28

A Taxonomy of Electronic Cash Schemes

Ernest Foo, Colin Boyd, William Caelli, Ed Dawson,
Information Security Research Centre,
School of Data Communications,
Queensland University of Technology,
2 George Street GPO Box 2434,
Brisbane Q4001,
Australia

Abstract

A large number of electronic cash schemes have been proposed in the literature and several commercial ventures have started which claim to provide an anonymous payment protocol. These schemes have been designed to provide certain security properties.

Not all the schemes have proven to be practical and the precise security properties of the different schemes are difficult to compare due to their complex protocols. In this paper the key services required by electronic cash are identified and their provision in different electronic cash schemes published in the literature is compared. In addition to the security services, the mechanisms used to implement these services are isolated.

Keywords

Electronic commerce, electronic cash, security services and mechanisms.

1. INTRODUCTION

Electronic commerce can be described as any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. Within electronic commerce there are three distinct payment methods, namely: credit payments, cheques and electronic cash. These can be compared with their physical equivalents and are designed to provide similar properties.

Electronic cash schemes are anonymous payment schemes. As the potential of Internet commerce applications has started to be realised, the importance of electronic cash protocols has begun to be widely recognised. The possible number of uses for electronic cash is enormous. There are considerable benefits to consumers, merchants and financial institutions alike which result from the following fundamental properties of electronic cash.

- As for all electronic transactions, removal of the physical process leads to faster and more accurate processing.
- Electronic cash is of intrinsic value, allowing users immediate use of funds.

Most of the currently implemented systems rely on smart card technology. However, at present there exist only small experimental systems with a limited number of cards in circulation. One form of electronic card which is currently in wide-spread use is the telephone card; although a form of anonymous payment in its widest sense, these do not allow the user to refresh or refill the value of the card. Furthermore, such a system does not really encapsulate our design criteria since these cards cannot be used universally as an item of value. An electronic cash scheme should provide a secure payment system which allows a user to anonymously purchase, in principle, any goods and services.

1.1 What is Electronic Cash?

When trying to determine the required properties of electronic cash it is worthwhile to consider the usual properties of physical cash. Webster's Dictionary states that cash is:

1. ready money,
2. money or its equivalent paid promptly after purchase.

Physical cash has the following characteristics:

- "Value." It can be traded for goods or services.
- "Anonymous." Previous owners of the cash are not known by the current owners and the banks and government do not keep track of by whom, and where, the cash is spent.
- "Security." Cash currency is specifically designed to deter counterfeiting.

As mentioned above, it is the anonymous nature of cash that distinguishes it from other forms of payment scheme. Thus we are led to the following definition.

> Electronic cash is a payment system in which no information is retained such that the identities of the parties to a transaction may be deduced, after the successful completion of the transaction.

We would like to include within our definition of electronic cash any electronic payment scheme which has the same characteristics as physical cash. In addition there are other requirements of electronic cash which arise due to the electronic medium but which do not apply to physical cash. One of the properties of physical cash is that it is granted value by the local governing body. Currently electronic cash is not legal tender and is only granted value by the distributing body.

This paper classifies the properties of ideal practical electronic cash systems, which we term *electronic cash services*. These are considered in detail in section 2. Electronic cash services have been implemented in practice through many different specific processes or *electronic cash mechanisms*. Some mechanisms provide several services simultaneously. Section 3 details various mechanisms and how they provide

the required services. Many electronic cash systems have been described in the literature and several have already been implemented, at least in prototype form. The final section compares which electronic cash services are provided in existing electronic cash payment schemes and what mechanisms are used.

1.2 Terminology

The following terms are commonly used in the literature:

Coin A unit of electronic cash. Coins can have different values.

Bank The warehouse and administrator of electronic cash. The bank monitors the electronic cash coins for security violations.

Customer The entity which spends electronic coins.

Merchant or Shop The entity which receives electronic coins.

To date, all electronic cash schemes include at least three types of transactions: withdrawal, payment and deposit.

1. *Withdrawal* occurs when a customer either converts some funds from an account in the bank or is granted an overdraft of funds from the bank. In any case the withdrawal transactions transfers some electronic coins to the customer.
2. *Payment* occurs when the customer spends electronic coins. The electronic coins are transferred to the merchant. This payment usually involves the reciprocal transfer of goods or services from the merchant, although such transfer is typically not part of the electronic cash payment schemes.
3. *Deposit* occurs when a merchant or customer transfers electronic coins back into real currency. This involves interaction with the bank or other similar authority.

Some schemes have an additional procedure usually conducted before any other transactions occur. This is often referred to as the *opening procedure* and is similar to opening an account with the bank. The opening procedure typically enables the bank to give the user a password which will identify the user to the bank as a valid user.

2. ELECTRONIC CASH SERVICES

A concise list of electronic cash services was introduced by Okamoto and Ohta (1992). These include privacy, security, transferability and divisibility. Additional services, more geared towards a wide scale practical implementation of electronic cash, include scalability and acceptability. The need for these properties was first described by in Medvinsky and Neuman (1993) in their NetCash specification. Of these services only the two properties of privacy and security are common to all electronic cash schemes and may be called *compulsory* services. The other services are termed *optional*.

2.1 Privacy ("Untraceability" or "Anonymity")

The privacy of the user should be protected. A fundamental property of physical cash is that the relationship between users and their purchases is untraceable. This means that even if all the banks and merchants colluded they would not discover the identity of the purchaser provided the purchaser has not breached security. This property causes many governments to be cautious about promoting anonymous payment schemes. Because electronic cash does not require physical confirmation (i.e. presence of physical coinage) it may allow any number of illegal transactions to occur without the possibility of tracing. For example, the ability to transfer funds over the Internet across international boundaries in an anonymous manner (and currently with no restriction) will be of great concern to national governing bodies.

2.2 Security

The aim of security in cash payment protocols, as in other payment protocols, is to prevent any party from cheating the system. This includes entities involved in the transaction as well as external adversaries. For customers and external adversaries the forms of cheating security which are specific to payment schemes are:

- double spending of coins.
- creation of false coins (forgery) during payment.

From the merchant's side it is essential that genuine coins can be identified. Similarly banks must be sure that merchants do not double deposit or create false coins during the deposit transaction.

In electronic cash schemes, the security services traditionally applied in financial transactions must also be maintained. For customers, banks and merchants authentication and non-repudiation are necessary across all transactions. During the withdrawal transaction the bank must be sure that the correct customer received the electronic coin and not an entity masquerading as the customer. All parties must ensure that the transaction has occurred legally.

2.3 Transferability

The transferability service allows the transfer of coins from individual to individual. Cash schemes which do not allow this service must return a coin to the bank after it has been spent; the coins are non-transferable and can only be spent once before being reset. Non-transferable cash systems can emulate a transferable system by having the electronic coins sent through the bank reset before being transferred to the intended recipient of the transfer.

It is feasible that transferable cash schemes may use coins which are *never* deposited back to the bank. This would mean that the coins are circulated constantly much like physical coins. This scenario is problematic in the case of electronic coins as the longer the coin is left in circulation the longer adversaries have to decipher the coin structure. Most schemes which offer the transferability service also include a "used by" date which requires the bank to refresh the coin after a period of time.

2.4 Divisibility

The divisibility service allows a coin to be divided into smaller denominations. Each subdivision is worth any desired value as long as all values add up to the original value. Without divisibility, a customer must withdraw a coin of the desired value whenever a transaction occurs or withdraw many coins of various values and conduct a series of transactions which total to the cost of the goods or services to be purchased. The divisibility service is not one which is specific to anonymous payment schemes; other electronic payment schemes also require this service.

The unrestricted ability to subdivide introduces the issue of minimum value. It is likely that using electronic payment schemes vendors will charge a small amount to access information on the world wide web. Is it valid to charge one hundredth of a cent for each page? If so what happens if the customer no longer wishes to use the remaining ninety-nine percent of the cent and attempts to deposit it at the bank?

2.5 Scalability

Scalability is the ability to handle the addition of users and resources without suffering a noticeable loss of performance. In a system where a wide circulation of coins and a large user base is anticipated this service is essential. Scalability ensures that the scheme can be easily expanded to handle more transactions. Most scaleable electronic cash schemes do not contain just one central server (bank) but rely on multiple servers.

2.6 Acceptability

Acceptability refers to the ability of banks to accept coins minted by other banks. In a cash system which has acceptability with multiple banks a customer may withdraw coins from a bank and transfer those coins to a merchant. At the end of the day the merchant should be able to deposit the coins at any bank.

Without acceptability coins can only be used between parties that share a common bank. This would not be practical in a cash system with a large number of potential customers and merchants. Ideally acceptability should occur automatically without loss of performance. Many theoretical payment schemes do not take into account the importance of this property.

3. ELECTRONIC CASH MECHANISMS

Electronic cash mechanisms are the protocols and procedures that electronic cash scheme designers have used to implement the services that their schemes provide. We identify several mechanisms which implement key services; it should be noted that several mechanisms provide more than one service.

- There are several mechanisms which are used to provide the security service. *On-line operation* may be used in place of cryptographic mechanisms to prevent double spending. Other mechanisms are *cut and choose, line method, single term coins, blind certification* and *electronic licenses* which detect double spending or forgery, and reveal the identity of the perpetrator. These cryptographic mechanisms are not

essential for cash schemes which are dependent on *tamper-proof hardware* for security.

- *Blind digital signatures* provide aspects of the privacy service.
- The divisibility service is usually implemented by a *binary tree mechanism* or a *continuous hash* mechanism. These mechanisms also provide the transferability service.
- The scalability and acceptability services are usually provided through the use of *tamper-proof hardware* devices. No hardware independent electronic cash schemes directly address the issues of scalability and acceptability.

3.1 On-line Operation

In an on-line operation the validity of the transaction is verified while the transaction is occurring. When a cash scheme is on-line a coin being spent is sent to the bank and verified during the payment transaction. The bank is able to ensure that the coin has not been tampered with or previously spent. The bank then sends the coin to the intended recipient. The advantage of this system is that the bank can flag an attempt at an illegal operation as it is occurring and prevent it.

Most electronic cash schemes are off-line. In an off-line operation the validity of the transaction is verified a period of time after the transaction has occurred. Off-line schemes are more complex and are less secure than on-line schemes. Some authors, such as Simon (1996), argue that off-line operation is too risky whether tamper-resistant hardware is used or not. However, on-line schemes are widely regarded as too inefficient to be practical in most applications.

3.2 Tamper-Proof Hardware

Electronic cash schemes which do not use tamper-proof hardware do not rely on any physical properties (e.g. smart card, wallets) to maintain the security service, but rely only on cryptographic methods. This means that users will have access to the bit string values that represent the cash, but it must be infeasible, or at least unattractive, for the user to exploit this by copying the strings and using them multiple times. An advantage of hardware independent schemes is that they may be easily used for software implementation for Internet transactions.

In contrast, schemes dependent on tamper-proof hardware may employ both cryptographic methods and check physical conditions to ensure security. These schemes are usually more secure than hardware independent schemes. With hardware dependent observers off-line cash schemes can be as secure as on-line cash schemes with the obvious reduction in implementation complexity.

3.3 Blind Digital Signatures

Blind signatures were originally developed by Chaum (1983). The main aim of the blind signature mechanism is to allow a user to obtain another party's signature on a particular message without revealing that message. This is often compared to signing an envelope which contains a message on a piece of paper with a carbon paper backing. When the envelope is signed the pressure on the envelope combined with the carbon paper will cause the same signature to be impressed onto the message paper.

The mechanism is used to allow banks to validate coins by signing them, without knowing the coin details which would allow tracing. Customers choose randomised, but pre-formatted, coins which are then presented to the bank for signing. Any signed and properly formatted coin will be accepted as genuine. The customer usually selects a random number which is called the blinding factor. This number is multiplied with the message before sending it to the bank. The bank signs the hidden message and returns it to the customer. The customer can then remove the blinding factor and retain the signed message from the bank.

There are many variations on the blind signature theme. All the cash schemes surveyed for this paper use one of its forms to maintain the privacy service for the scheme.

3.4 Cut and Choose

Cut and choose was first introduced by Rabin (1978) as a zero knowledge proof technique. It was first used for electronic cash by Chaum, Fiat and Naor (1990) in conjunction with blind signatures to prove that a signature had been correctly formed. This technique was very popular with some of the earlier cash schemes and is still one of the most widely discussed mechanisms in the electronic cash scheme literature. The basic idea uses three distinct phases.

Withdrawal

The customer prepares a number of coins ready for signing by the bank. As well as randomising values and formatting, these must include some value which will be used to trace the customer in the event that he spends a coin twice. For example, it might contain the customer's identity split into two parts which are independently hidden cryptographically. All the coins are blinded and revealed to the bank. The bank chooses some (say half) and the customer 'unblinds' them which allows the bank to check that the customer is acting properly. Depending on the parameters used, there is a high probability that a cheating customer is caught and the bank then takes whatever action it decides. If the bank is satisfied that the customer is acting properly then the remaining coins are signed and returned to the customer, and the customer's account is debited.

Payment

This is an interactive protocol during which the customer presents a coin to the merchant and the merchant chooses randomly to see some of the customer information contained in it. For example, this information may be one part of the split identity. Double spending cannot be detected during payment.

Deposit

The merchant returns the coin to the bank where its random serial number is checked to see if it has been spent before. If so, then the two parts of the customer information are combined and, depending on the parameters used, the customer's identity is revealed with high probability. If the coin is spent only once, the information is not sufficient to find anything about the customer's identity.

Unfortunately cut and choose is a very inefficient method for proving that a customer has not breached security because it requires interactive protocols for both payment and withdrawal and only half of the coins prepared by the customer are used.

3.5 Line Method

The line method was developed by Franklin and Yung (1993) as a new mechanism which would decrease the amount of traffic. The line method uses a very similar mechanism to the cut and choose method called *oblivious authentication* which also uses blind digital signatures to provide the privacy service.

This mechanism requires a smaller amount of network handshaking than the cut and choose method but the size of the coins is still very large. This is because each coin must hold two points and the slope for several lines. The number of lines required to ensure a secure scheme determines the efficiency of the mechanism.

3.6 Single Term Coin

The single term coin mechanism was developed by Ferguson (1994). A similar mechanism was later used by Eng and Okamoto (1995). The single term coin is much more efficient than the cut and choose method because instead of using k coins to return $k/2$ useable coins, only one is required. This is similar to the line method in that only one challenge term is used, but here the challenge term is much smaller.

This mechanism uses a variation of the blind digital signature scheme called the *randomised blind signature scheme*. The randomised blind signature scheme requires both multiplicative and exponential blinding factors. The amount and size of the network traffic required is considerably smaller than that required by the cut and choose mechanism but the increased efficiency also results in increased complexity.

3.7 Electronic License

The electronic license mechanism was introduced by Okamoto (1995). The electronic license is a signed document authorising the user to spend coins issued by the bank and is used together with a bit commitment scheme and a binary tree representation of the coin to provide the security service. The electronic license and bit commitment prove that the customer has a valid coin from the bank and thus prevents forgery. A simple blind digital signature is used to provide the privacy service. The electronic license mechanism is more efficient than the original cut and choose scheme but like the single term coin mechanism it is more complex.

The electronic license mechanism is fairly efficient in its withdrawal, payment and deposit transactions. However, the opening transaction which issues the customer with an electronic license can involve the transfer of a lot of data, especially in the bit commitment section.

3.8 Blind Certification

The blind certification mechanism was first used by Yacobi (1995) and later used by Brands (1995) and Mao (1996). This security mechanism requires that each customer obtain a blind certificate. A blind certificate is similar to an ordinary certificate which

contains a public key and the holder's identity but the identity of the customer is hidden using Chaum's blind signature technique.

The security of blind certification is dependent on Schnorr's one-time signature scheme (Schnorr 1990). This scheme was originally designed for the generation of signatures for use in smartcards. Schnorr's scheme uses a property of El-Gamal signature scheme which causes the identity of the customer in the blind certificate to be revealed if a customer attempts to sign two different messages using the same signature. Using this property double spending can be exposed.

3.9 Binary Tree

Divisibility may be implemented by using a binary tree. This mechanism was first used by Okamoto and Ohta (1992) and then used again in Eng and Okamoto's (1995) scheme with the single term coin mechanism. Lately the binary tree mechanism has been used in conjunction with Okamoto's (1995) electronic license mechanism.

The key to the binary tree method is the way the binary tree nodes are allocated values. If a cash scheme uses the binary tree mechanism, each coin of worth $w = 2^L$ is associated with a binary tree of $(1+L)$ levels and w leaves. Each node of the tree represents a certain denomination.

When dividing the value of the coin two rules are followed:

1. **Route Node Rule**: When a node is used, all descendant nodes and all ancestor nodes of this node cannot be used.
2. **Same Node Rule**: No node can be used more than once.

The divisibility service provided by the binary tree mechanism is implemented in the payment transaction.

3.10 Continuous Hash

The continuous hash divisibility technique was originally designed for micropayment schemes. It was first used in Rivest and Shamir (1996) for their *MicroMint* micropayment scheme. Mao (1996) adapted this mechanism for use in an anonymous payment scheme. Instead of using a binary tree to represent the coins, continuous hash consists of a series of coins chained together. The n-th coin is the seed number. The $(n - 1)$-th coin is the seed number hashed once. The $(n - 2)$-th coin is the seed number hashed twice, the $(n - 3)$-th coin is the seed hashed three times and so on. The following is a description of how Mao (1996) adapts the continuous hash mechanism for anonymous cash schemes.

Withdrawal

1. Hash a secret number n times, where n is the desired number of coins.
2. Link the hashed coins together in a chain as described above.
3. Get the bank and customer to sign the first coin.

Payment

1. The customer sends the chain of coins to merchant.
2. The merchant selects x-th coin and recursively hashes it x times.

3. Thus the merchant has computed the first coin.
4. The merchant now has the bank's signature.
5. The merchant signs the bottom coin and returns the chain of coins to the customer.

The customer can now spend the remaining coins. The merchant signed coin is now the top coin.

4. EXISTING ELECTRONIC CASH SYSTEMS

There are currently a number of electronic cash systems in use. The schemes with the widest circulation like CAFE (Conditional Access for Europe) (Boly et al. 1994) and Mondex depend on hardware devices to ensure security. Digicash, Cybank and VisaCash are three other companies providing an anonymous cash payment scheme. Unfortunately all of these schemes (except CAFE) have not published their protocols in the literature and so it is not possible to establish that these schemes are anonymous or secure.

We have classified thirteen electronic cash schemes, which have been fully described in the open literature, according to the services and mechanisms outlined in sections 2 and 3. Table 1 details the desired services for several electronic cash schemes. Table 2 indicates which mechanisms the electronic cash schemes in table 1 used to implement these services.

Mechanisms seem to be easily combined to form new electronic cash schemes. This is most easily demonstrated by looking at the use of the binary tree mechanism. This was first used with the cut and choose mechanism to form the cash scheme presented by Okamoto and Ohta (1992). Another combination using the binary tree mechanism is Eng and Okamoto's (1995) scheme which uses binary tree and single term coin mechanisms. Finally a third combination is Okamoto's (1995) scheme which uses binary tree and electronic license to present a new cash scheme.

		Services					
Designers	Electronic Cash Schemes	Anonymity	Security	Transferability	Divisibility	Scalability	Acceptability
Brands '95	Electronic Cash on the Internet	x	x	x		x	x
Chaum '89	Online Cash Checks	x	x		x		
Chaum, Boer et. al. '89	Efficient Offline Electronic Checks	x	x		x		
Chaum, Fiat and Naor '88	Untracable Electronic Cash	x	x				
Ferguson '93	Single Term Offline Coins	x	x				
Franklin and Yung '93	Secure and Efficient Offline Digital Money	x	x				
Hayes '90	Anonymous One Time Signatures and Flexible Untraceable Electronic Cash	x	x				
J.P. Boly et. al. '94	CAFE	x	x		x	x	
Mao '96	Lightweight Micro-Cash for the Internet	x	x	x	x		
Medvinsky and Neuman '93	NetCash	x	x	x		x	x
Okamoto '95	An Efficient Divisible Electronic Cash Scheme	x	x		x		
Okamoto and Ohta '91	Universal Electronic Cash	x	x	x	x		
Yacobi '94	Efficient Electronic Money	x	x				

Table 1 A Summary of Electronic Cash Services

Designers	Electronic Cash Schemes	Mechanisms										
		Cut and Choose	Line Method	Single Term Coins	Electronic License	Blind Certification	Online Operation	Offline Operation	Hardware Dependent	Blind Digital Signatures	Binary Tree	Continuous Hash
Brands '95	Electronic Cash on the Internet					x		x	x			
Chaum '89	On-line Cash Checks						x			x		
Chaum, Boer et. al. '89	Efficient Off-line Electronic Checks	x						x		x		
Chaum, Fiat and Naor '88	Untraceable Electronic Cash	x						x		x		
Ferguson '93	Single Term Off-line Coins			x				x		x		
Franklin and Yung '93	Secure and Efficient Off-line Digital Money		x					x		x		
Hayes '90	Anonymous One Time Signatures and Flexible Untraceable Electronic Cash	x								x		
J.P. Boly et. al. '94	CAFE							x	x	x		
Mao '96	Lightweight Micro-Cash for the Internet					x		x				x
Medvinsky and Neuman '93	NetCash	x						x	x	x		
Okamoto '95	An Efficient Divisible Electronic Cash Scheme				x			x		x	x	
Okamoto and Ohta '91	Universal Electronic Cash	x						x		x	x	
Yacobi '94	Efficient Electronic Money					x		x				

Table 2 A Summary of Electronic Cash Mechanisms

The list of mechanisms in this paper is not complete. It is likely that new mechanisms will be designed to implement various services and be incorporated with some of the older mechanisms to develop new cash schemes. Designers need to be careful which mechanisms are selected. The advantages and disadvantages of specific mechanisms will also be included in the new cash schemes which contain them.

5. CONCLUSION

Electronic cash is an anonymous payment system which allows users to purchase goods or services electronically with privacy and security. This paper has identified some of the important services which a practical cash system should provide. These services include: security, privacy, transferability, divisibility, scalability and acceptability.

Once these required services were identified the paper investigated some of the mechanisms used to implement these services. The most common mechanisms used in the literature were: the cut and choose zero knowledge proof and off-line operation to provide security, blind digital signatures to provide anonymity and privacy, and the binary tree mechanism to provide divisibility of the electronic coin. Not all mechanisms were investigated in this paper. It is likely that new electronic cash scheme design will consist of a combination of existing mechanisms or of new mechanisms which provide the electronic cash services stated above.

There are a number of important issues that have not been covered in this paper but which must be considered in any practical electronic cash scheme. In particular the complexity analysis of the competing protocols and associated algorithms is a prime concern, especially because most schemes are implemented using smart cards. Other issues include interaction with legal and policy matters; recent schemes (Jakobsson and Yung 1996) have already suggested ways to limit anonymity with the cooperation of a trustee. We intend to cover all these concerns in future reports.

6. REFERENCES

J.-P. Boly et al. (1994) "The ESPRIT Project CAFE - High Security Digital Payment Systems", *Computer Security - ESORICS '94,* pp. 217-230, Springer-Verlag.

S. Brands (1995) "Electronic Cash on the Internet", In *Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security*, pp. 64-84.

D. Chaum (1983) "Blind Signatures for Untraceable Payments", In *Advances in Cryptology - Proceedings of CRYPTO '82*, pp. 199-203, Plenum Press.

D. Chaum (1989) "Online Cash Checks", *Advances in Cryptology - Proceedings of EUROCRYPT '89*, pp. 288-301.

D. Chaum, A. Fiat and M. Naor (1990) "Untraceable Electronic Cash", *Advances in Cryptology - Proceedings of CRYPTO '88,* pp. 319-327, Springer-Verlag.

T. Eng and T. Okamoto (1995), "Single-Term Divisible Electronic Coins", *Advances in Cryptography - Proceedings of EUROCRYPT '94 (LNCS 950),* pp. 306-319, Springer-Verlag.

N. Ferguson (1994), "Single Term Off-Line Coins", *Advances in Cryptology - Proceedings of EUROCRYPT '93,* pp. 318-328, Springer-Verlag, 1994.

M. Franklin and M. Yung (1993) "Secure and Efficient Off-Line Digital Money", In *Proceedings of ICALP '93 (LNCS 700),* pp. 265-276, Springer-Verlag, 1993.

B. Hayes (1990) "Anonymous One-Time Signatures and Flexible Untraceable Electronic Cash", *Advances in Cryptology - AUSCRYPT '90,* pp. 294-305, Springer-Verlag.

M. Jakobsson and M. Yung (1996) "Revokable and Versatile Electronic Money", *Third ACM Conference on Computer and Communications Security*, ACM Press, pp. 76-87.

W. Mao (1996) "Lightweight Micro-Cash for the Internet", *Computer Security - ESORICS '96*, Springer-Verlag, pp.15-32.

G. Medvinsky and B. C. Neuman (1993) "NetCash: A Design for Practical Electronic Currency on the Internet", *Proceedings of First ACM Conference on Computer and Communications Security*, pp. 102-196, ACM Press.

T. Okamoto (1995) "An Efficient Divisible Electronic Cash Scheme" *Advances in Cryptology - Proceedings of CRYPTO '95,* pp. 438-451, Springer-Verlag.

T. Okamoto and K. Ohta (1992) "Universal Electronic Cash", *Advances in Cryptology - Proceedings of CRYPTO '91,* pp. 324-337, Springer-Verlag.

M. O. Rabin (1978), "Digitalized Signatures", In *Foundations of Secure Computation*, Academic Press, NY.

R. L. Rivest and A. Shamir (1996) "PayWord and MicroMint: Two simple micropayment schemes", *RSA Security Conference*, January 1996.

C. P. Schnorr (1990) "Efficient Signature Generation for Smart Cards", *Advances in Cryptology - Proceedings of CRYPTO '89,* pp. 239-252, Springer-Verlag.

D. R. Simon (1996) "Anonymous Communication and Anonymous Cash", *Advances in Cryptology - Proceedings of CRYPTO '96*, Springer-Verlag, pp.61-73.

Y. Yacobi (1995) "Efficient Electronic Money", *Advances in Cryptology - Proceedings of ASIACRYPT '94,* pp. 153-163, Springer-Verlag.