ESSAYS

HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH*

LAURIE LAW
SUSAN SABETT
JERRY SOLINAS

TABLE OF CONTENTS

Introduction 1132
I. What Is Electronic Cash? 1133
A. Electronic Payment 1133
B. Security of Electronic Payments 1134
C. Electronic Cash 1135
D. Counterfeiting 1136
II. A Cryptographic Description 1137
A. Public-Key Cryptographic Tools 1137
B. A Simplified Electronic Cash Protocol 1139
C. Untraceable Electronic Payments 1140
D. A Basic Electronic Cash Protocol 1141
III. Proposed Off-line Implementations 1143
A. Including Identifying Information 1143
B. Authentication and Signature Techniques 1144
C. Summary of Proposed Implementations 1148
IV. Optional Features of Off-line Cash 1149
A. Transferability 1149
B. Divisibility 1151

---

* This research Essay was prepared by NSA employees in furtherance of the study of cryptography. The contents of the report do not necessarily represent the position or policies of the U.S. Government, the Department of Defense, or the National Security Agency.

The authors are mathematical cryptographers at the National Security Agency's Office of Information Security Research and Technology.

V. Security Issues 1154
A. Multiple Spending Prevention 1154
B. Wallet Observers 1155
C. Security Failures 1157
1. Types of failures 1157
2. Consequences of a failure 1158
D. Restoring Traceability 1158
Conclusion 1161

INTRODUCTION

With the onset of the Information Age, our nation is becoming increasingly dependent on network communications. Computer-based technology is impacting significantly our ability to access, store, and distribute information. Among the most important uses of this technology is *electronic commerce*: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment systems. The need for security is highlighted by the rise of the Internet, which promises to be a leading medium for future electronic commerce.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards, and stored value cards ("SVC"). The usual security features for such systems are privacy (protection from eavesdropping), authenticity (identification and message integrity), and nonrepudiation (prevention of later denying having performed a transaction).

This Essay focuses on electronic cash. As the name implies, electronic cash is an attempt to construct an electronic payment system modelled after our paper money system. Paper money has such features as: portability (easily carried); recognizability (as legal tender), and thus readily acceptable; transferability (without involvement of the financial network); untraceability (no record of where money is spent); anonymity (no record of who spent the money); and the ability to make "change." The designers of electronic cash focused on preserving the features of untraceability and anonymity. Thus, electronic cash is defined to be an electronic payment system that provides, in addition to the above security features, the properties of user anonymity and payment untraceability.

Electronic cash schemes that use digital signatures[1] to achieve

1. Editors' Note: For a thoughtful discussion of digital signatures, see Randy V. Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed First*

security and anonymity are worrisome from a law enforcement perspective because of the anonymity feature. In particular, the dangers of money laundering and counterfeiting with electronic cash are potentially far more serious than with paper money. The widespread use of electronic cash would increase the vulnerability of the national financial system to "information warfare" attacks.[2] This Essay discusses measures to manage the risks associated with electronic cash; these safeguards, however, will have the effect of limiting user anonymity.

Part I defines the basic concepts surrounding electronic payment systems and electronic cash. Part II provides the reader with a high-level cryptographic description of electronic cash protocols in terms of basic authentication mechanisms. Part III describes specific existing implementations. The optional features of transferability and divisibility for off-line electronic cash are presented in Part IV. Part V discusses the security issues associated with electronic cash. Finally, this Essay concludes with a summary of the risks that are magnified by the presence of anonymity in electronic payment systems.

I. WHAT IS ELECTRONIC CASH?

The term "electronic cash" often is applied to any electronic payment scheme that superficially resembles money. In fact, however, electronic cash is a specific kind of electronic payment scheme, defined by certain cryptographic properties.

A. Electronic Payment

The term electronic commerce refers to any financial transaction involving the electronic transmission of information. The packets of information being transmitted commonly are called electronic tokens. One should not confuse the token, which is a sequence of bits, with the physical media used to store and transmit the information.

The storage medium generally is referred to as a "card" because it usually takes the form of a wallet-sized card made of plastic or cardboard. Two obvious examples are credit cards and ATM cards. However, the "card" also could be a computer memory.

An *electronic payment* is a particular kind of electronic commerce. An electronic payment protocol involves a series of transactions, resulting in a payment being made using a token issued by a third

---

Step Toward Signing on the Digital Dotted Line, 46 AM. U. L. REV. 511 (1996).

2. *See* CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 49 (Kenneth W. Dam & Herbert S. Lin eds., 1996).

party. The most common example is the electronic approval process used to complete a credit card transaction; neither payer nor payee issues the token in an electronic payment.[3]

The electronic payment scenario assumes three kinds of players:[4]

- a payer or consumer ("Alice"),
- a payee, such as a merchant ("Bob"), and
- a financial network with whom both Alice and Bob have accounts (the "Bank").

B. Security of Electronic Payments

With the rise of telecommunications and the Internet, it is increasingly common that electronic commerce takes place using a transmission medium not under the control of the financial system. It therefore is necessary to take steps to ensure the security of the messages sent along such a medium.

The necessary security properties are:

- *Privacy*, or protection against eavesdropping, which is important for transactions involving information such as credit card numbers sent on the Internet.
- *User identification*, or protection against impersonation.
- *Message integrity*, or protection against tampering or substitution, which ensures that the recipient's copy of the message is the same as what the sender sent.
- *Nonrepudiation*, or protection against later denial of a transaction.

The last three properties collectively are referred to as authenticity.

These security features can be achieved in several ways. One technique that is gaining widespread use is the establishment of an authentication infrastructure. In such a setup, privacy is attained by encrypting each message using a private key known only to the sender and the recipient. Authenticity is attained via key management, that is, the system of generating, distributing, and storing the users' keys.

Key management is carried out using a certification authority or a trusted agent who is responsible for confirming a user's identity. Certification is conducted for each user (including banks) who is issued a digital identity certificate. The certificate can be used whenever the user wishes to identify himself or herself to another user. Such certificates make it possible to set up a private key between users in a secure and authenticated way. The private key

---

3. In this sense, electronic payment differs from such systems as prepaid phone cards and subway fare cards, in which the token is issued by the payee.

4. Part IV.A generalizes this scenario in a discussion of transferability.

then is used to encrypt subsequent messages. This technique can be implemented to provide any or all of the above security features. Without a trusted certification authority and a secure authentication infrastructure, those security features cannot be achieved, and electronic commerce becomes impossible over an untrusted transmission medium.

The following discussion assumes that some authentication infrastructure is in place providing the four security features.

C. Electronic Cash

This Essay has defined privacy as protection against eavesdropping on one's communications. One privacy advocate, however, defines the term far more expansively.[5] To David Chaum, genuine "privacy" implies that one's history of purchases is not available for inspection by banks and credit card companies, and by extension, the government. To achieve this, one needs anonymity in addition to privacy. In particular, one needs (1) payer anonymity during payment; and (2) payment untraceability so that the bank cannot tell whose money is used in a particular payment.

These features are not available with credit cards. Indeed, the only conventional payment system offering these features is cash. Thus Chaum and others have introduced electronic cash (or digital cash) as an electronic payment system that offers both features.

The sequence of events in an electronic cash payment is as follows:

(1) withdrawal, in which Alice transfers some of her wealth from her Bank account to her card;
(2) payment, in which Alice transfers money from her card to Bob's; and
(3) deposit, in which Bob transfers the money he has received to his Bank account.

These procedures can be implemented in either of two ways:

- On-line payment means that Bob calls the Bank and verifies the validity of Alice's token[6] before accepting her payment and delivering his merchandise. This resembles many of today's credit card transactions.
- Off-line payment means that Bob submits Alice's electronic coin for verification and deposit sometime after the payment transaction is

5. *See generally* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96; David Chaum, *Security Without Identification: Transactions to Make Big Brother Obsolete*, 28 ASS'N COMPUTING MACHINERY 1030 (1985).

6. In the context of electronic cash, the token usually is called an electronic coin.

completed. This method resembles making small purchases today by personal check.

Note that with an on-line system, the payment and deposit are not separate steps.

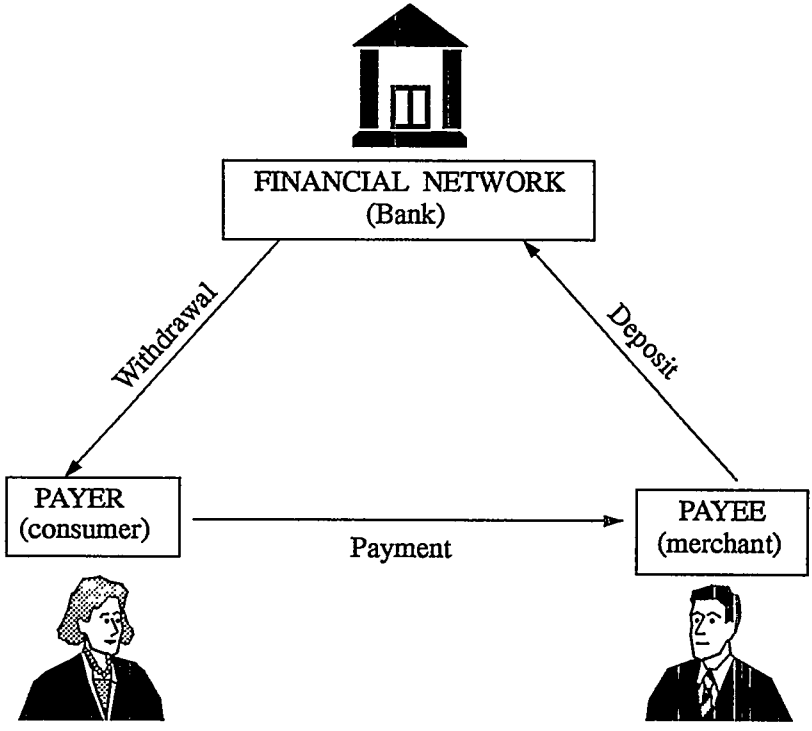

Figure 1. The three types of transactions in a basic electronic cash model.

D. Counterfeiting

As in any payment system, there is a potential for criminal abuse, with the intention either of cheating the financial system or of using the payment mechanism to facilitate some other crime. Part V will discuss criminal abuse further, but the issue of counterfeiting must be considered here, as the payment protocols contain built-in protections against it.

Two abuses of an electronic cash system are analogous to counterfeiting of physical cash:

- Token forgery, or creating a valid-looking coin without making a corresponding Bank withdrawal.
- Multiple spending, or using the same token over again. Because an electronic coin consists of digital information, it appears as valid after it has been spent as it did before.

Counterfeiting can be addressed by prevention or by detection after the fact in a way that identifies the culprit. Prevention clearly is preferable.

Although it is tempting to imagine electronic cash systems in which the transmission and storage media are secure, there certainly will be applications where this is not the case. An obvious example is the Internet, the users of which are notoriously vulnerable to viruses and eavesdropping. Thus, techniques other than physical security must be established to address counterfeiting.

- To protect against token forgery, one relies on the usual authenticity functions of user identification and message integrity. Note that the "user" being identified from the coin is the issuing Bank, not the anonymous spender.
- To protect against multiple spending, the Bank maintains a database of spent electronic coins. Coins already in the database are to be rejected for deposit. If the payments are on-line, this will prevent multiple spending. If the payments are off-line, detection of multiple spending is the only available precaution. To protect the payee, then, it is necessary to identify the payer. This means that the anonymity mechanism in the case of multiple spending must be disabled.

The features of authenticity, anonymity, and multiple-spender exposure are achieved most conveniently using public-key cryptography. Parts II and III will discuss how these features are accomplished using public key cryptography.

II. A CRYPTOGRAPHIC DESCRIPTION

Part II provides a high-level description of electronic cash protocols in terms of basic authentication mechanisms.

A. Public-Key Cryptographic Tools

Part A begins by discussing the basic public-key cryptographic techniques upon which the electronic cash implementations are based.

One-Way Functions. A one-way function is a correspondence between two sets that can be computed efficiently in one direction but not the other. In other words, the function ϕ is one-way if, given s in the domain of ϕ, it is easy to compute $t = \phi(s)$, but given only t, it is hard

to find *s*. (The elements are typically numbers, but also could be points on an elliptic curve, for example.[7])

Key Pairs. If ϕ is a one-way function, then a key pair is a pair *s*, *t* related in some way via ϕ. *s* is the secret key and *t* is the public key. As the names imply, each user keeps his secret key to himself and makes his public key available to all. The secret key remains secret even when the public key is known, because the one-way property of ϕ insures that *s* cannot be computed from *t*.

All public-key protocols use key pairs. For this reason, public-key cryptography often is called asymmetric cryptography, as opposed to conventional cryptography, which often is called symmetric cryptography, as one can both encrypt and decrypt with the private key but do neither without it.

Signature and Identification. In a public key system, a user identifies herself by proving that she knows her secret key without revealing it. She does this by performing some operation using the secret key that anyone can check or undo using the public key. This process is called identification. If one uses a message as well as one's secret key, one is performing a digital signature on the message. The digital signature plays the same role as a handwritten signature: identifying the author of the message in a way that cannot be repudiated and confirming the integrity of the message.

Secure Hashing. A hash function is a map from all possible strings of bits of any length to a bit string of fixed length. Such functions often are required to be collision-free: that is, it must be computationally difficult to find two inputs that hash to the same value. If a hash function is both one-way and collision-free, it is said to be a secure hash.

The most common use of secure hash functions is in digital signatures. Messages might come in any size, but a given public-key algorithm requires working in a set of fixed size. Thus one hashes the message and signs the secure hash rather than the message itself. The hash is required to be one-way to prevent signature forgery, that is, constructing a valid-looking signature of a message without using the secret key.[8] The hash must be collision-free to prevent repudiation, or denial of having signed one message by producing another message with the same hash.

---

7. *See* ALFRED J. MENEZES, ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS 13 (1993).

8. Note that token forgery is not the same thing as signature forgery. Forging the Bank's digital signature without knowing its secret key is one way of committing token forgery, but not the only way. A bank employee or hacker, for instance, could "borrow" the Bank's secret key and validly sign a token. This key compromise scenario is discussed in Part V.C.

B. A Simplified Electronic Cash Protocol

The example below is a simplified electronic cash system protocol, without the anonymity features.

PROTOCOL 1: On-line electronic payment.
Withdrawal:
Alice sends withdrawal request to Bank.
Bank prepares electronic coin and digitally signs it.
Bank sends coin to Alice and debits her account.
Payment/Deposit:
Alice gives Bob coin.
Bob contacts Bank[9] and sends coin.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank consults its withdrawal records to confirm Alice's withdrawal. (optional)
Bank enters coin in spent-coin database.
Bank credits Bob's account and informs Bob.
Bob gives Alice merchandise.

PROTOCOL 2: Off-line electronic payment.
Withdrawal:
Alice sends withdrawal request to Bank.
Bank prepares electronic coin and digitally signs it.
Bank sends coin to Alice and debits her account.
Payment:
Alice gives Bob coin.
Bob verifies Bank's digital signature. (optional)
Bob gives Alice merchandise.
Deposit:
Bob sends coin to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank consults its withdrawal records to confirm Alice's withdrawal. (optional)
Bank enters coin in spent-coin database.

---

9. One should keep in mind that the term "Bank" refers to the financial system that issues and clears the coins. For example, the Bank might be a credit card company, or the overall banking system. In the latter case, Alice and Bob might have separate banks. If that is so, then the "deposit" procedure is slightly more complicated: Bob's bank contacts Alice's bank, "cashes in" the coin, and puts the money in Bob's account.

Bank credits Bob's account.

The above protocols use digital signatures to achieve authenticity. Although the authenticity features could have been achieved in other ways, digital signatures must be used to allow for the anonymity mechanisms to be added in the following discussion.

C. Untraceable Electronic Payments

In Part C, the above protocols are modified to include payment untraceability. To achieve untraceability, it is necessary that the Bank not be able to link a specific withdrawal with a specific deposit.[10] This is accomplished using a special kind of digital signature called a blind signature.

Examples of blind signatures are provided in Part III.B, but a high-level description is given here. In the withdrawal step, the user changes the message to be signed using a random quantity. This step is called "blinding" the coin, and the random quantity is called the blinding factor. The Bank signs this random-looking text, and the user removes the blinding factor. The user now has a legitimate electronic coin signed by the Bank. The Bank will see this coin when it is submitted for deposit, but will not know who withdrew it because the random blinding factors are unknown to the Bank. Obviously, it no longer will be possible to check the withdrawal records, which was an optional step in the first two protocols.

Note that the Bank does not know what it is signing in the withdrawal step. This introduces the possibility that the Bank might be signing something other than what it is intending to sign. To prevent this, a Bank's digital signature by a given secret key is valid only as authorizing a withdrawal of a fixed amount. For example, the Bank could have one key for a $10 withdrawal, another for a $50 withdrawal, and so on.[11]

PROTOCOL 3: Untraceable On-line electronic payment.
Withdrawal:

Alice creates electronic coin and blinds it.

Alice sends blinded coin to Bank with withdrawal request.

---

10. To achieve either anonymity feature, it is of course necessary that the pool of electronic coins be a large one.

11. One also could broaden the concept of "blind signature" to include interactive protocols in which both parties contribute random elements to the message to be signed. An example of this is the "randomized blind signature" occurring in the Ferguson scheme discussed in Part III.C.

Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.
Payment/Deposit:
Alice gives Bob coin.
Bob contacts Bank and sends coin.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin in spent-coin database.
Bank credits Bob's account and informs Bob.
Bob gives Alice merchandise.

PROTOCOL 4: Untraceable Off-line electronic payment.
Withdrawal:
Alice creates electronic coin and blinds it.
Alice sends blinded coin to Bank with withdrawal request.
Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.
Payment:
Alice gives Bob coin.
Bob verifies Bank's digital signature. (optional)
Bob gives Alice merchandise.
Deposit:
Bob sends coin to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin in spent-coin database.
Bank credits Bob's account.

D. A Basic Electronic Cash Protocol

Part D takes the final step in modifying the protocols to achieve payment anonymity. The ideal situation (from the point of view of privacy advocates) is that neither payer nor payee should know the identity of the other. This makes remote transactions using electronic cash completely anonymous: no one knows where Alice spends her money or who pays her.

Unfortunately, however, this level of anonymity is not possible: there is no way in such a scenario for the consumer to obtain a signed receipt. Thus, payer anonymity is all that can be achieved.

If the payment is to be on-line, Protocol 3, can be used (implemented, of course, to allow for payer anonymity). In the off-line case,

however, a new problem arises. If a merchant tries to deposit a previously spent coin, he will be turned down by the Bank, but neither will know who the multiple spender was, as she was anonymous. Thus, it is necessary for the Bank to be able to identify a multiple spender.

The solution is for the payment step to require the payer to have, in addition to her electronic coin, some sort of identifying information that she is to share with the payee. This information is split in such a way that any one piece reveals nothing about Alice's identity, but any two pieces are sufficient to identify her fully.

This information is created during the withdrawal step. The withdrawal protocol includes a step in which the Bank verifies that the information is present and corresponds to Alice and to the particular coin being created. To preserve payer anonymity, the Bank will not actually see the information, but only verify that it is there. Alice carries the information along with the coin until she spends it.

At the payment step, Alice must reveal one piece of this information to Bob. Thus only Alice can spend the coin, as only she knows the information. This revealing is done using a challenge-response protocol. In such a protocol, Bob sends Alice a random "challenge" quantity and, in response, Alice returns a piece of identifying information. The challenge quantity determines which piece she sends. At the deposit step, the revealed piece is sent to the Bank along with the coin. If all steps proceed properly, the identifying information never will point to Alice. Should she spend the coin twice, however, the Bank eventually will obtain two copies of the same coin, each with a piece of identifying information. Because of the randomness in the challenge-response protocol, these two pieces will be different. Thus the Bank will be able to identify her as the multiple spender. Because only Alice can dispense identifying information, it is clear that her coin was not copied and re-spent by someone else.

PROTOCOL 5: Off-line cash.
Withdrawal:
Alice creates electronic coin, including identifying information.
Alice blinds coin.
Alice sends blinded coin to Bank with withdrawal request.
Bank verifies that identifying information is present.
Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.

Payment:
Alice gives Bob coin.
Bob verifies Bank's digital signature.
Bob sends Alice challenge.
Alice sends Bob response (revealing one piece of identifying information).
Bob verifies response.
Bob gives Alice merchandise.
Deposit:
Bob sends coin, challenge, and response to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin, challenge, and response in spent-coin database.
Bank credits Bob's account.

Note that, in this protocol, Bob must verify the Bank's signature before giving Alice the merchandise. In this way, Bob can be sure that either he will be paid or he will learn Alice's identity as a multiple spender.

III. PROPOSED OFF-LINE IMPLEMENTATIONS

Having described electronic cash in a high-level format, this Essay now will describe the specific implementations that have been proposed. These implementations will be given for the off-line case only. The corresponding on-line protocols are just simplified versions of those provided below.

A. Including Identifying Information

Part A explains more specifically how to include (and access when necessary) the identifying information meant to catch multiple spenders. There are two ways to accomplish this task: the cut-and-choose method and zero-knowledge proofs.

Cut and Choose. When Alice wishes to make a withdrawal, she first constructs and blinds a message consisting of K pairs of numbers, where K is large enough that an event with probability 2^{-K} never will happen in practice. These numbers have the property of enabling one to identify Alice given both pieces of a pair; unmatched pieces remain useless. Alice then obtains signature of this blinded message from the Bank. This is done in such a way that the Bank can check that the K pairs of numbers are present and that they have the required properties despite the blinding.

When Alice spends her coins with Bob, his challenge to her is a string of K random bits. For each bit, Alice sends the appropriate

piece of the corresponding pair. For example, if the bit string starts *0110* . . ., Alice sends the first piece of the first pair, the second piece of the second pair, the second piece of the third pair, the first piece of the fourth pair, etc. When Bob deposits the coin at the Bank, he sends on these K pieces.

If Alice re-spends her coin, she is challenged a second time. Because each challenge is a random bit string, the new challenge is bound to disagree with the old one in at least one bit. Thus Alice will have to reveal the other piece of the corresponding pair. When the Bank receives the coin a second time, it takes the two pieces and combines them to reveal Alice's identity.

Although conceptually simple, this scheme is not very efficient, as each coin must be accompanied by $2K$ large numbers.

Zero-Knowledge Proofs. The term zero-knowledge proof refers to any protocol in public-key cryptography that proves knowledge of some quantity without revealing it or making it any easier to find. In this case, Alice creates a key pair such that the secret key points to her identity. This is done in such a way that the Bank can check via the public key that the secret key in fact reveals her identity, despite the blinding. In the payment protocol, Alice gives Bob the public key as part of the electronic coin. She then proves to Bob via a zero-knowledge proof that she possesses the corresponding secret key. If she responds to two distinct challenges, the identifying information can be put together to reveal the secret key and thus her identity.

B. Authentication and Signature Techniques

Part B describes the digital signatures that have been used in implementation of the above protocols and the techniques that have been used to include identifying information.

Two kinds of digital signatures appear in electronic cash protocols. Suppose the signer has a key pair and a message M to be signed.

- *Digital Signature with Message Recovery.* For this kind of signature, there is a signing function S_{SK} using the secret key SK, and a verifying function V_{PK} using the public key PK. These functions are inverses, so that:

  Equation 1: $$V_{PK}\,(S_{SK}\,(M)) = M.$$

  The function V_{PK} is easy to implement, but S_{SK} is easy only if one knows SK. Thus S_{SK} is said to have a trapdoor, or secret quantity that makes it possible to perform a cryptographic computation which is otherwise infeasible. The function V_{PK} is called a trapdoor one-way function, because it is a one-way function to anyone who does not know the trapdoor.

In this kind of scheme, the verifier receives the signed message $S_{SK}(M)$ but not the original message text. The verifier then applies the verification function V_{PK}. This step both verifies the identity of the signer and, by using Equation 1, recovers the message text.

- *Digital Signature with Appendix.* In this kind of signature, the signer performs an operation on the message using his own secret key. The result is taken to be the signature of the message, sent as an attached appendix to the message text. The verifier checks an equation involving the message, the appendix, and the signer's public key. If the equation checks, the verifier knows that the signer's secret key was used in generating the signature.

Specific algorithms are provided below.

RSA Signatures. The most well-known signature with message recovery is the RSA signature. Let N be a hard-to-factor integer. The secret signature key s and the public verification key v are exponents with the property that

$$M^{sv} \equiv M \pmod{N}$$

for all messages M. Given v, it is easy to find s if one knows the factors of N, but difficult otherwise. Thus the "v^{th} power (mod N)" map is a trapdoor one-way function. The signature of M is

$$C := M^s \pmod{N};$$

to recover the message (and verify the signature), one computes

$$M := C^v \pmod{N}.$$

Blind RSA Signatures. The above scheme is easily blinded. Suppose that Alice wants the Bank to produce a blind signature of the message M. She generates a random number r and sends

$$r^v M \pmod{N}$$

to the Bank to sign. The Bank does so, returning

$$r M^s \pmod{N}.$$

Alice then divides this result by r. The result is $M^s \pmod{N}$, the Bank's signature of M, even though the Bank never has seen M.

The Schnorr Algorithms. The Schnorr family of algorithms includes an identification procedure and a signature with appendix. These algorithms are based on a zero-knowledge proof of possession of a secret key. Let p and q be large prime numbers with q dividing $p - 1$. Let g be a generator; that is, an integer between 1 and p such that

$$g^q = 1 \pmod{p}.$$

If s is an integer (mod q), then the modular exponentiation operation on s is

$$\phi : \; s \geq g^s \pmod{p}.$$

The inverse operation is called the discrete logarithm function and is denoted

$$\log_g t \leq t.$$

If p and q are chosen properly, then modular exponentiation is a one-way function. That is, it is computationally infeasible to find a discrete logarithm. Now suppose we have a line:

Equation 2: $y = mx + b$

over the field of integers (mod q). A line can be described by giving its slope m and intercept b, but we will "hide" it as follows. Let

$$c = g^b \pmod{p},$$
$$n = g^m \pmod{p}.$$

Then c and n give us the "shadow" of the line under ϕ. Knowing c and n does not give the slope or intercept of the line, but it does enable us to determine whether a given point (x, y) is on the line. If (x, y) satisfies Equation 2, then it also must satisfy the relation below:

Equation 3 $g^y = n^x c \pmod{p}.$

Conversely, any point (x, y) satisfying Equation 3 must be on the line. The relationship in Equation 3 can be checked by anyone, because it involves only public quantities. Thus anyone can check whether a given point is on the line, but points on the line can be generated only by someone who knows the secret information. The basic Schnorr protocol is a zero-knowledge proof that one possesses a given secret quantity m. Let n be the corresponding public quantity. Suppose one user (the "prover") wants to convince another (the "verifier") that she knows m without revealing it. She does this by constructing a line (Equation 2) and sending its shadow to the verifier. The slope of the line is taken to be secret quantity m, and the prover chooses the intercept at random, differently for each execution of the protocol. The protocol then proceeds as follows:

Schnorr proof of possession:

(1) Alice sends c (and n if necessary) to Bob.

(2) Bob sends Alice a "challenge" value of x.

(3) Alice responds with the value of y such that (x, y) is on the line.

(4) Bob verifies via Equation 3 that (x, y) is on the line.

Bob now knows that he is speaking with someone who can generate points on the line. Thus Alice must know the slope of the line, which is the secret quantity m.

An important feature of this protocol is that it can be performed only once per line. For example, if Bob knows any two points (x_0, y_0) and (x_1, y_1) on the line, he can compute the slope of the line using the familiar "rise over run" formula

$$m \equiv (y_0 - y_1) \,/\, (x_0 - x_1) \pmod{q},$$

and this slope is the secret quantity m. That is why a new intercept must be generated each time a message is sent. This is known as the *two-points-on-a-line principle.* This feature will be useful for electronic cash protocols, because we want to define a spending procedure that reveals nothing of a secret key if used once per coin, but reveals the key if a coin is spent twice.

Schnorr identification. The above protocol can be used for identification of users in a network. Each user is issued a key pair, and each public key is advertised as belonging to a given user. To identify herself, a user need prove only that she knows her secret key. This can be accomplished using the above zero-knowledge proof, because her public key is linked with her identity.

Schnorr Signature. It is easy to convert the Schnorr identification protocol to produce a digital signature scheme. Rather than receiving a challenge from an on-line verifier, the signer simply takes x to be a secure hash of the message and of the shadow of the line. This proves knowledge of his secret key in a way that links his key pair to the message.

Blind Schnorr Signature. Suppose that Alice wants to obtain a blind Schnorr signature for her coin, which she will spend with Bob. Alice generates random quantities (mod q) which describe a change of variables. This change of variables replaces the Bank's hidden line with another line, and the point on the Bank's line with a point on the new line. When Bob verifies the Bank's signature, he is checking the new point on the new line. The two lines have the same slope, so that the Bank's signature will remain valid. When the Bank receives the coin for deposit, it will see the protocol implemented on the new line, but it will not be able to link the coin with Alice's withdrawal because only Alice knows the change of variables relating the two lines.

Chaum-Pedersen Signature. A variant of Schnorr's signature scheme is used in electronic cash protocols.[12] This modified scheme is a kind of "double Schnorr" scheme. It involves a single line and point but uses two shadows. This signature scheme can be blinded in a way similar to the ordinary Schnorr signature.

Implementations of the Schnorr Protocols. The Schnorr algorithms have been described in terms of integers modulo a prime p. The protocols, however, work in any setting in which the analogue of the discrete logarithm problem is difficult. An important example is that of elliptic curves.[13] Elliptic curve based protocols are much faster and require the transmission of far less data than non-elliptic protocols giving the same level of security.

C. *Summary of Proposed Implementations*

Part C presents summaries of the three main off-line cash schemes: Chaum-Fiat-Naor,[14] Brands,[15] and Ferguson.[16]

Chaum-Fiat-Naor was the first electronic cash scheme, and is the simplest conceptually. The Bank creates an electronic coin by performing a blind RSA signature to Alice's withdrawal request, after verifying interactively that Alice has included her identifying information on the coin. The prevention of multiple spending is accomplished by the cut-and-choose method. For this reason, the scheme is relatively inefficient.

Brands' scheme is Schnorr-based.[17] Indeed, a Schnorr protocol is used twice: at withdrawal the Bank performs a blind Chaum-Pedersen signature, and then Alice performs a Schnorr possession proof as the challenge-and-response part of the spending protocol.

The withdrawal step produces a coin that contains the Bank's signature, authenticating both Alice's identifying information and the shadow of the line to be used for the possession proof. This commits Alice to using that particular line in the spending step. If she respends the coin, she must use the same line twice, enabling the Bank to identify her.

---

12. *See* David Chaum & Torben P. Pedersen, *Wallet Databases With Observers*, 1992 ADVANCES IN CRYPTOLOGY—CRYPTO '92, LECTURE NOTES IN COMPUTER SCI. 89, 93-94.

13. *See* MENEZES, *supra* note 7, at 13.

14. *See* David Chaum et al., *Untraceable Electronic Cash*, 1988 ADVANCES IN CRYPTOLOGY—CRYPTO '88, LECTURE NOTES IN COMPUTER SCI. 319.

15. *See* Stefan Brands, *Untraceable Off-line Cash in Wallets with Observers*, 1993 ADVANCES IN CRYPTOLOGY—CRYPTO '93, LECTURE NOTES IN COMPUTER SCI. 302.

16. *See* Niels Ferguson, *Single Term Off-line Coins*, 1993 ADVANCES IN CRYPTOLOGY—EUROCRYPT '93, LECTURE NOTES IN COMPUTER SCI. 318.

17. For ease of exposition, we give a simplified account of Brands' protocol.

The Brands scheme is considered by many to be the best of the three, for two reasons: (1) it avoids the awkward cut-and-choose technique; and (2) it is based only on the Schnorr protocols, and this can be implemented in various settings such as elliptic curves.

Ferguson's scheme is RSA-based like Chaum-Fiat-Naor, but it uses the "two-points-on-a-line" principle like Brands. The signature it uses is not the blind RSA signature as described above, but a variant called a randomized blind RSA signature. The ordinary blind RSA scheme has the drawback that the Bank has absolutely no idea what it is signing. As mentioned above, this is not a problem in the cut-and-choose case, but in this case it can allow a payer to defeat the mechanism for identifying multiple spenders. The randomized version avoids this problem by having both Alice and the Bank contribute random data to the message. The Bank still does not know what it is signing, but it knows that the data was not chosen maliciously. The rest of the protocol is conceptually similar to Brands' scheme. The message to be signed by the Bank contains, in addition to the random data, the shadow of a line the slope and intercept of which reveal Alice's identity. During payment, Alice reveals a point on this line; if she does so twice, the Bank can identify her. Although Ferguson's scheme avoids the cut-and-choose technique, it is the most complicated of the three (due largely to the randomized blind RSA signature). Moreover, it cannot be implemented over elliptic curves because it is RSA-based.

IV. OPTIONAL FEATURES OF OFF-LINE CASH

Part IV discusses two features that can be added to off-line cash to make it more convenient to use.

A. Transferability

Transferability is a feature of paper cash that allows a user to spend a coin that he has received in a payment without having to contact the Bank first. A payment is referred to as a transfer if the payee can use the received coin in a subsequent payment. A payment system is transferable if it allows at least one transfer per coin. Figure 2 shows a maximum length path of a coin in a system that allows two transfers. The final payment is not considered a transfer because it must be deposited by the payee. Transferability would be a convenient feature for an off-line cash system because it requires less interaction with the Bank. It should be noted that a transferable electronic cash system is off-line by definition, as on-line systems require communication with the Bank during each payment.

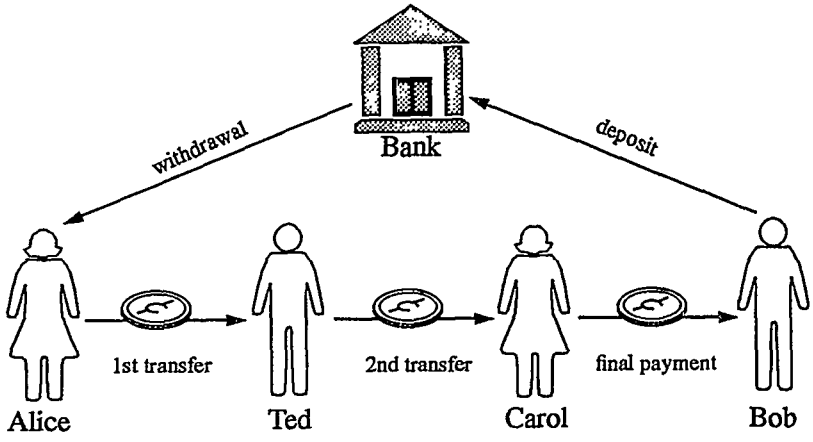

Figure 2. A maximum length path of a coin in a system which allows 2 transfers per coin.

Transferable systems have received little attention in academic literature. The schemes presented in Part III.C are not transferable because the payee cannot use a received coin in another payment; his only options are to deposit or exchange it for new coins at the Bank. Any transferable electronic cash system has the property that the coin must "grow in size" (i.e., accumulate more bits) each time it is spent, because the coin must contain information about every person who has spent it so that the Bank maintains the ability to identify multiple spenders.[18] This growth makes it impossible to allow an unlimited number of transfers. The maximum number of transfers allowed in any given system will be limited by the allowable size of the coin.

Other concerns with any transferable electronic cash system exist, even if the number of transfers per coin is limited, and the anonymity property is removed. Until the coin is deposited, the only information available to the Bank is the identity of the individual who originally withdrew the coin. Any other transactions involving that withdrawal can be reconstructed only with the cooperation of each consecutive spender of that coin. This poses the same problems that paper cash poses for detecting money laundering and tax evasion: no records of the transactions are available.

18. *See generally* David Chaum & Torben P. Pedersen, *Transferred Cash Grows in Size*, 1992 ADVANCES IN CRYPTOLOGY—EUROCRYPT '92, LECTURE NOTES IN COMPUTER SCI. 390.

In addition, each transfer delays detection of re-spent or forged coins. Multiple spending will not be noticed until two copies of the same coin eventually are deposited. By then it may be too late to catch the culprit, and many users may have accepted counterfeit coins. Detection of multiple spending after the fact, therefore, may not provide a satisfactory solution for a transferable electronic cash system. Rather, a transferable system may have to rely on physical security to prevent multiple spending.[19]

B. Divisibility

Suppose that Alice is enrolled in a non-transferable, off-line cash system, and she wants to purchase an item from Bob that costs $4.99. If she happens to have electronic coins the value of which adds up to exactly $4.99 then she simply spends these coins. Unless Alice has stored a large reserve of coins of each possible denomination, however, it is unlikely that she will have the exact change for most purchases. She may not wish to keep such a large reserve of coins on hand for some of the same reasons an individual does not carry around a large amount of cash: loss of interest and fear of the cash being stolen or lost. Another option is for Alice to withdraw a coin of the exact amount for each payment, but that requires interaction with the Bank, making the payment on-line from her point of view. A third option is for Bob to pay Alice the difference between her payment and the $4.99 purchase price. This puts the burden of having an exact payment on Bob, and also requires Alice to contact the Bank to deposit the "change."

A solution to Alice's dilemma is to use divisible coins: coins that can be "divided" into pieces the total value of which is equal to the value of the original coin. This allows exact off-line payments to be made without the need to store a supply of coins of different denominations. Paper cash obviously is not divisible, but lack of divisibility is not as much of an inconvenience with paper cash because it is transferable. Coins that are received in one payment can be used again in the next payment, so the supply of different denominations is partially replenished with each transaction.

Three divisible off-line cash schemes have been proposed, but at the cost of longer transaction time and additional storage. Eng/Okamoto's divisible scheme is based on the "cut and choose"

19. *See infra* Part V.A.

method.[20] Okamoto's scheme is much more efficient and is based on Brands' scheme but also will work on Ferguson's scheme.[21] Okamoto and Ohta's scheme is the most efficient of the three, but also the most complicated.[22] It relies on the difficulty of factoring and on the difficulty of computing discrete logarithms.

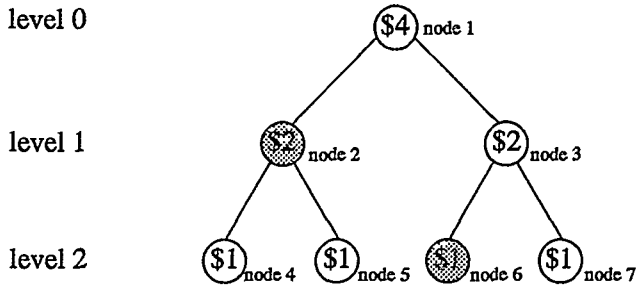

Figure 3. A binary tree for a divisible coin worth $4.00, with a minimum unit of $1.00. A $3.00 payment can be made by spending the shaded nodes. Node 1 cannot be used in a subsequent payment because it is an ancestor of nodes 2 and 6. Nodes 4 and 5 cannot be used because they are descendants of node 2. Node 3 cannot be used because it is an ancestor of node 6. Nodes 2 and 6 cannot be used more than once, so node 7 is the only node which can be spent in a subsequent payment.

All three of these schemes work by associating a binary tree with each coin of value $\$w$. Each node is assigned a monetary value as follows: the unique *root* node (the node at level 0) has value $\$w$, the two nodes at level 1 each have value $\$w/2$, the four nodes at level 2 each have value $\$w/4$, etc. Therefore, if $w = 2^l$, then the tree has $l+1$ levels, and the nodes at level j each have value $\$w/2^j$. The *leaves* of the tree are the nodes at level l, and have the minimum unit of value.

To spend the entire amount of value $\$w$, the root node is used. Amounts less than $\$w$ can be spent by spending a set of nodes the values of which add up to the desired amount.

Initially, any whole dollar amount up to $\$w$ can be spent. Subsequent payments are made according to the following rules:

---

20. *See* Tony Eng & Tatsuaki Okamoto, *Single-Term Divisible Electronic Coins*, 1994 ADVANCES IN CRYPTOLOGY—EUROCRYPT '94, LECTURE NOTES IN COMPUTER SCI. 311, 313.

21. *See generally* Tatsuaki Okamoto, *An Efficient Divisible Electronic Cash Scheme*, 1995 ADVANCES IN CRYPTOLOGY—CRYPTO '95, LECTURE NOTES IN COMPUTER SCI. 438.

22. *See generally* Tatsuaki Okamoto & Kazuo Ohta, *Universal Electronic Cash*, 1991 ADVANCES IN CRYPTOLOGY—CRYPTO '91, LECTURE NOTES IN COMPUTER SCI. 324.

(1) Once a node is used, none of its descendant and ancestor nodes[23] can be used; and

(2) No node can be used more than once.

These two rules ensure that no more than one node is used on any path from the root to a leaf. If these two rules are observed, then it will be impossible to spend more than the original value of the coin. If either of these rules are broken, then two nodes on the same path are used, and the information in the two corresponding payments can be combined to reveal the identity of the individual who over-spent in the same way that the identity of a multiple spender is revealed.

More specifically, in the Eng/Okamoto and Okamoto schemes, each user has a secret value s, which is linked to his identity. Uncovering s will uncover the user's identity, but not vice-versa. Each node i is assigned a secret value, t_i. Thus, each node i corresponds to a line

$$y = sx + t_i .$$

When a payment is made using a particular node n, t_i will be revealed for all nodes i that are ancestors of node n. The payee then sends a challenge x_i and the payer responds with

$$y_1 = sx_1 + t_n .$$

This reveals a point (x_1, y_1) on the line $y = sx + t_n$, but does not reveal the line itself. If the same node is spent twice, then responses to two independent challenges, x_1 and x_2, will reveal two points on the same line: (x_1, y_1) and (x_2, y_2). The secret value s can be recovered using the two-points-on-a-line principle described in Part III.B.

If someone tries to overspend a coin, then two nodes in the same path will be used. Suppose that nodes n and m are in the same path, and node n is farther from the root on this path. Spending node n will reveal t_m, because node m is an ancestor of node n. If node m also is spent, then the response to a challenge x_1 will be $y_1 = sx_1 + t_m$. But t_m was revealed when t_n was spent, so sx_1 and hence s will be revealed. Therefore, spending two nodes in the same path will reveal the identity of the over-spender. The Okamoto/Ohta divisible scheme also uses a binary tree with the same rules for using nodes to prevent multiple and over-spending, but when nodes are used improperly, a different technique is used to determine the identity of the spender. Instead of hiding the user's identifying secret in a line

23. A descendant of a node n is a node on a path from node n to a leaf. An ancestor of node n is a node on the path from node n to the root node.

for which a point is revealed when a coin is spent, the user's identifying secret is hidden in the factorization of an RSA modulus. Spending the same node twice, or spending two nodes on the same path will provide enough information for the Bank to factor the modulus (which is part of the coin) and then to compute the user's secret identifying information.

Although these three divisible schemes are untraceable, payments made from the same initial coin may be "linked" to each other, meaning that it is possible to tell if two payments came from the same coin and thus the same person. This does not reveal the payer's identity if both payments are valid (following Rules 1 and 2, *supra*), but revealing the payer's identity for one purchase would reveal that payer's identity for all other purchases made from the same initial coin.

Although providing divisibility complicates the protocol, it can be accomplished without forfeiting untraceability or the ability to detect improper spenders using any of these schemes. The most efficient divisible scheme has a transaction time and required memory per coin proportional to the logarithm of N, where N is the total coin value divided by the value of the minimum divisible unit. More improvements in the efficiency of divisible schemes are expected, as the most recent improvement was presented in 1995.

V. SECURITY ISSUES

Part V discusses some issues concerning the security of electronic cash. First, Parts A and B discuss ways to prevent multiple spending in off-line systems and describe the concept of wallet observers. Part C discusses the consequences of an unexpected failure in the system's security. Finally, Part D describes a solution to some of the law enforcement problems that are created by anonymity.

A. Multiple Spending Prevention

Part I.D explained that multiple spending can be prevented in on-line payments by maintaining a database of spent electronic coins, but there is no cryptographic method for preventing an off-line coin from being spent more than once. Instead, off-line multiple spending is detected when the coin is deposited and compared to a database of spent coins. Even in anonymous, untraceable payment schemes, the identity of the multiple-spender can be revealed when the abuse is detected. Detection after the fact may be enough to discourage multiple spending in most cases, but it will not solve the problem. If someone were able to obtain an account under a false identity, or

were willing to disappear after re-spending a large sum of money, he could cheat the system successfully.

One way to minimize the problem of multiple spending in an off-line system is to set an upper limit on the value of each payment. This would limit the financial losses to a given merchant from accepting coins that had been deposited previously. However, this will not prevent someone from spending the same small coin many times in different places.

In order to prevent multiple spending in off-line payments, one must rely on physical security. A "tamper-proof" card could prevent multiple spending by removing or disabling a coin once it is spent. Unfortunately, a truly "tamper-proof" card does not exist. Instead, we will refer to a "tamper-resistant" card that physically is constructed so that it is very difficult to modify its contents. This could be in the form of a smart card, a PCMCIA card, or any storage device containing a tamper-resistant computer chip. A tamper-resistant card will prevent abuse in most cases, because the typical criminal will not have the resources to modify the card. Even with a tamper-resistant card, however, it still is essential to provide cryptographic security to prevent counterfeiting and to detect and identify multiple spenders if the tamper-protection somehow is defeated. Additionally, setting limits on the value of off-line payments would reduce the cost-effectiveness of tampering with the card.

Tamper-resistant cards also can provide personal security and privacy to the cardholder by making it difficult for adversaries to read or modify the information stored on the card, such as secret keys, algorithms, or records.

B. Wallet Observers

All of the basic off-line cash schemes presented in Part III.C can cryptographically detect the identity of multiple spenders, but the only way to prevent off-line multiple spending is to use a tamper-resistant device such as a smart card. One drawback of this approach is that the user must put a great deal of trust in the device, because the user loses the ability to monitor information entering or leaving the card. It is conceivable that the tamper-resistant device could leak private information about the user without the user's knowledge.

Chaum and Pedersen proposed the idea of embedding a tamper-resistant device into a user-controlled outer module in order to achieve the security benefits of a tamper-resistant device without

requiring the user to trust the device.[24] They call this combination an electronic wallet. The outer module (such as a small hand-held computer or the user's PC) is accessible to the user. The inner module, which cannot be read or modified, is called the "observer." All information that enters or leaves the observer must pass through the outer module, allowing the user to monitor information that enters or leaves the card. The outer module, however, cannot complete a transaction without the cooperation of the observer. This gives the observer the power to prevent the user from making transactions that it does not approve of, such as spending the same coin more than once.

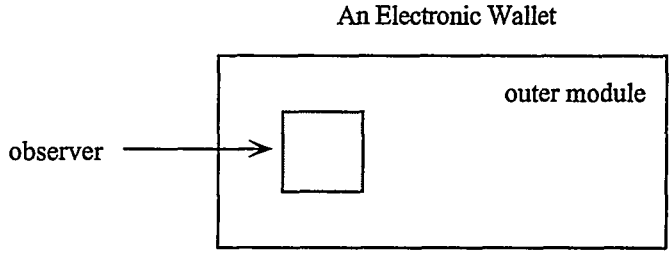

Figure 4. An electronic wallet.

Brands and Ferguson both have shown how to incorporate observers into their respective electronic cash schemes to prevent multiple spending.[25] Brands' scheme incorporates observers in a much simpler and more efficient manner. In Brands' basic scheme, the user's secret key is incorporated into each of his coins. When a coin is spent, the spender uses his secret key to create a valid response to a challenge from the payee. The payee will verify the response before accepting the payment. Using Brands' scheme with wallet observers, this user-secret key is shared between the user and his observer. The combined secret is a modular sum of the two shares, so that one share of the secret reveals no information about the combined secret. Cooperation of the user and the observer is necessary to create a valid response to a challenge during a payment transaction. This is accomplished without either the user or the observer revealing any information about its share of the secret to the

24. *See* Chaum & Pedersen, *supra* note 12, at 92-93.

25. *See generally* Brands, *supra* note 15; Niels Ferguson, *Extensions of Single-term Coins*, 1993 ADVANCES IN CRYPTOLOGY, LECTURE NOTES IN COMPUTER SCI. 292.

other. It also prevents the observer from controlling the response; thus the observer cannot leak any information about the spender.

An observer also could be used to trace the user's transactions at a later time, as it can keep a record of all transactions in which it participates. However, this requires that the Bank (or whoever is doing the tracing) be able to obtain the observer and analyze it. Also, not all types of observers can be used to trace transactions. Brands and Ferguson both claim that they can incorporate observers into their schemes and still retain untraceability of the users' transactions, even if the observer used in the transactions has been obtained and can be analyzed.

C. Security Failures

1. Types of failures

In any cryptographic system, there is some risk of a security failure. Such a failure in an electronic cash system would result in the ability to forge or duplicate money. There are a number of different ways in which an electronic cash system could fail.

One of the most serious types of failure would occur if the cryptography (the protocol or the underlying mathematics) does not provide the intended security.[26] This could enable someone to create valid looking coins without knowledge of an authorized bank's secret key, or to obtain valid secret keys without physical access to them. Anyone who is aware of the weakness could create coins that appear to come from a legitimate bank in the system.

Another serious type of failure could occur in a specific implementation of the system. For example, if the bank's random number generator is not a good one, an individual may be able to guess the secret random number and use it to compute the secret keys that are used to create electronic money.

Even if the cryptography and the implementation are secure, the security could fail because of a physical compromise. If a computer hacker, a thief, a dishonest bank employee, or a rogue state were to gain access to the bank's secret key it could create counterfeit money. If it gains access to a user's secret key it could spend that user's money. If it modifies the user or bank's software they could destroy the security of the system.

---

26. The authors are unaware of anything in the literature that would suggest this type of failure with the protocols discussed in this Essay.

The above failure scenarios apply not only to the electronic cash system, but also to the underlying authentication infrastructure. Any form of electronic commerce depends heavily on the ability of users to trust the authentication mechanisms. If, for example, an attacker could demonstrate a forgery of the certification authority's digital signature, it would undermine the users' trust in the ability of the parties to identify each other. Thus, certification authorities must secured as thoroughly as banks.

2. Consequences of a failure

All three of the basic schemes described in this Essay are anonymous, which makes it impossible for anyone to connect a deposited coin to the originating bank's withdrawal record of that coin. This property has serious consequences in the event of a security failure leading to token forgery. When a coin is submitted for deposit, it is impossible to determine if it is forged. Even the originating bank is unable to recognize its own coins, preventing detection of the compromise. It is conceivable that the compromise will not be detected until the bank realizes that the total value of deposits of its electronic cash exceeds the amount that it has created with a particular key. At this point the losses could be devastating.

After the key compromise is discovered, the bank still will be unable to distinguish valid coins from invalid ones, as deposits and withdrawals cannot be linked. The bank would have to change its secret key and invalidate all coins that were signed with the compromised key. The bank can replace coins that have not been spent yet, but the validity of untraceable coins that already have been spent or deposited cannot be determined without cooperation of the payer. Payment untraceability prevents the Bank from determining the identity of the payer, and payer anonymity prevents even the payee from identifying the payer.

It is possible to minimize this damage by limiting the number of coins affected by a single compromise. This could be done by changing the Bank's public key at designated time intervals, or when the total value of coins issued by a single key exceeds a designated limit. This kind of compartmentation, however, reduces the anonymity by shrinking the pool of withdrawals that could correspond to a particular deposit and vice versa.

D. Restoring Traceability

The anonymity properties of electronic cash pose several law enforcement problems because they prevent withdrawals and deposits

from being linked to each other. Part C explained how this linking problem prevents detection of forged coins. Anonymity also makes it difficult to detect money laundering and tax evasion because there is no way to link the payer and payee. Finally, electronic cash paves the way for new versions of old crimes such as kidnapping and blackmail[27] where money drops now can be carried out safely from the criminal's home computer.[28]

One way to minimize these concerns is to require large transactions or large numbers of transactions in a given time period to be traceable. This would make it more difficult to commit crimes involving large sums of cash. Even a strict limit such as a maximum of $100 a day on withdrawals and deposits can add up quickly, however, especially if one can open several accounts, each with its own limit. Also, limiting the amount spent in a given time period would have to rely on a tamper-resistant device.

Another way to minimize these concerns is to provide a mechanism to restore traceability under certain conditions, such as a court order. Traceability can be separated into two types by its direction. Forward traceability is the ability to identify a deposit record (and thus the payee), given a withdrawal record (and thus the identity of the payer). In other words, if a search warrant is obtained for Alice, forward tracing will reveal where Alice has spent her cash. Backward traceability is the ability to identify a withdrawal record (and thus the payer), given a deposit record (and thus the identity of the payee). Backward tracing will reveal who Alice has been receiving payments from.

A solution that conditionally restores both forward and backward traceability into the cut-and-choose scheme is presented by Stadler, Piveteau, and Camenisch.[29] In the basic cut-and-choose scheme, an identifying number is associated with each withdrawal record and a different identifying number is associated with each deposit record, although there is no way to link these two records to each other. To provide a mechanism for restoring backward traceability, the withdrawal number (along with some other data that cannot be associated with the withdrawal) is encrypted with a commonly trusted entity's public key and incorporated into the coin itself. This

---

27. *See* Sebastiaan von Solms & David Naccache, *On Blind Signatures and Perfect Crimes*, 11 COMPUTERS & SECURITY 581, 582-83 (1992).

28. This Essay does not focus on such crimes against individuals, concentrating instead on crimes against the government, the banking system, and the national economy.

29. *See generally* Markus Stradler et al., *Fair Blind Signatures*, 1995 ADVANCES IN CRYPTOLOGY—EUROCRYPT '95, LECTURE NOTES IN COMPUTER SCI. 209.

encrypted withdrawal number is passed to the payee as part of the payment protocol, and then passed along to the bank when the coin is deposited by the payee. The payer performs the encryption during the withdrawal transaction, but the bank can insure that the encryption was done properly. If the required conditions for tracing are met, the payment or deposit can be turned over to the trusted entity holding the secret key to decrypt the withdrawal number. This withdrawal number will allow the bank to access its withdrawal records, identifying the payer.

To provide a mechanism for restoring forward traceability, the payer must commit to a deposit number at the time that the coin is withdrawn. The payer encrypts this deposit number with a commonly trusted entity's public key (along with some other data that cannot be associated with the deposit) and must send this value to the bank as part of the withdrawal protocol. The bank is able to determine that the payer has not cheated, although it only sees the deposit number in encrypted form. If the required conditions for tracing are met, the withdrawal record can be turned over to the trusted entity holding the secret key to decrypt the deposit number. The bank can use this deposit number to identify the depositor (the payee).

Stadler, Piveteau, and Camenisch have shown that it is possible to provide a mechanism for restoring traceability in either or both directions. This can be used to provide users with anonymity, while solving many of the law enforcement problems that exist in a totally untraceable system. The ability to trace transactions in either direction can help law enforcement officials catch tax evaders and money launderers by revealing who has paid or who has been paid by the suspected criminal. Electronic blackmailers can be caught because the deposit numbers of the victim's ill-gotten coins could be decrypted, identifying the blackmailer when the money is deposited.

The ability to restore traceability does not solve one very important law enforcement problem, namely detecting forged coins. Backward tracing will help identify a forged coin if a particular payment or deposit (or depositor) is under suspicion. In that case, backward tracing will reveal the withdrawal number, allowing the originating bank to locate its withdrawal record and to verify the validity of the coin. If a forged coin makes its way into the system, however, it may not be detected until the bank whose money is being counterfeited realizes that the total value of its electronic cash deposits using a particular key exceeds the values of its withdrawals. The only way to determine which deposits are genuine and which are forged would require obtaining permission to decrypt the withdrawal numbers for

each deposit of electronic cash using the compromised key. This would violate the privacy that anonymous cash was designed to protect.

Unfortunately, the Stadler-Piveteau-Camenisch scheme is not efficient because it is based on the bulky cut-and-choose method. However, it may be possible to apply similar ideas to restore traceability in a more efficient electronic cash scheme.

CONCLUSION

This Essay has described several innovative payment schemes that provide user anonymity and payment untraceability. These electronic cash schemes have cryptographic mechanisms in place to address the problems of multiple spending and token forgery. Some serious concerns about the ability of an electronic cash system to recover from a security failure have been identified, however. Concerns about the impact of anonymity on money laundering and tax evasion also have been discussed.

Because it is simple to make an exact copy of an electronic coin, a secure electronic cash system must have a way to protect against multiple spending. If the system is implemented on-line, then multiple spending can be prevented by maintaining a database of spent coins and checking this list with each payment. If the system is implemented off-line, then there is no way to prevent multiple spending cryptographically, but it can be detected when the coins are deposited. Detection of multiple spending after the fact is useful only if the identity of the offender is revealed. Cryptographic solutions have been proposed that will reveal the identity of the multiple spender while preserving user anonymity.

Token forgery can be prevented in an electronic cash system as long as the cryptography is implemented soundly and securely, the secret keys used to sign coins are not compromised, and integrity is maintained on the public keys. If there is a security flaw or a key compromise, however, the anonymity of electronic cash will delay detection of the problem. Even after the existence of a compromise is detected, the Bank will not be able to distinguish its own valid coins from forged ones. Because there is no way to guarantee that the Bank's secret keys never will be compromised, it is important to limit the damage that a compromise could inflict. This could be accomplished by limiting the total value of coins issued with a particular key. Lowering these limits, however, also reduces the anonymity of the system as there is a smaller pool of coins associated with each key.

The untraceability property of electronic cash creates problems in detecting money laundering and tax evasion because there is no way to link the payer and payee. To counter this problem, it is possible to design a system that has an option to restore traceability using an escrow mechanism. If certain conditions are met (such as a court order), a deposit or withdrawal record can be turned over to a commonly trusted entity holding a key that can decrypt information connecting the deposit to a withdrawal or vice versa. This will identify the payer or payee in a particular transaction. It is not a solution to the token forgery problem, however, because there may be no way to know which deposits are suspect. In that case, identifying forged coins would require turning over all of the Bank's deposit records to the trusted entity to have the withdrawal numbers decrypted.

This Essay also has examined two optional features of off-line electronic cash: transferability and divisibility. Because the size of an electronic coin must grow with each transfer, the number of transfers allowed per coin must be limited. Also, allowing transfers magnifies the problems of detecting counterfeit coins, money laundering, and tax evasion. Coins can be made divisible without losing any security or anonymity features, but at the expense of additional memory requirements and transaction time.

In conclusion, the potential risks in electronic commerce are magnified when anonymity is present. Anonymity creates the potential for large sums of counterfeit money to go undetected by preventing identification of forged coins. Anonymity also provides an avenue for laundering money and evading taxes that is difficult to combat without resorting to escrow mechanisms. Anonymity can be provided at varying levels, but increasing the level of anonymity also increases the potential damages. It is necessary to weigh the need for anonymity with these concerns. It may well be concluded that these problems are best avoided by using a secure electronic payment system that provides privacy, but not anonymity.