add line algorithms, the authentication protocol will be able to make the protocol's computation better at the computation of the cryptographic operation such as pairing, multiplication, hash and even in the generating of the private/public key. The proposed modified scheme has a big effect on MTC group's authentication especially when a large number of MTC devices send access message to the LTE/LTE-A network simultaneously which causes the network to experience signalling congestion caused by the high signals/computation overhead. A double-and-add algorithms are presented to provide an efficient computation that can enhance MTC group authentication protocol and obtain verification of each MTC device since each device group has its own session key. The following are the contributions of this study:

1. The proposed group authentication protocol can simultaneously authenticate a group of MTCDs by adopting the encapsulated double-and-add algorithms over Tate pairing and aggregate message authentication code which minimises the signal overhead and reduces the computational overhead.

2. The enhanced protocol largely reduces signalling overhead and the burden of eNBs and MME because the MME can verify a group of all MTC devices simultaneously using aggregation technology.

1.7 Organization of Thesis

This thesis is organised into five chapters. Chapter 1 is the introductory chapter while Chapter 2 provides a review of past studies on Machine-type communication over LTE/LTE-A networks. It also discusses related researches that have been conducted recently concerning group authentication protocols on MTC. Chapter 3 presents the methodology used to optimise the system as well as a detailed explanation of its operation and parameters, which is an adaptation of the distribution method. Chapter 4 discusses the results obtained from the implementation of the system. In this study, each implementation was conducted according to the parameters offered by the authentication protocol, and the results were obtained after fixing two of the parameters and adjusting the other for a range of values. Finally, Chapter 5 presents the conclusion and suggestions for future work.

BIBLIOGRAPHY

Alam, M., Yang, D., Rodriguez, J., and Abd-Alhameed, R. A. (2014). Secure device-to-device communication in lte-a. *IEEE Communications Magazine*, 52(4):66–73.

Amokrane, A., Ksentini, A., Hadjadj-Aoul, Y., and Taleb, T. (2012). Congestion control in the context for machine type communication. In *IEEE International conference on communication (ICC) Ottawa, Canada*.

Ateniese, G., Steiner, M., and Tsudik, G. (2000). New multiparty authentication services and key agreement protocols. *IEEE journal on selected areas in communications*, 18(4):628–639.

Barreto, P. S., Kim, H. Y., Lynn, B., and Scott, M. (2002a). Efficient algorithms for pairing-based cryptosystems. In *Annual International Cryptology Conference*, pages 354–369. Springer.

Barreto, P. S., Lynn, B., and Scott, M. (2002b). Constructing elliptic curves with prescribed embedding degrees. In *International Conference on Security in Communication Networks*, pages 257–267. Springer.

Benson, K., Shacham, H., and Waters, B. (2013). The k-bdh assumption family: Bilinear map cryptography from progressively weaker assumptions. In *Cryptographers' Track at the RSA Conference*, pages 310–325. Springer.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Annual International Cryptology Conference*, pages 213–229. Springer.

Boneh, D., Lynn, B., and Shacham, H. (2001). Short signatures from the weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 514–532. Springer.

Bresson, E., Chevassut, O., Essiari, A., and Pointcheval, D. (2004). Mutual authentication and group key agreement for low-power mobile devices. *Computer Communications*, 27(17):1730–1737.

Bresson, E., Chevassut, O., Pointcheval, D., and Quisquater, J.-J. (2001). Provably authenticated group diffie-hellman key exchange. In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 255–264. ACM.

Cao, J., Li, H., and Ma, M. (2015a). Gahap: A group-based anonymity handover authentication protocol for mtc in lte-a networks. In *2015 IEEE International Conference on Communications (ICC)*, pages 3020–3025. IEEE.

Cao, J., Li, H., Ma, M., and Li, F. (2015b). Ugha: uniform group-based handover authentication for mtc within e-utran in lte-a networks. In *2015 IEEE International Conference on Communications (ICC)*, pages 7246–7251. IEEE.

Cao, J., Ma, M., and Li, H. (2012). A group-based authentication and key agreement for mtc in lte networks. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 1017–1022. IEEE.

Cao, J., Ma, M., and Li, H. (2015c). Gbaam: group-based access authentication for mtc in lte networks. *Security and Communication Networks*, 8(17):3282–3299.

Chatterjee, S., Sarkar, P., and Barua, R. (2004). Efficient computation of tate pairing in projective coordinate over general characteristic fields. In *International Conference on Information Security and Cryptology*, pages 168–181. Springer.

Chen, Y.-W., Wang, J.-T., Chi, K.-H., and Tseng, C.-C. (2012). Group-based authentication and key agreement. *Wireless Personal Communications*, 62(4):965–979.

Choi, D., Choi, H.-K., and Lee, S.-Y. (2015a). A group-based security protocol for machine-type communications in lte-advanced. *Wireless Networks*, 21(2):405–419.

Choi, H.-K., Han, C.-K., and Choi, D.-S. (2015b). Improvement of security protocol for machine type communications in lte-advanced. In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1301–1306. IEEE.

Cremers, C. and Feltz, M. (2012). Beyond eck: Perfect forward secrecy under actor compromise and ephemeral-key reveal. In *European Symposium on Research in Computer Security*, pages 734–751. Springer.

De Caro, A. and Iovino, V. (2011). jpbc: Java pairing based cryptography. In *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*, pages 850–855, Kerkyra, Corfu, Greece, June 28 - July 1.

Dong, L. and Chen, K. (2012). *Cryptographic protocol: security analysis based on trusted freshness*. Springer Science & Business Media.

Dutta, R. and Barua, R. (2008). Provably secure constant round contributory group key agreement in dynamic setting. *IEEE Transactions on Information Theory*, 54(5):2007–2025.

El Mrabet, N. and Joye, M. (2017). *Guide to Pairing-Based Cryptography*. CRC Press.

Elenin, S. A. and Kitakami, M. (2011). Performance analysis of static load balancing in grid. *International Journal of Electrical & Computer Sciences IJECS/IJENS*, 11(03):57–63.

Frey, G., Muller, M., and Ruck, H.-G. (1999). The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Transactions on Information Theory*, 45(5):1717–1719.

Fu, A., Song, J., Li, S., Zhang, G., and Zhang, Y. (2016). A privacy-preserving group authentication protocol for machine-type communication in lte/lte-a networks. *Security and Communication Networks*.

Ghavimi, F. and Chen, H.-H. (2015). M2m communications in 3gpp lte/lte-a networks: architectures, service requirements, challenges, and applications. *IEEE Communications Surveys & Tutorials*, 17(2):525–549.

Goldwasser, S. and Bellare, M. (1996). Lecture notes on cryptography. *Summer course "Cryptography and computer security" at MIT*, 1999:1999.

Hankerson, D., Menezes, A. J., and Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.

Izu, T. and Takagi, T. (2002). Efficient computations of the tate pairing for the large mov degrees. In *International Conference on Information Security and Cryptology*, pages 283–297. Springer.

Jiang, R., Lai, C., Luo, J., Wang, X., and Wang, H. (2013). Eap-based group authentication and key agreement protocol for machine-type communications. *International Journal of Distributed Sensor Networks*, 2013.

Joux, A. (2000). A one round protocol for tripartite diffie–hellman. In *International Algorithmic Number Theory Symposium*, pages 385–393. Springer.

Jung, K.-R., Park, A., and Lee, S. (2010). Machine-type-communication (mtc) device grouping algorithm for congestion avoidance of mtc oriented lte network. In *Security-Enriched Urban Computing and Smart Grid*, pages 167–178. Springer.

Katz, J. and Yung, M. (2003). Scalable protocols for authenticated group key exchange. In *Annual International Cryptology Conference*, pages 110–125. Springer.

Khan, J., Abbas, H., and Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*, 56:376–383.

Kim, A., Kniss, V., Ritter, G., Sloan, S. M., et al. (2011). An approach to communications security for a communications data delivery system for v2v/v2i safety: technical description and identification of policy and institutional issues. Technical report, United States. Joint Program Office for Intelligent Transportation Systems.

Kumano, A. and Nogami, Y. (2015). An improvement of tate paring with supersingular curve. In *Information Science and Security (ICISS), 2015 2nd International Conference on*, pages 1–3. IEEE.

Lai, C., Li, H., Li, X., and Cao, J. (2015). A novel group access authentication and key agreement protocol for machine-type communication. *Transactions on emerging telecommunications technologies*, 26(3):414–431.

Lai, C., Li, H., Lu, R., Jiang, R., and Shen, X. (2013). Lgth: a lightweight group authentication protocol for machine-type communication in lte networks. In *2013 IEEE Global Communications Conference (GLOBECOM)*, pages 832–837. IEEE.

Lai, C., Li, H., Lu, R., Jiang, R., and Shen, X. (2014). Segr: A secure and efficient group roaming scheme for machine to machine communications between 3gpp and wimax networks. In *2014 IEEE International Conference on Communications (ICC)*, pages 1011–1016. IEEE.

Lee, S., Kim, Y., Kim, K., and Ryu, D.-H. (2003). An efficient tree-based group key agreement using bilinear map. In *International Conference on Applied Cryptography and Network Security*, pages 357–371. Springer.

Li, J., Wen, M., and Zhang, T. (2016). Group-based authentication and key agreement with dynamic policy updating for mtc in lte-a networks. *IEEE Internet of Things Journal*, 3(3):408–417.

Lu, R. (2012). Security and privacy preservation in vehicular social networks.

Maas, M. (2004). Pairing-based cryptography. *Master's thesis, Technische Universiteit Eindhoven*.

Maeder, A., Rost, P., and Staehle, D. (2011). The challenge of m2m communications for the cellular radio access network. In *Proc. Würzburg Workshop IP, Joint ITG Euro-NF Workshop "Vis. Future Gener. Netw." EuroView*, pages 1–2.

Meffert, D. (2009). *Bilinear pairings in cryptography*. PhD thesis, Master's thesis, Radboud Universiteit Nijmegen.

Menezes, A. (2009). An introduction to pairing-based cryptography. *Recent trends in cryptography*, 477:47–65.

Menezes, A. J. (2012). *Elliptic curve public key cryptosystems*, volume 234. Springer Science & Business Media.

Menezes, A. J., Okamoto, T., and Vanstone, S. A. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory*, 39(5):1639–1646.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer.

Miller, V. S. (2004). The weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261.

Nam, J., Lee, J., Kim, S., and Won, D. (2005). Ddh-based group key agreement in a mobile environment. *Journal of Systems and Software*, 78(1):73–83.

Sakai, R. (2000). Cryptosystems based on pairing. *SCIS 2000*.

Schütze, T. (2011). Automotive security: Cryptography for car2x communication. In *Embedded World Conference*, volume 3.

Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media.

Stallings, W. (2003). *Cryptography and network security: principles and practice*. Pearson Education India.

Sun, J., Zhang, R., and Zhang, Y. (2016). Privacy-preserving spatiotemporal matching for secure device-to-device communications.

Taleb, T. and Kunz, A. (2012). Machine type communications in 3gpp networks: potential, challenges, and solutions. *IEEE Communications Magazine*, 50(3).

Verheul, E. R. (2001). Evidence that xtr is more secure than supersingular elliptic curve cryptosystems. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 195–210. Springer.

Whyte, W., Weimerskirch, A., Kumar, V., and Hehn, T. (2013). A security credential management system for v2v communications. In *Vehicular Networking Conference (VNC), 2013 IEEE*, pages 1–8. IEEE.

Zhang, C., Lu, R., Lin, X., Ho, P.-H., and Shen, X. (2008). An efficient identity-based batch verification scheme for vehicular sensor networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 246–250. IEEE.

Zhang, M. and Fang, Y. (2005). Security analysis and enhancements of 3gpp authentication and key agreement protocol. *IEEE Transactions on wireless communications*, 4(2):734–742.

Zhang, W., Wang, X., Zhou, Y., Deng, H., and Wang, Y. (2015). A gaa-based batch authentication and key agreement for lte networks. *International Journal of Embedded Systems*, 7(3-4):289–295.

Zhang, Y., Chen, J., Li, H., Cao, J., and Lai, C. (2014). Group-based authentication and key agreement for machine-type communication. *International Journal of Grid and Utility Computing 4*, 5(2):87–95.

Zhang, Y., Chen, J., Li, H., Zhang, W., Cao, J., and Lai, C. (2012). Dynamic group based authentication protocol for machine type communications. In *Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on*, pages 334–341. IEEE.

BIODATA OF STUDENT

The student, **Haqi Khalid Ismail**, was born in May 1991. Obtained his bachelor degree in computer science from Al Yarmouk University College in 2015. He is currently enrolled a master study in the area of Computer network security. His research interest involves with designing a group authentication protocol by depending on cryptographic mathematic. The student can be reached via email address; Haqikhalid1@gmail.com.

LIST OF PUBLICATIONS

The following are the list of publications that arise from this study.

Journal articles:

Haqi Khalid, Kweh Yeah Lun, Mohamed Othman, and Idawaty Ahmad (2017). AUTHENTICATION GROUPS WITH PRIVACY-PROTECTION OF MACHINE-TO- MACHINE IN LTE/LTE-A NETWORKS , *Journal of Theoretical and Applied Information Technology* (Published).

Haqi Khalid, Kweh Yeah Lun, Mohamed Othman, and Idawaty Ahmad (2018). Tate Pairing for Group Authentication Protocol of Machine-To-Machine in LTE/LTE-A Networks. *Journal of Cogent Engineering* (Submitted)

UNIVERSITI PUTRA MALAYSIA
STATUS CONFIRMATION FOR THESIS/PROJECT REPORT AND COPYRIGHT
ACADEMIC SESSION: 2018/2019

TITLE OF THE THESIS/PROJECT REPORT:
A Modified Group Authentication Scheme For Machine Type Communication in LTE/LTE-A Networks

NAME OF STUDENT: Haqi Khalid Ismail

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as:

*Please tick(✓)

☐	CONFIDENTIAL	(contain confidential information under Official Secret Act 1972).
☐	RESTRICTED	(Contains restricted information as specified by the organization/institution where research was done).
☐	OPEN ACCESS	I agree that my thesis/project report to be published as hard copy or online open acces.

This thesis is submitted for:

☐	PATENT	Embargo from _____until _____. (date) (date)

Approved by:

(Signature of Student)
New IC No/Passport No.:850523-10-5567

Date:

(Signature of Chairman of Supervisory Committee)
Name: **Kweh Yeah Lun**

Date:

[Note: If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]