

# Cryptographically Secured Micro Payment Scheme

Tanushka Sajith Balasooriya

158203K

Degree of Master Science

Department of Computer Science & Engineering

University of Moratuwa  
Sri Lanka

January 2019

# Cryptographically Secured Micro Payment Scheme

Tanushka Sajith Balasooriya

158203K

Degree of Master Science

Department of Computer Science & Engineering

University of Moratuwa  
Sri Lanka

January 2019

# Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non - exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works.

---

Tanushka Sajith Balasooriya:

---

Date

Approved by:

---

LtCol Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Copyright Statement

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retrain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

---

Tanushka Sajith Balasooriya:

---

Date

I have supervised and accepted this thesis/dissertation for the award of the degree.

---

LtCol Dr Chandana D. Gamage  
Department of Computer Science and Engineering  
University of Moratuwa

---

Date

# Abstract

As more and more commercial activity moves online and electronic commerce becomes the common way by which transactions are conducted, electronic payment systems will become a critical requirement for the success of many applications. The commonly used electronic payment scheme is to facilitate the online transmission of payment card data from credit cards or debit cards and to process such transactions through a payment gateway. Also, other schemes such as PayPal or ezCash provide a service where the payment is processed online using identification data specific to the service but using funds that are based on a pre-stored credit card, debit card or stored-value card system.

All these existing online payment schemes are similar in their design and operation to credit card based payments. While such schemes called macro payment systems are appropriate for transactions with a relatively high value compared to the service charges of the online payment providers, there are many e-commerce applications that are being developed for which such credit card style payment schemes are inappropriate.

As a solution to this problem, research has been conducted on an area called micro payment systems. The design of micro payment systems need to be radically different from the macro payment schemes as properties such as online real time availability of all participants, use of public cryptography schemes, availability of high computation power, etc that is common for macro payment systems are not desirable in micro payment systems. Taking into consideration the context in which micro payment schemes operate, where a transaction value is very low, micro payment systems need to be designed with a careful trade-off between reliability and cost of implementation.

This proposed research is intended to study the properties of existing micro payment systems, evaluate the strengths and weaknesses of those schemes, and prepare a model for a micro payment scheme with only the most essential properties. The research further envisages the selection of cryptographic mechanisms and development of protocols to implement this micro payment model.

# Acknowledgements

First of all I would like to thank my supervisor Dr. Chandana Gamage whose encouragement, guidance, support, and criticism from start to the very end, allowed me to understand the objectives and challenges of a master degree thesis. I would also like to thank Dr. Indika Perera (Course Cordinator) for extensive advice, helpful feedback, and constant support.

Furthermore, my special thanks go to Dr. Shantha Fernando who provided an excellent, supporting, innovative, and inspiring environment in which it was a pleasure to create this thesis.

Finally, words alone cannot express the thanks I owe Mr. Premaratne my father, Mrs. Amara Weerasinghe my mother, Ms. Jeewantha Sandamalee my sister and Ms. Lakmi Bandara my loving girl friend for all the encouragement extended.

# Abbreviations

CA - Certificate Authority  
CAFE - Conditional Access for Europe  
CSP - Communicating Sequential Processes  
DoS - Denial-of-Service  
FSTC - Financial Services Technology Consortium  
ISP - Internet Service Provider  
PAT - Protocol Analysis Toolkit  
PKI - Public-key Infrastructure  
POC - Proof of Concept  
RSA - RivestShamirAdleman  
SET - Secure Electronic Transaction  
GSM - Global System for Mobile communication  
NFC - Near Field Communication  
SMS - Short Messaging Service  
EMV - Europay MasterCard Visa

# Table of Contents

<b>Declaration</b>	<b>v</b>
<b>Copyright Statement</b>	<b>vi</b>
<b>Abstract</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>viii</b>
<b>Abbreviations</b>	<b>ix</b>
<b>List of Tables</b>	<b>xiv</b>
<b>List of Figures</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Concept of Micro Payment . . . . .	1
1.2 How Micro Payment Differentiate with Macro Payments . . .	2
1.3 General Payment Gateway . . . . .	3
1.4 Cryptography . . . . .	6
1.5 Classic Cryptography . . . . .	6
1.6 Modern Cryptography . . . . .	7
1.6.1 Symmetric-key Cryptography . . . . .	7
1.6.2 Asymmetric Cryptography . . . . .	8
1.7 Research Problem . . . . .	10
1.8 Methodology . . . . .	11
1.9 Thesis Outline . . . . .	11
<b>2 Literature Review</b>	<b>14</b>
2.1 Introduction . . . . .	14
2.2 History of Micro Payment System . . . . .	14



2.3	Properties and Requirements . . . . .	15
2.4	Transaction Costs of Micro Payments . . . . .	18
2.4.1	Fixed Technical Costs . . . . .	18
2.4.2	Storage Costs . . . . .	18
2.4.3	Computational Costs . . . . .	19
2.4.4	Communication Costs . . . . .	19
2.4.5	Administrative Cost . . . . .	19
2.5	Micro Payment Schemes . . . . .	20
2.5.1	MILLICENT . . . . .	20
2.5.2	MPAY . . . . .	21
2.5.3	PAYWORD . . . . .	23
2.5.4	NETPAY . . . . .	24
2.5.5	PPAY: Micro Payments for Peer-to-Peer Systems . . . . .	26
2.5.6	WHOPAY . . . . .	27
2.5.7	PEPPERCOIN . . . . .	29
2.5.8	Swing-Pay . . . . .	30
2.6	EMV Tokenised Payment to offline environment . . . . .	31
2.7	Summary of Micro Payment Schemes . . . . .	31
2.8	Outstanding Challenges . . . . .	33
2.8.1	Security Challenges . . . . .	33
2.8.2	Legal and Ethical Challenges . . . . .	34
2.8.3	Psychological Challenges . . . . .	35
2.8.4	Deployment Challenges . . . . .	36
<b>3</b>	<b>Protocol for e-Cash using Standard Digital Signatures</b>	<b>37</b>
3.1	Notations . . . . .	37
3.2	Registration . . . . .	38
3.3	Spending e-cash . . . . .	38
3.3.1	Obtaining e-cash from a bank . . . . .	38
3.3.2	Spending e-cash at a merchant . . . . .	39
3.3.3	Depositing e-cash at the bank . . . . .	40
3.4	Detailed protocol . . . . .	40
3.4.1	Registration with the bank . . . . .	40
3.4.2	Obtaining e-cash from a bank . . . . .	41
3.4.3	Spending e-cash at a merchant . . . . .	41
3.4.4	Depositing e-cash at the bank . . . . .	42
3.5	Analysing the properties . . . . .	42

3.5.1	Double spending . . . . .	42
3.5.2	Non-Repudiation . . . . .	43
3.5.3	Authentication . . . . .	43
3.5.4	Integrity . . . . .	43
3.5.5	Availability . . . . .	44
3.5.6	Transferability . . . . .	44
3.5.7	Payment mode . . . . .	44
3.5.8	Usability . . . . .	44
3.5.9	Validation . . . . .	45
3.5.10	Transaction cost . . . . .	45
3.5.11	Anonymity . . . . .	46
3.6	Problems with proposed solution . . . . .	46
3.6.1	Minor limitations . . . . .	46
3.6.2	Major limitations . . . . .	47
3.7	Summary . . . . .	47
<b>4</b>	<b>Protocol for e-Cash using Ring Signatures</b>	<b>48</b>
4.1	RSA based Ring Singature Scheme . . . . .	48
4.1.1	Ring Signature Generation . . . . .	48
4.1.2	Ring Signature Verification . . . . .	49
4.2	e-Cash Scheme using Ring Signatures . . . . .	49
4.3	Spending e-cash . . . . .	49
4.3.1	Obtaining e-cash from a bank . . . . .	49
4.3.2	Spending e-cash at a merchant . . . . .	50
4.3.3	Depositing e-cash at the bank . . . . .	51
4.4	Analysing the properties . . . . .	51
4.4.1	Achieving anonymity using ring signature . . . . .	51
4.5	Problems of Ring signature based solution . . . . .	52
4.5.1	Minor limitations . . . . .	52
4.6	Summary . . . . .	53
<b>5</b>	<b>Analysing the protocol</b>	<b>54</b>
5.1	Communicating Sequential Processes (CSP) . . . . .	54
5.2	Analysing Client Registration process with Bank . . . . .	55
5.3	Analysing customer e-cash obtaining process with Bank . . . . .	59
5.4	Spending e-cash at a merchant . . . . .	62
5.5	Depositing e-cash at the bank . . . . .	65

5.6	Summary . . . . .	67
<b>6</b>	<b>Proof-of-Concept Implementation</b>	<b>68</b>
6.1	Client Registration process with Bank . . . . .	68
6.2	e-cash obtaining process with Bank . . . . .	70
6.3	Customer payment process with Merchant . . . . .	72
6.4	Withdraw e-cash to a bank account . . . . .	73
6.5	Summary . . . . .	75
<b>7</b>	<b>Conclusions</b>	<b>76</b>
	<b>References</b>	<b>79</b>
<b>A</b>	<b>PAT Analyser</b>	<b>82</b>
<b>B</b>	<b>Proof of Concept</b>	<b>88</b>

# List of Tables

2.1	Comparison of existing payment gateways. . . . .	32
2.2	Example of labels with amount. . . . .	35

# List of Figures

1.1	General Payment Model . . . . .	4
1.2	Iterated Block Cipher Diagram . . . . .	8
2.1	Millicent Payment Model . . . . .	20
2.2	MPay Payment Model . . . . .	22
2.3	Payword Payment Model . . . . .	23
2.4	Netpay Payment Model . . . . .	25
2.5	Whopay Payment Model . . . . .	28
5.1	PAT Analyser Generated Graph for Registration Process . . . . .	57
5.2	PAT Analyser Verification for Registration Process . . . . .	58
5.3	PAT Analyser Generated Graph for Obtaining e-cash Process . . . . .	60
5.4	PAT Analyser Verification for Registration Process . . . . .	61
5.5	PAT Analyser Generated Graph for spending e-cash Process . . . . .	63
5.6	PAT Analyser Verification for spending e-cash Process . . . . .	64
5.7	PAT Analyser Generated Graph for depositing e-cash Process . . . . .	66
5.8	PAT Analyser Verification for depositing e-cash Process . . . . .	67
6.1	Mobile application interfaces for Registration . . . . .	69
6.2	Mobile application interfaces for top up . . . . .	71
6.3	Customer and Merchant initial interfaces before starting payment process . . . . .	73
6.4	Customer and Merchant interfaces during payment process . . . . .	74
6.5	Customer/ Merchant interfaces for withdrawal process . . . . .	75