E-Cash Payment Protocols

Shweta Srivastava
Department. of Computer Science and Engineering
Maharishi Markandeshwar University
Mullana, Ambala
shwetasrivastava.cse@gmail.com

Vandana Saraswat
Department of Information Technology
Gurgaon College of Engineering
Gurgaon
vndana.saraswat@gmail.com

***Abstract*- E-cash is a payment system designed and implemented for making purchases over open networks such as the Internet. Need of a payment system which enables the electronic transactions are growing at the same time that the use of Internet is growing in our daily life. Present days electronic payment systems have a major problem, they cannot handle the security and the users anonymity and at the same time these systems are secure on the cost of their users anonymity. This paper shows the payment protocols for digital cash and discusses how a digital cash system can be formed by presenting a few of the present days digital cash systems in details. We also provide a comparison and determine them together to see which one of them fulfils the properties for digital cash and the required security level.**

Keywords*: *E-cash; Payment Protocol; Double spending; Blind Signature.

I. INTRODUCTION

DigiCash is a private company founded in 1989 by Dr David Chaum. It has created an Internet money product, now patented, and called 'ecash' [2]. DigiCash's ecash has been used for many different types of transactions. It is a stored-value cryptographic coin system that facilitates Internet-based commerce using software that runs on personal computers. It provides a way to implement anonymous electronic payments in an environment of mutual mistrust between the bank and the system users. The value of DigiCash is represented by cryptographic tokens that can be withdrawn from bank accounts, deposited in bank accounts, or transferred to another people. Its ideal properties include security, anonymity, portability, off-line capability, user-friendly, wide acceptability [3].

In section 2, we discuss different authentication and signature techniques that are currently used to implement e-cash protocols while in section 3, we cover present days e-cash protocols and in section 4 we present the comparison between the ideal e-cash protocols based on different categories.

II. AUTHENTICATION AND SIGNATURE TECHNIQUES

This section describes the digital signatures that have been used in the implementations of the protocols, and also the techniques used to include identifying information [12].

There are two kinds of digital signatures, and both kinds appear in electronic cash protocols. Suppose the signer has a key pair and a message *M* to be signed.

A. Digital Signature with Message Recovery

For this kind of signature, we have a signing function S_{SK} using the secret key SK, and a verifying function V_{PK} using the public key PK.

$$(*) \qquad V_{PK}(S_{SK}(M)) = M$$

In this kind of scheme, the verifier receives the signed message $S_{SK}(M)$ but not the original message text. The verifier then applies the verification function V_{PK}. This step both verifies the identity of the signer and, by (*), recovers the message text.

B. Digital Signature with Appendix

In this kind of signature, the signer performs an operation on the message using his own secret key. The result is taken to be the signature of the message; it is sent along as an appendix to the message text. The verifier checks an equation involving the message, the appendix, and the signer's public key. If the equation checks, the verifier knows that the signer's secret key was used in generating the signature.

RSA Signatures: The most well-known signature with message recovery is the RSA signature. Let *N* be a hard-to-factor integer. The secret signature key *s* and the public verification key *v* are exponents with the property that

$$M^{sv} = M \pmod{N}$$

for all messages M. Given v, it is easy to find s if one knows the factors of N but difficult otherwise. The signature of M is

$$C := M^{s} \pmod{N};$$

to recover the message (and verify the signature), one computes

$$M := C^{v} \pmod{N}$$

III. PAYMENT PROTOCOLS

Cash protocols can be implemented in either of two ways Off-line or On-line. An ideal cash system is the one which works off-line [12].

Protocol 1: Offline electronic payment

Off-line payment means that merchant submits user's electronic coin for verification and deposit sometime after the payment transaction is completed. It means that with an offline system user can freely pass value to merchant at any time of the day without involving any third party like a bank. This is achieved by adding an additional component in the model called the "Temper – Resistant Device" similar to smart card reader at the point of sale. The device is trusted by the bank and is used to verify the authenticity of the coin but does not check whether the coin has been double spent. Although off-line systems are preferable from a practical viewpoint, they are however susceptible to the multi-spending problem and therefore suitable for low value transactions. Over the past years, some off-line cash systems have been designed that can not only guarantee security for the bank and shops, but also privacy for the users [7, 10].

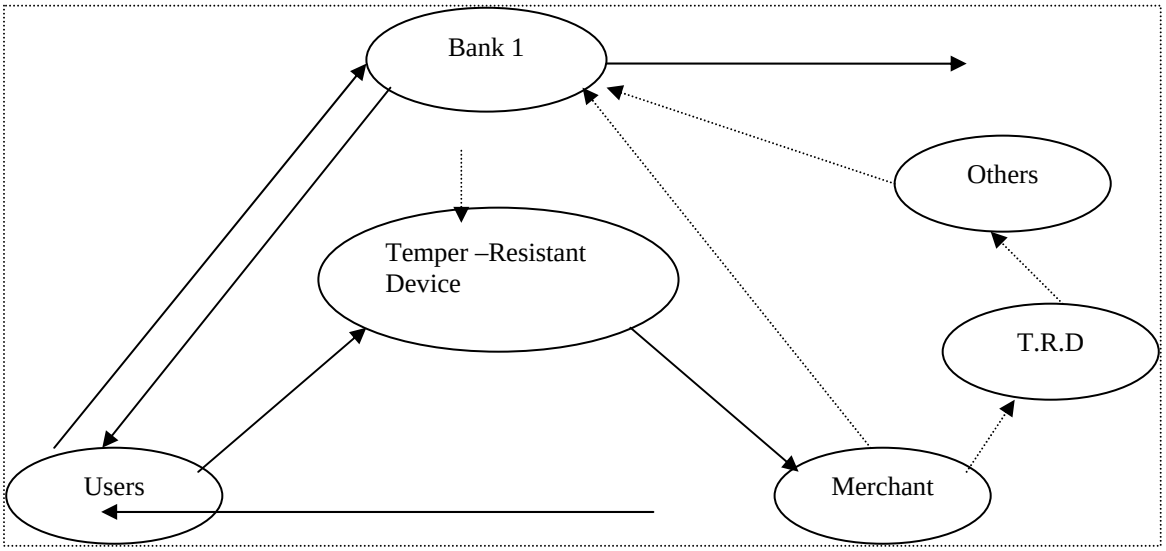

Figure 1 Off-line Cash Model

Withdrawal:

- User sends a withdrawal request to the Bank.
- Bank prepares an electronic coin and digitally signs it.
- Bank sends coin to user and debits her account.

Payment:

- User gives merchant the coin.
- Merchant verifies the Bank's digital signature. *(optional)*
- Merchant gives user the merchandise.

Deposit:

- Merchant sends coin to the Bank.
- Bank verifies the Bank's digital signature.
- Bank verifies that coin has not already been spent.
- Bank consults its withdrawal records to confirm user's withdrawal. (optional)
- Bank enters coin in spent-coin database.
- Bank credits merchant's account.

TABLE 1: A LIST OF OFFLINE SCHEME WHICH HAS BEEN PROPOSED [8].

Scheme	Proposing Year
Pfitzmnn and Waidner	1988
Chaum, Fiat and Naor	1988
Okamoto and Ohta	1989
Damgård	1990
Brands	1993
Cramer and Pedersen	1993
Franklin and Yung	1993
Chan, Frankel and Tsiounis	1995
Chan, Frankel and Tsiounis	1996

Protocol 2: Online electronic payment

On-line payment means that merchant calls the bank and verifies the validity of user's token by a simple question like "have you already seen this coin" before accepting her payment and delivering his merchandise (This resembles many of today's credit card transactions.). On-line payment remains necessary for transactions that need a high value of security. With an on-line system, the payment and deposit are not separate steps. On-line systems require communication with the bank during each payment, which costs more money and time (communication costs, database-maintenance costs and turn-around time), however the protocols are just simplification of off-line protocols. Since on-line systems have to be able to check the credibility of payers for shops, it is almost impossible to protect the anonymity of its users, besides as on-line systems require communication with a third party during the payment transaction, then we cannot have transferable coin if the system is an on-line one [7].

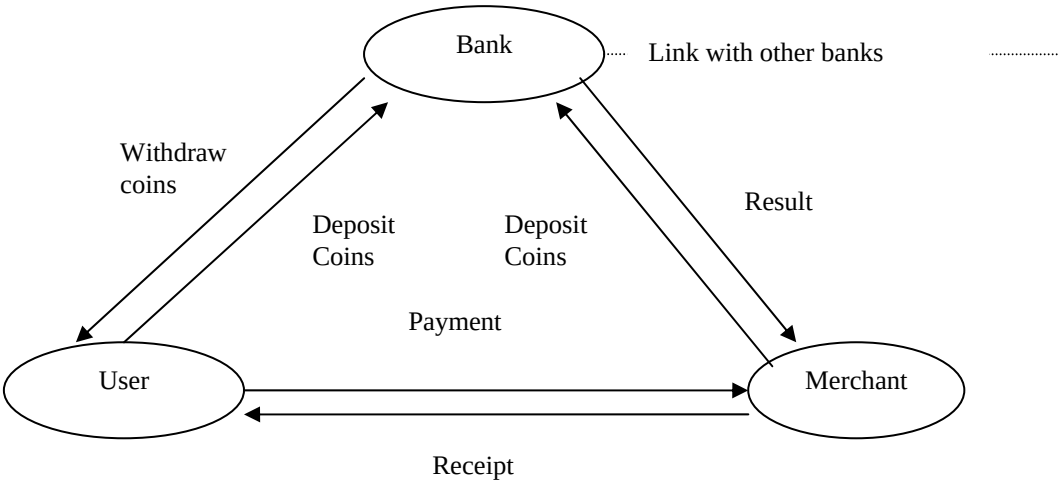

Fig 2 Online Cash Model

Withdrawal:

- User sends a withdrawal request to the Bank.
- Bank prepares an electronic coin and digitally signs it.
- Bank sends coin to user and debits her account.

Payment/Deposit:

- User gives Merchant the coin.
- Merchant contacts Bank and sends coin.
- Bank verifies the Bank's digital signature and verifies that coin has not already been spent.
- Bank then consults its withdrawal records to confirm user's withdrawal. *(optional)*. It then enters coin in spent-coin database and credits merchant's account and informs the merchant.
- Merchant gives user the merchandise.

The next 3 protocols are the modified version of online and offline payment protocols that include payment untraceability. For this, it is necessary that the Bank not be able to link a specific withdrawal with a specific deposit. This is accomplished using a special kind of digital signature called a *blind signature* [4, 5].

Using RSA, a blind signature can be implemented in the following way:

1. User chooses a blinding factor r such that $\gcd(r, n) = 1$, where

(n, e) is the bank's public key and

(n,d) is the private key and

she presents her bank with $m' = mr^e \pmod n$, where *m* is her original message.

2. User's bank signs it:

$s' = (m')^d \bmod n = (mr^e)^d \bmod n$

3. User divides out the blinding factor:

$s = s'/r \bmod n$

4. User uses $s = m^d$ for paying her bills.

Since *r* is random, User's bank cannot determine *m*. Therefore, it cannot connect the signing with User's payment. This signature scheme is secure as the factoring and root extractions remain difficult. However, regardless of the status of these problems the signature scheme is unconditionally "blind" since *r* is random. The random *r* does not allow the signer to learn about the message.

Protocol 3: Untraceable online electronic payment

Withdrawal:

- User creates an electronic coin and blinds it and sends the blinded coin to the Bank with a withdrawal request.
- Bank digitally signs the blinded coin and sends the signed blinded coin to user and debits her account.
- User unblinds the signed coin.

Payment/Deposit:

- User gives merchant the coin.
- Merchant contacts Bank and sends the coin.
- Bank verifies the Bank's digital signature and verifies that coin has not already been spent.
- Bank enters coin in spent-coin database.
- Bank credits merchant's account and informs merchant.
- Merchant gives user the merchandise.

Protocol 4: Untraceable offline electronic payment

Withdrawal:

- User creates an electronic coin and blinds it and sends the blinded coin to the Bank with a withdrawal request.
- Bank digitally signs the blinded coin and sends the signed blinded coin to user and debits her account.
- User unblinds the signed coin.

Payment:

- User gives merchant the coin.
- Merchant verifies the bank's digital signature(*optional).*
- Merchant giver user the merchandise.

Deposit:

- Merchant sends coin to the Bank.
- Bank verifies the Bank's digital signature and verifies that coin has not already been spent.
- Bank enters coin in spent-coin database.
- Bank credits merchant's account.

Protocol 5: Off-line Cash

Withdrawal:

- User creates an electronic coin, including identifying information and then blinds the coin.
- User sends the blinded coin to the Bank with a withdrawal request.
- Bank verifies that the identifying information is present and digitally signs the blinded coin.
- Bank sends the signed blinded coin to user and debits her account.
- User unblinds the signed coin.

Payment:

- User gives merchant the coin.
- Merchant verifies the bank's digital signature(*optional).*

- Merchant sends user a challenge.
- User sends merchant a response (revealing one piece of identifying info).
- Merchant verifies the response.
- Merchant gives user the merchandise.

Deposit:

Merchant sends coin, challenge, and response to the Bank.

- Bank verifies the Bank's digital signature and verifies that coin has not already been spent.
- Bank enters coin, challenge, and response in spent-coin database.
- Bank credits merchant's account.

Note that, in this protocol, Merchant must verify the Bank's signature before giving User the merchandise. In this way, Merchant can be sure that either he will be paid or he will learn User's identity as a multiple spender.

IV. COMPARISON BETWEEN PAYMENT PROTOCOLS

The following table shows some of the major differences that has been analysed.

S.No.	Category	Online	Offline
1.	Synchronization between bank servers	Need of Synchronization	Synchronization is kept to a minimum
2.	Reusability of coins	Not reusable	Could be reusable
3.	Additional hardware	Don't require additional secure hardware	Require additional secure hardware
4.	Double Spending	Prevent double spending problem	Might not prevent double spending problem
5.	Anonymity	Fully anonymous	Anonymous unless double spend
6.	Payment/Deposit	Not separate steps	Separate steps
7.	Turn-around time	High	Low
8.	Communication Cost	High	Low
9.	Database Maintenance Cost	High	Low
10.	Scalability	Difficult to scale	Highly scalable
11.	Security	High	Low
12.	Flexibility	Low	High
13.	Performance	Low	High
14.	Architecture	Centralized	Decentralized

V. CONCLUSION

Our study for this survey revealed many electronic cash payment protocols. However, some protocols are quite similar, and differ only in some minor details. We distinguished two major categories of protocols i.e. online and offline. Such modes have different strengths and weaknesses with respect to their requirements: security, anonymity, reusability, ease of use, communication cost, additional cost (e.g. point of sale hardware), scalability etc.

VI. REFERENCES

[1] David Chaum Amos Fiat and Moni Naor, "*Untraceable Electronic Cash*", in Advances in Cryptology - CRYPTO '88 Proceedings.

[2] Lara Srivastava and Robin Mansell, "*Electronic Cash and the Innovation Process: A User Paradigm*", ACTS/FAIR Working Paper No. 35, Brighton: SPRU, March.

[3] Michelle Baddeley, "*Using E-Cash in the new economy: An Economic Analysis of Micropayment Systems*, in Journal of Electronic Commerce Research, VOL. 5, NO.4, 2004.

[4] David Chaum, "*Blind signature systems*", in David Chaum, editor, Advances in Cryptology —CRYPTO '83, page 153. Plenum Press, 1983.

[5] Ravi Kalakota, Andrew B. Whinston, "*Frontiers of Electronic Commerce*". Pearson Edition, Eighth Impression, 2009.

[6] David Chaum, Amos Fiat, and Moni Naor, "*Untraceable electronic cash*", in Shafi Goldwasser, editor, Advances in Cryptology — CRYPTO '88, volume 403 of LNCS, pages 319–327. Springer Verlag, 1988

[7] Stefano Cattani, Amit, Hiren, Kevin, Kai, "*Digital Cash*", 2004.

[8] Tsiaunis S., "*Efficient electronic cash, new Notions and techniques*", 1997.

[9] Matthew Franklin and Moti Yung, "*Towards provably secure efficient electronic cash*", Technical Report TR CUSC-018-92, Columbia University, Dept. of Computer Science, April 1992. Also in: Proceedings of ICALP 93, Lund, Sweden, July 1993, volume 700 of LNCS, Springer Verlag.

[10] Berry Schoenmakers, "*Basic Security of the ecash Payment System*", Version of April 1997. Appears in B. Preneel and V. Rijmen (eds.) State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography, Leuven, Belgium, June 3–6, 1997, vol. 1528 of Lecture Notes in Computer Science, pp. 338–352. Springer-Verlag.

[11] Jena, D., S.K. Jena, and B. Majhi, "*A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in Off-Line Digital Cash"*, in Proceedings of the 10th International Conference on Information Technology, 2007, IEEE Computer Society. p. 19-22.

[12] Laurie Law, Susan Sabett, Jerry Solinas, "*How To Make A Mint: The Cryptography Of Anonymous Electronic Cash"*, The American University Law Review [Vol. 46:113], 1997.