Customers of Australia's Advance Bank can avail themselves of its electronic cash software. The topmost screen shows transaction history—personal information stored on the user's computer and not accessible by the bank or by anyone else.

The bottom screen shows the user interface. The readout states the amount of Australian dollars stored in the form of this electronic cash on the user's computer. The buttons access [from left] bank account information, the log of transactions, payment controls, and help system.

The remaining screen shows the user withdrawing 25 Australian dollars from the bank onto his or her computer. The password unlocks the user's secret key, which is then used to authenticate the withdrawal.

‘Minting’ electronic cash

Electronic equivalents of traditional cash payment systems are being launched worldwide.
The interest in electronic replacements for traditional forms of payment has exploded in recent years. In addition to many field trials for value stored in chips on plastic cards (smartcards), many major software, telecommunications, and financial services organizations are working on their own electronic payment techniques. While most of these aim at enhancing credit cards, a few companies have gone further and developed electronic replacements of traditional cash payment. How far the extent to which the different systems succeed in preserving the unique benefits of traditional cash and exploiting the new medium's advantages varies substantially.

Traditional cash money is a bearer instrument. It allows instantaneous payment from person to person. Cash payments are not normally traceable by a third party and therefore offer privacy. On the other hand, transporting, protecting, and refreshing coins and bank notes make them very costly for banks to handle. Bank notes can be forged on sophisticated color copier machines, coins are too heavy to carry around in any large number, and both are easily lost or stolen. Because coins are virtually indistinguishable, and coins and bank notes can be passed from person to person many times without the involvement of a bank or other third party, cash is the preferred method of payment in criminal activities like extortion, money laundering, and bribery. Another inherent shortcoming has become particularly confining of late: the requirement for physical proximity of payer and payee.

The introduction of debit and credit cards has helped to overcome many of these problems. With these payment forms, the actual value resides at all times within the banks, and so the risks of large-scale theft and loss are reduced. A fundamental problem of these payment forms is that payments must be verified on-line by the bank, this makes transactions more expensive and can lead to unacceptable delays. Another problem is that the actual transfer of value is performed by banks, from source to destination account, and thus payments are inherently traceable. This traceability enables intrusive profiling of spending behavior and, by inference, all sorts of other characteristics of the user. Anti-fraud laws can offer only limited protection against criminal use of spending and inferred habits, since such use typically becomes visible (if at all) only once the damage has already been done.

Electronic cash can combine the benefits of traditional cash with those of payment by debit and credit card, while circumventing both their shortcomings. As with traditional cash, electronic cash should have high acceptability and be suitable for low-value payment from person to person. With the possible exception of on-line payment platforms such as the Internet, it is preferred that payments be verifiable off-line, without the banks' involvement, for reasons of cost-effectiveness and speed. To facilitate electronic cash payments over the phone and the Internet, physical proximity of payer and payee should not be necessary.

Methods of authentication

Of utmost importance for the security of any electronic cash system is that an attacker cannot inject extra money into the system. In effect, receiving devices must be able to distinguish authentic paying devices from attackers that try to pass for paying devices. To prove their authenticity, paying devices need to be equipped by the bank with secret keys. Correspondingly, receiving devices must be able to recognize whether they are communicating with a device holding a secret key installed by the bank.

A basic model

Each participant in an electronic cash system is represented by at least one hardware device, equipped with a chip having computing capabilities and nonvolatile memory. How to embody the devices depends on: the target payment platform (say, a PC, possibly in combination with a PC Card or a smartcard, may be used for Internet payments, while a hand-held device with display and keyboard is more appropriate for on-the-street payment); the offered functionality (smartcards may be most appropriate for purposes of cross-platform portability); and the required security levels. When the holder of an account at a bank that issues electronic cash wants to withdraw some of it, his computing device engages in an execution of a withdrawal protocol with a computing device of the bank, when connected to one of its terminals (by direct or infrared communication, dial-in, the Internet or other methods). At the end of the protocol execution, the computing device of the account holder holds an amount of electronic cash, represented in some suitable form, and his bank has charged the account holder by taking an equivalent amount of traditional money out of his bank account and moving it into a float pool; electronic cash is pre-paid by the account holder.

To transmit to a payee who accepts electronic cash issued by the payer's bank, the account holder connects his computing device to that of the payee (again, by direct or remote communication), and the two computing devices execute a payment protocol. As a result, the representation of the electronic cash amount held by the account holder's device is adjusted to reflect the new amount. In the case the payer's bank is not involved in the payment, the payee's computing device should correspondingly represent in some way the received payment amount, this is called an off-line payment. Otherwise, the payee must communicate with the bank during the payment; this is called an on-line payment.

Ultimately, a party holding electronic cash will need to sell it back to the issuing bank. Redemption is needed in most systems because electronic cash received in one payment cannot be reused in subsequent payments, or can be reused only up to a predetermined number of times. To this end, the party connects his computing device to a terminal of the issuing bank (or of his own bank, which can then settle with the issuing bank), either by direct or remote communication, and a deposit protocol is performed. As a result, the account of the party depositing the electronic cash is credited with an equivalent amount of money [Fig. 1].

Methods of authentication

Of utmost importance for the security of any electronic cash system is that an attacker cannot inject extra money into the system. In effect, receiving devices must be able to distinguish authentic paying devices from attackers that try to pass for paying devices. To prove their authenticity, paying devices need to be equipped by the bank with secret keys. Correspondingly, receiving devices must be able to recognize whether they are communicating with a device holding a secret key installed by the bank.

A secure authentication protocol should resist replay. In this kind of attack, a wire-tapped transcript of an execution of an authentication protocol is reused by an attacker in order to pass for a paying device. The paying device should therefore perform a computation (presented by the other device in the form of a challenge) that is feasible only when knowing the secret key, rather than transmitting the secret key itself. The outcome of the computation is called the response to the challenge, and should be verifiable by the receiving device, this enables it to conclude that the outcome must have been generated by a paying device that holds the secret key.

DAVID CHAUM & STEFAN BRANDS
DigiCash Inc.
One way for a receiving device to verify the response of a paying device is to have prior knowledge of the latter’s secret key. The receiving device then simply computes the response to its own challenge as well, and verifies it for equality with the response provided; this process is known as symmetric authentication. Receiving devices need to know (or be able to generate) the secret keys of all the paying devices they have to conduct transactions with, and for this reason they must be tamper-resistant as well. Hence they must be issued by or on behalf of the bank, which takes care of installing the keys of all paying and receiving devices.

Since it is dangerous to have all paying devices use the same secret key, yet cumbersome for receiving devices to store and maintain unique keys, the recommended approach is to use so-called “diversified” keys. In this method, each receiving device stores a master key, generated at random and installed by the bank. The secret key of a paying device is computed as a function of the master key and an ID number unique to the paying device. This function should be such that the master key cannot be computed from a device secret key. In case a paying device has its key extracted by an attacker, and so can be simulated, the compromised device can be traced and blacklisted as soon as the fraud is detected.

A weak point of symmetric authentication is the presence of the master key in all receiving devices, so that a successful attack on any one of them enables an attacker to simulate any paying device. This vulnerability vanishes when asymmetric instead of symmetric authentication is used. As before, to prove its authenticity to a receiving device, the paying device computes a response, known as a digital signature, which is based on its secret key and a challenge; but this time to verify the response, the receiving device applies a public key of the paying device, corresponding to its secret key. Knowledge of the public key does not enable the computation of the secret key, so that receiving devices need not contain secrets that are correlated to secret keys of paying devices.

Another advantage over symmetric authentication is that digital signatures cannot be forged. The receiving device can subsequently demonstrate to the bank (or to other devices) that the proof took place by showing the digital signature of the paying device. There is no need for receiving devices to be tamper-resistant.

**Representation of value**

Two fundamental ways exist for representing electronic cash in computing devices, whether paying or receiving devices. First is to indicate the amount of electronic cash by means of the value of a counter, maintained in a chip register. For example, 100 electronic dollars spendable in 1-cent increments would be represented by a counter value of 10,000. This representation is referred to as register-based cash. Since money can be forged when counters can be updated without bank authorization or bypassed, security relies critically on the tamper-resistance of the devices.

When an authentication method is combined with a register-based cash representation in paying devices, the paying device as well as the amount that is transferred must be authenticated. To this end the receiving device must decrement the register value to reflect the amount that is transferred, and it must have been programmed by the bank to do so only when its current value represents an amount exceeding the payable amount.

The other way to represent electronic cash value is purely informationally: public-key cryptographic tokens with an associated denomination and currency. Such tokens are called electronic coins. Electronic coins must be unforgeable and verifiable solely by using a public key of the bank, their value and currency are independent of tamper-resistance, so that they form a bearer instrument in the same manner as traditional cash does. The security of electronic coins relies on the secrecy of the signature secret key of the bank.

Electronic coins can be implemented with either of two methods, depending on whether payments are verified on- or off-line. In its simplest form, an electronic coin is a pair, <message, digital signature>, referred to as a coin of the “two-part form.” The coin digital signature is computed by the bank by applying its signature secret key to the coin message. On the assumption that suitable coins are available to pay a specified amount, the paying device decrypts the coins using a session key derived from its secret key, erases the coins from memory, and sends the encrypted coins to the receiving device. The receiving device decrypts to recover the coins, verifies them using the public key of the bank, and then stores them. The encryption prevents wiretappers from copying the coins while they are in transit. With this method, the receiving device must be tamper-resistant as well, because otherwise the received coins could be spent many times over without there being a way to determine the origin of the fraud.

The alternative is for the paying device to encrypt the coins for the bank, using an encryption public key of the bank, instead of for the receiving device. The receiving device must then pass the encrypted coins on to the bank, for decryption and verification (Fig. 2, top). The advantage of this approach is that the receiving device does not actually get to see the coins, and so cannot reuse them, but the downside is that off-line payment capability is lost.

For off-line payment, an electronic coin is best defined as a triple, <secret key, public key, certificate>, or a coin of the “three-part form.” The coin secret key belongs to the paying device, and may not be known to anyone else besides the device (and possibly the bank); the coin public key corresponds to the coin secret key, and the coin certificate is a digital signature of the bank on the coin public key. To spend a coin of the three-part form, the paying device computes a digital signature on a challenge message of the receiving device, using the coin secret key, and sends this to the receiving device together with the coin certificate and the coin public key. The receiving device cannot reuse the
received cash, as it has not been provided with the coin secret key, so cannot by itself compute a digital signature for another challenge. Instead, the receiving device must deposit the coin.

**Further security considerations**

Experience has shown that organized crime can command expertise comparable to that of national laboratores, and even individual computer criminals today have access to sophisticated tools. When secrets from paying or receiving devices can be extracted and abused, counterfeits are indistinguishable from electronic cash issued by the bank. When estimating the expected fraudulent profit that can be made, one also needs to take into consideration the economics of large-scale cracking, to crack a single smartcard, equipment and expertise running into hundreds of thousands of dollars may be needed, but this is largely a one-time investment. The damage that can be done ultimately depends on the measures incorporated in the system for preventing or discouraging unauthorized injection of electronic cash. At the very least, the bank should be able to detect and trace the injection of substantial amounts of forged electronic cash into the system. Once such a forgery has been detected, the bank should then be able to trace it to its source. (The ability to trace forgeries need not necessarily conflict with the inability to trace honest payments, as will be seen below.)

In order to hold a traced party responsible for all or part of the financial damage, it must be possible to isolate that party's liability, for example, so as to have firm ground for holding a traced party liable for the double-spending of coins, it must be ensured that the double-spending is unlikely to have been the work of a thief, unless the traced party ignored all manner of obligatory safeguards. Finally, it should be possible to quickly and efficiently distribute blacklists that enable payees to reject forged money (containment). A secure electronic cash system should provide for all of these.

To account holders, security aspects other than protection against forgery are of importance. The electronic cash held by the device of an account holder should not disappear in any other way than by being spent at the discretion of its legitimate holder. It should also not be possible for attackers to redirect a payment made by a device to any party other than the one intended by the legitimate holder of the device.

Account holders also need to be able to substantiate their position in case of erroneous or false accusations of fraudulent behavior. When parties with different interests authenticate their communications using symmetric authentication, the transcript of a communication cannot later on be used by one party to demonstrate that the communication with the other took place, since it could have computed the transcript by itself. True non-repudiation requires the use of secure digital signatures, since these can be computed only by the party associated with the public key needed for verification. When
crucial parts of the withdrawal, payment, and deposit requests are digitally signed, all parties can substantiate their position.

Achieving privacy

Privacy is by many deemed likely to decide the ultimate success of electronic cash with consumers. Two aspects of privacy in electronic payment systems can be discerned. The first, confidentiality of transaction content, refers to the ability of account holders to prevent wire-tappers from learning transaction details, such as the amount involved and the good or service purchased. Payment confidentiality can be achieved by encrypting all sensitive data sent during a protocol execution.

A more fundamental form of privacy is untraceability. If proper technical measures are not in place, electronic cash payments automatically leave detailed tracing information in the hands of a central party, typically the bank. Straightforward approaches to privacy (anonymous accounts, aggregated transaction logs that hide unique transaction identifiers, and anonymously issued paying devices) downgrade security for the bank by hindering the ability to trace counterfeiters, and at best offer a weak form of untraceability ("pseudo-anonymity"). Namely, payments by the same device are inherently linkable, and user-identification in a protocol one transaction (as when reloading from account) makes all payments of that user traceable.

Fortunately, strong cryptographic techniques exist that enable the bank to detect any unauthorized injection of electronic cash and moreover to trace it to the party that is responsible for the fraud, while at the same time offering strong privacy of payments to honest account holders.

The basic cryptographic paradigm is called blinding. Invented by author David Chaum, blinding enables a receiver to cooperate with a signer in an execution of a protocol to enable to obtain from the signer a digital signature on a message, in such a manner that both message and signature remain completely hidden from the signer. By representing coins in the two-part form, this technique enables an account holder to withdraw coins that cannot possibly be linked to the holder at the time of payment; this holds even if the bank were to have infinite computing power (Fig. 2, bottom).

On the other hand, the bank can always recognize its own coins, by verifying its own coin digital signatures, and can prevent double-spending by keeping track of a list of all deposited coins and checking for double-spending at the moment of payment, in case of a double-spending attempt, the bank can then simply send a message to the receiving device, telling it not to accept the payment. Note that paying devices need not be tamper-resistant, so that this method can be used to make on-line payments over the Internet using merely a personal computer and a software package.

A defect in the above blinding paradigm is that the bank can never trace double-spending attempts, since all payments are unconditionally untraceable. Consequently, while suitable for on-line payments, the basic blinding paradigm is inappropriate for off-line payments.

An important extension of the basic blinding paradigm exists that enables off-line payment verification while maintaining security against double-spending. This extension is known as the one-show blinding paradigm, also invented by Chaum.

The one-show blinding paradigm requires the design of a withdrawal and a payment protocol that act securely in parallel. Two practical cryptographic techniques known for this purpose have been developed by author Stefan Brands.

When (one-show) blinding is performed by tamper-resistant devices issued by or on behalf of the bank, users have no guarantee that the blinding is performed properly, or that no additional or subliminal information is leaked by their devices during payment. To overcome this final problem, Chaum has proposed the so-called observer paradigm, whereby the functionality of the paying device is separated into two parts, each provided by a separate device. One device (referred to as the observer) is tamper-resistant and ensures prior restraint of double-spending, while the other is a user-controlled computer that controls all the blinding operations. The observer is interfaced to the user-controlled device in such a manner that all information flowing from the observer to the outside world, and vice versa, necessarily passes through the user-controlled computer, natural hardware embodiments are a smartcard in combination with a PC, for use on the Internet, or a smart-card in combination with a handheld device for on-the-street payment. The software for the user-controlled device, and the device itself, may be purchased from any source (and could even be manufactured or modified by the user himself), so that at least in principle each user can verify for himself that the device is properly performing its tasks.

This hardware configuration enables the user-controlled device to stop any added identity-related information from being revealed by the tamper-resistant device when making a payment. Also, given proper cryptographic design of the withdrawal and payment protocols, the user-controlled computer should prevent any subliminal channels between the tamper-resistant device and the outside world. Practical cryptographic techniques for this purpose have been invented by Brands, based on his techniques for realizing the one-show blinding paradigm.

Electronic cash today

True electronic cash (bearer instrument with privacy) was first demonstrated publicly at the first World Wide Web conference (May 25, 1994) between Geneva and Amsterdam over the Web. Subsequently, a trial began for which over 70,000 people signed up to receive 100 Cyberbucks (a trademark) and in which over 70 merchants participated. U.S. dollar-denominated electronic cash was then launched by Mark Twain Bank, Saint Louis, Mo. Since then, banks on three continents have licensed the technology and are offering their own national currency over the Internet. The technology enables on-line payments and is based on the basic blinding paradigm.

The first electronic wallet with observer has been built for the European Commission-sponsored project Conditional Access for Europe (CAFE), which is running a trial in the Commission headquarters in Brussels. The project involved 13 partners from several European countries, including leading scientific research centers and industrial partners. This system enables on-line payments, based on the one-show blinding paradigm.

About the authors

David Chaum is the founder and chief technology officer of DigiCash Inc., Amsterdam, and is a member of its board. He earned his Ph.D. at the University of California at Berkeley and was on the faculty at New York University and the University of California. Until 1992, he headed the cryptography group at the Center for Mathematics and Computer Science (CWI) in Amsterdam. Holder of over a dozen basic patents in cryptography, he founded the International Association for Cryptologic Research, and is on the editorial board of its journal.

Stefan Brands did his Ph.D. research at CWI and after working for his own consultancy company, joined DigiCash in 1997 with the title of Distinguished Scientist. He holds patents on cryptographic techniques for all kinds of privacy-protecting electronic tokens. His techniques for untraceable off-line electronic cash form the basis of the CAFE system, and are being implemented by DigiCash.