**A SECURE ON-LINE PAYMENT SYSTEM BASED ON PAYWORD**

Md. Martuza Ahamad

Md. Ibrahim Abdullah

Dept. of Computer Science and Engineering  
Islamic University

November 2017

**Chapter - 1**

**Introduction**

Now a day’s online shopping is going to be very popular. People buy and sale their daily necessary products from various e-commerce website. And people take many online services from various online service providers. So we know that in that services online payments are very useful. Consumer pay for product or service then merchant deliver product or give that service. In that type of payment system consumers transfer his/her payment amount to merchant over open network. So that are online transaction. These transactions have to concern about security and privacy.

**1.1 Electronic Payment**

Electronic payment (E-payment) system is a way to pay for products or any kinds of services over internet without using any hard cash. E-payment is a huge flourishing field of online transactions as a result of accelerated growth of internet based banking and shopping. Due to rabid development of technology a lot of secure online shopping websites known as e-commerce websites are available and a lot of online payment methods are also available where secure money transfer is too easy now.

Electronic payment method can be classified two areas based on payment system [1]

1. Cash payment system
2. Credit payment system

**1.1.1 Cash payment system**

**Electronic Fund Transfer (EFT):** Electronic fund transfer is a technique to transfer money via internet from one account to another account in a specific bank.

Electronic Fund Transfer is a system which is constructed using many payment system concepts:

**Direct debit:** Direct debit is a system, where money can be transfer from customer account to merchant account directly over internet. It is used for buying goods or paying for any kinds of services.

**Electronic-Check (E-Check):** E-Check is a special kind of check alternative of traditional paper check. It is used, when it is needed to transfer money from one account to another account.

**Electronic billing:** It is a method for collecting payment from customers used by merchants/companies in transferring funds over internet.

**Electronic Cash (E-Cash):** It is a system of electronic cash, in where certain amounts are stored in electronic devices. It is a form of digital cash accessible from electronic devices installed specific software in computer or any other electronic devices.

Stored value card: It is as like as gift card. Where a certain amount of money are stored in a card. It is another form of Electronic Fund Transfer (EFT) system.

**1.1.2 Credit payment system**

**Credit Card:** It is a another form of e-payment system. Where needed a financial corporation for issuing cards. That helps to payment online using that credit card without using cash payment.

**E-Wallet:** E-Wallet is a another type of prepaid account where credit and debit card information’s are stored and make online transactions more easier.

Smart Card: It is a plastic microprocessor embedded card. It is used to transfer funds very instantly. Actually is a small electronic chip, a reader is used to read card information and transfer amounts.

Electronic payment system also can be classify two categories based on amount of transaction [2] –

1. Micro payment
2. Macro payment

**1.2.1 Micro Payment**

Micro-payment is an electronic payment system where a small amount (less than 1$ or few cents) is to be pay. It has less security concern so when the system of micro-payment is designed light weight cryptographic technique has been used. So the system is light weight and less time and computational cost is required for every transaction. Frequent transaction is possible within very short of time. Because of this system transfer very few amounts so it’s security also needed less. Fraud rate of micro-payment is less because the gain amount is very small than effort of cheating. But some security is needed for micro-payment in the field of consumer merchant authentication, consumer issuer signing etc.

**1.2.2 Macro Payment**

Macro-payment is also an electronic payment system where a large amount (more than 1$) is to be pay. Because of this system handle a large sum of amount is should have a trusted secure payment method. So it use more secure authentication cryptographic algorithms for authentication. It has needed more space to store transaction information’s. And needed more computational time and steps. For authentication it uses public key cryptographic algorithms.

**1.3 Scope of online payment**

In our growing economy businesses are spread out it’s dimension. Many new business idea’s are grown up as well as traditional old version business. For that reason electronic commerce known as e-commerce is a new growing field of today’s business. It has a great opportunities and a future. In last decades e-commerce has enough grown up.

**1.4 Benefits of e-commerce**

There are many benefits of e-commerce comparing with traditional businesses [1].

1. Easy to buy and sale: it is too easy to buy or sale any kinds of goods using internet
2. Low communication and product transfer cost: for the reason of online bill payment and one way product delivery is ensures very low communication and product transfer cost.
3. More sales: by advertising reaching new customers
4. More efficient and effective transactions: without wasting more customer valuable time, it is possible to order and pay for products within very few seconds, even only one or more clicks.
5. Convenience: in here customer needs only a reliable internet connection.
6. Very low transaction cost.

From the above discussion we have to ensure that, e-commerce is a growing field in today’s business. In where the order of products, payments and delivery all of things are held in one way, in very short time and with a very secure manner. Specially payment procedure should be held on more secure manner. In payment procedure transactions are executed between consumer to issuer and consumer to merchant. So authentication is very important factor in this system.

We want to design and implement a new payment system where customer can pay his/her bills to merchant with the help of issuer. We think it will be more secure and trustful comparing to existing system in terms of some criteria.

In this system has two phases, issuing phase and redemption phase. In issuing phase, firstly consumer want to buy some products or want to get some services from merchant so he/she send a request to issuer for some coin. Then issuer authenticate consumer with some verifications then issue some coins. Then consumer send a buy request to merchant with that coins. Then merchant send the products or service to consumer. In redemption phase, merchant send redemption request to issuer with coins, issuer verify the coins and if it was valid coin then issuer send balances to merchant account or give cash payment.

**Chapter - 2**

**Security Techniques**

Security is one of the most buzz word in today’s online world. Many security techniques are used to ensure virtual data. Now social network websites, online marketing, online money transfer, online banking etc are going to most popular. For those communication keep safe and keep data’s are private online security systems are most important and significant.

There are many cryptographic algorithms and many security protocols are used to ensure those security. In here we discuss some most used cryptographic algorithms and some security protocols.

**2.1 Cryptographic algorithms**

There are two types of cryptographic algorithms [5] –

1. Symmetric key algorithms
2. Asymmetric key algorithms

**2.1.1 Symmetric key algorithm**

It is single key cryptographic algorithm. It is also known as private key algorithm. A single key is used in both end, encryption and decryption process. The sending end use a key to encrypt messages and the receiving end also use same key to decrypt that message. So the main challenge of symmetric key algorithms of course key distribution. It must be needed to ensure that the key must keep secret at both end. The cryptographic schemes will be either stream cipher or block cipher. In stream cipher algorithm encryption or decryption will be held on every bit of message. But in block cipher algorithm encryption or decryption will be held on a block of bits, like 64, 128, 192, 256 or so on. DES, Triple DES, AES, IDEA, TEA, Blowfish etc are most popular symmetric key algorithms.

2.1.2 **Asymmetric key algorithm**

Asymmetric key algorithm also known as public key algorithm [9]. It is used two type of key, one is private key and another is public key. Two key of course mathematically related to each other. Private key is used to encrypt messages and public key is used to decrypt that messages. Suppose if there will be to parties A and B, and if A want to send a message after encrypt using asymmetric key algorithms to B then A will encrypt that message using private key and B will decrypt that message using public key at another end. RSA, ELGAMAL, ECC etc are the most popular asymmetric key algorithms.

**2.2 Security Protocols**

For secure transactions or any another secure data communication system some security protocols are used to ensure security. Those security protocols are well defined designed and passed by various dangerous attacks.

Some of security protocols are describes bellow –

**2.1.1 Secure Socket Layer (SSL)**

SSL stands for secure socket layer. SSL is a secure certificate creator which ensure that a certain connection is secure or not. If a connection is secure then SSL gives a green SSL locked signal to web browser and then any user can use that certain website, can login with password, upload his/her contents etc. SSL encrypt users information’s, so user information stay secure. But if the connection is not secure enough then SSL warn the user with red unlocked signal. If any user use that connection after getting that danger signal then the user information can be theft by any third parties.

In SSL certificate, some certificate issuer issue certificates for websites. When any user request to visit any website then web browser automatically send a request to certificate issuer and issuer check that certificate and give a feedback valid or invalid. If certificate is valid then that website is real and trustful but if certificate is invalid then that website is not real, trustful and secure.

Everyday millions of online transactions are executed via internet so it is essential to check the websites are real or not [4]. The all transactions are depends on SSL certification. Not only transactions but also any types of communications, if certifications are not valid then any third parties are lick our private messages.

**2.1.2 Kerberos**

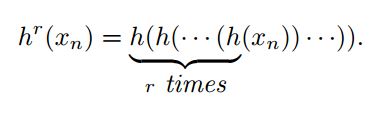
Kerberos is an authentication service of third-party, trusted by clients. It was first presented by Needham and Schroeder. It is trusted by each client by the sense of it can identify the identity of other clients accurately. Every Kerberos system maintain a database, which holds each clients and their private keys. The large number of private key only known by Kerberos. When an user use a password Kerberos encrypt that password. To authenticate, need a network service to register with Kerberos system. Then client can use that system. At the time of registration user provide his/her private key to Kerberos.

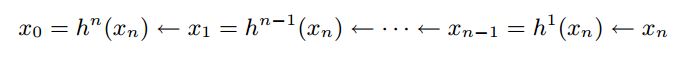
When one client claim any messages from another client Kerberos can creates messages for first one because of Kerberos knows all of private keys. Kerberos also generates session key, which is temporary key. Kerberos provides that session key to only two clients and no one else. To encrypt messages between two parties a session key can be used [4].

**2.1.3 One-Way Hash Chain**

One-way hash chain [10] is a cryptographic system as like as one time password. It is use a encryption algorithm as a hash function. Any password is encrypt using that algorithm the size of chain times. And each time each distinct password is used for authentication. The hash functions would be SHA, MD5, HAVAL or any other encryption algorithms. In internet based system many authentication system is used but most of are technically complex, computational speed is high and time consuming. So in light weight system these are not suitable so far. It is needed a system which is light weight, fast and trustful. One-Way hash chain is one of the such kind of cryptographic system which fulfill most of security and efficiency demands.

The mathematical notations of one-way hash chain is in following [6] –



If we need a r length hash chain then we have to encrypt the original message xn , r times using any crypto algorithm SHA, MD5 or any others.  
Figure 2: One-Way Hash Chain [6]

**2.1.4 Blind Signature**

Blind signature is one the new technique of digital signature [11]. It is an important technique of authentication and hiding message with a trusted signature for verification. In here, a signer sign a message without knowing what is that message is. Firstly a requester send a request to signer for a signature, then signer sign that message using cryptographic system and send back blinded message to requester with signature. Requester can unbinds that message with that signature. And latter when needed verification it is possible to verify that signature. Many cryptographic systems are used for blinding message, such as RSA, DSA, ECC etc. Blind signature are used in electronic voting system, many e-commerce sites payment system etc. Blind signature is used in such a sector where sender privacy is more important issue.

**2.1.4.1 RSA Blind Signature**

RSA is one of the public key cryptographic algorithm [12] in a application of blind signature. According to the melode-algoritma [6] –

“A traditional RSA signature is calculated by rising the message m to the secret exponent d modulo modulas N. public The blind version uses a random value r, so r is relatively prime to N (i.e. gcd(r,N)=1. r is raised to the public public exponent of e modulo N, and the resulting value is re mod N used as a dazzing factor. The author of the message counts the product of the message and dazzing factor, that is,

mʹ ≡ mre (mod N)

and sends the resulting value to the signing authority, Since r is a random value and mapping r\ Maps to is the following permutation that mʹ r re mod N re mod N random as well. This means that mʹ does not divulge any information about m. The signing authority then counts the signature’s blind as

sʹ ≡ (mʹ)d (mod N).

sʹ send back to the author of the message, which can then remove the blinding factor to reveal s, RSA valid signature m:

s ≡ sʹ . r-1 (mod N)

This works because the RSA key satisfies the equation and thus then s is indeed the signature of m. red ≡ r (mod N)

s ≡ sʹ . r-1 ≡ (mʹ)dr-1 ≡ mdredr-1 ≡ mdrr-1 ≡ md (mod N).”

**Chapter – 3**

**Related Work**

If we give a look at the state the situations from January 2012 to March 2016 in US, we can get a brief idea about the growth rate of e-commerce [3].

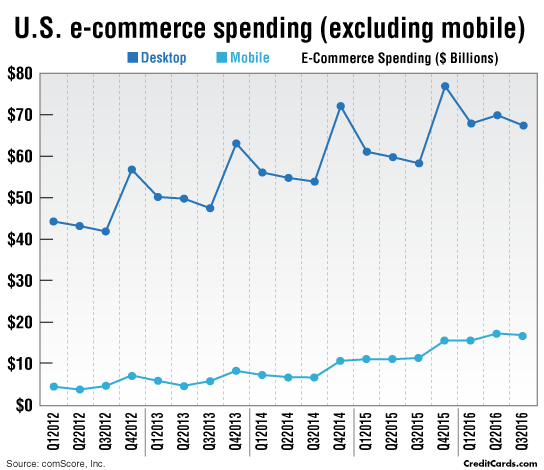


Figure 1.1: Growth rate of ecommerce in both desktop and mobile device from 2012 to 2016 [3]

In figure 1.1 we saw that from January 2012 to March 2016 the growth rate of e-commerce in US is shown. In mobile transaction, in 2012 it was only under 5 billion dollar, within only four years it increases highly and reached approximately near 15 billion dollar.

In desktop transaction, in 2012 it was only near 40 billion dollar but till 2015 it was reached near 80 billion dollar. So the increment rate is too high.

In past there are many works had been done for ensuring security and privacy issue of online payments. They uses many security protocols and many encryption techniques in various way. Some of are well enough for a particular angle but they have some limitations in different angle. So it is too hard to design and implement a system which is perfect for all angle of view.

Some systems security and privacy concerns are very good but computational steps are complex, mathematical calculations are complex and time complexity are too high. There are also some systems, which are light weight in design, computational step, and time complexity but these are also light weight in security issue. So it is need a well defined system which is light weight but security issues are also well defined.

Here we focuses some works those are designed previously for online payment security and privacy.

In paper [2], “A Study of Micro-payment Based on One-Way Hash Chain” they design and implement a system based on one-way hash chain. In this work, there are four phase of operation, registration phase, blinding phase, transaction phase and redemption phase. In registration phase both consumer and merchant needed registration (create an account) to issuer/bank. In blinding phase, consumer sends a withdrawal request to bank. In here four step computation will be done using electric curve cryptography (ECC) and one-way hash chain and consumer get a signature from bank. In transaction phase, consumer buy or want to get service from merchant browsing merchant website. For payment consumer send transaction request to bank for merchant service. Then bank verify the pre-signing blind signature for verification. If the signature is valid then bank transfer balance to merchant account from consumer account. Here also used electric curve cryptography (ECC) and one-way hash chain. In redemption phase, after sometimes merchant withdraw its balance from bank.

In this work, for security issue it concerns with this facts like, blindness, unforgeability and untraceability. And it uses double spending detection. It provides multiple transaction facility also.

In paper [13], “A Protocol for Micro-transactions” named by “Stroem” focuses a micropayment system. It is mainly uses for bitcoin transaction but also usable for any kind of currency transaction. The transaction flow is use promissory notes to interact with consumer to issuer and consumer to merchant. There are three different parties in stroem consumer S, issuer I and merchant M.

To facilitate payments to merchant from consumers for buying products and services, intermediaries works as payment hubs which provide the services of issuing and redeeming promissory notes. The intermediaries act as various role, such as, for payments consumers have some issue promissory notes, for merchant it has some redeem notes, it uses when merchant demands payments and some trade notes between themselves.

When a consumer want to pay for goods or services to merchant, consumer send a request to issuer for a promissory note for an individual amount of coin then issuer send back a promissory note to consumer after some authentication. Then consumer transfer that promissory note to merchant after adding information specifying what is purchased. All of steps will be done within a short period of time.

And when merchant want to redeem one or more promissory notes from a specific issuer it sends promissory notes to issuer without the information of goods that purchased for consumer privacy. And merchant add the details about how the redemption payment should be done. Then issuer verify all of promissory notes and pay all of payment to merchant such a way that merchant want.

In paper [8], explains two different type of micro-payment system, “PayWord  
 and “MicroMint”.

PayWord is a credit based system where issuer pay for user to broker when user send a request to issuer for a payment. Then user renew his/her balance to issuer. In here, Consumer and broker establish their account for all kinds of transactions. And then user and broker both gets digitally signed PayWord Certificates containing the broker’s name, the user’s name and IP-address, the user’s public key, the expiration date and others information. The certificate can be renewed if broker or user want to renew. In PayWord, it don’t use any complex cryptographic algorithm. It uses simple one way hash chain [6]. Any kinds of authentication will be held based on one way hash chain. When user firstly want to connect with broker for a specific goods or services, both signs a “commitment” to new user-specific and vendor specific chain of paywords w1, w2, ……., wn. The user creates the payword chain in reverse order by picking the last payword wn at random, and then computing

wi = h(wi+1)

for i = n-1, n-2, . . . , 0. Here w0 is the root of the payword chain, and is not a payword itself. The commitment contains the root w0, but not any payword wi for i > 0.

MicroMint is a another payment system which is designed for feasible security at very low cost. It is mainly used for low-value payments. It has no use of public key operations, which causes for complex computations. Broker firstly sell coins to user and then user use that coins to buy goods or service from vendor. Then vendor returns to broker for cash payment.

According to paper [8], “A coin is a bit-string whose validity can be easily checked by anyone, but which is hard to produce. This is similar to the requirements for a public-key signature, whose complexity makes it an overkill for a transaction whose value is one cent.” MicroMint also use one hash function to creating coins. Hash function collisions are uses to create new coin, such as it uses k-way collisions. It has three phases, selling coins, making payments and redemptions. In selling coin phase, broker sell his coins to issuer. Then user give that coins to vendor as a currency for services in payment phase. At the end the redemption phase will be executed, in here vendor returns the coins to broker and get real cash payment.

**Chapter 4  
Propose System**

In business demand we already realized that, in micropayment system there should be some important issues that must completely or partially completely fulfill. These are –

1. System will be light weight
2. Minimize inter transaction cost
3. Minimize operational time
4. Avoid complex computations
5. Use low computational and operational cost cryptographic algorithm
6. Should concern about internet traffic
7. Keep secrete consumer, merchant and issuer information to each other
8. Must keep concern about security about any type of attack

We preview some payment system in a short in previous sections. And we realize that every system has some limitations although they are very renowned and have a lot of facilities also. So it will be clear if we summarize and go back at a glance in back.

In paper [2], they discusses a nice model of micropayment based transaction. They focuses mostly about security system but not focuses so much at system complexity. They uses blind signature implemented by elliptic curve cryptography (ECC) and one-way hash chain. In this system, in blinding phase authentication of consumer to issuer and in transaction phase authentication of consumer to merchant will be held on using blind signature. In each blind signature four step communication needed over internet for authentication. And in each step of computation there are one or more complex mathematical operations are needed. So we say that, this system is complex enough at the aspect of micropayment scheme.

In paper [13], “Stroem”, it is a international standard payment system. It’s transaction flow is too simple enough and implementation is very convenient for any kind of payment. It permits to implement using any kind of cryptographic algorithms. But it mainly designed for bitcoin transaction.

In paper [8], “PayWord”, it is also international standard payment system, which is used most popularly in a lot of application areas. But it has also some limitations. This system generate individual long length hash chain for each vendor. Each hash chain is used for individual vendor. So that the unused paywords of each hash chain is wasted. So that the system performance is going to low for generating unnecessary paywords. We improve this system in this area using only hash chain for all of vendors.

In “MicroMint” system [8], firstly for a month broker allocate a certain amount of coin for a certain consumer. After end of month the unused coins are going to back to broker. So it is a limitations that, time, cost and complexity are increases.

So we design and implement a payment system which can minimize the limitations of those systems. In our system we take helps from previous models. Such as we use “stroem” [13] transaction flows, that is consumer payment system stay same as “stroem” but in redemption phase we changes a slide changes, here there is no redeemer. Issuer directly interfere with merchant in redemption phase. In paper [2], they use blind signature with elliptic curve cryptography (ECC) for authentication but here we use RSA blind signature for creating coin when consumer want to get coins from issuer. It is credit based system, issuer issues coins without any kind of instant hard cash or any other cash transactions. And for system simplicity and to decrease system complexity we use one-way hash chain as “PayWord” in other sections.

In order to preserve security, public key cryptography will be used in the system. That is, a signature scheme is implemented in the system and it requires the computation of exponential evaluations. Instead of modular exponentiations, hash functions are applied.

Now we discuss the brief description about our proposed system bellow –

**4.1 Symbols and Notations**

In here, we use some symbols and notations. We use public-key cryptography (e.g. RSA with a short public exponent). The public keys of the Issuer I, Consumer U , and Merchant M are denoted PKI, PKU, and PKM, respectively; their secret keys are denoted SKI, SKU, and SKM. A message M with its digital signature produced by secret key SK is denoted {M}SK. This signature can be verified using the corresponding public key PK .

We let h denote a cryptographically strong hash function, such as MD5[17] or SHA[16]. The output (nominally 128 or 160 bits) may be truncated to shorter lengths as described later. The important property of h is its one-wayness and collision-resistance; a very large search should be required to find a single input producing a given output, or to find two inputs producing the same output. The input length may, in some cases, be equal to the output length.

**4.2 Transaction flow**

Our system will be credit based system, that means a consumer can spend his certain amount of credits (credit limit will varies user to user). So for that firstly consumer request for coins to issuer then issuer issue some coins for its consumer. Then consumer send that coin to merchant and merchant verify that coin and send back services. And in redemption phase merchant send back its coins to issuer and issuer give hard cash or any other bank cash transfer.

**4.2.1 Registration Phase**

In registration phase, consumer send his information’s such as, his name, location, profession, gender etc as the information needed to open a bank account to issuer. Then issuer creates an account for that consumer. Issuer generates some identification numbers and some keys for that consumer such as, identity, public key, account no. and credit limit. Credit limit will be vary user to user and it will be increase or decrease on the reliability of consumer.

**4.2.2 Consumer Certificate Creation**

In this phase, consumer certificate will be generated by issuer. Let C is a consumer and I is a issuer then C send his account information’s such as, his identity, his public key, his account number and his credit limit. Then using RSA blind signature I creates a certificate for consumer C. This certificate will be,

Cert(C) = sigI(I, C, KI, KC, exp, info)SKI

where KI is public key of the issuer, KC is the public key of consumer, exp is the expire date of the certificate and info is the additional information such as, account no. credit limit etc. Consumer can verify that certificate using issuers public key in offline.

**4.2.3 Consumer Payment**

This is the payment phase. In here consumer can pay coins as a payword. Firstly when consumer want to get some goods or take any services from a vendor then consumer start his procedure as bellow –

User make two hash chain h1 and h2 length of n1 and n2, generates two random secret number cn and dm then –

cn-1 = h1(cn), cn-2 = h1(cn-1), ………. c1 = h1(c2), c0 = h1(c2)

and

dm-1 = h2(dm), dm-2 = h2(dm-1), ………. d1 = h2(d2), d0 = h2(d2)

where

cn – Consumer randomly generate secret for first hash chain h1

dm – Consumer randomly generate secret for second hash chain h2

Each hash chain item is act as a payword for payment except c0 and d0. c0 and d0 are the root of hash chains. In hash chain h1 each payword value is 1 quantity and in hash chain h2 each payword value is 10 quantity. So that using two hash chain with different quantity value there is no need to generate extremely long hash chain.

The i-th payment (for i = 1; 2; : : :) from C to M consists of the pairs (ci, i) and (di, i) which the merchant can verify using ci-1 and di-1. Each such payment requires no calculations by C, and only a single hash operation by M .

Now consumer C computes a commitment commit (I) such as –

commit (C) = sigC(M, cert(C), c0, d0, d, info)SKC

Here,

M – Merchant identity

cert(C) – certificate for consumer C issued by issuer I

c0 –  the root of the first hash chain h1

d0 - the root of the second hash chain h2

d – current date

info – additional information – length of the chain etc.

Now consumer send this commit to each merchant. Merchant can verify this commit by using consumer public key and check issuer certificate using cert(C) with issuer public key in offline. When consumer want to pay a certain amount then firstly try to pay from hash chain h2 then pay from hash chain h1 rest of the quantities. Such a example if consumer want to pay 24 cents then we know second hash chain’s each payword value is 10 cents so it’s needed 2 paywords to pay 20 cents, so it send 2 payword from h2 and the remaining cent are 4, so for 4 cents needed 4 paywords from h1 because in h1 each payword value is 1 cent.

In first time when consumer pay a vendor then for i quantity pay consumer send (ci, i) and (dj,i) to vendor and save consumers cache the vendors identity, (ci, i) and (dj,i).

Here

ci – i’th hash value for hash chain h1

i – sequence of hash chain h1

di – i’th hash value for hash chain h2

j – sequence of hash chain h2

But in second time or so on consumer firstly read the value of i and j which is already saved at cache then compute the needed payword size in hash chain h1 is p and compute the needed payword size in hash chain h2 is q. Then compute

p = amount / 10.

q = mod(amount,10).

i = i + p and j = j + q;

Then send the new hash values (ci, p) and (dj,q) to merchant. Merchant only save the last payword and its sequence no. because there is no need to store previous paywords. For example if a merchant receive (c2,2) for first payment it means he receive 2 cent for this payment and (c7,5) for second payment it means that he receives 5 cent for this payment. So the total payment is (2+5) = 7. Which represents the last payword so merchant save the last payword as (c7,7).

**4.2.4 Redemption**

In this phase merchant send his paywords and consumers commit(C) to issuer then issuer verify the consumer signature using consumer public key and he also recognize his self signature. If both signature is verified successfully then issuer pay to merchant hard cash or any other bank money transaction.

**Chapter 5**

**Analysis**

In this chapter we will try to analyze the system and compare it with others system.

**5.1 System Efficiency**

To enhance this system efficiency we need to focuses the main two sectors. First one is transfer some of the computations offline. Which reduce network traffic and communication cost and earn good system performance. Another one is need to reduce complex computations such as exponential calculations replaces with some modular calculations. And it is required to reduce the calculation of a lot of hash chain with a long length.

Now we focuses at firstly to transfer some of the computations offline –

* Issuer creates Consumer certificate, verify his own certificate and verify consumers commitment offline. Only it transmit consumers certificate to consumer in online.
* Consumer verify its certificate, generate his commitment and create hash chains in offline. Only he send his commitment and paywords to merchant in online.
* Merchant verify consumer certificate, consumer commitment and paywords in offline. Only he send paywords to issuer for redemption in online.

So that in this system the maximum calculations are performed in offline. So the system performance would be better.

Now if we focuses the other computations then we saw that – it uses RSA digital signature for digital signature scheme [18] to signing certificates and commitments, it is comparatively costly. But it uses hash function it is very efficient than any kind of digital signature. Hash functions such as MD5 [5] and SHA [16], can be used to more efficiently compute a random number. Rivest and Shamir pointed out that hash operations are about 100 times faster than RSA signature verification, and 10000 times faster than RSA signature generation. We can see that the computation of the signature scheme is much more costly in comparison with hash functions. Therefore, to reduce the number of public key operations we will apply the hash function instead of modular operations whenever possible.

In payword [8], in payment section, for a individual merchant an individual consumer generates a variable length individual hash chain. But with a individual merchant he pay a few numbers of paywords only. The rest of the paywords are wasted. For another merchant consumer generates another hash chain and so on. So we saw that a lot of computational time and space is wasted and system performance decreases significantly.

To solve this problem we design a nice solution. We creates only one hash chain for all of merchants. All operations will be performed on only that hash chain. It will be use as a overlapped fashion. A payword can be use for different payment in of course in different merchant. Same payword cannot use for duplicate payment in same merchant. So there are no need to generate separate hash chain for each merchant. Of course this way increases our system performance and decreases computations and computational time also.

But in proposed system there need a long length hash chain because this is common hash chain. To overcome this problem we propose a new way, that is we generate two hash chain instead of one. First hash chain’s each payword value will be 1 cent and the second hash chain’s payword value will be 10 cents. To pay a large amount firstly use second hash chain then use first hash chain. This proposed two hash chain mechanism decreases the length of hash chains. So it decreases system overhead.