Middle East University for Graduate Studies

Faculty of Information Technology

Designing a Secure E-Payment Protocol

A thesis submitted in partial fulfillment of the requirements for the Master Degree in Computer Science

By

Mahmmoud Muslem Ishtean AL-Tarawneh

Department Of Computer Science

Faculty of Information Technology

Supervisor

Professor Dr. Mohammad AL-Fayoumi (PhD)

Dean of Information Technology Faculty

Middle East University for Graduate Studies

Amman- Jordan

August, 2009

إقرار تفويض

أنا محمود مسلم اشتيان الطراونه أفوض جامعة الشرق الأوسط للدراسات العليا بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأفراد عند طلبها.

التوقيع:

التاريخ:

Authorization Statement

I am **Mahmmoud Muslem Ishtean Al-Tarawneh;** authorize the Middle East University for Graduate Studies to supply copies of my thesis to libraries, establishments or individuals upon their request.

Signature:

Date:

Committee Decision

This Thesis (**Designing a Secure E-Payment Protocol**) was successfully defended and approved on

Examination Committee signatures:

Declaration

I do, hereby, declare the present research work has been carried out by me under the supervision of Professor Dr. Mohammad Al Fayoumi and this work has not been submitted elsewhere for any other degree, fellowship or any other similar title.

Name: Mahmmoud Al -Tarawneh

Signature:

Date:

Dedication

I dedicate my thesis to my loving parents.

Acknowledgments

I would like to express my gratitude to my supervisor Professor Dr. Mohammad Ahmed Al-Fayoumi and to other people who helped me through my thesis; to all those who provided support, talked things over, read, wrote, offered comments, allowed me to quote their remarks and assisted in the editing, proof reading and design.

Last and not least, I beg forgiveness of all those who have been with me over the courses of the years and whose names I have failed to mention.

Contents

List of Figures

List of Tables

List of Abbreviations

U : User

M : Merchant

B : Bank

ID_E : Identity of entity E , such that $E \in \{U, M, B\}$

A_E : Address of entity E

m : Message

$\oplus$: XOR

PK_E : Public key of entity E

SK_E : Private Key of entity E

K : Secret key of bank B

r_E : Arbitrary number selected by entity E

C_U : User certificate

CE_U : User certificate expiry information

I_U : User certificate serial number credit card information

OI : Order information (category, amount, etc)

EI_R : Expiry information for redemption

h : Secure hash function

$||$: Concatenation

DoS : Denial of Service

Abstract

The vast spread of information in the last decade has led to great development in e-commerce. This has become a very important issue in the Internet services that implement e-transaction from any place in the world. This helps the merchant and bank to ease the financial transaction process and to give the user friendly services at any time.

The cost of communications falls down considerably while the cost of the trusted authority and protecting information is increased. E-payment operations are now one of the most central research areas in e-commerce, mainly, regarding online and payment scenarios.

In this thesis, we will discuss an important e-payment protocol; namely, Kim and Lee's scheme and examine its advantages and delimitations. This encourages the researcher to develop more efficient scheme that keeps all characteristics intact without concession of the security robustness of the protocol. The suggested protocol employs the idea of public key encryption scheme using the thought of hash function. We will compare the proposed protocol with Kim and Lee's protocol and demonstrate that the proposed protocol offers more security and efficiency; which makes the proposed protocol practicable for the real world services.

Keywords: e-payment protocol, public key cryptography, signature scheme, blind signature scheme, e-commerce

الملخص بالعربيـة:

أدى الانتشار الواسع للمعلومات في العقد الماضي إلى التطور الكبير في مجال التجارة الإلكترونية . حيث تعتبر التجارة الإلكترونية من أهم خدمات الإنترنت التي تقوم بتنفيذ المعاملات الإلكترونية من أي مكان في العالم. يساعد ذلك على تخفيف حده عملية المعاملات المالية لتقديم خدمات سهلة للمستفيدين في أي وقت.

ومع ذلك، فأن تكلفة الاتصالات تتناقص بشكل كبير في الوقت الذي تزداد تكلفة حماية عمليات الوسطاء.و يعتبر الدفع الإلكتروني احد أهم مجالات البحث في التجارة الإلكترونية ، وخصوصا عمليات الدفع التي تتم بالاتصال المباشر بين أطراف عمليات الدفع الالكتروني أو التي تتم بدون الحاجة إلى الاتصال الفوري.

في هذه الرسالة سنقوم بدراسة لبروتوكول 'Kim and Lee' ووضع نظام ذو كفاءة عالية معتمدا على النظام السابق ومحققا مزايا إضافية تعزز النظام المقترح. و يستخدم النظام المقترح نظام التشفير باستخدام المفتاح العام مضافا إليها تقنية 'Hash Function'سنقوم بمقارنة النظام المقترح مع النظام المذكور أعلاه وسنبين أن النظام المقترح يوفر المزيد من الأمنية والكفاءة، الأمر الذي يجعل النظام أكثر قدرة على التطبيق في واقع الخدمات الحقيقة.

مفتاح الكلمات:بروتوكول الدفع الالكتروني،التشفير بالمفتاح العام،نظام التوقيع،التجارة الالكترونية

Chapter One: E-Payment Systems

1.1 Introduction

Internet is designed to allow computers to be easily interconnected and to assure that network connections will be maintained even when various links may be damaged. But this versatility also makes it easy to compromise data security and privacy protection for e-commerce application since e-payment is a subject of great economic, political and research and since security is an important factor for the wide acceptance of the e-commerce services.

E- Payment system allows people to carry out commercial activities in an e-domain [19], where e-payment system is conventionally divided into those that are on-line and those that are off-line. The main difference between an on-line and an off-line e-payment system is that the payment protocol in the case of the on-line systems is monitored, checked and authorized by a trusted third party such as the bank. In the off-line systems, the payment protocol is executed only between the client and the merchant without a trusted third party. So this kind of e-payment systems can guarantee more freedom for customers, as the on-line e-payment systems, but their main disadvantage is that the fraud detection can be made only after the payment in the deposit protocol. This is the reason, why the on-line payment systems are more often used than the off-line systems. We can say that in the on-line e-payment system is ensures the preventive integrity and not only the degradation integrity (off-line case, increased security) [28]. It is easier to implement the on-line system than the off-line system since most of the checking can be done on-line.

A secure e-payment-system-protecting privacy can be seen as a protocol involving a user, merchant and bank. Its goal is to transfer money in a secure way from the user's account to the account of the merchant.

Since the anonymity of the participant is an important requirement for e-commerce, in particular, for payment systems, because anonymity could be in conflict with law enforcement. Currently, researches concentrate on accepting e-payment protocols where the anonymity of the coins is cancelable by a trustee in case of criminal entities.

Therefore, in order to make anonymous payment system acceptable, they must have the following requirements:

- The entity needs to have anonymous e-payment service
- The bank needs to ensure that the e-payment scheme will not be abused.

It is easier to implement the on-line system than off-line system since most of the checking can be done on-line. The most difficult task for off-line system is the detection of over-spending. When over-spending is suspected, the participant identity must be traceable as suggested in [18, 32], but, it is the on-line payment system. In [18], she proposed a new e-payment system which possesses recoverability and un-traceability simultaneously and still remains off-line. There are many systems which build high trusted relations between bank, user and merchant; these trusted relations may lead both merchant and bank to exploitation these relations to impersonate the user without being noticed [21].

1.2 Problem Definition

Internet has changed everything in the world; more and more users have access to the web at home and at work; and e-payment becomes a subject of great economic, political and research importance.

The most important requirement for some applications in e-commerce for payment system is the anonymity of all the parties involved in the payment systems where it allows a person to keep their personal commerce private.

Since the e-payments are stored and then converted to digital type, this will cause new difficulties during developing the secure e-payment protocol. The payment is simply duplicated against the conventional physical paying methods. As the digital payment is characterized as simple sequences of bits, nothing in them stops them copying. When a security of the payment protocol is reliant on the method, the payments are hidden from unknown.

We proposed a system that keeps the e-payment transaction anonymous as an essential issue using the idea of blind signature scheme that will be used in the protocol for reaching better efficiency without concession on security characteristics and efficiency

1.3 Objectives

The objectives of this thesis are as follows:

1. To design e-payment protocol to support the business measures.
2. To generate a secured and efficient e-payment protocol that provides the anonymity, non-repudiation and traceability.
3. To make the protocol usable as much as possible.

1.4 Motivation

The motivation of this scheme is summarized as follows:

- Most of existing protocols do not support anonymity and privacy of the e-payment transactions between user, merchant and the bank.
- The efficiency of the proposed protocol is enhanced compared with less efficient existing protocol.

1.5 Significant

The benefits of this thesis are as the follows:

1. Organizations, banks, merchants will be able to make e-payment without misusing the system by fraud. This will give them more time to concentrate on the development process rather than on the protection process.
2. The Ministry of Information and Communication Technology in HKJ, especially, E-government program for services that are needed by the citizens.
3. Previous studies concentrated on one aspect and neglected other problems while this thesis tries to examine several aspects and conditions.

1.6 Thesis Organization

The organization of the rest of this thesis is as follows:

Chapter Two describes the overview of e-payment systems

Chapter Three describes the proposed protocol and how it works.

Chapter Four describes the protocol analyses and discussions

Chapter Five describes the conclusions and future work.

Chapter Two: The Overview of E-Payment Systems

2.1 Introduction

The Internet has brought about innumerable changes to enterprises business. An essential problem to be solved before the widespread commercial use of the Internet is to provide a trustworthy solution for e-payment.

E-payment lowers costs for businesses. The more payments they can process electronically, the less they spend on paper and postage. Offering e-payment can also help businesses improve customer retention. A customer is more likely to return to the same e-commerce site where his or her information has already been entered and stored.

E-payment is very convenient for the customer. In most cases, you only need to enter your account information such as your credit card number and shipping address once. The information is then stored in a database on the retailer's web server. When you come back to the web site, you just log in with your username and password. Completing a transaction is as simple as clicking your mouse: All you have to do is to confirm your purchase and you are done.

Many e-payment systems rely on or extend non e-payment systems. Often they use existing infrastructures such as banks or credit card companies and create an e-communication system between vendor, customer, and bank. New e-payment systems have been introduced which focus on reduction of transaction costs, transaction speed and anonymity of the customer.

A good overview of e-payment systems can be found in [13]. In [23] links to websites are offered, describing payment mechanism designed for the Internet. In [4] information is provided on e-money products that are in use today or are being planned in 68 countries or territories.

2.2 Requirements for Internet Payment Systems

The e-payment protocol encompasses three participants

1. **User:** The user (customer) purchases e-currency from the bank employing actual money by e-payment. The user can then utilize e-currency to carry out e-payment to buy goods.
2. **Merchant:** The merchant is the data storage which provides user with both services and information.
3. **Bank:** The bank is the trusted authority. It mediates between user and merchant in order to ease the duties they carry out. In general, the bank acts like a broker who offers the e-coins for the e-payments. The following diagram shows the general e-payment system.

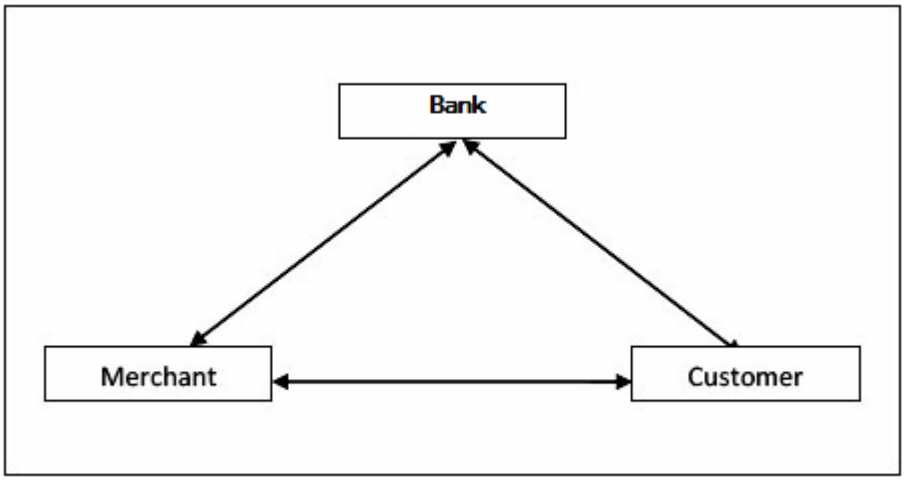

Figure 2.1:E-Payment System

E- Payment solutions can be assessed by the following properties [22]:

- **Atomicity:** The transaction must occur completely or not at all.
- **Security:** Transactions must be secure and no misuse of e-money should be possible.
- **Anonymity/Privacy:** It should not be possible to trace the flow of money so that the privacy of the user is affected.

- **Scalability:** Payment systems should scale to growing numbers of users.
- **Interoperability:** It must be possible to move value back and forth between different currencies.

The following sections give details on those properties.

2.2.1 Atomicity

When a payment transaction fails, it should be possible to recover the last consistent state so that the user is not harmed. It should be guaranteed that the purchase process is committed or rolled back as a unit. This requirement is similar to transactional database systems.

2.2.2Security

Security remains one of the important obstacles to the general acceptance of e-payment, forging paper bills is difficult; so, it can only be done by criminal experts with adequate hardware. E-currency on the other hand is just data and can be copied easily. Copying or double spending of e-currency must be prevented and be detectable. Ideally, the illegal creation, copying, and reuse of e-cash should be unconditionally or computationally impossible.

Since this is very hard to achieve most systems rely on detection and punishment of double-spending instead. The payment transaction itself must be secure against eavesdropping and modification.

2.2.3Anonymity

The identity of an individual using e-currency should not be disclosed. Some payment schemes ignore privacy issues at all and it is possible to track payments of individual users. Other protocols are unconditionally untraceable, where an individual spending cannot be determined even if all parties collude. For some transactions, weaker forms of anonymity may be appropriate, for example traceability can be made difficult enough that the cost of obtaining such information is higher than the benefit [24].

2.2.4 Scalability

Payment systems must be able to handle the addition of users and load in a certain range without negative impact on performance. The number of central servers where the transactions must be processed or checked limits the scale of the system.

Besides, the mechanism used to detect double spending directly affects scalability. Most e-cash protocols assume that a currency server will record all coins that already have been spent and consulted this database when verifying a transaction. The database will grow over time and it will be increasing the cost to detect double spending.

2.2.5 Interoperability

In real systems, multiple servers are needed to achieve scalability. Moreover, not all users are customers of the same server. In such an environment, it is important that currency produced by one currency server is accepted and can be checked by others

worldwide. Without mutual acceptance, e-currency could only be used between parties that share a common currency.

When currency minted by one server is exchanged between servers of the same payment protocol conversion of the currency should occur automatically.

2.3 Classification of Payment Systems

E-payment systems can be classified according to the following criteria:

2.3.1 On-line vs. Off-line Operation

Anonymity can be improved if two parties can make a safe transaction without first having to contact the server who issued the currency. So, no database can be built up which stores full details of every purchase made by an individual. A disadvantage of an off-line e-cash system is that fraud can only be detected after it has occurred.

2.3.2 Hardware vs. Software Solution

Some e-cash protocols rely on tamper-proof hardware to enhance software solutions such as client authentication, logon, and secure e-mail. An example is smart cards which provide tamper resistant storage for protecting private keys and other forms of personal information. They isolate security critical computations involving authentication, digital signatures, and key exchange from possible attacks to the payment system software.

2.3.3 Macro-payment vs. Micropayment

Credit cards and cheque payments are not always adequate solutions for e-payments. The standard e-payment methods cannot be applied for buying inexpensive objects for instance, stock prices since transaction costs are too high. Fees for bundled products often are high enough to be paid by credit cards or cheques. But when inexpensive objects are purchased individually, the transaction costs become a significant or even dominant component of the total price. A so-called micro-payment [24] system is needed for purchasing low-price products.

Micropayments and unbundling will be a natural response to a growing number of customized products.

All E-payment systems share the goal of minimizing the cost overhead of a single transaction. Most e-payment systems try to save costs, both monetary such as bank and transactions and network (packet round trips). The payment server must process transactions at a high rate because the profit made out of transactions is not very high. This must also be taken into consideration for transaction security: high security leads to high costs and computation time. For e-payments low security can be applied. When something goes wrong, the loss is negligible because of the low amount. Also the overall time for checking payments must be also kept minimal to make the payment system profitable.

2.4 Related works

This section provides an overview of related works and identifies the fundamental weaknesses of the existing e-payment schemes.

In 1982 (Chaum) [10] proposed a scheme entitled “Blind signature for untraceable payment”. He aimed to create an e-version of money; he introduced the notion of coins and blind signature which allow a message to be signed without revealing to the signer any information on the message. He claimed that a coin cannot be easily traced from the bank to the shop; furthermore, two spending for the same user cannot be linked together. He defined an e-coin as a number with a certificate (signature) produced by the bank; it is withdrawn from the bank, spent by the customer and deposited by the shop. This scheme does not provide transferability and fairness that might be misused by a fraud to perform a perfect crime.

In 1988 (Chaum, Fiat, Naor) [9] proposed a scheme entitled “Untraceable electronic cash”. In this scheme, they introduced the first practical e-cash system through using the blind signature paradigm to provide privacy and security for all the involved parties and they removed, in their approach, the requirement that the shopkeeper must contact the bank during every transaction.

In 1995, (Brickell, Peter and David) [6] proposed a scheme entitled “Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Exchange”. In this scheme, they introduced the e-payment system which incorporates with trustee to trace the anonymity if it misused but otherwise provably protect user anonymity. They also introduced an on-line anonymous change-making protocol which addresses a major stumbling block for anonymous payment system to exchange anonymously one set of coins for another set of coins of equal total value but different denominations. The system protection against multiple-spending of e-money and other fraud remains intact.

Also in 1995, (Stadler, Pivetaeu, Camenisch) [33] proposed a scheme entitled “Fair Blind Signature”. In this scheme, they proposed a new type of blind signatures called fair blind signature which was used to design a payment systems protecting privacy. The proposed scheme allows meeting the requirements of all parties. It guarantees the anonymity of the payment customer but it helps the trustee to revoke anonymity when it is required, for example legal reasons and it provides a solution against money laundering and blackmailing. This system cannot list all coins owned by a particular user.

In 1996, (Jan, Ueli, Stadler) [8] proposed a scheme entitled “Digital payment system with passive anonymity revoking trustee”. In this scheme, they proposed the efficient anonymous payment system in which a trustee is neither involved in payment transaction nor in the opening of an account; but, only in case of a justified suspicious transaction, a trustee is completely passive unless he is asked to

revoke the anonymity of a customer. It can also be used in on-line or off-line payment system; they introduce the concept of fairness for (non-transferable) e-payment.

Also in 1996, (Rivest and Shamir) [30] proposed a scheme entitled "PayWord and Micro Mint-two simple micro-payment schemes". In this scheme, they introduced a system that considered a credit-based system; it works as follows: First the customer sets up an account with a broker using a macro-payment protocol. Then the broker delivers a certificate to the user which must be renewed monthly. The certificate authorizes the user to generate a chain of hash values so-called pay words $w_0, w_1,\ldots, w_n$ where $w_{n-1} = h(w_n)$.h() is a cryptographically strong hash function. Each hash represents a pay word and has the same value for instant 1 US cent. The final chain is the concatenation of these *n* repeated hashes. This payword chain represents user credit at a specific vendor. A payword chain is only valid for one vendor. For a new vendor a new chain must be generated. The certificate also guarantees that a broker will redeem the paywords. By using fast hash functions instead of slow public key encryption more payment transaction per second are possible.

When the first transaction with a vendor is effected, a so-called commitment is sent from the user to the vendor. A commitment includes the root of the pay word $w_0, w_1,\ldots, w_n$, for the vendor name, the certificate of the customer, the actual date and additional information. For the following transactions the $i-th$ payment from the user to the vendor consists of the pair (w_i, i). The payword sent can be checked by applying the hash on w_i for i times, so that $w_0 = h(...h(w_i)...)$. At the end of the day the vendor contacts the appropriate broker and sends its pay-word with the highest index. The broker debits the account of the user and pays the vendor. The following figure shows the pay word transaction process.

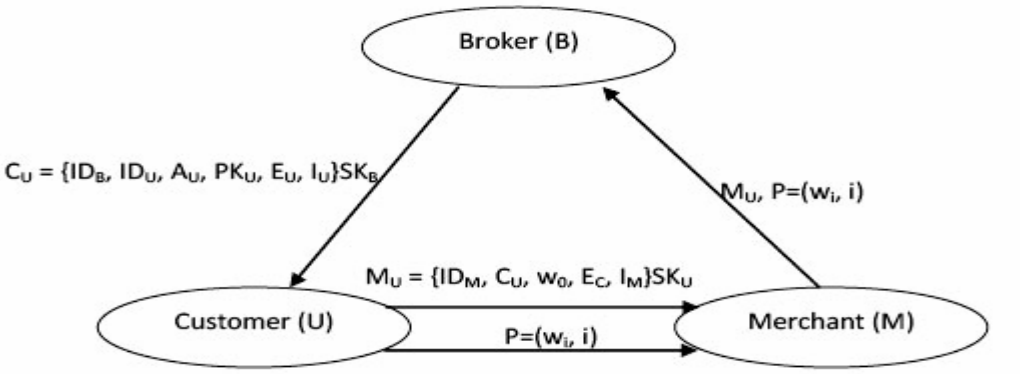

Figure 2.2: The PayWord scheme

In 1997,(Donal, Michael and Hitesh) [13] proposed a scheme entitled "Electronic Payment systems" in which they proposed e-cash that provides anonymous digital cash and uses blind signatures [10] to ensure anonymity of the customer. Strong security is provided by the use of symmetric and asymmetric cryptography. Three partners are involved in an e-cash system: clients, vendors, and banks. Customers and vendors must have accounts at the same bank which supports the e-cash payment system. The user can withdraw e-coins against his normal bank account and store them in a so-called cyber wallet at the user's computer. The coins are minted by the wallet of the user by applying serial numbers to it. These coins are then sent to the bank where they are signed blindly with digital signatures. So the coins become valid for later purchases. With these coins the user can now pay all vendors who accept e-cash. The vendor then sends the coins to the bank where they are checked for validity by verifying the signatures and double-spending. The bank must record every coin that is deposited back to the bank. So double-spending is not possible. If the coins are valid they will be deposited into the account of the vendor.

In 1997, (Davida, Frankel, Tsiounis and young) [11] proposed the protocol entitled "Anonymity control in E-cash Systems" in which they introduced the concept of Millicent that is considered as a lightweight and secure protocol for e-commerce over the Internet. Then it was developed by Compaq which uses a form

of e-currency called scrip. Millicent is intended for small value transactions, from a minimum of one cent or less to a maximum of approximately $5.00.

In 2001, (Joseph, Patrick, Wong) [19] proposed a scheme entitled "Recoverable and Untraceable E-cash". In this scheme they, proposed that an e-cash protocol which supports recoverability and un-traceability properties of e-cash systems simultaneously, such that it allows users to recover their lost e-cash while maintaining anonymity which provided that they have not double-spent their e-cash. Their system is still off-line and it combines the advantage of debit-based and credit-based systems together.

In 2003, (Kim, Lee) [16] proposed a scheme entitled "A Pay-word-based micro-payment protocol supporting multiple payments". In this scheme, they proposed the system in which they solved the problem that exists in Pay-Word system. The customer has to spend pay-word to a specific vendor by making the bank creates new hash chain values that enable a user to make payments with multiple vendors. The new chain is generated by hashing w_i and s_i where s_i is based on a shared user-broker secret. Unlike a normal chain, the user signs a commitment to the chain root and releases each following w_i as the payment. Since the final hash w_n is never fixed, the chain can be extended indefinitely by continuing to generate further w_i values. However, because of s_i is secret, the vendor is unable to verify any of the pay-words off-line. The vendor must trust the user to send valid pay-words. Indeed, even if the user cheats, the vendor cannot later prove this later.

In 2004, (Song, Kabra) [32] proposed a scheme entitled " How to Make e-Cash with Non-Repudiation and Anonymity". In this scheme, they proposed that an e-cash system in which a one-time public key (temporary anonymous) is embedded in the partial blind signature to provide the non-repudiation services against the problem which exists in e-cash systems like denying, losing, misusing,

stealing and double-spending and they also demonstrate that the combination of partial blind digital signature and anonymous digital signature make the e-cash systems more robust and fair than before. This scheme depends on high trust relation between the bank, user and trustee; so, the bank and the trustee can impersonate the user without being noticed.

In 2005, (Aboud and Al-Fayoumi) [2] proposed a scheme entitled "Blind Decryption and Privacy Protection". In their paper, they suggested a blind protocol employing ElGamal algorithm based on discrete logarithm which is considered an efficient way of protecting user's privacy in e-payment transaction, for example hiding information about user purchases from the merchant.

Also in 2005, (Binh) [5] proposed a scheme entitled "Fair Payment System with Online Anonymous Transfer". In this scheme, he proposed e-cash system that supports anonymous transfer and fairness using group signature protocol and he provides a flexible and privacy fundamental to e-commerce while providing an avenue for law enforcement to expose the users who abuse the system for illegal activities. The proposed protocol can deal with off-line payment and micropayment but, it is unable to stop extortion threats and the employs of blindfolded schemes.

In 2007, (Aboud and Al-Fayoumi) [1] proposed a scheme entitled "Anonymous and Non-Repudiation E-Payment Protocol". In this scheme, they suggest an efficient protocol for e-payment scheme that offers a good level of security with appreciate to its efficiency. The proposed protocol prevents the blind office and the bank from impersonating an entity, so that the entity could not repudiate it when the entity misused a coin.

In 2008, (Marina) [20] proposed a scheme entitled "Improved Conditional E-Payments". In this scheme, she depended on the "conditional e-payment" that was introduced by Shi et al. She proposed in her scheme that a payer obtains an e-coin

and can transfer it to a payee under a certain condition. In her work, she formalized the security of a conditional e-payment scheme and gave a solution based on CL-signatures and she completely avoided cut-and-choose techniques. She also eliminated the need for the bank to be involved in all conditional transfer protocols by making the protocol off-line.

In 2009, (Praneetha and Manik) [25] proposed a scheme entitled "An Improved and Efficient Micro-payment Scheme". In this scheme, they discussed the requirements of micro-payment and reviewed two micro-payment systems based on PayWord and hash chain. They also presented an alternate blinding phase using the RSA signature algorithm, but it is not efficient enough because their proposed scheme needs long key size at least 1024-bit which is considered a storage cost.

Chapter Three: The Proposed Protocol

3.1 Introduction

In 1976 Diffie and Hellmam [12] created the first revolutionary research in public key cryptography. They presented a new idea in cryptography and they challenged experts to generate cryptography algorithms that faced the requirements for public key cryptosystems. However, the first reaction to the challenge was introduced in 1978 by RSA [29]. The RSA scheme is a block cipher in which the original message and cipher message are integer values in the interval $[0...n-1]$ where n is composite modulus. The security of the RSA is based on the difficulty of finding the private encryption exponent d given only the public key, namely the public modulus n and the public encryption exponent e. The other reaction to this challenge is introduced in 1984 by ElGamal [14]. The ElGamal encryption algorithm is based on the discrete logarithm problem. The ElGamal encryption scheme is deterministic whereas the RSA is probabilistic in which, unlike the RSA algorithm, there are some public parameters which can be shared by a number of users. These are called domain parameters.

Algorithm finds a generator g of Z_p^*

Before going to discuss this algorithm, we should study the generator of a cyclic group. Suppose now that G is a cyclic group of order n. Then for any divisor of n the number of elements of order d in G is exactly $\theta(d)$, where θ is the Euler phi function. In particular, G has exactly $\theta(n)$ generators and hence the probability of a random element in G being a generator is $\theta(n)/n$. Using the low bound for the Euler phi function, this probability can be seen to be at least $1/(6\ln\ln n)$. This suggests the following efficient randomized algorithm for finding a generator of a cyclic group.

Algorithm: Finding a generator of a cyclic group

INPUT: a cyclic group G of order n and the prime factoring $n = p_1^{e_1} * p_2^{e_2} ... p_k^{e_k}$

OUTPUT: a generator g of G

1. Choose a random element g in G
2. For i from 1 to k do
   Compute $d = g^{n/p_i}$
   If $d = 1$, then go to step 1
3. Return (g)

Example

Suppose that $p = 11, \therefore \theta(p) = 10$, so the factors of $n = 2$ and 5

1. Suppose that $g = 2$
2. Compute $d = 2^{10/2} \bmod 11 = 10$, compute $d = 2^{10/5} \bmod 11 = 4$
3. $\therefore g$ is a generator

3.2 Algorithms Used

The algorithms used in the proposed protocol are as follows:

3.2.1 ElGamal keys generations

To generate the keys entity A must do the following:

1. Generate a large random prime number p by which we mean one with equally around 1024 bits, such that $p-1$ is divisible by another medium private q of around 160 bits and a random integer generator a an element of the multiplicative group Z_p^* of the integer mode p
2. Select a random integer $x, 1 \le x \le p-2$, which represents the private key
3. Compute the public key $h = a^x \bmod p$
4. Determine entity A's public is (p, g, h); and A's private key is x.

3.2.1.1 Example: keys generation

1.1. Selects $p = 11$.

1.2. Choose the generator $g = 2$.

1.3. Choose the private key $x = 5$.

1.4. Compute $d = 2^5 \bmod 11 = 10$

1.5. Public key is $(p = 11, g = 2, d = 10)$
while private key is ($x = 5$.)

3.2.3 Blind Signature

Blind signature schemes are a special form of signature schemes because they include an additional requirement [15].

A signer can sign a document without knowing its content. This requirement could be achieved by giving the signer a document which is encrypted or disturbed in some way. The unlinkability is an additional security requirement of a digital blind signature:

- No one can derive a link between one of the messages which the signer has received and a valid blind signature, except the signature requester.

The following figure demonstrates the process of blind signature:

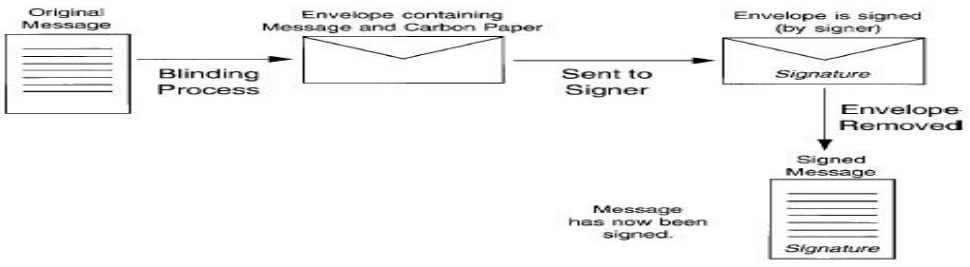

Figure 3.1: Blind Signature

3.2.3.1 Blind ElGamal signature scheme

Assume that the bank has a public key (*g, p, and d*) and a private Key *x*. Also suppose that user sends a message x_0 to bank. The user randomly selects an integer r less than $p-2$ and find $c_1 = g^r \bmod p$ and $c_2 = x_0 * d^r \bmod p$. Then send (c_1, c_2) to bank. Now the protocol is as follows:

- User randomly picks e less than $p-1$,find $\bar{x} = c_1^e \bmod p$ and sends $\bar{x}$ to bank
- Bank finds $\bar{y} = (\bar{x})^x \bmod p$ and sends $\bar{y}$ to User
- User employs the private key e to recover x_0 as follows:
  - Compute $z = (\bar{y})^{-1} \bmod p$
  - Compute $\bar{z} = (\bar{y}^{-1})^{\bar{y}} \bmod p$
  - Compute $x_0 = \bar{z} * c_2 \bmod p$

Example:

Suppose that the bank has a public key (*g=2, p*=2357, *and d*=1185) and a private key *x*=1751. Also suppose that user send a message $x_0 = 2035$ to bank. User randomly selects an integer $r = 1520$ less than $p-2$ and find $c_1 = 2^{1520} \bmod 2357 = 1430$ and $c_2 = 2035 * 1185^{1520} \bmod 2357 = 697$. Then send $(c_1 = 1430, c_2 = 697)$ to bank. Now the protocol is as follows:

- User randomly picks $e = 21$ less than $p-1$,find $\bar{x} = 1430^{21} \bmod 2357 = 1881$ and sends $\bar{x}$ to bank
- Bank finds $\bar{y} = 1881^{1751} \bmod 2357 = 313$ and sends $\bar{y}$ to user
- User employs the private key e to recover x_0 as follows:
  - Compute $z = 313 * 1860 \bmod 2357 = 1$
  - Compute $\bar{z} = 1860^{313} \bmod 2357 = 872$
  - Compute $x_0 = 872 * 697 \bmod 2357 = 2035$

3.2.4 Hash Function

A hash chain is a successive application of a cryptographic hash function $h(x)$ to a string where the idea of hash function was first proposed by Lamport [17] in 1981 and suggested to be used extensively in various cryptographic systems such as one- time passwords, server supported signatures, secure address resolution, certificate revocation, micropayments etc. To facilitate safeguarding, one time password schemes (OTPs) from 'eavesdrop and replay' kinds of attack. Since then it has been employed in a wide range of applications. Hash chains have interesting properties while employing nothing more than a fast one way hash function.

When the function in the iteration is instantaneous with a one-way hash function, such as SHA, the result is a one-way hash function as shows in Figure element x_i is computed as $h^{n-r}x_n$.

$$W_0 = h^n(W_n) \leftarrow W_1 = h^{n-1}(W_n) \leftarrow W_2 = h^{n-2}(W_n) \leftarrow \dots \leftarrow W_{n-1} = h^1(W_n) \leftarrow W_n$$

Figure 3.2 : One-way Hash Function

3.3 Kim and Lee Protocol

In 2003, Kim and Lee [16] proposed e-payment protocol that supports multiple merchants. The protocol is divided into three schemes: certificate issuing scheme, payment scheme and redemption scheme.

3.3.1Certificate Scheme

User U requests a certificate to a bank B by sending his secret information through a pre-established secure channel. The bank B passes C_U , which guarantees to be justified and S_U which will be employed for the root value in payment scheme later. Every user U creates his public and secret key pair (PK_U, SK_U) and passes

PK_U with I_U that contains the maximum number of merchants N, the size of hash chain n with his credit card information to the bank B. As a user certificate signed by a bank B, those who intend to employ this key should trust him. The bank B generates special information T_U, which acts as a key factor of the root value. It is employed to make clear that the new hash values created by the bank B are published to whom, because no individual except the bank B can generate it.

$T_U = h(U, r_B, K)$, where K is the private key of the bank B

$S_U = (s_i \mid s_i = h(s_{i+1}, T_U), i = N-1,...,0)$, where s_i is created by a shared user-bank private key.

The certificate C_U, in which all the elements as well as the expiry date of the certificate E_U are signed by the bank B and pass to the user U with S_U and a nonce r_U.

$C_U = (ID_B, ID_U, PK_U, T_U, I_U, E_U)SK_B$. We will show the transaction process of Kim and Lee protocol in Figure 3.3.

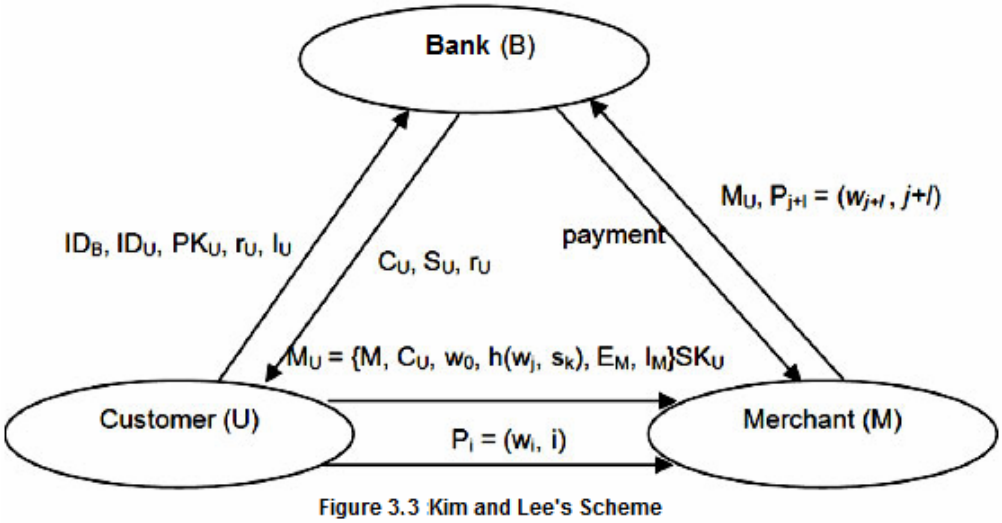

Figure 3.3 :Kim and Lee's Scheme

3.3.2 Payment Scheme

The root value of pay-words is merged with s_i that is obtained from the bank B, which enables the user U to employ the rest of the unspent pay-words in chain for multiple payments to other merchants. The user who obtains the certificate in preceding scheme can now generate pay-words and commitment. The commitment contains the identity of the merchant with whom a user intends to do commerce, the certificate, the root element which is modified into $\mathrm{wj, h(wj, sk),}$ the expiry date of the commitment E_M, and other data I_M, such that $0 \le j \le n$ employed to setup root value for other merchants. Then the user U signs the elements $M_U = (V, C_U, w_0, h(w_j, s_k), E_M, I_M)SK_U$

To spend the remainder of the pay-words in chain, the user U must set the root value of pay-words to be spent in subsequently payment scheme with the merging of hash chain values respectively created by a user U and the bank B. For instance, when it is supposed that a user U employed pay-words as many as w_{j-1} in preceding transactions and spent l pay-words at the present transaction with k^{th} merchant, the root value of pay-words must be identical with $\mathrm{h(wj, sk)}$ to be suitable for the payments. The user U can apply his pay-words to other merchants up to the maximum transaction limit of N unless the last pay-word surpasses wn. The merchant keeps the last received payment data of $\mathrm{Pj+1 = (wj+1, j+1)}$ and the commitment, and finishes the payment scheme.

3.3.3 Redemption Scheme

Merchant must perform the redemption process with a bank B within a pre-agreed period of time. The bank B verifies if the payment request of the merchant is correct or not by checking the certificate.

First, the merchant orders for redemption to a bank B by passing the user U commitment and payment parameter. From this information, the bank B checks his signature noticeable at the certificate and redeems p_{j+1} to an equivalent amount of money. We note that the bank B can check pay-words only from w_j to w_{j+1} for that order. However, since the equivalent source value is w_{j+1}, the only thing imposed to the bank B is that the last received pay-word w_{j+1} is identical with w_j by applying hash function l times. The bank B processes redemption orders from merchants less than N before being overdue. Finally, the bank B completes the redemption process when the last received value w_l is less than the maximum value of the hash.

3.4 Proposed Protocol

We will suggest an efficient protocol in this section which gives more efficiency than its present version of the pay-word scheme. We describe this protocol a bit more on in order to make a simple comparison between both. Thus, gauging the efficiency and security of the protocol will be described in Chapter Four. However, the protocol is divided into four schemes, registration scheme, blind scheme, transaction scheme, and redemption scheme. Also in this section, we will introduce a blind scheme using the ElGamal-typed blind signature. We will show that this improvement makes the pay-word protocol more efficient and keeps all other characteristics consistent.

3.4.1Blind Protocol

1. Protocol Steps

The user passes a withdrawal order to the bank prior to his order for any service from merchant. The steps of the scheme are as follows:

Step 1: Bank

1.1. Select the prime numbers p

1.2. Choose the generator g of Z_p^*.

1.3 Choose the private key x.

1.4. Compute $d = g^x \bmod p$

1.5. Public key is (p, g, d)

while private key is (x)

1. 6.Select an arbitrary number $x_1 < p$ and pass x_1 to the user

Step 2: User

2.1. Select arbitrary three numbers, e , z *and* r_1 less than p

2.2. Calculate $a = e^d * h(x_0)(z^2 + 1) \bmod p$

2.3. Calculate $b_2 = e * r_1$

2.4. Calculate $\beta = (b_2)^d * (z - x_1) \bmod p$ to the bank

2.5. Pass (b, a, β) to the bank

Note that information b can indicate the expiry date; the value of cash (higher limit) that the user can employ that is the funds of every hash currency, where b less than p .

Step 3: Bank

3.1. Calculate $V = \beta^{-1} \bmod p$

3.2. Compute $t_1 = h(b)^x * (a(x_1^2 + 1) * \beta^{-2})^{2*x} \bmod p$

3.3. Pass (V, t_1) to the user

Step 4: User

4.1. Calculate $c_1 = (z * x_1 + 1) * V * (b_2)^d = (z * x_1 + 1)(z - x_1)^{-1} \bmod p$

4.2. Calculate $s_1 = t_1 * e^2 * (r_1)^4 \bmod p$

The following figure illustrates the steps of the proposed protocol:

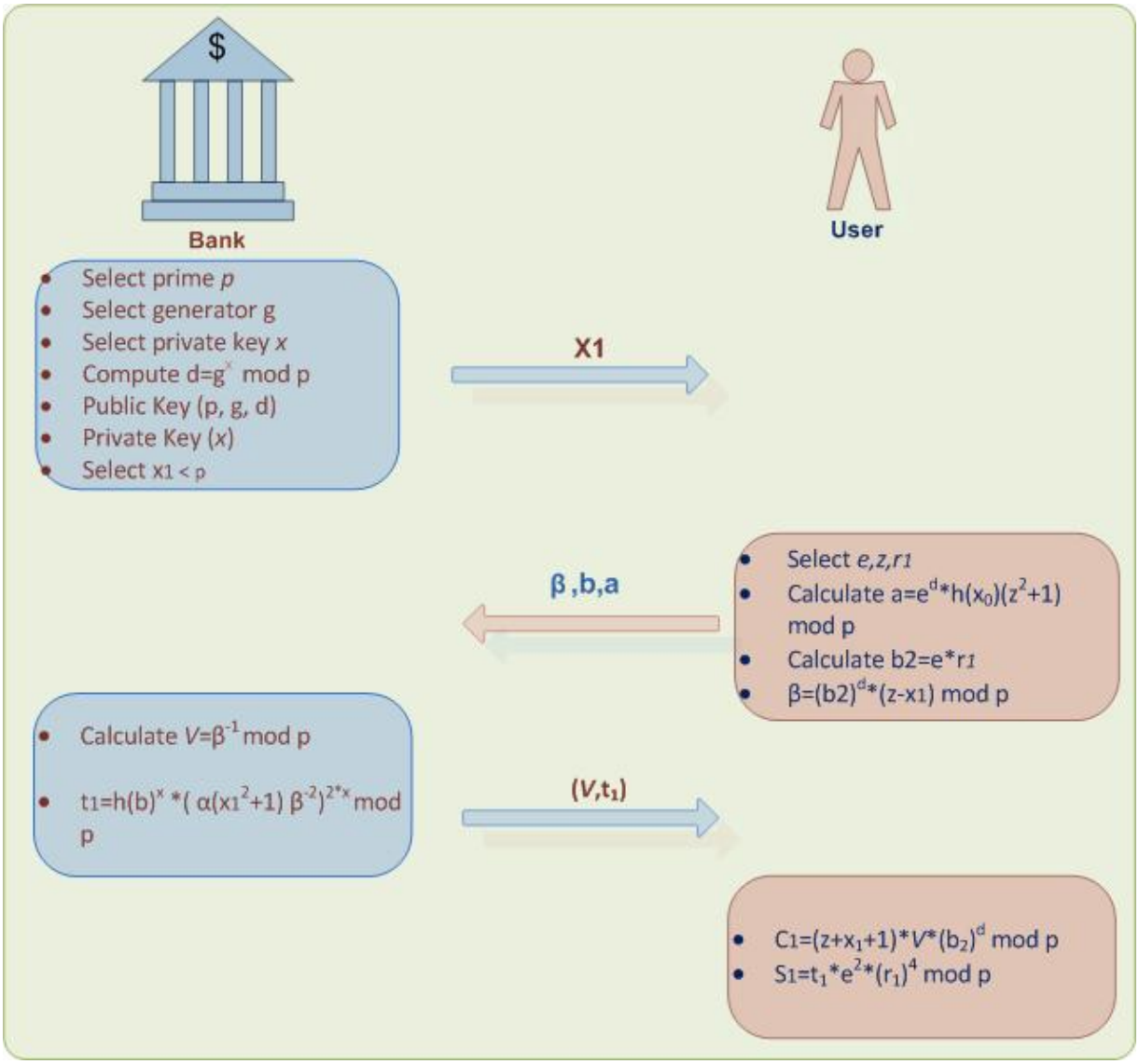

Figure 3.4: Blinding Protocol

2. Verification

The parameter $(b, c_1.s_1)$ is the signature on message x_0. Anybody can check this signature by verifying if $s_1^d \equiv h(b)h(x_0)^2 * (c_1^2 + 1)^2 \bmod(p-1)$

3.4.2 Proposed protocol Correctness

$$s_1^d \equiv t_1 * e^2 * r_1^4 \bmod (p-1)$$

- $(h(b)^x (a(x_1^2+1)\beta^{-2})^{2rx} * e^2 * r_1^4)^d \bmod (p-1)$
- $(h(b)^x (e^d h(x_0)(z^2+1)(x_1^2+1)e^{-2d} r_1^{-2d}(z-x_1)^{-2})^{2rx} * e^2 * r_1^4)^d \bmod (p-1)$
- $(h(b)^x (r^d h(x_0)(z^2 x_1^2 + x_1^2 + z^2 + 1)e^{-2d} r_1^{-2d}(z-x_1)^{-2})^{2rx} * e^2 * r_1^4)^d \bmod (p-1)$
- $(h(b)^x (e^d h(x_0)((z x_1 + 1)^2 + (z-x_1)^2)e^{-2d} r_1^{-2d}(z-x_1)^{-2})^{2rx} * e^2 * r_1^4)^d \bmod (p-1)$
- $(h(b)^x (e^d h(x_0)(c_1^2 + 1)e^{-2d} r_1^{-2d})^{2rx} * e^2 * r_1^4)^d \bmod (p-1)$
- $(h(b)^x (e^{2drx} h(x_0)^{2rx}(c_1^2+1)^{2rx} e^{-4drx} r_1^{-4drx}) e^2 * r_1^4)^d \bmod (p-1)$
- $\equiv (h(b)^x * e^{2d} * h(x_0)^{2dx} * (c_1^2+1)^{2dx} * e^{-4d} * r_1^{-4d} * e^{2d} * r_1^{4d}) \bmod (p-1)$
- $h(b)^x * h(x_0)^2 * (c_1^2+1)^2 \bmod (p-1)$

Where:

- $\beta = b^2 (z-x)$
- $b = e * r_1$
- $((z x_1 + 1)^2 + (z-x_1)^2)(z-x_1)^{-2} = (z x_1 + 1)^2 (z-x_1)^{-2} + (z-x_1)^2 (z-x_1)^{-2}$

$= (z x_1 + 1)^2 (z-x_1)^{-2} + 1$, Where $c_1 = (z x_1 + 1)(z-x_1)^{-1} = c_1^2 + 1$

3.4.3 Example

The following example illustrates the result of proposed scheme. The steps of the scheme are as follows:

1. Protocol Steps

Note: for simplicity we will suppose hash values identical (i.e. $h(x_0) = x_0$).

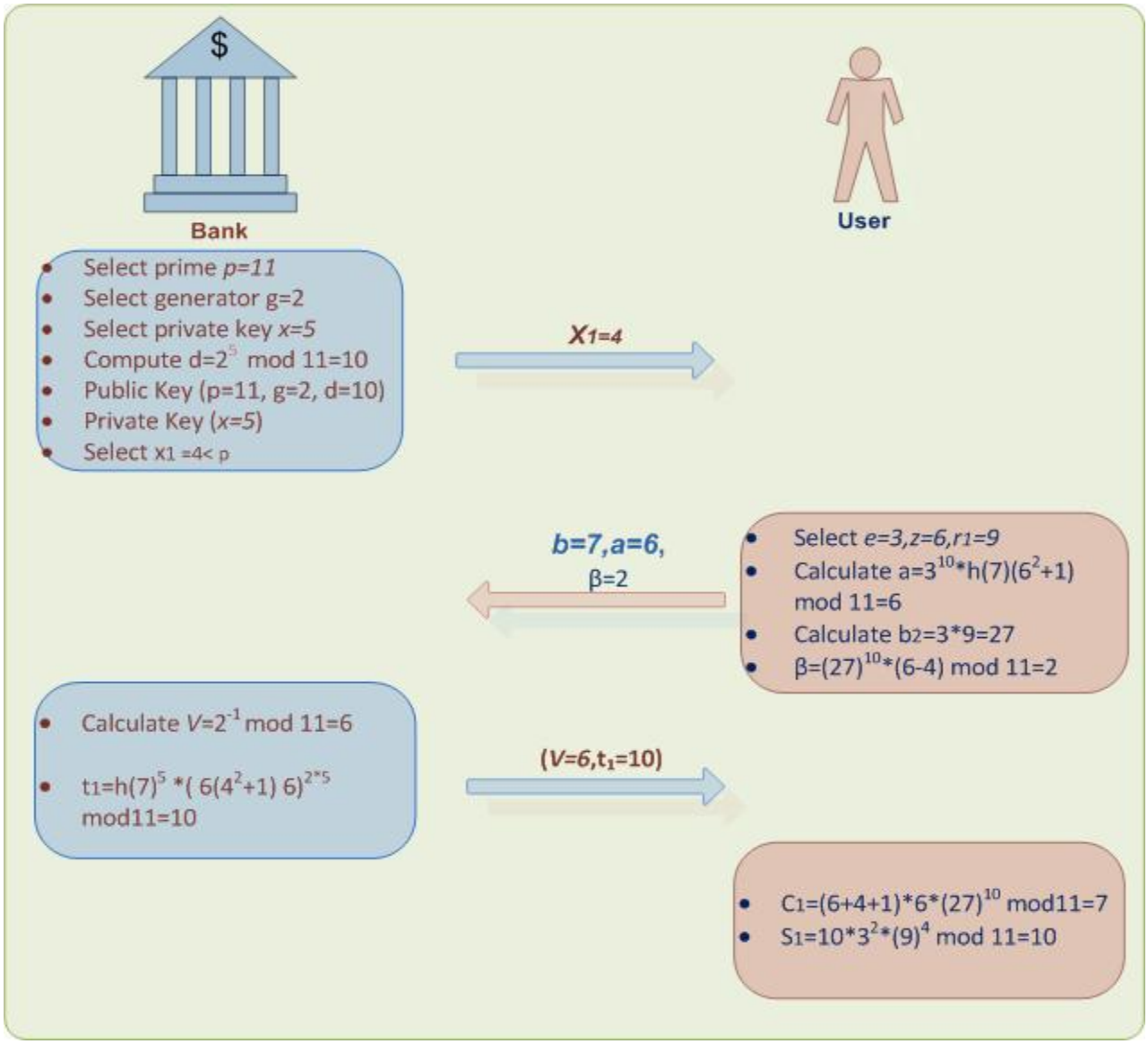

Figure 3.5: Blinding protocol Example

Step 1: Bank

1.3. Select $p = 11$.

1.4. Choose the generator $g = 2$.

1.3. Choose the private key $x = 5$.

1.4. Compute $d = 2^5 \bmod 11 = 10$

1.5. Public key is $(p = 11, g = 2, d = 10)$
while private key is $(x = 5.)$

1.6 Select an arbitrary number $x_1 = 4 < 11$ and pass $x_1 = 4$ to the user

Step 2: User

2.1. Select arbitrary three numbers, $e = 3$, $z = 6$ *and* $r_1 = 9$

2.2. Calculate $a = 3^{10} * h(7) * (6^2 + 1) \bmod 11 = 6$

2.3. Calculate $b_2 = 3 * 9 = 27$

2.4. Pass $\beta = (27)^{10} * (6 - 4) \bmod 11 = 2$ to the bank

2.5. Pass $(b = 7, a = 6, \beta = 2)$ to the bank

Step 3: Bank

3.1. Calculate $V = 2^{-1} \bmod 11 = 6$

3.2. Compute $t_1 = h(7)^5 * (6(4^2 + 1) * 6)^{10} \bmod 11 = 10$

3.3. Pass $(V = 6, t_1 = 10)$ to the user

Step 4: User

4.1. Calculate $c_1 = (6 * 4 + 1) * 6 * (27)^{10} \bmod 11 = 7$

4.2. Calculate $s_1 = 10 * 9 * 6561 \bmod 11 = 10$

2. Verification

The parameter $(b = 7, c_1 = 7. s_1 = 10)$ is the signature on message x_0. Anybody can check this signature by verifying if $s_1^d \equiv h(b)h(x_0)^2 * (c_1^2 + 1)^2 \bmod (p - 1)$ is equal then the blinding successes.

CHAPTER Four: Protocol Analyses and Discussions

In this section, we will discuss both the security and efficiency of the proposed protocol.

4.1. Security Analyses

The proposed protocol withstands the following threats:

4.1.1. Forgery Detection

The user U gets the bank B signature on x_0 prior to any transaction. The blind signature is relied on ElGamal scheme, which is extensively employed a secure signature scheme. Besides, in order to process an accurate redemption, the merchant M should have information of the payment transaction. It is almost unfeasible for any entity to forge the user U payment without knowing the private key.

4.1.2. Overspending Prevention

In our proposed protocol, the following are included: the credit card number, the maximum length of paywords, and the maximum length of hash chains in the user's private information *IM*. It could be protected from the customer's overspending beyond the limitation since there is such factor as the maximum length of payword in *IM*.

4.1.3 Multiple Payments

In the transaction phase, the user U sends an order to the bank B, and generates the payment transaction which contains special data T_u and S_u to enable the user carry out the purchasing with multiple merchants.

4.1.4 Connectivity Unallowable

For any provided valid signature (b, c_1, s_1) no one except the requester can connect the signature to its preceding signing order. This means that the signer is incapable

of getting the connection between the signature and its equivalent signing process order.

4.2. Efficiency

In order to gauge the efficiency of the proposed protocol, we compare the enhanced blind protocol with the Kim protocol [16]. The time complexity of the remaining scheme stays the same in both protocols. We employ the following notation to gauge the efficiency of the schemes.

T_h: Calculation time for Hash function

T_a: Calculation time for modular multiplication

T_m: Calculation time for modular exponentiation

T_e: Calculation time for asymmetric key encryption

Table 4.1: Time complexity comparing with Kim protocol

	Compared Protocols
The Kim Protocol	$5*T_h + 9*T_a + 5*T_m + 3*T_e$
Proposed Protocol	$2*T_h + 6*T_a + 7*T_m + 3*T_e$

Actually, the modular exponentiation is a costly operation in comparison with multiplication operations. As a result, it is simple to observe from table 4.1 that the proposed protocol is more efficient than the Kim protocol because it is T_h and T_a are less than the same value in Kim although that Kim has T_m less than the proposed protocol but in general the proposed protocol is more efficient.

Table 4.2: Time complexity with Hwang and Song Scheme

	Compared Protocols
Hwang and Song Scheme	$4*T_h + 7*T_a + 3*T_m + 1*T_e$
Proposed Protocol	$2*T_h + 6*T_a + 7*T_m + 3*T_e$

Actually, the modular exponentiation is a costly operation in comparison with multiplication operations. As a result, it is simple to observe from table 4.2 that the proposed protocol is more efficient than **Hwang and** Song scheme because its T_h and T_a are less than the same value in improved although that improved has T_m less than the proposed protocol but in general the proposed protocol is more efficient. Furthermore, when any entity chooses small public key e; for example 7, then the proposed protocol becomes more efficient. This makes public key operations quicker while the secret key operations remaining unchanged. So, the proposed protocol decreases expensive exponential operation and has better time efficiency.

4.3 Comparisons

Table 4.2 shows comparison results and contains three systems, our new system and two old ones. The comparison covers several properties.

Table 4.3: Comparison of schemes based on general security properties

	PayWord	Kim and Lee	Proposed Scheme
Anonymity	**X**	**X**	✓
Double Spending Detection	✓	✓	✓
Forgery Prevention	✓	✓	✓
Non-Repudiation	**X**	✓	✓
Overspending Prevention	**X**	✓	✓
Multiple Payment	**X**	✓	✓

✓ **:** Satisfied **X**: Not Satisfied

CHAPTER FIVE: Conclusions and Future Work

5.1 Conclusions

The technological evolutions in accordance with the modern techniques can be applied by governance and finance sectors in order to build the ideal e-government and e-finance systems.

The proposed e-payment protocol described offer good level of security with appreciates to its efficiency. So, we described the characteristics of e-payment protocol and evaluated one of the most important e-payment protocols that relied on a hash function [16]. A hash function typed scheme gives anonymity security characteristic besides other security features of e-payment protocol. The use of the blind signature scheme and one-way hash function made the protocol more efficient and it guaranteed the payment untraceable. We noticed that the blind scheme of the protocol [24] took significantly more computing time and we presented an alternate blind scheme using the ElGamal signature scheme that gave more efficiency than the existing protocols. The proposed protocol will be beneficial to small value payments.

This thesis described an efficient designed scheme with three characteristics of anonymity, non-repudiation and traceability, as well as evaluation of a provably secure

remote e-payment system. Based on our knowledge, this has not been done before. It provided stronger security than previously implemented e-payment systems. It was one of the first protocols that achieved prevention of any type of extortion threats. It could be used for secure internet e-payment and efficient e-purse and in e-government services that require payment over internet where the efficiency and security requirements are completely different.

Perhaps the most important contribution of this work is strong evidence that, contrary to conventional wisdom, secure e-payment is possible and even feasible. We are optimistic about the future of payment systems constructed, like this work, using principled techniques.

5.2 Future Works

The results in this thesis also provide a strong foundation to continue for future work to build very well e-payment schemes over the entire world. One area of future work is in combining the knowledge gained about increasing the privacy and the anonymity of the user especially in on-line shopping and purchasing to build secure online payment scheme.

Another area is in applying the results studied here to many real-world situations which need payment schemes to apply some research to make all government operations in one consistent scheme including services that need payment to reach full e-government at the end.

The research work accomplished in this thesis has vast future prospects and can be extended towards a substantial protocol using hash function so that the modular exponentiation and costly operation can be shunned and also similar security depth can be reached.

Mobile telephony is a growing market over all the world, and the e-commerce is an open circumstance on the open network especially, wireless network environment ,mobile users can buy services from multiple internet service provider more securely and efficiently.

REFERENCES

[1] Aboud S., M. Al-Fayoumi. Anonymous and Non-Repudiation E-Payment Protocol. American Journal of Applied Sciences 4 (8): 538-542, 2007.

[2] Aboud S., M. Al-Fayoumi. Blind Decryption and Privacy Protection. American Journal of Applied Sciences 2 (4): 873-877, 2005.

[3] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[4] Bank for International Settlement. Survey of electronic money developments, May 2000.

[5] Binh, D. A Fair Payment Scheme with Online Anonymous Transfer. M.Sc Thesis. MIT, pp: 3-27. 2007

[6] Brickell, E., P. Gemmell and D. Kravitz, Trustee-based Tracing Extensions to anonymous Cash and the Making of Anonymous Exchange. Proceeding of 6th Intl. Conference of ACM-SIAM SODA: 457-466, 1995

[7] Carmenisch J. L., J.-M. Pivetaeu and M.A. Stadler. Blind signature based on the discrete logarithm problem EURO-CRYPT '94, Perugia, Italy,1995

[8] Camenisch, M and M. Stadler. Digital Payment Systems with Passive anonymity revoking trustees: Computer Security- ESORICS96, Lecture Notes in Computer Security 1146. Springer-Verlag, PP: 33-34. 1996.

[9] Chaum, D., Amost, F, and Moni, N, "Untraceable Electronic Cash", Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 318-327, 1988

[10] Chaum D. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology Proceedings of Crypto 82*, pages 199–203, 1982.

[11] Davida G., Y. Frankel, Y. Tsiounis, M. Yung. Anonymity Control in E- Cash Systems. In Financial Cryptography ’97, Springer-Verlag, LNCS 1318, pp.1–16, 1997.

[12] Diffie W. and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory IT-22*, pages 644–654, 1976.

[13] Donal, O. Michael P, and Hitesh T. *Electronic Payment Systems*. Artech House Computer Science Library, June 1997.

[14] ElGamal T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transaction on Information Theory, 1985.

[15] Frank N. , Diploma Thesis, Development of a lattice based blind signature scheme- Darmstadt University of Technology Department of Computer Science Cryptography and Computer algebra, 2007.

[16] Kim, S. and Lee, W, A Pay-word-based micro-payment protocol supporting multiple payments, Proceeding of the International Conference on Computer Communications and Networks, pp. 609-612, 2003.

[17] Lamport, L. "Password authentication with insecure communication," Commun. Of ACM, vol. 24, no.11, pp. 770-772, 1981.

[18] Liisa, K. The Perfect Payment Architecture, Technical Document Mobley Forum, www.mobeyforum. 2001.

[19] Liu, J., K. Wei and S. Wong, Recoverable and Untraceable E-Cash, EUROCON' 2001: Trends in Communications. Intl. Conference on Information Technology, Vol. (1): 342-349. 2001.

[20] Marina, b. improved conditional e-payment. Department of Computer Science and Engineering, University of Notre Dame.pp.18-19. 2008.

[21] Micali, S. Simple and Fast Optimistic Protocols for fair e- exchange. Proceeding in Intl. Conference of 22nd Annual ACM Symposia: On Principles of distributed Computing (PODC'03). ACM Press: 12-19. 2003.

[22] Michael, P. An implementation of the Millicent micro-payment protocol and its application in a pay-per-view business model, Distributed Systems Group, 2000.

[23] Michael P. Payment mechanisms designed for the Internet. http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html

[24] Michel T. Micropayment's overview, October 2000. http://www.w3.org/ECommerce/Micropayments/

[25] Praneetha R.and Manik Das. An Improved and Efficient Micro-payment Scheme. Journal of Theoretical and Applied Electronic Commerce Research, Vol4/pp91 100, 2009.

[26] National Institute of Standards and Technology (NIST). Federal Information Processing Standard (FIPS) Publication 180-1: Secure Hash Standard, April 1995.

[27] NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems: U.S National Computer Center. 2000.

[28] Otto, P, O. Novac and S, Vári-Kakas, Analysis of an Electronic Payment System Using Simulation, Department of Computer Science, Faculty of Electrical Engineering and Information Technology, University of Oradea Univeritatii Str., nr.1, Oradea, Romania: 325-332.

[29] Rivest R.L., A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems .*Communications of the ACM*, 21(2):120–126, 1978.

[30] Ronald L. Rivest and Adi Shamir. Payword and micro mint– two simple micropayment schemes. In *Proceedings of 1996 International Workshop on Security Protocols, Lecture Notes in Computer Science v.1189*, pages 69-87.Springer, 1997. 30

[31] Simon D. Anonymous Communication and Anonymous Cash. In *Crypto'96*, Springer-Verlag, LNCS 1109, pp.61–73, 1996.

[32] Song, R and L. Korba,. How to Make E-cash with Non- Repudiation and Anonymity. Proceedings of the Intl. Conference on Information Technology: Coding and Computing, (ITCC'04):167-172. 2004.

[33] Stadler, J.M. Piveteau, and J. Camenisch. Fair blind signature. In Proc. EUROCRYPT 95, pages 209–219. Springer-Verlag .LNCS Vol. 921. 1995.

APPENDICES

APPENDIX A: Proposed protocol Complexity

Step 1: Bank

1.1. Selects the prime numbers p

```
Dim isPrim As Boolean = False
Dim p, number As Integer
While isPrim = False
   p = InputBox("select prim number:")
    For i As Integer = 1 To p
      If p Mod i = 0 Then
         If i <> 1 Or i <> p Then
            MsgBox("try again")
            isPrim = False
            Exit For
         Else
            isPrim = True
         End If
      End If
   Next
End While
```

1.2. Choose the generator g of Z_p^*.

```
Dim g As Integer = InputBox("select Generator:")
```

1.3 Choose the private key x.

```
Dim x As Integer = -1
While x < 1 Or x > p
   x = InputBox("Choose the private key:")
End While
```

1.4. Compute $d = g^x \bmod p$

```
Dim d As Integer = (g ^ x) Mod p
```

$$1*T_m$$

1.5. Public key is (p, g, d)
while private key is (x)

Dim **PublicKey() = {p, g, d}**
Dim **PrivateKey = x**

1. 6.Select an arbitrary number $x_1 < p$ and pass x_1 to the user

Dim **rand** As **Random**
Dim **x1** As Integer = **rand.Next(p)**

PassToUser(x1, user) → $1*T_e$

Step 2: User

2.1. Select arbitrary numbers, e , z *and* r_1 less than p

Dim **e** As Integer = **rand.Next()**
Dim **z** As Integer = **rand.Next()**
Dim **r1** As Integer = **rand.Next()**

2.2. Calculate $a = e^d * h(x_0)(z^2 + 1) \bmod p$

Dim **x0** As Integer = **InputBox(**"select x0:"**)**

Dim **hx0** As Integer = **hashFunction(x0)**

$1*T_h$

Dim **a** As Double = **(e ^ d * hx0 * (z ^ 2 + 1))** Mod **p**

$1*T_a$ $2*T_m$

2.3. Calculate $b_2 = e * r_1$

Dim **b2 = e * r1**

$2*T_a$

2.4. Calculate $\beta = (b_2)^d * (z - x_1) \bmod p$ to the bank

Dim **Beta** As Double = **(b2 ^ d * (z - x1))** Mod **p**

$3*T_a$ $3*T_m$

2.5. Pass (b, a, β) to the bank

Dim **Arr()** As Integer = **{b, a, Beta}**

PassToBank(Arr(), Bank) → $2*T_e$

Note that information b can indicate the expiry date; the value of cash (higher limit) that the user can employ that is the funds of every hash currency. Where b less than p .

Step 3: Bank

3.1. Calculate $V = \beta^{-1} \bmod p$

Dim **V** As Double = **Beta ^ -1** Mod **p**

$4*T_m$

3.2. Compute $t_1 = h(b)^x * (a(x_1^2 + 1) * \beta^{-2})^{2*x} \bmod p$

Dim **b** As Double = **InputBox(**"select b:**")**
Dim **hb** As Double = **hashFunction (b)**

$2*T_h$

Dim **t1** As Integer = **((hb ^ x) * (a * (x1 ^ 2 + 1) * Beta ^ -2) ^ (2 * x))** Mod **p**

$4*T_a$ $5*T_m$

3.3. Pass (V, t_1) to the user

Pass(V, t1, user) → $3*T_e$

Step 4: User

4.1. Calculate $c_1 = (z * x_1 + 1) * V * (b_2)^d = (z * x_1 + 1)(z - x_1)^{-1} \bmod p$

Dim **C1** As Integer = **((z + x1 + 1) * V * (b2) ^ d)** Mod **p**

$5*T_a$ $6*T_m$

4.2. Calculate $s_1 = t_1 * e^2 * (r_1)^4 \bmod p$

Dim **S1** As Integer = **(t1 * e ^ 2 * (r1) ^ 4)** Mod **p**

$6*T_a$ $7*T_m$

- **The complexity calculation is:** $2 * T_h + 6 * T_a + 7 * T_m + 3 * T_e$

"تم بحمد الله"