A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL

TAN SOO FUN

THESIS SUBMITTED IN FULFILLMENT FOR THE DEGREE OF MASTER OF SCIENCE

LABUAN SCHOOL OF INFORMATICS SCIENCE
UNIVERSITI MALAYSIA SABAH
2009

CERTIFICATION

JUDUL: A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL

IJAZAH: MASTER OF SCIENCE (COMPUTER SCIENCE)

SESI PENGAJIAN: 2007 – 2009

Saya, TAN SOO FUN mengaku membenarkan tesis sarjana ini disimpan di perpustakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalan hak milik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. TIDAK TERHAD

Disahkan oleh

Penulis: TAN SOO FUN

TANDATANGAN PUSTAKAWAN

(Signature)

Penyelia: Assoc. Prof Dr. Hj Rozaini Roslan

(Signature)

Penyelia: En. Mohd Yuszren Yusak

(Signature)

Penyelia: En. Jonathan Likoh Juis

Tarikh : 2009

NAME : **TAN SOO FUN**

MATRIC NO : **PI20078017**

TITLE : **A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL**

DEGREE : **MASTER OF SCIENCE**

VIVA DATE : **31 MARCH 2009**

DECLARED BY

1. SUPERVISOR

(Assoc. Prof Dr. Hj Rozaini Roslan) *(Signature)*

2. CO-SUPERVISOR

(En. Mohd Yuszren Yusak) *(Signature)*

3. CO-SUPERVISOR

(En. Jonathan Likoh Juis) Jonathan *(Signature)*

4. INTERNAL EXAMINER

(Assoc. Prof. Assoc. Prof. Dr. Patricia Anthony) *(Signature)*

5. DEAN/DIRECTOR

(Dr. Ag Asri Hj Ag Ibrahim) *(Signature)*

ACKNOWLEDGEMENT

In preparing this valuable piece of work, I received much excellent encouragement, guidance and advices from many people. These people certainly have contributed toward me achieving this. Firstly, I would like to express my deepest gratitude to Dr. Hj. Rozaini Roslan, Mr. Mohd Yuszren Yusak and Mr. Jonathan Likoh Juis as my thesis supervisors for giving me fully support and faithfulness in all guidance, advices and commitment upon on effort since the beginning of this thesis. Besides, I also would like to present my special thanks to all the lectures that have given me theirs guidance and advices. I also would like to express my sincere appreciation for my family members who always encourage and give me fully support for doing this research. Finally, I am also very thankful to my friends for their supports and assistances at various occasions. Indeed, the encouragement and support are deeply appreciated.

Tan Soo Fun
1 June 2009

ABSTRAK

Perdagangan Mobil tidak dapat disangkalkan lagi menjadi satu kebiasaan dan bidang aktif dalam pembayaran elektronik. Ia membenarkan pengguna mobil untuk membeli dan membayar barangan, bil-bil ataupun membuat taruhan melalui telefon mudah alih semasa bergerak di mana-mana dan pada bila-bila sahaja. Malangnya, beberapa cabaran dari segi kebertanggungjawaban dan privasi telah wujud ekoran daripada penggunaan pembayaran elektronik yang meluas kebelakangan ini. Terdapat banyak protocol pembayaran mobil yang berdasarkan kriptografi kekunci umum telah diusulkan. Walau bagaimanapun, kebolehan yang terhad pada peranti mudah alih (kuasa pemprosesan yang kurang, kapasiti bateri yang rendah dan ingatan storan yang terhad), kekurangan Keupayaan rangkaian wayarles (lebar jalur dan kebolehpercayaan yang kurang dan kependaman yang tinggi) serta kos penyambungan rangkaian wayarles yang tinggi turut menjejaskan kesesuaian protokol-protokol tersebut dalam rangkaian mobil. Dalam penyelidikan ini, protokol pembayaran mobil yang selamat dicadangkan di mana ia melibatkan operator rangkaian mobil serta menggunakan operasi-operasi kekunci simetri. Adalah tidak realistik untuk mengandaikan semua pihak tidak kira yang membayar ataupun dibayar dikehendaki mempunyai akaun-akaun dengan beberapa operator rangkaian mobil. Protokol yang dicadangkan akan menyokong antara-operasi di antara pelbagai operator rangkaian mobil yang mempunyai pelanggan dan peniaga masing-masing. Kelebihan ini mengizinkan pelanggan daripada satu operator rangkaian mobil membuat pembayaran dengan peniaga bagi operator rangkaian mobil lain. Teknik kriptografi simetrik yang diaplikasikan dalam protokol yang dicadangkan bukan saja dapat mengurangkan operasi-operasi dan komunikasi antara pihak-pihak yang terlibat, malahan dapat mencapai perlindungan privasi yang lengkap bagi pembayar dan turut memenuhi kesemua kriteria keselamatan bagi keperluan pihak-pihak terlibat termasuklah ketidaksangkalan. Protokol pembayaran mobil ini dianalisiskan dengan menggunakan teknik logik kebertanggungjawapan Kungpisdan et al. Keputusan menunjukkan bahawa protokol ini telah memenuhi kesemua keperluan keselamatan dalam pembayaran elektronik. Secara kesimpulan, protokol pembayaran mobil yang diusulkan telah meningkatkan lagi tahap keselamatan berbanding dengan protokol-protokol yang sedia ada serta mengurangkan operasi-operasi kriptografi dalam protokol pembayaran mobil yang sedia wujud.

ABSTRACT

A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL

Mobile commerce (m-commerce) has undoubtedly become an omnipresent and an active area in electronic payments. It allows mobile user to buy and pay for things, pay his bill or make a bet via mobile phone when on move, anywhere and at any time. However, several challenges in accountability and privacy properties have emerged with the widespread of mobile payments in recent years. Consequently, many public-key cryptography based mobile payment protocols have been proposed. However, limited capabilities of mobile devices (poor computation power, low battery capacity and limited storage memory), limitation of wireless networks (less bandwidth and reliability, and higher latencies), and higher wireless networks connection cost make these protocols unsuitable for mobile network. In this paper, a lightweight and private mobile payment protocol involving mobile network operators (MNOs) and employing symmetric key operations is proposed. It is unrealistic to expect all payers and all payees to have accounts with multiples MNOs. Therefore, the proposed protocol supports the interoperability among multiple MNOs, each with its own customer (payer) and merchant (payee), allowing customers of one MNO to make purchases from merchants of the other MNO. The symmetric cryptographic technique applied into the proposed protocol not only reduces the number of cryptographic operations and communication passes between the involved parties, but also achieves completely privacy protection of payer and satisfies all the criteria of end-to-end security property, party's requirements including non-repudiation. The proposed mobile payment protocol is analyzed with Kungpisdan *et al.* accountability logic (KP Logic). The result shows that the proposed protocol satisfies all security requirements in electronic payment transaction, enhances privacy protection and reduces the number of cryptographic operations in existing mobile payment protocols.

LIST OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

2G	The second generation of wireless technology. Usually identified as GSM
2.5G	Between the second and third generations of wireless technology. Usually identified as GPRS
3G	Third generation of wireless technology. Usually identified as UMTS
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CCI	Credit Card Information
CLDC	Connected Limited Device Configuration
DES	Data Encryption Standard
E-Commerce	Electronic Commerce
EDGE	Enhanced Data for GSM Evolution
EFTPOS	Electronic Funds Transfer at Point of Sales
FSP	Financial Service Providers
GPRS	General Packet Radio Services
GSM	Global System for Mobile communication
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL (secure socket layer)
IrDA	Infrared
IrFM	Infrared Financial Messaging

i KP	Internet Key Protocol
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition
J2MEWTK	Java 2 Micro Edition Wireless Toolkit
J2SE	Java 2 Standard Edition
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
JVM	Java Virtual Machine
MAC	Message Authentication Code , also called as Message Integrity Code (MIC)
MD2	Message Digest Algorithm 2
MD4	Message Digest Algorithm 4
MD5	Message Digest Algorithm 5
M-Commerce	Mobile Commerce
MIDlet	The J2ME™ Application
MIDlet Suite	A bundle of MIDlets in the same application.
MIDP	Mobile information Device Profile
MNO	Mobile Network Operator, also called as Network Services Operators
NFC	Near Field Communications
P2P	Person to Person
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure

POS	Point-of-Sale
PSP	Payment Service Providers
RFID	Radio Frequency Identification
RTT	Radio Transmission Technology
SAT	SIM application Toolkit
SET	Secure Electronic Transaction
SHA-1	Secure Hash Algorithm Version 1, also called as Secure Hash Standard(SHS)
SIM	Subscriber Identity Module
SMS	Short Message Service
TSC	Time Stamp Center
TTP	Trusted Third Party
WAP	Wireless Application Protocol
UMTS	Universal Mobile Telecommunication System
W-CDMA	Wideband Code Division Multiple Access
WIM	Wireless Identity Module. Usually associated with SIM
WTLS	Wireless Transport Layer Security
WWW	World Wide Web

LIST OF NOTATIONS

$\{\Phi, \Psi\}$ A set of statements that derived from messages

$\xrightarrow{K} Q$ The symmetric key K can be used to refer Q

AI_P Account Information of Party P, which including credit limit for each transaction, type of account (post-paid or prepaid account)

AMOUNT Payment transaction amount and currency

AuthReq Authentication Request message

AuthRes Authentication Response message

BrandID Brand of card that will be used in the payment , such as VISA

CapAmt Payment Capture Amount

CapID Payment Capture Message ID

CapCode Payment Capture Code

CapReq Payment Capture Request message

CapRes Payment Capture Response message

Cap_Token Payment Capture Token

$Cert_P$ A certificate of party P which contains $\{ID_P, K_P\}$

Chall_C Client's Challenges variable used in the merchant's to guarantee the freshness of the communication

Chall_M Merchant's Challenges variable to guarantee the freshness of the communication

{C, M, PG, I, A, Payee, Payer, Payee's MNO, Payer's MNO, TSC} A set of engaging parties, which are Client, Merchant, Payment Gateway, Issuer, Acquirer, Payee, Payer, Payee's MNO, Payer's MNO and Time Stamp Center respectively.

DATE	Date of payment execution
DESC	Payment Description, which may includes delivery address, purchase order details and so on. Payer will include only the information that he/she wish to disclosure to Payee.
$E_{P\text{-}P'}$	Message X singed and encrypted by the user ID_P to a specified received $ID_{P'}$.
H(M)	The one way hash function of the message *M*
ID_P	*Identity of engaging party* P
InqReq	Inquiry Request message
InqRes	Inquiry Response message
i	Used to identify the current session key of X_i, where $i = 1,2,\ldots,n$
K-is-decrypting-key-for-{M}K	The symmetric key *K* can be used to decrypted *{M}K*
$K_{P\text{-}P}$	The secret key *K* shared between Payer's MNO and Payee's - MNO.
K_P	Public key of Party *P*
K_P^{-1}	Private key of Party *P*
LID_C	A local *ID* for the transaction
MAC(M,K)	The Message Authentication Code (*MAC*) of the message *M* with the key *K*
MID_{Req}	The request for ID_M
$\{M\}K_P$	The message *M* encrypted with the public key of the party *P*
$\{M\}K_P^{-1}$	The message *M* signed with the private key of the party *P*
{M}K	The message *M* symmetrically encrypted with the shared key *K*
NID_C	Nick Name of Client

NONCE	Random number and timestamp generated to protect against replay attack, that is ensure old communication cannot reused in replay attack.
OI	Order Information
$P \xleftrightarrow{K} Q$	The symmetric key *K* is the shared key between party *P* and party *Q*
$PayeeID_{Req}$	The request for *ID* of payee.
PI	Payment Information which contains Credit Card Information (*CCI*)
PIN_P	Party *P* selected Password Identification Number (*PIN*)
PInitReq	Payment Initialization Request message
PInitRes	Payment Initialization Response message
PReq	Payment Request message
PRes	Payment Response message
P believes Φ	A party *P* believes that the statement Φ is true by doing some actions.
P has M	A party *P* possesses a message *M*. Party *P* can send *M* to other parties or use it for further computations.
P says M	A party *P* has sent a message *M*.
P sees M	Some party has sent a message *M* to party *P* and party *P* is able to read *M*
P CanProve Φ *to Q*	A party *P* can prove to party *Q* that statement Φ is true by sending a message *M* to party *Q*. After party *Q* receives *M*, he believes that the statement Φ is true
P authorized Payment (P, Q, AMOUNT, DATE)	A party *P* has authorization on making the payment amount *(AMOUNT)* to party *Q* on the date of transaction (*DATE*).

P authorized value-subtraction (P, Q, AMOUNT, DATE)	A party *P* has authorization on requesting party *Q* to deduct the amount *(AMOUNT)* from party *P* account on the date of the transaction *(DATE)*.
P authorized value-claim (P, Q, AMOUNT, DATE)	A party *P* has authorization on requesting party *Q* to transfer the amount *(AMOUNT)* to party *P* account on the date of transaction (*DATE*).
$P \longrightarrow Q$	Party *P* sends a message to party *Q*
Received	Payment receivable update status, which includes the received payment amount
R	Payer's nick name, random number and timestamp generated by payer act as payer's pseudo-ID, which uniquely identifies payer to payee
Success/Failed	The registration status, whether the registration process is success or failed
TC	The type of card used in the purchase process, (*TC={Credit, Debit}*).
Thums	Optional list of certificates (*Thumbs*) already stored by the cardholder software. This list consists of a thumbprint (SHA hash) of each certificate held
TID	Identity of transaction
TID_{Req}	The request for *TID*
X_{payer}	Payer's public value used in the signature process
A-is-fingerprint-of-B	*A* is a fingerprint of *B*
Yes/No	The status of transaction approved/rejected

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.1 Overview

The increasing development of wireless networks and the widespread popularity of handheld devices such as Personal Digital Assistants (PDAs), mobile phones and wireless tablets, have led to numerous applications ranging from mobile banking, location-based tracking to mobile advertising. According to Durlacher (1999), mobile commerce (m-commerce) refers as any transaction with a monetary value that is conducted via a mobile telecommunications network. Mobile payment is defined as any transaction that is carried out via mobile device, involves either direct or indirect exchange of monetary values between two or more parties involved (Krueger, 2001; Pousttchi, 2003; Jun *et al.*, 2005). Wolcox (2008) predicts that the rapidly evolving market for money transfer and remittances via mobile phones resulting more than 100 million global users will use their mobile phones to make international money transfers by 2013.

According to Malte (2001) and Wolcox (2008), two basic forces indicate a positive future of mobile payments. Firstly, the increasing spread of mobile phones and technologies. The number of worldwide mobile phones users will reach 4.5 billion on 2013 (Business News and Technology News 2009). The mobile device's storage, computing and data transmission capabilities have made mobile phone an ideal device to store everything that is normally carried in wallet, including coins, cash, ATM cards, debit cards and credit cards. Secondly, mobile payment can be accepted as universal payment method for daily financial transactions such as web store-front payment, physical Point-of-Sale (POS) purchase, Person-to-Person (P2P) payment, and payment for mobile commerce application. Muller-Veerse (2000) and Vilmos and Karnouskos (2003) highlighted the attractiveness of m-commerce and mobile payment such as ubiquity, reachability, personalization, localization, convenience and coverage. These allow great flexibility and creativity for businesses to increase their volume of transactions and offer their volume of transactions and offer customers more ways of making payment.

1.2 Background and Problem Statements

Some issues hampering the widespread acceptance of mobile payment such as ease of use, expenses, security, universality and technical feasibility. According to Cervera (2002), Kungpisdan *et al.* (2003a) and Pousttchi *et al.* (2007), security issues are very fundamental of critical success factor in making mobile payment a reality. However, designing secure mobile payment protocol is more challenging than Internet payment protocol due to the constraints of wireless network and mobile devices. Firstly, the limitations of mobile devices such as lower power, computational and storage capabilities. Secondly, the constraints of wireless network such as lower bandwidth, less reliability and higher latencies than wired network. Furthermore, the cost of wireless network connection is higher than wired network (Cimato, 2002; Halonen, 2002; Tellez *et al.*, 2007). These resulting existing Internet payment protocol such as Secure Electronic Protocol (SET) and Internet Payment Protocol (*i*KP) cannot be directly adopted in wireless environments as they designed for wired network and do not meet all the challenges of wireless environments (Chari *et al.*, 2001; Marvel, 2001; Cimato, 2002; Halonen, 2002; Tellez *et al.*, 2007).

Currently, several mobile payment protocols have been proposed. However, most of them (Bellare *et al.*, 2000; Vilmos and Karnouskos, 2003; Tellez *et al.*, 2007) are based on Public Key Infrastructure (PKI) which are inefficient to be applied into wireless networks. The PKI is a technology and management needed for a certificate authority (CA) to create public key and private key pairs, distribute private keys, issue digital certificates, and maintain certificate revocation list. With public key encryption, client needs to perform high computational operations, and his mobile device is required to have sufficient storage to store public-key certificates (Ramfos *et al.*, 2004; Jun *et al.*, 2005; Li and Hu, 2008). Although some mobile devices are equipped with special processors (VISA, 2007), performing such operations on them still requires longer procession time (Kungpisdan *et al.*, 2004a). Furthermore, during a transaction, each certificate sent to the payer has to be verified by a Certificate Authority (CA) located in a fixed network, which results in an additional communication passes between engaging parties (Kungpisdan *et al.*, 2004a; Wang and Leung, 2005; Tellez *et al.*, 2007; Li and Hu, 2008).

To solve the PKI problems, Kungpisdan *et al.* (2003a) proposed KSL payment protocol by reducing computational tasks at payer's wireless devices. Tellez *et al.* (2007) proposed a digital signature scheme with message recovery using self-certified public keys to solve PKI problem. Although some payment schemes (Kungpisdan *et al.*, 2003a, 2003b; Tellez *et al.*, 2007), public-key cryptography have been reduced to certain degrees, these schemes are still impractically feasible apply into mobile payment (Kungpisdan *et al.*, 2004a; Wang and Leung, 2005; Li and Hu, 2008). Hence, Kungpisdan *et al.* (2004a) proposed another mobile payment protocol to enhance their KSL payment protocol (2003a) by employs symmetric key operations not only for payer side but also for all engaging parties.

Wang and Leung (2005), Tiwari *et al.* (2007) and Li and Hu (2008) further pointed out several limitations of existing mobile payment protocol. Firstly, the privacy of the payer is not protected during the transaction. The payer's identity and the transaction details are revealed not only to the payee, but also to the payment gateway and the banks. Secondly, some existing mobile payment protocols (Mastercard and Visa 1997; Bellare *et al.*, 2000; Kungpisdan *et al.*, 2003a, 2004a) are based on full-connectivity scenario as stated by Tellez *et al.* (2007), which does not consider the situation of payee who is not under the coverage of communication connection, or is unaffordable due to the inconvenience and costs. Thirdly, some payment schemes (Mastercard and Visa 1997; Bellare *et al.*, 2000; Kungpisdan *et al.*, 2003a, 2004a) were designed to preserve the traditional flow of payment data (Payer - Payee- Payee's Bank). Therefore, it is vulnerable to violation like transaction or balance modification by payee and gaining illegal access to payer's account. These increasing the payer's risk which their credit or debit cards can be captured and used later to access a payer account without authorization. Besides that, there is no notification to the payer from the payer's bank after the successful transfer. The payer has to check his balance again. Lastly, some of mobile payment protocol schemes are bank dominated model (Kungpisdan *et al.*, 2003a, 2003b, 2004a; Tellez *et al.*, 2007). The involvement banks and financial institutions in mobile payment seem to burden their roles as financial services providers and trust dependency on them. The banks and other financial organizations lack wireless expertise (e.g. providing telecommunication facilities, support transmission of payment initiation and verification to or from the mobile device) and direct access to mobile users. As a result, they face large up-front costs in developing mobile payment technology (Varshney, 2002; Labrou *et al.*, 2004; Me and Strangio, 2006; Business News and Technology News, 2009). In comparison with banks and financial institutional, Mobile Network Operators (MNOs) have several advantages to take the role as Payment Service Provides (PSPs) in mobile payment. Firstly, MNOs have well-established billing system and relationship with the mobile phone users. Secondly, MNOs own the network and can identify who is using their network. Thirdly, MNOs have the technical expertise and lastly, MNO have a large customer base, which allows them to generate a critical mass of customer and merchant acceptance for a new payment schemes (Heijden, 2002; Zmijewska, 2005).

1.3 Aim and Objectives

The aim of this research is to create a lightweight and private mobile payment protocol by taking the advantage of symmetric key operations and the role of MNOs as PSPs. The proposed mobile payment protocol employs symmetric key encryption instead of public key encryption to reduce all engaging party's computational operations and communication passes. Several issues are not addressed by existing mobile payment schemes (Mastercard and Visa 1997; Bellare *et al.*, 2000; Kungpisdan *et al.*, 2003a, 2004a) such as privacy protection, problems of traditional payment data flow, problem of full-connectivity scenario, no notification to payer from payer's bank after successful payment. These issues will be addressed on this research. Besides that, the analysis part for this research focuses on most important property of payment protocol, which is accountability logic, which concerns about the ability to trace an action to particular parties who engaging in payment protocol and then hold them accountable or responsible for their actions