Electronic Cash System

1 Introduction

This invention relates to an electronic cash system. Such systems, which are also called 'digital cash', have been described in the literature [Cha] [CAFE] and provide a means for a customer to make a payment to a merchant over a computer network by sending messages called 'electronic coins' or 'digital coins' which the merchant can redeem for value.

There are a number of applications in which customers may wish to make a series of small payments to the same merchant over a network.

One specific application which motivates this invention is electronic publication. Publication is a broad field and encompasses the distribution of music, video films, books, newspapers, journals and worldwide web pages. The advent of multimedia systems may blur the distinction between some of these categories. However one persistent feature of the publishing business is that customers often make a series of small payments to the same merchant, as when purchasing periodicals from a newsagent or renting videos from a library.

Now that technology makes it possible for published material to be marketed in smaller packages, we may see the number of payments rise while their average value goes down.

For example, with learned publications, a customer will often wish to read only one specific article of a given journal issue, and may be discouraged if she has to purchase an entire volume of perhaps twelve issues. It would be more convenient, and it could encourage sales, if individual pages of the journal could be purchased online.

Another example is newspaper publishing. When a newspaper is made available online, its customers may be charged a subscription, a price per issue, or a small sum per page or per article. Again, the publisher may wish to make per-item charges an option for marketing reasons. However, if these charges are collected through a billing system, then this could involve significant overheads due to the large volumes of small transactions.

A third publishing example is the abstracts journal or database enquiry service. If a customer wishes, for example, to find all articles written in the last seven years and which refer to both thermodynamics and population genetics, she might use one of these to search for citations. At present such services are typically sold by subscription, and the cost of this may restrict their use to the libraries of large universities and companies. However with the advent of the world wide web, it is possible to publish an abstracts journal which contains a one paragraph summary of each article in a field plus a hypertext link to that article, and charge for every hypertext link that the customer follows up. However, as remarked above, billing systems are expensive to run and this motivates us to look for a more economic way to collect a large number of online charges of a few pennies each.

Another application area is prepayment utility meters as described in [AB]. Such meters nowadays accept electronic tokens rather than cash, in order to cut the costs of coin collection and of theft.

Another application area is in charging for computer facilities. A university may allow students to print a certain number of pages per term on a laser printer for free, and charge a certain amount per sheet thereafter. Running a billing system for such an application is expensive and the use of electronic cash could save money. In this case, too, the customer will want to make a series of small payments to the same merchant.

Another application area is transport payments, such as tickets for public transport and tolls for using roads, bridges, tunnels, car parks and other facilities. It is inconvenient for traffic to slow down and stop at toll gates, and so systems for collecting tolls from moving vehicles are under development. But rather than having a number of proprietary electronic devices for successive tolls on a journey, motorists could find it convenient to have a store of digital coins which would be accepted by many toll stations and which could be transmitted from a moving vehicle using radio or infrared. Again, such systems involve large numbers of payments to a small number of merchants.

A digital cash system need not be restricted to a single application. For example, if a university were to introduce digital coins to pay for computer service resources, then it might in time be extended to catering, photocopiers and other services, especially if the payments could be made using a portable device such as a smartcard.

2 Prior Art

A number of protocols have been proposed in the literature to facilitate electronic commerce. These include VISA's Secure Transaction Technology [STT] and MasterCard's Secure Electronic Payment Protocol [SEPP], both of which enable a customer to send a credit card order in encrypted form over a network. However both these proposals use the existing credit card infrastructure and their transaction costs may be too high for small payments.

Other protocols have been proposed which are claimed to be more suitable for low value payments, including NetBill [CMU] Millicent [DEC] and CAFE [CAFE]. There are also application specific protocols such as those used in electricity meters [AB].

The concept of electronic cash is thus well established, and the aim of the present invention is to provide an improved system in which large numbers of low value payments can be made at a low unit cost.

3 System requirements

An electronic cash system will typically be implemented using smartcards or other portable secure devices in which customers (and in some systems also merchants) store value. These devices typically contain a slow processor and a small amount of memory, so both computational complexity and secure storage requirements must be minimised.

In addition, the falling cost of bandwidth means that the costs of networking are dominated in many applications by the switching costs. So it is desirable to minimise the number of references which must be made to third parties such as banks and brokers during each run of a payment protocol.

An electronic cash system should also minimise administrative costs such as the costs of account opening and dispute resolution. The latter can be tackled in many applications by using digital coins of relatively low value. Where a substantial amount is in dispute, customers will insist on refunds and the cost of administering these can be significant. However, if the typical payment is only for a few pennies then it is not worth the customer's while to complain, and provided errors are infrequent, most customers may accept them as a cost of operating the system — as is the case for example with misrouted calls from public telephones.

It may also be desirable that the system should not have to give change. This is because a communications channel may be interrupted by equipment failure. The mechanisms for correct change recovery in such situations can add significant technical and administrative overheads.

There are also applications where it is desirable that the merchant should not have to purchase special purpose hardware. This means that the merchant should not have to perform onerous computations or keep secrets in tamper-proof hardware; in general purpose eftpos systems, for example, the major cost of introducing a new payment mechanism may be that of integrating new hardware with existing merchant systems. Another example is given by prepayment electricity meters; these must be manufactured at very low unit cost and thus contain low powered microcontrollers. This has prevented the use of public key cryptography, despite its potential benefits for key management [AB]. We may therefore require the merchant's part of the system to consist of a simple portable software module which does not use a lot of computational resources and which does not add any communications complexity.

4 Outline of invention

According to the present invention there is provided a system to be implemented in smartcards or other suitable secure hardware (or in certain circumstances in software) whereby a customer purchases a number of electronic coins from a coin vendor and spends them with one or more merchants. The merchants can then redeem the coins with the coin vendor.

Technical measures ensure firstly that the probability of a customer successfully passing an invalid coin to a merchant, or spending a valid coin with two different merchants, is low; and secondly that a customer who does succeed in such a forgery can be identified afterwards.

The above features are common to a number of digital cash systems [Cha] [CAFE]. The present invention reduces the amount of computation which has to be performed by the customer to one digital signature for each series of transactions with the same merchant. This is achieved by a recursive hashing technique which enables the customer to sign a whole stick of coins at the same time. The coins can then be pulled off the stick one by one and presented to the merchant, who is able to check that each coin was one of those signed by the customer. The merchant only has to perform one signature verification per customer, even when the costumer spends a lot of coins.

Customers may also use pseudonyms so that they do not have to reveal their identities to merchants. This helps protect privacy, and reduces the reporting requirements imposed on system participants by data protection legislation.

5 Specific embodiment of invention

We now describe a specific embodiment of the invention.

Customer keys

In some of the applications mentioned above, such as video rentals, the regulatory climate may require customer anonymity. In this case electronic coins might be supplied for cash, and a deposit required to discourage system abuse. In other applications, such as if the coins were legal tender, money laundering regulations might require the bank to keep a record of her identity. In yet other applications, such as road tolls, anonymity might be optional.

However the mechanisms (if any) for binding customer names to pseudonyms do not form part of this invention, and for the sake of simplicity we will hereafter refer to the coin vendor simply as the 'bank'.

The customer chooses a pseudonym P. She generates in her smartcard, or other secure device, a pair of keys with KP^{-1} being her secret signing key and KP her public signature verification key (for an introduction to the techniques of public key cryptography see Schneier [Sch]; for an introduction to cryptographic protocols see Anderson and Needham [AN]; for a suitable digital signature algorithm see [DSS]).

The bank then creates a certificate which contains the bank's name B, an expiry date e, the customer's credit limit \$, her pseudonym P and her public key KP, all signed using the bank's signature key KB^{-1}. Using the symbolism of [AN]:

$$CP = \{B, e, \$, P, KP\}_{KB^{-1}} \tag{1}$$

The public key KB required to verify the bank's signature on customer certificates must be reliably known to the merchants with whom the customer will spend the coins. Mechanisms for certifying bank keys are described in [STT] and [SEPP] for VISA and MasterCard affiliated banks respectively.

Coin withdrawal

Digital coins may be issued in a number of denominations, but for simplicity's sake we will consider them here to be all for the same amount. They consist of 64 bit strings and are constructed by encrypting a serial number and some redundancy under a secret key selected by the bank. The algorithm used for encryption may be two-key three-round DES or any other block cipher in which the bank has confidence. Different keys K_{BP} are chosen for each customer pseudonym P, and these keys are kept in a secure hardware device such as that described in [VSM] at the bank. They are not disclosed to any third party except possibly to a court in the case of dispute.

The customer may now purchase digital coins in sticks which in our specific embodiment contain 100 coins each. In general they may contain k coins and we will write the coins C_i. The j-th stick of coins will have

$$C_i = \{i \mid j \mid B\}_{K_{BP}} \tag{2}$$

where the bank's name B is used to provide redundancy, and $\mid$ denotes concatenation.

Each stick of coins is digitally signed by the bank. Again, the bank's name is inserted to provide redundancy, as is the issue date t, and the coin stick is thus supplied to the customer as

$$CS = C_1, C_2, \ldots, C_k, \{B, t, C_1, C_2, \ldots, C_k\}_{KB^{-1}} \tag{3}$$

The signature protects the customer against fraud by the bank or its employees; if the bank later fails to honour a coin or even wrongfully accuses her of having passed an invalid coin, she can produce the stick signature in her defence.

Payment

When the customer wishes to make a purchase from a merchant, she first sends a certificate which vouches for the genuineness of the coins which she is about to spend. She may not be able to tell in advance how many coins will be used, as she may not know how many pages of a learned journal she will have time to read, or how long her patient will stay in hospital. So she may take the precaution of vouching for a number of them, perhaps a whole stick. She does this by hashing the coins using a cryptographic hash function such as the Secure Hash Standard [SHS]; the hash function, which we will denote h, should have the properties that while it is easy to calculate $h(X)$ given X it is not feasible to calculate X given only $h(X)$, and it is also not feasible to find two unequal X and Y such that $h(X) = h(Y)$.

If the coins for which the customer wishes to vouch are $C_1, \ldots, C_k$ then she hashes them together as follows. Firstly, the last coin value is hashed to give $h_k = h(C_k)$. Then each of the coins is hashed into this value in turn:

for $i = k - 1$ downto 1 do

$$h_i = h(C_i \mid h_{i+1}); \tag{4}$$

Finally the customer signs h_1, her pseudonym P, the name of her bank B, the merchant's name M and the date d, and sends this to the merchant:

$$S = \{h_1, P, B, M, d\}_{KP^{-1}} \tag{5}$$

She also sends the merchant h_1 and her public key certificate CP. The effect of her signature S, which will be made explicit in her service contract, is that she vouches for the coins, in that she claims they were properly issued by a bank and have not been spent elsewhere in the meantime.

The merchant checks the certificate and the value S, and if these verify he signals her to begin the transaction. In order to spend the first coin, she sends the merchant the values C_1 and h_2. If $h_1 = h(C_1 \mid h_2)$ he accepts the coin as valid. To spend the second coin, she sends C_2 and h_3, and so on.

Redemption

In order to redeem the coins, the merchant presents to the bank the customer's signature S, the coins $C_1, \ldots, C_m$ actually spent by the customer and the corresponding hash values $h_1, \ldots, h_{m+1}$. The bank checks the coins using equation (2) above, verifies from its records that none of them has been spent before, and credits the merchant's account. The bank may guarantee the transaction so long as the signatures and hashes are consistent, and the total value spent does not exceed the customer's credit limit (otherwise the validity of the coins could be checked online as with credit card transactions over the merchant's floor limit). Such guarantees may be a necessary feature of systems which allow total anonymity of customers.

If there are multiple coin issuers in a system, then the merchant may use a different bank from that which issued the coins. In this case, an interbank settlement mechanism is constructed in the traditional way; the information presented by the merchant $\{M, P, B, d, S, C_1, \ldots, C_m, h_1, \ldots, h_{m+1}\}$ is treated as a cheque and sent to the bank B through a clearing house.

Implementation

The trusted computing base of the customer's system is implemented, in the case of the present specific embodiment of the invention, in a smartcard, and, as noted above, the coins are supplied by the bank in sticks of 100 coins. As these are signed with the bank's signature key, they may be stored on the disk drive on the customer's personal computer. The only security property required of this medium is availability, i.e. the sticks of unspent coins should not get lost, and for this purpose they can be backed up on removable media such as diskettes.

In order to activate the system, a stick of coins is loaded into the smartcard which checks the bank's signature and performs the hashing calculations in equations (4) and (5) above.

Once the customer has selected a merchant with whom to do business, she enters a password of eight characters which places the smartcard in payment mode, and passes to it the name of the merchant. The card now calculates S according to equation (5) and will dispense it together with the coin and hash values C_i, h_{i+1} as requested by the application. In order to prevent double spending, the card maintains a count of the coins which have been dispensed; it will reissue a coin in the event of communications failure, but it will not issue the same coin to two separate merchants. It also records the last 64 sticks of coins spent to prevent accidental double spending by the customer in the event, for example, that a backed up hard disk is restored.

When a customer finishes a transaction with a partially spent stick of coins in her card, she may wish to save this to disk, in order for example to switch from a library payment system whose coins are each worth several pence to a road toll system with coins worth tens of pence. In this case, the unspent coins of a stick can be saved signed with her own signature key. It can occasionally happen that the last coin issued by the card to pay a merchant is not in fact spent (for example, because of a communications failure); in that case a flag is set so that the customer may not commit this coin to another merchant. She may either use it in the next transaction with the original merchant or return it to the bank for a refund.

Advantages over the prior art

The current invention conforms more closely than the prior art to the system requirements set out above. Firstly, it greatly reduces the computational complexity in applications where a series of low value payments are made to the same merchant.

Existing digital cash protocols may require the use of a public key primitive such as a signature when each coin is spent, and as noted above, this has prevented the use of digital cash in prepayment meter systems. The present invention needs only one digital signature for each series of transactions between a customer and a merchant; the individual coins can then be checked at the cost of a single hashing operation.

Furthermore, the one digital signature can be generated at any time once the customer knows the name of the merchant and the transaction date. It could for example be implemented using a server-aided protocol with the customer's PC acting as server [Beg]. The result is that lower cost smartcards can be used by the customers. At the merchant end, there is no particular need for the tamper resistant hardware that is required for example with [STT] and [SEPP]; the merchant only needs to be able to verify hashes and signatures.

Some other protocols involve trusted third parties or intermediaries which can complicate the implementation, drive up networking costs and introduce additional points of failure. The present invention involves only the necessary parties, namely the bank, the customer and the merchant; and only the necessary transactions, namely cash withdrawal by the customer, payment from the customer to the merchant, and banking of the cash by the merchant.

Other protocols use relatively large units of electronic value and the merchant gives change at the end of most transactions. As noted, this is not optimal in many network applications.

Security

Payment systems typically have multiple controls to prevent fraud. In cash-like systems, the primary control is in the payment medium itself (banknotes should be hard to forge), while cheque-like systems rely on bookkeeping (as with the international credit card system). However, many systems also have secondary controls of the other type: banknotes are numbered and credit cards have holograms.

In a similar way, it is anticipated that the invention described herein may be used together with a bookkeeping and settlement system with which attacks may be quickly detected.

For example, we are relying on the tamper resistance of the smartcard to prevent a dishonest customer from obtaining unrestricted access to her signing key, and thus being able to create certificates which would vouch for invalid coins. However, such attacks are neither impossible [Ajl] nor unknown [Mcc], and so a prudent designer will anticipate them. In the case of the present invention, each penetration allows the attacker to forge coins only for that pseudonym, and thus he can expect only limited gains before the pseudonym is placed on a hot list or or its certificate expires.

The security of the system is thus based on a number of factors working together. It relies firstly on the properties of the cryptographic primitives involved (the hash function, the digital signature scheme and the block cipher used to create coins). It is based secondly on the tamper resistance of the smartcard, and of the corresponding secure devices used by merchants and banks to store their key material. Thirdly, it may employ bookkeeping systems to ensure that coins issued are in balance coins with coins redeemed, and thus to track users who succeed in forging transactions. Finally, unlike some current electronic banking systems, the bank's signature on issued coin sticks makes it harder for a fraud by a bank employee to be wrongly blamed on a customer.

6 Variants of the invention

There may be applications where cost pressures, a perceived low level of threat, or the regulatory environment lead to the current invention being implemented wholly in software on the customer's PC. In that case, a customer could use a debugging tool to get unrestricted access to her signing key. However, as in the case of the physical penetration of a smartcard implementation, her expected gains are limited and the exposure can be controlled by using a bookkeeping system to detect double spending.

The regulatory climate may also affect the choice of cryptographic primitives. There are countries where payment systems may use hash functions and digital signatures but the use of encryption by civilians is severely restricted. In such a case, the bank may generate the coins at random rather than by using an encryption function and detect replay attacks by storing them whether intact or in a hash table. Note that the main purpose of constructing the coins as in equation (2) above is to simplify the detection of double spending.

It may also be desired in some applications that the bank also sign h_1, so that the merchant can verify the bank's imprimatur on each coin spent. This facility does not of course prevent double spending for which there must still be effective recourse against the customer.

Finally, as mentioned above, certain applications may need to support a number of different denominations of coin, and for performance reasons (such as smartcard memory limitations) it may be desired to include multiple denominations in a single coin stick. In this case the customer will want to strip coins from the stick in an arbitrary combination. This can be supported by hashing the coins in each denomination separately and then hashing the totals together for signature. For example in the case of two denominations C^1 and C^2, a stick might contain coins $C^1_1, \ldots, C^1_j$ and $C^2_1, \ldots, C^2_k$. As before we would hash each of these substicks together with $h^1_j = h(C^1_j)$, $h^1_{j-1} = h(C^1_{j-1} \mid h^1_j)$ and so on until we get $h^1_1 = h(C^1_1 \mid h^1_2)$ and similarly h^2_1. We would then use in equation (5) above the value $h_1 = h(h^1_1 \mid h^2_1)$ and send the values h^1_1, h^2_1 along with the signature S and h_1 to enable the merchant to verify the coins.

References

[Ajl] "Two New Imaging Techniques Promise To Improve IC Defect Identification", C Ajluni, *Electronic Design* Vol 43 No 14 (10 July 1995) pp 37–38

[AB] "Cryptographic Credit Control in Pre-payment Metering Systems", RJ Anderson, SJ Bezuidenhout, *Proceedings, 1995 IEEE Symposium on Security and Privacy* pp 15–23

[AN] "Programming Satan's Computer", RJ Anderson and RM Needham, in *Springer Lecture Notes in Computer Science volume 1000*

[Beg] "Fast Server-Aided RSA Signatures Secure Against Active Attacks", P Béguin, JJ Quisquater, *Advances in Cryptology - CRYPTO 95*, Springer LNCS 963 pp 57–69

[Cha] "Achieving Electronic Privacy", D Chaum, *Scientific American* (August 92) pp 96–101

[CAFE] "The ESPRIT Project CAFE — High Security Digital Payment Systems", JP Boly, A Bosselaers, R Cramer, R Michelsen, S Mjølsnes, F Muller, T Pedersen, B Pfitzmann, P de Rooij, B Schoenmakers, M Schunter, L Vallée, M Waidner, in *Computer Security — ESORICS 94*, Springer Lecture Notes on Computer Science volume 875 pp 217–230

[CMU] "NetBill: An Internet Commerce System Optimized for Network-Delivered Services", M Sirbu, JD Tygar, *IEEE Personal Communications* August 1995 pp 34–39

[DEC] *The Millicent Proposal for Inexpensive Electronic Commerce*, S Glassman, M Manasse, M Abadi, P Gauthier, P Sobalvarro, Digital Systems Research Center Preprint, 1995

[DSS] *Digital Signature Standard*, Draft, US National Institute of Standards and Technology, August 30, 1991; FIPS 186, US Department of Commerce, 1993

[Mcc] "Has DSS been hacked?" J McCormac, *Electronics Now* (August 1995) pp 33–40 & 76

[Sch] *Applied Cryptography*, B Schneier, John Wiley and Sons

[SEPP] *Secure Electronic Payment Protocol*, MasterCard 1995

[SHS] *Secure Hash Standard*, Draft, US National Institute of Standards and Technology, 31 January 1992; FIPS 180, May 1993, amended as FIPS 180-1, April 1995, US Department of Commerce

[STT] *Secure Transaction Technology*, VISA 1995

[VSM] *VISA Security Module Operations Manual*, VISA, 1986

CLAIMS

1. An electronic cash system in which customers when transacting with merchants use digital signatures to vouch for digital coins or other electronic payment instruments, whose validity the merchant cannot check directly without going online to a bank, and in such a way that the customer may be held accountable if (s)he vouches for an invalid instrument.

2. An electronic payment system in which recursive cryptographic hashing is applied to a number of payment instruments to create a composite instrument which is then authenticated using a digital signature or challenge-response protocol or otherwise, and such that the original instruments can be revealed, whether in a given sequence or in any one of a number of sequences, in such a way that the authenticity of each instrument may be deduced or inferred from the single signature or other authentication mechanism.

3. An electronic cash system in which the bank issues the customer with electronic coins which have been generated at random and which the bank stores in a hash table or otherwise in order to detect double spending.

4. An electronic cash system in which some combination of the features described in claims 1, 2 and 3 above are employed.

5. A system in which recursive cryptographic hashing is applied to a number of objects to create a data structure which is then authenticated using a digital signature or otherwise, and such that the original objects can be revealed, whether in a given sequence or in any one of a number of sequences, in such a way that the authenticity of each object may be deduced or inferred from the single signature or other authenticator.

6. An electronic cash system substantially as specified herein.

7. An electronic system for supporting an abstracting or database search service in which customers make enquiries, the system finds potentially relevant references and the publisher or system operator then charges a certain amount to the customer for each reference or citation or hypertext link which the customer chooses to follow up.

8. An electronic system as described in claim 7 above in which the charge is paid using an electronic coin as described in claim 1 or in claim 2 or in claim 3 or in claim 4 or in claim 6.

ABSTRACT

An electronic cash system is specified with the following functionality. A bank issues a customer with a signed stick of digital coins. The customer when spending digital coins signs them to vouch for their authenticity. The merchant may rely on the customer's signature up to the value of her credit limit without having to check the coins online with the bank. The coins are hashed before signature in such a way that successive coins can be stripped off the stick and presented to the merchant without the need for further public key operations by either the customer or the merchant. Double spending is made difficult by using tamper-resistant smartcards, but if these are penetrated the bank's records can still trace double spenders. Pseudonyms are used to provide customer privacy. The system is suitable for hypertext based electronic publishing.