An Electronic Wallet for Digital Money

R. Hirschfeld

1. Background

The last quarter century has witnessed explosive growth in the technology for automated handling of information. This has resulted in many conveniences, but has also introduced new dangers, such as increasing opportunities for unauthorized access to sensitive or personal data, and for tampering with such data. With the advent of electronic commerce has come the need for electronic money, i.e., a digital representation of cash. Electronic money introduces additional associated security problems, such as forgery of money, respending the same money, and invasion of privacy of people's spending habits. The field of cryptography has addressed the problems of authentication and data security in general and of the security of electronic money in particular.

CWI has been conducting research in cryptography for over ten years, and is an internationally recognized leader in the areas of digital signatures and public-key cryptographic protocols. Early emphasis was placed on the security of ordinary users of automated systems, and particularly on the protection of individual privacy. CWI coordinated the European RACE project RIPE, which developed and evaluated a collection of cryptographic primitives. The company DigiCash, founded by D. Chaum and specializing in systems for consumer payments, has its roots in the CWI crypto group. In recent years, research has focused both on proofs of security of crypto-

Partner	Description	Country
CWI	National research institute for mathematics and computer science	The Netherlands
CardWare	consultant for the financial industry on electronic payment technologies	United Kingdom
IFS	social research institute	Germany
Gemplus	smart card manufacturer	France
DigiCash	software and hardware designer	The Netherlands
Ingenico	point-of-sale terminal manufacturer	France
Siemens	industrial electronics manufacturer	Germany
SEPT	national telecommunications and postal research institute	France
Katholieke Universiteit Leuven	university	Belgium
Royal PTT Nederland, PTT Research	national telecommunications	The Netherlands
SINTEF DELAB	university research institute	Norway
Aarhus University, Mathematics Institute	university research institute	Denmark
University of Hildesheim, Informatics Institute	university research institute	Germany

Figure 1. The CAFE Consortium.

graphic protocols and on techniques for achieving secure protocols that can be efficiently implemented and practically realized.

The project CAFE, which is carried out by a consortium of thirteen European institutions (see figure 1) and is funded by the European Commission's ESPRIT programme, has applied modern cryptographic techniques to produce a highly secure but also open and flexible system for consumer payments using electronic money. As a leader in theoretical research on electronic money and as coordinator of the CAFE project, CWI has played a major role in the development of the protocols used by the system.

2. ELECTRONIC PAYMENTS

2.1. Introduction

Europe leads the world in the introduction of smart cards, wallet-size cards with embedded computer chips. French bankcards and the telephone cards of several countries are chip-based. These early chip cards do not really

merit the name 'smart'—they contain memory chips and work in essentially the same way as magnetic stripe cards except that they are more difficult for a counterfeiter to overwrite. More recent systems incorporate microprocessor chips, so that the card can participate actively in transaction protocols. This allows the implementation of digital signature techniques, upon which electronic money is based.

An application such as a telephone card, in which the card issuer is the same as the service provider (so no clearing is necessary), and all points of payment are online, does not really require a sophisticated microprocessor on the card. But the availability of smarter cards has led to the introduction of prepaid electronic purse systems, in which value is stored on a card and can be used for payment at a variety of shops and other service providers. Because these transactions can be completed offline, they are suitable for small value payments for which cash is traditionally used; credit and debit cards require costly online authorization, which is infeasible for low-value payments. Electronic purse systems are undergoing trials in several European countries; the Dutch banks have recently introduced one in The Netherlands based on a system developed and currently under trial in Belgium.

2.2. Security

The security of electronic purse systems is based on digital signatures, a cryptographic method of certifying the origin of a digital message. Messages (which can represent banknotes or card balances) are signed by an algorithm that uses a secret key provided by the signer, and authentication is performed by another algorithm that also uses a key. In most of the electronic purse systems underway, the signing key and the authenticating key are the same. Because the authenticating key present at the point of sale could also be used to sign messages (i.e., create money), it is protected against discovery and possible misuse by storing it in a tamper-resistant hardware module. This reduces the flexibility of the system; it is difficult to combine multiple issuers of electronic money into the same system, and security modules cannot be given out indiscriminately, but only to service providers who can be trusted not to try to compromise them.

An alternative to symmetric systems that use the same key to create and to verify a signature is public-key digital signatures. In a public-key system, the signing and authenticating keys are different, and no knowledge of the signing key can be obtained from the authenticating key. Such an asymmetric system is ideal for an open and interoperable electronic purse environment, because the signing key need be known only to the issuer, and the authentication key can be made public and need not be protected in any way.

Despite their advantages, public-key signatures are not yet widely used in

One of the fundamental notions of modern cryptography is that of a one-way function—a function that is efficient to compute but impractical to invert. For example, it is easy to multiply large integers, but is thought to be difficult to factor a large integer product into its constituent prime factors. Similarly, modular exponentiation is relatively efficient, but its inverse, the discrete logarithm, remains intractable. Although no proof of the difficulty of either of these number-theoretic problems is known, they have thus far resisted all attempts at efficient solutions. Many cryptographic protocols are based upon assumptions of their intractability.

A related notion is that of a one-way trapdoor function, which is normally difficult to invert, but which becomes easy to invert if some additional information is known (this is the trap door). This additional information can form the secret key (or part of the key) in a cryptosystem. An example is the well-known RSA cryptosystem (named after its inventors: R.L. Rivest, A. Shamir, and L. Adleman, see figure 2), which is based on the observation that if $n = pq$, the product of two large primes, then computing powers mod n is easy but computing roots mod n seems difficult unless the factors p and q are known, in which case it is easy. Cryptosystems were originally developed for encryption rather than signing of messages. In general, a public-key cryptosystem consists of a public encryption algorithm E and a secret decryption algorithm D with the property that for a message m, $D(E(m)) = m$. Each person has their own pair of encryption and decryption algorithms. To send a secret message, the sender encrypts it using the recipient's E (which is publicly available), and then only the recipient can decrypt it, using his own secret D.

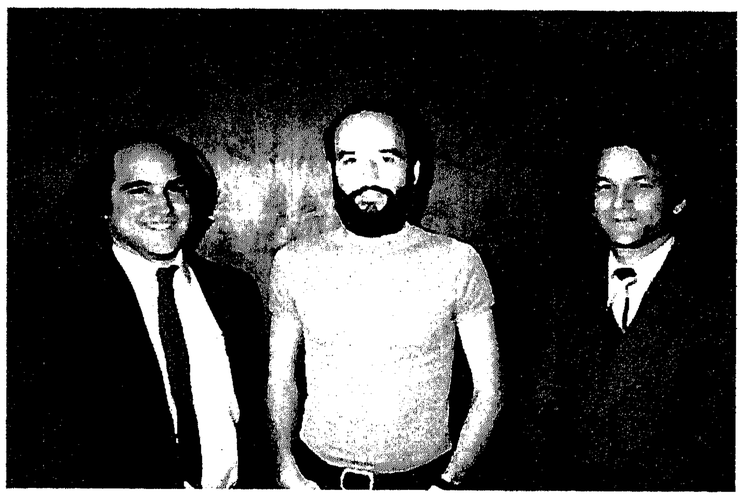

Figure 2. The inventors of the RSA cryptographic method. From left to right: R.L. Rivest, A. Shamir, L. Adleman. Photo courtesy RSA Data Security Inc.

Digital signatures turn this situation around. The secret algorithm D is used to sign messages, and the public algorithm E is used to authenticate them. The property required is that $E(D(m)) = m$. To sign a message, the signer applies her own secret algorithm D, and then anybody can verify it using her publicly available E. The RSA cryptosystem can be used for both encryption and for digital signatures because it has the property that $D(E(m)) = m = E(D(m))$, since encryption and decryption are the inverse operations of raising to a power and extracting a root.

Commercially, the most widely-used cryptosystem is the Data Encryption Standard (DES). This is a symmetric algorithm and is unsuited for public-key use, but has the advantage that it does not rely on time-consuming modular arithmetic. As hardware support for these operations becomes more widely available and inexpensive, however, this is becoming less of a consideration.

Figure 3. The CAFE infrared wallet (left) and card (right). Courtesy CAFE Project.

commercial systems. This is because they require more elaborate computation, and until recently performing this computation on a smart card chip has been too slow or too expensive. But with the development of specialized cryptographic smart card chips, which implement complex operations needed for public-key signatures in hardware, public-key electronic purses are now feasible. The CAFE project has developed a public-key system for electronic purses, and, more generally, for electronic wallets, which combine an electronic purse with other applications, such as digital passports, driver's licenses, house keys, etc.

In addition to a smart card, CAFE has developed a hand-held wallet that communicates with payment terminal via infrared (much like a television remote control (see figure 3), except bidirectional) and allows consumers to confirm payments with their own device and to complete the payment without the wallet ever leaving their hands.

3. CWI's role

CWI was the coordinating partner of the CAFE project, and as such was responsible for the overall management of the project. In addition, CWI played a major role in the design of the protocols used in the system, drawing

on its many years of active research experience in digital signatures and electronic money.

In collaboration with the other protocol partners, CWI worked on all aspects of the cryptographic protocols developed for CAFE, including not only the fundamental protocols for secure transactions (withdrawal, payment, deposit, etc.), but also currency exchange, tolerance of loss and faults, key management, and other related items.

CWI has also applied its special expertise on privacy protection and user-moderated transactions in the design of the wallet protocols and the provision of untraceability as a system option.

4. FUTURE PLANS

In 1995, the CAFE system began a trial on the premises of the European Commission in Brussels. If successful, this will expand to include other EU institutions in other cities and perhaps the surrounding communities. Although the currency exchange mechanism developed by the project is very general, the trial will focus on the introduction of an electronic ECU. Users will load their cards with any combination of their home currency and ECU, and (in the trial) they will be able to spend their home currency only in their home country, but the electronic ECU at a CAFE terminal in any country. The results anticipated include an evaluation of the technology, surveys of user opinions, and a cost assessment and business case analysis of the system.

After the end of the CAFE project, the trial will be expanded as part of a separate project to the premises of some of the sponsoring financial institutions, in different countries. This will provide a real test of the international capabilities of the system. A follow-up project with large-scale pilots of both the electronic purse and other applications is in the proposal stage.

CWI is also participating in a new European project called SEMPER, which is developing secure mechanisms for payments and other marketplace activities on computer networks, both the Internet and advanced high-speed networks. This project will include trials focused on multimedia applications.

By continued involvement in development projects, the CWI crypto group enriches its research scope. At the same time, research continues into the theoretical underpinnings of these applied systems, which is really the group's fundamental core.