The Implementation of Blind Signature in Digital Cash

Hariandi Maulid
Department of Informatics Engineering, School of Applied Science
Telkom University
hariandimaulid@tass.telkomuniversity.ac.id

Abstract

Digital cash, an electronic or digital simulation of real cash, has been used widely to buy or sell goods in the recent internet society. As it circulates via internet, all information regarding transaction using digital cash can be recorded. Hence, the anonimity and privacy become a serious concernto the payer and the payee. This paper will discuss how the implementation of blind signature can preserve the anonimity and the privacy of all digital cash user.

Keywords: blind signature, digital cash, digital signature,

1. Introduction

Money plays an important role in the development of human history. The most common form of money is shown as some actual objects, such as paper, argentine or gold. All forms of money have the value which people can use to buy or sell goods. Nowadays, digital cash, which represents money with both value and electronic form, has been widely used in the recent society. It can be categorized by anonymous or identified, used online or offline.

1.1 Digital cash

Digital cash, which is also called E-cash or E-money, was firstly produced by David Chaum in 1982 [3]. It can be seen as the electronic or digital simulation of real cash. It exists with the form of a series of encryption numbers, and circulates via the internet. This series of encryption numbers can identify values of the real cash. Digital cash is developed based on the development of Electronic Commerce.

Because of the particularity of internet and electronic form of digital cash, all the information of transaction using digital cash can be recorded. How to guarantee the anonymity and the privacy of the payer and payee has become the hottest research issue. Therefore, it is important for digital cash to build a safe and feasible digital signature scheme. By this reason, blind signature is invented.

1.2 Blind signature

Blind signature, which was firstly advanced by David Chaum in 1982 [3], is widely used in the process of digital cash currently. It is a special form of digital signature. The purpose of using blind signature is to protect the privacy of digital cash users. The signature applicant uses blind signature to change the message which need to be signed, then sends the "blind message" to the signatory, the signatory signs the message without knowing the content of the message. By this way, the anonymity and the privacy of all the digital cash users can be preserved.

From our point of view, a high quality blind signature scheme should contain four characteristics as follow:

1. Non-falsification. Besides the signatory, no one can use the signatory's name to generate an efficient blind signature to a message.
2. Non-repudiation. After signing a message, the signatory cannot deny himself on the signed message.
3. Untraceable. The signatory cannot confirm when and where a message is signed by the signatory himself.
4. Invisible. When the signatory sign a message, the signatory cannot get the content of this message.

Blind signature scheme can be used in both online or offline environment, which will be introduced in this paper. Before we present blind signature, principle of digital cash should be introduced.

2. Principle of Digital Cash

2.1 General structure of digital cash system

There are three actors involved in digital cash system [8]:

1. Financial network (Bank).
2. Payer or consumer (Alice).
3. Payee or shop (Bob).

During a digital cash procedure, we can divide them into following parts [6]:

1. Withdrawal, in which the payer (Alice) transfers some of her money from her bankaccount to her wallet or payment card.
2. Payment, in which Alice transfers the money from her wallet to the payee (Bob).
3. Deposit, in which Bob transfers the money received from Alice to his bank account.

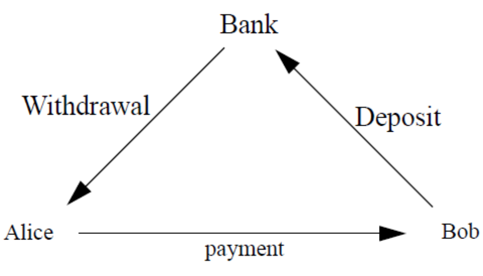

Figure 1: Type of transaction[8]

In order to provide a clear explanation, we provide a scenario below to give a specific analysis about blind signature in digital cash.

Alice as a payer would like to withdraw $20 digital cash from her bank as a financial network (withdrawal) to pay the ticket she bought from Bob (payment). Bob as a payee will claim the bank to put the money that Alice sent him into his account (deposit).

2.2 Online payment

The implementation of digital cash, as described above, can be either online or offline [6]. Online digital cash system requires that merchant (Bob) must contact and verify the validity of consumer's token or e-cash with each transaction before accepting Alice payment. If the bank finds that the e-cash has already been spent, it will alert Bob not to accept Alice payment. Hence, the transactions we described above represent the online digital cash system.

2.3 Offline payment

Unlike the online system, offlinedigital cash systems lets Alice completes transaction without involving a bank directly. Therefore, Bob submits Alice's payment for verification and deposits sometime after the transaction is completed. Smart Card Reader at the Point of Sale is such an example of this system. The device is trusted by the bank and is used to verify the authenticity of the coin/cash but does not check whether the coin has been double spent [1].

There are currently two different ways in which offline digital cash system can detect double spending. The first one is by creating a special smart card containing a tamper-proof chip which keeps track of the digital cash spent and will detect any endeavours to duplicate digital cash and not allow it. The second way is to encrypt the digital cash duplicates to identify the individual by the time the digital cash makes it ways to the bank [10].

3. Principle of Blind Signature

3.1 Definition

Blind signature is a special form of digital signature which aims at protecting the privacy of user. Unlike credit card system, bank has the ability of monitoring the consumption of an identified user, blind signature, however, keeps bank away from tracing the details of a transaction.

This notion was first proposed by Chaum in 1982. In digital cash scenario, it allows apayer to get a coin signed by bank without revealing any information about the deal. Thisexactly is the motivation of blind signature.

Similar to real world, here is a vivid analogy of familiar paper document which wasintroduced by Chaum [3]. It illustrates the basic concept of blind signature well. A paperin an envelope with blind signature can be carried out by steps as follows:

1. Take an envelope carbon paper lined;
2. Insert a slip of paper and close the envelope;
3. Send the envelope to a third party (bank) who signs the envelope form the outside and sends it back;
4. Extract the signed slip form the envelope;
5. Give the signed slip to someone. The third party will recognize its signature consequently;

3.2 Protocol

Before describing the specific protocol of blind signature, we will give five functions above all [3].

1. C': commuting function, known only to the payer.
2. C: inverse of C', known only to the payer.
3. S': signing function, known only to the bank.
4. S: inverse of S, publically known.

5. r: checking predicate

By providing a message x, we can conclude two equations:

$$S\left(S'(x)\right) = x \tag{1}$$

$$C'\left(S'(C(x))\right) = S'(x) \tag{2}$$

The protocol of blind signature then will be explained in the graph below:

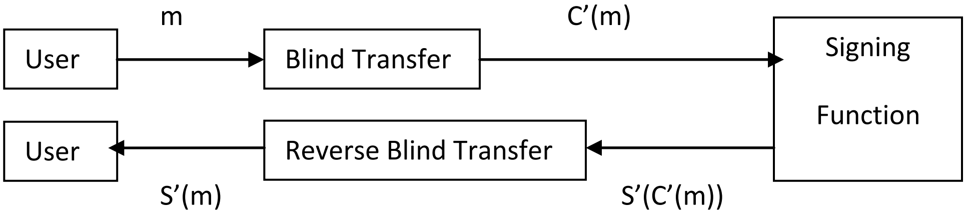

Figure 2. Protocol of Blind Signature [3]

According to the protocol, the implementation of digital cash in this model can be divided into 6 steps:

1. The payer Alice generates a message m at random such that r(m)
2. Alice computes m and forms C(m)
3. Alice then sends the C(m) to the bank for signature
4. Bank signs C(m) by applying S' and forms S'(C(m))
5. Bank returns the signed matter S'(C(m)) to Alice
6. Alice now strips the note by C' and gets the signed coin as C'(S'(C(m)))=S'(m)
7. Alice makes payment some time later by providing S'(m) to Bob
8. Bob verifies the authentication of coin and pause if false
9. Bob deposits S'(m) to bank
10. Bank verifies the authentication of coin and pause if false
11. Bank checks for multi-spending and pause if true
12. Bank credits account of Bob and informs the acceptance

3.3 Classification of blind signature [11]

Depending on the strength of anonymity given by the signature, we can distinguish four classes of blind signatures:

1. Hidden signature
   The bank does not know the details of transaction he signs, but he knows the signature parameters. If he stores them, he can recognize the signature later by comparingthem with a given signature.
2. Weak blind signature
   The bank does not know the details of transaction and the signature parameters, but he can also verify it later, because there remains a relation between signature parameters and unblended parameters.
3. Interactive blind signature
   The signature generation is the same as the case of weak blind signature. By demonstrating the knowledge of a signature with an interactive proof, the signer

does not get any knowledge about the relation between the blinded and unblended signature parameters. So he does not get any information about the relationship between a given document and his stored parameters. If it is necessary, the owner can be forged in case of a complaint to show the signature parameters which affects that the bank can find the relationship.

4. Strong blind signature
   The signer could not see a relation between any of his stored parameters and the shown signature parameters, so that the signature is really anonymous.

3.4 Typical Blind signature schemes

Generally, there are 3 (three) typical blind signature schemes:

1. RSA Bind Signature Scheme
   RSA-based blind signature is simple and practical, and as so far resisted attacks. Yet there seems little hope of proving its security based on the "standard" one-wayness assumption about the RSA function: it seems that the security of the scheme relies on different, and stronger, properties of RSA [9]. Its security is based on the factorization problem. It is one of best performance schemes and widely applied in digital cash system. In this paper, we will provide an example of RSA-based blind signature scheme.
2. Elgamal Bind Signature Scheme
   Elgamal Signature was first introduced by Elgamal in 1985. In this signature scheme the public key is used for encryption and signature verification [5]. Moreover, Elgamal signature possesses a unique feature which needs to generate a random number every time of signing to ensure the different results of the same message. Its security is based on the difficulties of discrete logarithm problem in the finite fields.
3. Schnorr Blind Signature Scheme
   Okamoto initially proposed the Schnorr blind signature scheme in 1993 which is relied on the intractability of discrete logarithm problem. Unlike RSA-base blind signature, it is more complex and concentrated on the process of interaction. Nevertheless, Schnorr blind signature scheme performs better than Elgamal in safety and length of signature result.
4. Nyberg-Rueppel Blind Signature Schemes
   In 1995, Jan L. Camenisch provided a blind signature scheme named Nyberg-Rueppel which is also based on the discrete logarithm problem.

4. Implementation

4.1Overview

Since the blind signature has advantages, such as correctness, authenticity, enforceability, non-reusability, non-repudiation, integrity, blindness and intractability [4], the blind signature schemes have been implemented into the digital cash systems. In this part, we will talk about the blind signature implementation of two digital cash schemes, one of which is online and the other is offline.

4.2Online – RSA Blind Signatures DigitalCash Scheme

Not only the concept of blind signature, but the first blind signature digital cash scheme, RSA, and its implementation were invented by David Chaum in 1982 [3]. This scheme is an online scheme. The implementation in online digital cash can be divided into three parts, registration, withdraw and payment.

1. Registration

   The bank needs to generate the public and private keys. Bank selects two large prime numbers, p and q. Let

   $$n = pq \tag{3}$$

   And the bank pics

   $$e < \phi\ (n), \phi(n) = (p-1)\ x\ (q-1) \tag{4}$$

   Then using Euchlid’s Algorithm to find d, let

   $$ed \equiv 1(mod\ \phi(n)) \tag{5}$$

   Now the pair of number (n,e) is the public key of bank, and e is the private key. The two number p and q are nolonger needed, and can be discarded by the bank. H() is the Hash function with no collisions.

2. Withdraw

   Alice applies to withdrawal money after proving her identification to the bank. The following is the protocol between Alice and the bank. First of all, Alice picks a random number x, and a randomly number $k \in Z_n^*$, called the (7)
   blinding factor. Then Alice binds the message

   $$m^{'} = k^{\varepsilon} H(x) mod\ n \tag{6}$$

   And sends it to the bank. After that, the bank signs the blinded message using its private key,

   $$s^{'} = (m')^{d}\ mod\ n$$

   And then the bank sends the signed blinded message back to Aice, Then, Alice conputs the message:

   $$s = s'r^{-1}\ \ mod\ n = H(x)^{d}\ mod\ n \tag{8}$$

   Then Alice gets the digital cash $\{x, H(x)^d\}$

3. Payment

   First of all, Alice sends the digital cash $\{x, H(x)^d\}$ to Bob. Then Bob checks

   $$(H(x)^{d})^{\varepsilon} = H(x) mod\ n \tag{9}$$

   If so, the digital cash will be sent to the bank, the bank will add the money to theaccount of Alice after ensuring the amount is right.

   During the process of signature of message *m*, the bank has no ideas about themessage content and the signature message. In this online blind signature digitalcash system, there are three parties, the bank, Alice and Bob. When Alice pays toBob to buy something, the bank must be online as well. Otherwise, Bob does notknow whether the digital cash has been paid. Addition, during the payment, thedigital cash cannot be divided, which means Alice has to pay only once.

4. Attacks

   Since this system is based on RSA, a possible attack against this system is a cooperation attack between Alice and Eve. If Alice has a transaction with Bob and sends her digital cash to Eve whom chosen by Bob, then Eve will have an exact payment history as Bob and the bank will not be able to determine which one of them is cheating [8].

4.3 Offline – Brands Blind Signatures Digital Cash Scheme

We will talk about the implementation of Brands blind signature in offline digital cash in details from four parts, registration, withdraw, payment and deposit.

1. Registration

   The bank generates the publicand private keys

   The bank picks two large prime numbers p, q, and q | p-1, g, g_1, g_2 are elements of Z_p^*. The bank picks a random $x \in Z_p^*$ as its private key. The bank computes

$$h = g^x mod\, p, h_1 = g_1 mod\, p, h_2 = g_2 mod\, p \tag{10}$$

   And the bank reveals $p, q, g, g_1, g_2, h, h_1, h_2$.

   $H()$and$H_0()$are two hash functions.

   Atlast, Alice reveals her identification.

$$I = g_1^{u1} mod\, p, z^{'} = h_1^{u1} h_2\, mod\, p = (Ig_2)^x mod\, p \tag{11}$$

2. Withdrawal

   The withdrawal protocols executedwhen the bank accepts Alice’s proof.

   Step 1. Thebank chooses a random $w \in Z_q^*$

$$a^{'} = g^w mod\, p, b^{'} = (Ig_2)^w mod\, p \tag{12}$$

   And then the bank sends $a^{'}, b'$ to Alice.

   Step 2. Alice picks random number$\{s, u, v, x_1, x_2 \in Z_q^*\}$, and computes

$$\begin{gathered} A = (Ig_2)^x, B = g_1^{x1} g_2^{x1} \\ z = (2^r)^s\, mod\, p \\ a = (a^v)^u\, gv\, mod\, p, b = (b^r)^{sn} A^v\, mod\, p \\ c = H(A, B, z, a, b), c^{'} = \frac{c}{u\, mod\, p} \end{gathered} \tag{13}$$

   And Alice sends c' to the bank.

   Step 3. The bank computes

$$r^{'} = c^{'} x + w\, mod\, p \tag{14}$$

   And sends it to Bob.

   Step 4. Alice accepts if and only if

$$g^{c'} = h^{c'} a^{'} mod\, q, (Ig_2)^{r^{'}} = (z^{'}) b^{'} mod\, p \tag{15}$$

   Then she computes

$$r = r^{'} u + v\, mod\, p \tag{16}$$

   And then Alice has her digital cash $\{A, B, z, a, b, r\}$ from the bank if and only if

(17)

$$g^r = h^C a \bmod p, A^r = z^c b \bmod p$$

3. Payment

   When Alice wants to buy something from Bob, she needs to provide (r_1, r_2) and u_1 to Bob. Then Bob can trust that Alice is the person with valuable digital cash.

   Step 1: Alice sends $\{A, B, z, a, b, r\}$ to Bob.

   Step 2: Bob computes $d = H_0(A, B, I_M, Data/time)$, and sends it to Alice. I_M is a random number choosen by Bob which is Bob's identification, and Data/Time is a current time for transaction.

   Step 3:Alice responses with

   $$r_1 = du_1 s + x_1 mod\ q, r_2 = ds + x_2 mod\ q \qquad (18)$$

   And sends it to Bob.

   Step 4: Bob computes $c = H(A, B, z, a, b)$ and then verifies whether (19)

   $$g^r = h^C a \bmod p, A^r = z^C b \bmod p, g_1^{r1} g_2^{r2} = A^d B \bmod p$$

   And if so, the digital is valuable and Bob accepts the payment.

4. Deposit

   Bob sends the transcript $\{d, r_1, r_2, (z, a, b, r)\}$ to the bank, and then the bank will pay to Bob after the bank checks that the signature is correct and the money has not been spent before.

5. Attacks

   Alice can spend digital cash many times without being identified by misbehaving in the registration. That is a kind of Brand's Scheme [8].

5. Conclusion

We introduce the definition of digital cash and blind signature scheme. And we analyse the principle of digital cash system and blind signature. Then we give the implementation of Online - RSA Blind Signatures Digital Cash Scheme and Offline - Brands Blind Signatures Digital Cash Scheme.

After been invented, Blind signature scheme has developed and improved fast. On onehand, blind signature is widely used not only in the field of digital cash, but also in otheronline systems, such as Electronic Voting System [10] and Anonymous Auction System[7]. On the other hand, the Law (In the UK, there are Electronic Communications Act2000 (ECA) and the Electronic Signatures Regulations 2002 (ESR)) confirms the legal status of digital signatures [12][13], which will protect and improve the development ofBlind signature.

In the future, the security of different blind signature schemes will be a hot researchissue. Concurrently, how to reduce the computation complexity and increase the computation efficiency of blind signature algorithm will also be the subjects we should pay attention to.

References

[1] Amit et. al., (2000), “Digital Cash”, School of Computer Science, University of Birmingham,UK. 2000 Available at http://www.cs.bham.ac.uk/ mdr/

[2] Davenport, Ben, Alan Newberger and Jason Woodard, (2000), “Creating a Secure DigitalVoting Protocol for Campus Elections”, April 2000. Available athttp://www.princeton.edu/ usgvote/technical/paper.html

[3] David Chaum, (1982), “Blind signatures for untraceable payments, Advances in Cryptology” -Crypto '82

[4]Debasish Jena, Sanja Kumar Jena and BanshidharMajhi, (2007), “A novel blind signaturescheme based on Nyberg-Rueppel signature scheme and applying in offline digital cash”.10th International Conference on Information Technology.

[5]Elsayed Mohammed et.al, (2000), “A blindsignature scheme based on Elgamal signature”.

[6]Gao, Jerry, (2000),”Electronic Cash Payment Protocols and Systems”, San Jose StateUniversity. 2000 Available at http://www.engr.sjsu.edu/gaojerry

[7]Kazem, H. Hasan, Q. Khan, R.Z., (2007),”Fraud/Privacy Protection in AnonymousAuction”, ICMP 2007

[8]MandanaJahanian Farsi, Adviser Mikael Simovits, (1997), “Digital Cash”.

[9] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko,(2001), “ The power of RSAinversion oracles and the security of Chaum's RSA-based blind signature scheme”.

[10]Miller, Jim, (2008), “Digital Cash Mini FAQ”, Department of Computer Science, School ofComputer Science and Statistic, Trinity College, Dublin, Dublin 2, Ireland. Available athttp://ntrg.cs.tcd.ie/mepeirce/Project/Mlists/minifaq.html

[11]Patrick Horster, Holger Petersen,(1994),“Classification of blind signature schemes andexamples of hidden and weak blind signatures”.

[12] UK Government, (2000),“Electronic Communications Act 2000”,Section 7-10.

[13]UK Government, (2000), “Electronic Signatures Regulations 2002”.