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 The value of DigiCash is represented by cryptographic tokens that can be withdrawn from bank accounts, deposited in bank accounts, or transferred to another people.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.

\[(*) \quad V_{PK} (S_{SK} (M)) = M \]

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
\[ M^v = M \pmod{N} \]

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](image-url)

**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].

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Proposing Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pfitzman and Waidner</td>
<td>1988</td>
</tr>
<tr>
<td>Chaum, Fiat and Naor</td>
<td>1988</td>
</tr>
<tr>
<td>Okamoto and Ohta</td>
<td>1989</td>
</tr>
<tr>
<td>Damgård</td>
<td>1990</td>
</tr>
<tr>
<td>Brands</td>
<td>1993</td>
</tr>
<tr>
<td>Cramer and Pedersen</td>
<td>1993</td>
</tr>
<tr>
<td>Franklin and Yung</td>
<td>1993</td>
</tr>
<tr>
<td>Chan, Frankel and Tsiounis</td>
<td>1995</td>
</tr>
<tr>
<td>Chan, Frankel and Tsiounis</td>
<td>1996</td>
</tr>
</tbody>
</table>

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. Online 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].
$(n, e)$ is the bank’s public key and
$(n, d)$ is the private key and
she presents her bank with $m' = m^r \pmod{n}$, where $m$ is her original message.

2. User’s bank signs it:
   \[ s' = (m'^{d} \pmod{n}) = (m^r)^{d} \pmod{n} \]

3. User divides out the blinding factor:
   \[ s = s'/r \pmod{n} \]

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

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

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