Anonymity Control in E-Cash Systems

George Davida[1] Yair Frankel[2] * Yiannis Tsiounis[3] ** Moti Yung[2]

[1] University of Wisconsin-Milwaukee. davida@cs.uwm.edu
[2] CertCo LLC, frankely,moti@certco.com, moti@cs.columbia.edu
[3] GTE Laboratories Incorporated. yt00@gte.com, yiannis@ccs.neu.edu

Abstract. Electronic cash, and other cryptographic payment systems, offer a level of user anonymity during a purchase, in order to emulate electronically the properties of physical cash exchange. However, it has been noted that there are crime-prevention situations where anonymity of notes is undesirable; in addition there may be regulatory and legal constraints limiting anonymous transfer of funds. Thus pure anonymity of users may be, in certain settings, unacceptable and thus a hurdle to the progress of electronic commerce.
The conceptual contribution of this work is based on the claim that given the legal, social, technical and efficiency constraints that are imposed, anonymity should be treated as a *Control Parameter* facilitating flexibility of the level of privacy of note holders (determined by the dynamic conditions and constraints).
In light of this parameterization, we review recently developed technical tools for tracing and anonymity revocation (e.g., owner tracing and coin tracing). We elaborate on the differences in the various technologies with respect to security assumptions and we discuss practical considerations of computational, bandwidth and storage requirements for user, shop, bank and trustees as well as whether the trustees must be on-line or off-line. We also claim that while anonymity revocation can potentially reduce crime it can also produce instances where the severity of the crime is increased as criminals try to social engineer around tracing revocation. To prevent this we suggest the notion of "distress cash." On the technical side, we provide efficiency improvements to a protocol for coin tracing and point at a technical solution for distress cash.

1 Introduction

Electronic cash provides user anonymity against both the bank and shops during a purchase, in order to emulate the perceived anonymity of regular cash transactions. There are many arguments for, as well as against, anonymous payment systems. Protection of users' privacy and prevention of the compilation of personal data are often cited in support of anonymity for e-cash [Fro96b, Cha83]. However, anonymous e-cash may also facilitates fraud and criminal acts such as

* Research performed while at Sandia National Laboratories. This work was performed under U.S. Department of Energy Contract number DE-AC04-76AL85000.
** Research performed while at Northeastern University, Boston, MA.

money laundering [vSN92], anonymous (perfect) blackmailing and illegal purchases. Given the actual legal and social constraints and additional technological limitations (of bandwidth, computational and storage efficiencies) that electronic implementations may impose, we suggest to treat anonymity as a *Control Parameter* that can be changed by allowing flexibility in the level of user anonymity as conditions require.[4]

Anonymity revocation is activated by the anonymity control parameter and should therefore be enabled selectively, based on discriminators. These determine which e-coins should be "opened" and which ones should remain anonymous. Potential discriminators are time of purchase and the shop where the purchase is made at. Other discriminators may also need to be incorporated in the e-cash system to make anonymity revocation useful.

The current state of the art regarding levels of anonymity revocation consists of two separate models: 1) *coin tracing* to identify the coin withdrawn from a bank, as proposed by [SPC95] and 2) *owner tracing* to identify the owner of an e-coin, as independently suggested by [BGK95] and [SPC95]. With owner tracing the anonymity control parameter allows for trustees to determine the owner of a coin after payment has been made. Its primary purpose is to allow for "after the purchase" tracing for legal and regulatory requirements of large monetary exchanges. Owner tracing, however, is not useful in preventing many types of fraud because the discriminators are based on the purchase (i.e., time, amount, shop) rather than anything directly related to the coin. Coin tracing, similar to tracking by serial numbers, provides a "before the purchase" tracing to help law enforcement to track coins. With coin tracing, the trustees are able to determine the e-coin that was withdrawn from the bank and link the withdrawal to the purchase. Hence the discriminator for coin tracing is information directly related to the coin. Coin tracing's primary purpose is to track fraud and other criminal activities in a manner similar to tracking based on serial numbers on notes; in actuality it is even more effective since transferability [CP93a] is usually not enabled in e-cash—for liability and storage reasons—while the same (central) bank is used for withdrawal and deposit.

Anonymity revocation can indeed reduce crime but it can also produce instances where the severity of the crime is increased as criminals try to social engineer around the anonymity revocation. For example, it has been suggested that concerning car theft prevention, "The Club"[5] may have decreased the number of cars stolen in the USA but has increased the more dangerous crime of car-jacking. Hence less cars were stolen but in some cases a criminal would obtain a car but by committing a more serious crime (e.g., murdering the owner). This has led the legislators in the USA to make car-jacking a federal offense. An analogous situation could happen with coin tracing. A criminal forces a victim to withdraw e-coins from the victim's account. Since coin tracing is enabled the criminal must kill the victim so that s/he can spend the money before it is discov-

[4] We concentrate on anonymity in the e-cash application level while ignoring other issues of anonymity in computer systems, e.g., traceable Internet addresses.

[5] This is a device that prevents the steering wheel on a car from being moved.

ered that the victim is missing. We suggest *Distress Cash* to resolve this concern.

Organization: In section 2 we present types of anonymity, legal issues regarding anonymity and extract requirements for *anonymity-controlled e-cash*. In section 3 we discuss various models to control anonymity, namely the various tracing mechanisms that can be added to anonymous cash schemes. We discuss the security aspects of each of the anonymity controlled schemes. Under some of the models anonymity is unconditional (it is only assumed that one has a good source of randomness) whereas others assume conditional security based on defined cryptographic assumptions. In section 4 we present a comparative survey of the tracing mechanisms that have recently appeared in the literature. In section 5 we present a coin tracing protocol which is more efficient than earlier proposals, and present the entire anonymity control system. In section 6, we suggest the needs for, and the idea of distress cash, and point at ways to implement it. Thus, combining the solutions of the last two sections gives a system that fulfills the entire set of the requirements we have put forth.

What is E-cash: Let us first give a short description of electronic cash. Such systems (in particular off-line untraceable electronic cash) have sparked wide interest among cryptographers ([CFN90, FY93, Oka95, CP93b, CP93a, CP93c, PW92, Bra93, FY94, BGK95, DC94, EO94, OO92, FTY96, CMS96, Pai93, CFMT96, Sim96, Tsi97], etc.). In its simplest form, an e-cash system consists of three parties (a bank $\mathcal{B}$, a user $\mathcal{U}$ and a shop $\mathcal{S}$) and four main procedures (account establishment, withdrawal, payment and deposit). In a coin's life-cycle, the user $\mathcal{U}$ first performs an *account establishment protocol* to open an account with bank $\mathcal{B}$. To obtain a coin $\mathcal{U}$ performs a *withdrawal protocol* with $\mathcal{B}$ and during a purchase $\mathcal{U}$ spends a coin by participating in a *payment protocol* with the shop $\mathcal{S}$. To deposit a coin, $\mathcal{S}$ performs a *deposit protocol* with the bank $\mathcal{B}$. An e-cash system is *anonymous* if the bank $\mathcal{B}$, in collaboration with the shop $\mathcal{S}$, cannot trace the coin to the user. The system is *off-line* if during payment the shop $\mathcal{S}$ does not communicate with the bank $\mathcal{B}$. For the bank's security in an off-line system, if a coin is double spent, the user's identity is revealed with overwhelming probability. Note that an off-line system can be operated on-line where the bank checks for double spending at purchase time (the cost is, off course, the involvement of the bank). Formal models of security of off-line e-cash are given in [FY93, Tsi97] and for on-line systems in [Sim96]. We now restrict our discussions mainly to off-line systems, but the notions we discuss apply in a wider context.

2 Anonymity control parameter requirements

We now investigate the needs for controlling anonymity—due to regulation, operation, fraud and risk.

The primary reason for incorporating user anonymity into e-cash was to simulate physical cash. And indeed, one of the motivating aspects of using physical

cash is that it reduces the ability to link a user to a purchase.

It should be noted that even physical cash is not completely anonymous since the shop can see the buyer during a purchase (potentially taped with an in-store video), fingerprints may be on the notes, or serial numbers and locality of purchase may reveal the user to some degree [Fro96b]. Indeed, electronic cash has the potential for providing added anonymity. On the other hand, electronic cash purchases performed over digital networks require anonymous re-routers to provide a strong level of anonymity.

There are two issues in providing anonymity in e-cash: 1) The strength of the anonymity protection mechanism and 2) linkability amongst different coins of a single user. The cryptographic strength of anonymity pertains to what cryptographic assumptions are made to guarantee user anonymity, whereas linkability of coins is related to whether coins from an account are linkable to each other but not directly to the account.

Types of anonymity: The original e-cash and some of the subsequent electronic cash systems [Cha83, CFN90, Bra93, Fer93, EO94, Pai93, CP93b, CP93c, BGK95, PW92] provided for anonymity under the strongest form cryptographically possible, i.e., under no cryptographic assumption—other than the availability of a source of true randomness. Hence, independently of the strength of the adversary, it is not possible to determine the user's identity with a strategy better than just guessing.

There are also e-cash systems [Oka95, FTY96, OO92, FY93, CMS96] where anonymity is based on some, preferably well established, cryptographic assumptions. In these schemes an adversary with a high degree of computational power, or change in technology (e.g., discovering how to factor large numbers) may allow for the breaking of anonymity. Hence, one can expect after time that anonymity may be broken in these schemes, hopefully when the user does not care.

Now concerning the second issue of linkability of sub-coins. With some e-cash schemes a *pseudonym* ("nym") which is not traceable to one's identity is obtained by the user during the account establishment protocol. This pseudonym is visible with all coins withdrawn from the bank. Coins are thus anonymous but *linkable*, since the bank knows that they originate from the same pseudonym and therefore they belong to the same user. As pointed out by [Oka95, OO92, PW92, FTY96] this allows tracing the identity by conventional means, such as correlating payments' locality, type, time, or by identifying the user in one transaction. We do not concentrate on this type of anonymity.

Legal issues regarding anonymity: Governments have a strong interest in controlling their currency since they have a vested stake in making sure that electronic cash does not hurt their economies. Also, governments have rules and regulations effecting monetary exchanges across different countries and when the transaction amounts are large. Electronic cash can make money laundering more difficult since a coin must make a full cycle from the bank during withdrawal to the same bank for deposit. However, making many small purchases in seconds is possible with e-cash—unlike physical cash. Hence large exchanges of funds could potentially be hidden. An interesting overview of these issues is available

in [Fro96b]. It should also be noted that recently the National Security Agency has stated that escrowing of e-cash is vital for the United States' national interest [LSS96].

Requirements: In light of the above discussion we suggest the following requirements for anonymity controlled e-cash:

(1) *Anonymity* for legitimate users: Electronic coins should be anonymous and unlinkable for the legitimate users, with double-spenders (in off-line e-cash) being identified by the bank.

(2) *Revocation* upon warrant presentation: Anonymity should be revocable, but only by a trusted party (trustee) and when necessary. Necessity can be, e.g., determined by a judge's order, and the trusted party may be the judge per se or any combination of parties.

(3) *Separation* of power: The trustee(s) should not have any power other than tracing; in particular they should not be able to forge coins, or impersonate users.

(4) *No framing:* The bank, even in collaboration with the trustee(s) or other parties (e.g., malicious users/shops), should not be able to frame users. Additional properties may be specified to assure proper service for users (e.g., a proof of purchase, receipt or contract may be supplied to the user (for needed evidence)).

(5) *Selectivity:* Revocation must be selective; that is, only the transaction for which a judge's order is given must be de-anonymized. The system must behave as a fully traceable system with respect to this transaction, but remain fully anonymous for the rest—even for transactions of the same user.

(6) *Efficiency:* not only should tracing (anonymity revocation) be performed efficiently, but the added burden to the basic system should be minimal for all involved parties—trustees, bank, users and shops. In particular, trustees must be involved *only when revocation is required* and remain off-line otherwise.

(7) *Crime prevention*: Anonymity revocation should not –even indirectly– motivate crimes more serious than those it protects against.

We want to stress the importance of the efficiency requirement (6), as an inefficient system is of no practical importance. An implication of this requirement is that the trustee(s) must be *off-line*, that is they should not be involved in the protocols, except of course when tracing is required. Otherwise we would in effect ask a judge to participate in coin withdrawals or payments, which is undesirable and may prevent practical applications. At most the system can request the trustee(s) to be involved in each user's account establishment: in this case the trustees help in the creation of a "pseudonym" which is then used for the user's withdrawals; however, in this case the user's coins are linkable, violating requirement (1). In addition, if tracing is ever requested for one coin, anonymity for all the coins of this user is lost, violating requirement (5) above.

3 Anonymity Control models

We now review the various models for anonymity control and describe how each satisfies the needs of the various parties (users, shops, banks, government). In order to satisfy requirement (1) above we concentrate on tracing mechanisms that operate as additions to anonymous e-cash systems.

3.1 Tracing mechanisms

The literature discusses two protocols which, when added to an electronic cash scheme, provide for anonymity control:

- An *owner tracing* protocol exposes the identity of the owner of a specific coin. In this protocol the bank gives to the trustees the information it received during the deposit protocol. The trustees then return information which the bank can use to identify the owner (via its account databases). Owner tracing allows the authorities to prevent money laundering, since they can find the origin of dubious coins. It also allows the authorities to identify customers making an illegal purchase, after the illegal seller has been identified. Finally, it affords compliance with governmental requirements for tracing customers, as required, e.g., by the U.S. telephony bill or similar laws worldwide.
- A *coin tracing* protocol traces the coin(s) that originated from a withdrawal. In this protocol, the trustees obtain information from the bank about a specific withdrawal and return information that will appear when the coin is spent. Hence the discriminator is a particular withdrawal and tracing provides a "serial number," linking that withdrawal to a payment/deposit.

  Coin tracing allows the authorities to find the destination of suspicious withdrawals. Thus it can be used to identify the seller of illegal goods, by finding the destination of coins used to buy them: for example if a user is suspected of buying illegal drugs, then tracing his coins will lead to the seller's (dealer's) account.[6] In addition it prevents the blackmailing problem [vSN92]: a customer is blackmailed and forced to anonymously withdraw electronic coins, so that the blackmailer can use these coins without ever being identified, in effect committing a "perfect crime" (of course the victim has to complain and point at withdrawals). Lastly, the mechanism also enables tracing of activities of a suspect user that is on a criminal list at the time of his withdrawals.

For the selectivity requirement (5), note that coin tracing and owner tracing require different functionality: if a specific coin needs to be traced and only owner tracing is supported, the trustee is forced to break the anonymity of *all coins* in order to find a coin that originated from the particular withdrawal. Conversely, if only coin tracing is supported then finding the owner of a specific coin would require invoking coin tracing for *all withdrawals*, until the particular

[6] Wouldn't it be nice if a suspected drug user would point directly to his dealer, as this type of mechanism does?

coin is found. Thus an anonymity controlled system must include both means of tracing in order to satisfy selectivity (5). A formal tracing model is given in [FTY96].

4 Survey of previous work

We now survey the relevant technical literature, identifying schemes that conform to our requirements.

The vulnerability of anonymity of e-cash to the "perfect (i.e., anonymous) crime" was first noticed by [vSN92]. The first tracing mechanism proposed to resolve some of the legal and regulatory issues, developed independently by [SPC95] and [BGK95], was owner tracing; in the absence of coin tracing in these systems, some actions, such as blackmailing protection, result in non-selectivity. For this reason [SPC95] introduced the notion of coin tracing, thus providing a list of complete tracing mechanisms. These proposals all required the trustee(s) to be *on-line* during withdrawal,[7] which is not as efficient as in requirement (6) above, and worked under the unconditional (anonymity) model. Although unconditional security for anonymity is preferable, [FTY96] proved that indeed unconditional security for anonymity with *either* owner *and/or* coin tracing implies that the trustees must be active in each withdrawal.

[CPS96] extended the ideas of [SPC95] on "fair blind signatures" to create owner and coin tracing; however, the trustees are again on-line. [JY97] showed how the same distributed authority can construct blind signatures and then revoke blinding factors in what they call "magic ink signatures"; (this enables the tracing authority to be the signing authority by enforcing separation of duties via threshold (quorum) control).

Owner and coin tracing with off-line trustees were proposed independently by [CMS96] and [FTY96]; these schemes satisfy our requirements (1)–(6). Both schemes propose efficient modular additions to variations of the same basic off-line e-cash scheme [Bra93], which is one of the most efficient to date. The tracing protocols of [CMS96] are approximately twice as efficient as the ones in [FTY96]. However, the owner tracing of [CMS96] only provides a link to the withdrawal transcript, rather than the account-establishment of a user; thus for owner tracing the bank must perform a search on the withdrawal database, which is potentially much larger than the account database. We also note that owner and coin tracing with off-line trustees can be achieved using a recent result in verifiable secret sharing [Sta96]; however this procedure is not as efficient as the former ones.

In addition, the following alternative models have appeared in the literature. [FY94] proposed an on-line e-cash system in which a trusted entity collaborates with the bank at withdrawal to construct a weak signature (based on finite field algebra) rather than a real signature for a blinded coin, and at deposit

[7] In [BGK95] the trustee(s) is allowed to be off-line, but he is required to do some computation for each withdrawn coin; in effect the trustee can pre-compute his involvement in the withdrawal.

to verify this weak signature; the purpose of the scheme is to show a design without a digital signature computation. Tracing of coins based on this model is straightforward when the trusted entity and the bank collaborate. Note that the trustee needs to be on-line both at withdrawal and deposit. [M'R96] proposed a similar model where the trustee ("blinding office") collaborates with the bank ("certification authority") in order to simplify the computations at withdrawal; this system requires also on-line trustees and framing is possible in its plain form. To limit the efficiency impact it is proposed, as in [SPC95, CPS96], that some linkability of coins is allowed; hence the trustees are involved only when a user creates a new "pseudonym," with all the coins created by the same pseudonym being linkable; this limits full anonymity.

Lastly, [JY96] proposed a much stronger tracing model: in this the trustee ("ombudsman") has the additional power to invalidate coins and it shares a "hidden alarm channel" with the bank. Thus, in the case of a bank robbery or theft of the bank's private key (which are indeed extremely strong attacks), the thief is left with invalid coins. However, the trustee now has to be on-line in many cases: at withdrawal and, if a bank robbery is suspected, also at payment.

5 Technical Solutions

We now concentrate on efficient off-line trustees. The model is presented in detail in [FTY96]. Here we build on the results of [FTY96], but we simplify coin tracing along the lines of [CMS96]. The coin tracing protocol is new and is significantly more efficient than before. The resulting scheme is twice as efficient as [FTY96] at withdrawal while providing the same functionality. Moreover, it can be extended to a system which satisfies all our requirements from Section 2.

The basic solution of [FTY96] (which we employ here) possesses the properties of: anonymity (1), revocation (2), separation (3) and selectivity (5) are satisfied due to the underlying scheme. No framing (4) is covered if the underlying basic scheme (without the tracing) avoids framing; this is the case in Brands' [Bra93] scheme which is used as a basic protocol. To avoid framing or claims against the user or the shop we may require additional signatures on transactions (as a universal solution), which can then serve as receipts. Efficiency (6) is covered by the fact that the trustee(s) are *off-line*, i.e., they are only involved when tracing is required, and since our scheme poses minimal burden to the bank, users, shops and trustee(s), as can be seen in the detailed description below. Finally, crime prevention (7) is handled by the introduction of the notion of *Distress Cash* which we discuss how to implement in our context in the next section.

We now proceed to describe the scheme; we start with a preliminary protocol which is used as a building block.

5.1 Proving equality of logarithms

A basic tool for both owner and coin tracing is an efficient proof of equality of logarithms. Such proofs have appeared independently in [FTY96, CMS96] and

they are based on Schnorr proofs of knowledge [Sch91]. We give an informal description here.

Setup: A probabilistic polynomial-time *(p.p.t.)* prover $\mathcal{P}$ and a p.p.t. verifier $\mathcal{V}$. Common input is A, B, a, b, with a, b generators of G_q, a subgroup of prime order q of the multiplicative group Z_p^* for some large prime p.
Secret input to $\mathcal{P}$ is x, such that $A \equiv a^x \pmod p, B \equiv b^x \pmod p$ (for simplicity we henceforth use the notation $A = a^x$).
The **proof** appears in Figure 1.

$\mathcal{P}$ will prove to $\mathcal{V}$ that $\log_a A = \log_b B$:

$\mathcal{P}$		$\mathcal{V}$
$y \in_R Z_q$		
$A' = a^y, B' = b^y$		
	$\xrightarrow{A', B'}$	
		$c \in_R Z_q$
	$\xleftarrow{c}$	
$r = c \cdot x + y$	$\xrightarrow{r}$	Verify:
		$a^r \stackrel{?}{=} A^c \cdot A'$
		and $b^r \stackrel{?}{=} B^c \cdot B'$

Fig. 1. *Proof of equality of logarithms.*

The proof is essentially a set of parallel Schnorr knowledge proofs and can be used to prove equality of more than two logarithms. As is the case in [Sch91], this minimal-knowledge proof can be made non-interactive and transferable under the random oracle model with the challenge c being computed as a hash function of $\{A, A', a, B, B', b\}$ and the hash function behaving like a random oracle.

5.2 Anonymity controlled e-cash

Bank's setup protocol: (performed once by $\mathcal{B}$)
Primes p and q are chosen such that $|p - 1| = \delta + k$ for a specified constant δ and security parameter k, and $p = \gamma q + 1$, for a specified small integer γ. Then a unique subgroup G_q of prime order q of the multiplicative group Z_p^* and generators g, g_1, g_2, g_3 of G_q are defined. Secret key $X_{\mathcal{B}} \in_R Z_q$ is created.[8] Hash functions $\mathcal{H}, \mathcal{H}_0, \mathcal{H}_1, \ldots$, from a family of random oracle-like hash functions are also defined. $\mathcal{B}$ publishes $p, q, g, g_1, g_2, g_3, (\mathcal{H}, \mathcal{H}_0, \mathcal{H}_1, \ldots)$ and its public keys $h = g^{X_{\mathcal{B}}}, h_1 = g_1^{X_{\mathcal{B}}}, h_2 = g_2^{X_{\mathcal{B}}}, h_3 = g_3^{X_{\mathcal{B}}}$.

[8] We assume, for simplicity, that only one denomination is used. A different key can be used for each denomination.

Trustee's setup protocol: (performed once by $\mathcal{T}$)
Choose a private key $x_{\mathcal{T}} \in_R Z_q$ and publish the public key $f_2 = g_2^{x_{\mathcal{T}}}$.

CA establishment: A Certificate Authority for the users' public keys is established which is independent of the bank or trustees. (See [Sta95, ABAT96, Fro96a] for legal aspects of establishing a CA).

User's setup (account opening) protocol: (performed for each user $\mathcal{U}$)
The bank $\mathcal{B}$ associates user $\mathcal{U}$ with $I = g_1^{u_1}$ where $u_1 \in_R G_q$ is generated by $\mathcal{U}$ and $g_1^{u_1} g_2 \neq 1$. $\mathcal{U}$ also proves (using the Schnorr identification scheme [Sch91]) to $\mathcal{B}$ that he knows how to represent I w.r.t. g_1. The user's communication is signed by the user and is verifiable by the bank with the user's public key certificate generated by the CA.

Withdrawal: (over an authenticated channel between $\mathcal{B}$ and $\mathcal{U}$ where $\mathcal{U}$ signs its transmissions)
The withdrawal protocol creates a "restrictively blind" signature [Bra93] of I. $\mathcal{U}$ will end up with a Schnorr-type [Sch91] signature on $(Ig_2)^s g_3$, where s is a random number (chosen by $\mathcal{U}$ and kept secret). The exact form of the signature is $sig(A, B) = (z, a, b, r)$ satisfying:

$$g^r = h^{\mathcal{H}(A,B,z,a,b)} a \quad \text{and} \quad A^r = z^{\mathcal{H}(A,B,z,a,b)} b \tag{1}$$

The withdrawal protocol appears in Figure 2.

Payment: (performed between $\mathcal{U}$ and $\mathcal{S}$ over an anonymous channel)
At payment time $\mathcal{U}$ supplies information to the shop $\mathcal{S}$ (which is later forwarded to the bank) so that if a coin is double-spent the user $\mathcal{U}$ is identified. If the framing requirement demands a proof of purchase, then it suffices to add the description of the purchased goods in the challenge: $d = \mathcal{H}_1(A_1, B_1, A_2, B_2, I_{\mathcal{S}},$ date/time, item(s) purchased). This proof can be used by both the shop and the user. For the shop's framing protection (i.e., preventing a user from making a fictitious purchase) the shop's signature must be included in, e.g., $I_{\mathcal{S}}$.
The payment protocol appears in Figure 3.

The security of this scheme depends on the Brands scheme [Bra93] on which it is based, and on the *Matching Diffie-Hellman* assumption introduced in [FTY96] for a similar protocol. Its efficiency is apparent as it requires only a few more steps than [Bra93] at withdrawal.

Coin tracing Tracing of coins is straightforward: the bank sends to the trustee a transcript of a withdrawal protocol. Similar to [CMS96], the trustee computes

$$A_2'^{(x_{\mathcal{T}}^{-1})} = g_2^s = A_2 \ ,$$

and sends it back to the bank; the bank can then trace the coin originating from this withdrawal since A_2 appears at payment/deposit.

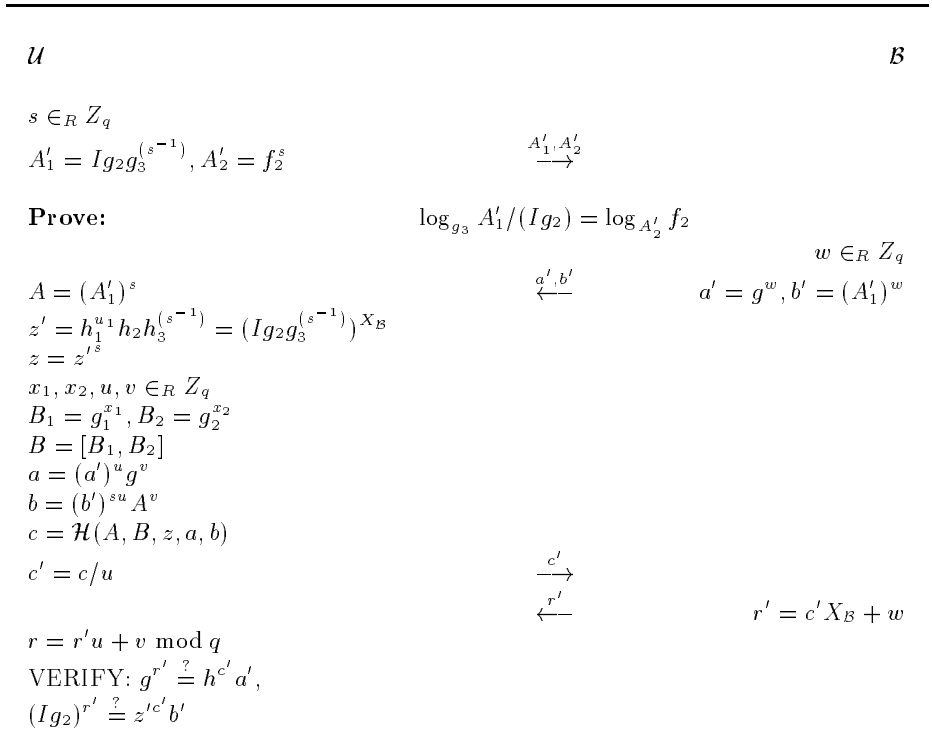

Fig. 2. *The withdrawal protocol.*

Owner tracing Although owner tracing to the withdrawal database (as in [CPS96, CMS96]) is quite straightforward (similar to [CMS96] the trustee needs to calculate $A_2^{x_\mathcal{T}} = A_2'$) we instead adopt the method of [FTY96] as it allows tracing via a smaller search (i.e., on the account database rather then the withdrawal database) while adding only a small amount of computation at payment. One of the things we would like to emphasize is this difference in search requirements: the account data base is typically much smaller than the withdrawal one. The coin in [FTY96] is the same as here, except from A which is only a product of A_1, A_2: $A = A_1 \cdot A_2$. Hence the owner tracing protocol is directly applicable to our scheme (full description is in [FTY96]).

At payment the user $\mathcal{U}$ constructs an El-Gamal encryption of his identity I based on the trustee's public key f_2, and proves to the shop $\mathcal{S}$ that (1) the encryption is based on the trustee's key and (2) it encrypts the same identity as the one in the coin. The tool used here is an *indirect discourse proof*. However, this proof is non-transferable, hence the user must also prove the equality of a few logarithms to the shop. The necessary additions to the payment protocol are shown in Figure 4.

This protocol only adds 11 exponentiations for the user and shop. Further-

$\mathcal{U}$			$\mathcal{S}$
$A_1 = g_1^{u_1 s}$			
$A_2 = g_2^s$	[1]	$\xrightarrow{A_1, A_2, A, B_1, B_2, (z,a,b,r)}$	$A \stackrel{?}{=} A_1 A_2 g_3,\ A/g_3 \stackrel{?}{\neq} 1$
			$sig(A,B) \stackrel{?}{=} (z,a,b,r)$
$r_1 = d(u_1 s) + x_1$	[2]	$\xleftarrow{d}$	$d = \mathcal{H}_1(A_1, B_1, A_2, B_2, I_S, \text{date/time})$
$r_2 = ds + x_2$			
	[3]	$\xrightarrow{r_1, r_2}$	$g_1^{r_1} \stackrel{?}{=} A_1^d B_1$
			$g_2^{r_2} \stackrel{?}{=} A_2^d B_2$

Fig. 3. *The payment protocol ($\mathcal{U}$ and $\mathcal{S}$ agree on date/time).*

$\mathcal{U}$			$\mathcal{S}$
$m \in_R Z_q$			
$D_1 = I g_2^{X_\mathcal{T}\ m}, D_2 = g_2^m,$			
$D_\mathcal{T} = D_1^s$			
$E_1 = A_1 h_2^{m s}, E_2 = g_2^{m s}$	[1′]	$\xrightarrow{D_1, D_2, D_\mathcal{T}, E_1, E_2}$	$D_2 \stackrel{?}{\neq} 1$
Prove:		$\log_{g_2}(A_2) = \log_{D_2}(E_2) = \log_{D_1}(D_\mathcal{T})$	
		$\log_{h_2/f_2}(E_1/D_\mathcal{T}) = \log_{g_2}(E_2)$	
			$s_0, s_1, s_2 \in_R Z_q$
			$D' = {D_1}^{s_0} g_2^{s_1} {D_2}^{s_2}$
	[2′]	$\xleftarrow{D', f_2'}$	$f_2' = {f_2}^{s_0} g_2^{s_2}$
$V = \mathcal{H}_1((D')^s/(f_2')^{m s})$	[3′]	$\xrightarrow{V}$	$V \stackrel{?}{=} \mathcal{H}_1(A_1^{s_0} A_2^{s_1})$

Fig. 4. *Additions to the payment protocol for owner tracing. (i.e., $[i]+[i']$ is new flow i in the payment protocol.)*

more, since the indirect discourse proof is non-transferable, at deposit only the proof of equality of logarithms is given; hence the bank needs to perform only 8 exponentiations, plus one for the decryption of (E_1, E_2). The protocol's security is discussed in detail in [FTY96].

6 Distress Cash

As mentioned in the introduction, traceability may force a criminal to social engineer a crime in order to bypass some of the protection mechanisms. For instance, with e-cash there is the concern that a criminal may kill or kidnap a victim if coin tracing is used. The reason is that the criminal wants a long

delay between the time he spends the e-cash and when the tracing is performed. Hence, if the criminal murders the user, the criminal may extend the amount of time he can spend the e-cash.

The solution to this problem that we suggest uses a covert or subliminal channel during withdrawal. A channel potentially embedded in the user authentication protocol is incorporated so that a signal of distress is transmitted to the bank when the user needs to flag the bank. We suggest that the authentication protocol be preferably embedded in a smart-card, or some other tamper resistant device, and the user will have two personal identification numbers (PINs) to activate the device. One PIN for normal operation and the other PIN to send a distress message via the subliminal (or covert) channel.

One can think of this solution as similar to the prisoner dilemma problem of Simmons where two prisoners coordinate an alibi via channels hidden in signature schemes applied to messages that the warden inspects but cannot trace [Sim84]. The user and bank are "prisoners" and the criminal is the "warden". The user can then transmit a signal in its authentication channel which remains hidden from the criminal. If the withdrawal protocol includes the user's signature, as has been proposed for our implementation, then a subliminal channel can be employed there to signal distress and activate the tracing.

7 Conclusion

We have proposed that anonymity should and can be controlled in e-cash systems. We have pointed out various law enforcement and regulatory issues and presented requirements for anonymity controlled e-cash. We also discussed the issue of distress cash as a crime prevention mechanism. We believe that flexible crime prevention and regulation compliance mechanisms, as presented here, will ease the deployment of e-cash systems without compromising anonymity for honest users.

Acknowledgements: We would like to thank Agnes Chan for valuable comments and discussions.

References

[ABAT96] Information Security Committee of the Section on Science American Bar Association and Technology. Draft digital signature guidelines, January 1996. Available online at http://www.state.ut.us/ccjj/digsig/dsut-gl.htm The guidelines are currently being revised.

[BGK95] E. F. Brickell, P. Gemmell, and D. Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Symposium on Distributed Algorithms (SODA)*, Albuquerque, NM, 1995. Available at http://www.cs.sandia.gov/~psgemme/.

[Bra93] S. Brands. Untraceable off-line cash in wallets with observers. In *Advances in Cryptology — Crypto '93, Proceedings (Lecture Notes in Computer Science 773)*, pages 302–318. Springer-Verlag, 1993. Available at http://www.cwi.nl/ftp/brands/crypto93.ps.Z.

[CFMT96] A. Chan, Y. Frankel, P. MacKenzie, and Y. Tsiounis. Mis-representation of identities in e-cash schemes and how to prevent it. In *Advances in Cryptology — Proceedings of Asiacrypt '96 (Lecture Notes in Computer Science 1163)*, pages 276–285, Kyongju, South Korea, November 3–7 1996. Springer-Verlag. Available at http://www.ccs.neu.edu/home/yiannis/pubs.html.

[CFN90] D. Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *Advances in Cryptology —Crypto '88 (Lecture Notes in Computer Science)*, pages 319–327. Springer-Verlag, 1990.

[Cha83] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology. Proc. Crypto'82*, pages 199–203, Santa Barbara, 1983. Plenum Press N. Y.

[CMS96] J. Camenisch, U. Maurer, and M. Stadler. Digital payment systems with passive anonymity-revoking trustees. In *Esorics '96*, Italy, 1996. To appear. Available at http://www.inf.ethz.ch/personal/camenisc/publications.html.

[CP93a] D. Chaum and T.P. Pedersen. Transferred cash grows in size. In *Advances in Cryptology — Eurocrypt '92, Proceedings (Lecture Notes in Computer Science 658)*, pages 390–407. Springer-Verlag, 1993.

[CP93b] D. Chaum and T.P. Pedersen. Wallet databases with observers. In E. Brickell, editor, *Advances in Cryptology — Crypto '92, Proceedings (Lecture Notes in Computer Science)*, pages 90–106. Springer-Verlag, New York, 1993. Santa Barbara, California.

[CP93c] R. Cramer and T. Pedersen. Improved privacy in wallets with observers. In *Advances in Cryptology: Eurocrypt '93, Proceedings (Lecture Notes in Computer Science 765)*, pages 329–343. Springer-Verlag, 1993.

[CPS96] J. Camenisch, J. M. Piveteau, and M. Stadler. An efficient fair payment system. *ACM-CCS*, March 1996.

[DC94] S. D'amingo and G. Di Crescenzo. Methodology for digital money based on general cryptographic tools. In *Advances in Cryptology, Proc. of Eurocrypt '94*, pages 157–170. Springer-Verlag, 1994. Italy, 1994.

[EO94] T. Eng and T. Okamoto. Single-term divisible electronic coins. In *Advances in Cryptology — Eurocrypt '94, Proceedings*, pages 306 – 319, New York, 1994. Springer-Verlag.

[Fer93] N. Ferguson. Single term off-line coins. Technical Report CS–R9318, CWI (Centre for Mathematics and Computer Science), Amsterdam, 1993. Anonymous ftp: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9318.ps.Z.

[Fro96a] A. M. Froomkin. The essential role of trusted third parties in electronic commerce, October 14 1996. Available on-line at http://www.law.cornell.edu/jol/froomkin.html.

[Fro96b] A. M. Froomkin. Flood control on the information ocean: living with anonymity, digital cash, and distributed databases, 1996. Available on-line at http://www.law.cornell.edu/jol/froomkin.html.

[FTY96] Y. Frankel, Y. Tsiounis, and M. Yung. Indirect discourse proofs: achieving fair off-line e-cash. In *Advances in Cryptology, Proc. of Asiacrypt '96 (Lecture Notes in Computer Science 1163)*, pages 286–300, Kyongju, South Korea, November 3–7 1996. Springer-Verlag. International patent pending. Available at http://www.ccs.neu.edu/home/yiannis/pubs.html.

[FY93] M. Franklin and M. Yung. Secure and efficient off-line digital money. In *Proceedings of the twentieth International Colloquium on Automata, Languages and Programming (ICALP 1993), (Lecture Notes in Computer Science 700)*, pages 265–276. Springer-Verlag, 1993. Lund, Sweden, July 1993.

[FY94] M. Franklin and M. Yung. Blind weak signature and its applications: Putting non-cryptographic computation to work. In *Advances in Cryptology, Proc. of Eurocrypt 94, (Lecture Notes in Computer Science), Springer-Verlag*, pages 71–83, Perugia, Italy, May 9–12, 1994.

[JY96] M. Jakobson and M. Yung. Revokable and versatile e-money. In *Proceedings of the third annual ACM Symp. on Computer and Communication Security*, March 1996.

[JY97] M. Jakobson and M. Yung. Distributed "magic ink" signatures. In *Proceedings of Eurocrypt 97 (Lecture Notes in Computer Science), Springer-Verlag* May 1997.

[LSS96] L. Law, S. Sabett, and J. Solinas. How to make a mint: the cryptography of anonymous electronic cash. No. 96-10-17, National Security Agency, Office of Information Security Research and Technology, Cryptology Division, June 18 1996. For a copy e-mail to 21stCen@ffhsj.com or call at (202) 639-7200. See also the 21st Century Banking Alert page at URL: http://www.ffhsj.com/bancmail/bancpage.html.

[M'R96] D. M'Raïhi. Cost-effective payment schemes with privacy regulation. In *Advances in Cryptology. Proc. of Asiacrypt '96 (Lecture Notes in Computer Science 1163)*, Kyongju, South Korea, November 3–7 1996. Springer-Verlag.

[Oka95] T. Okamoto. An efficient divisible electronic cash scheme. In Don Coppersmith, editor, *Advances in Cryptology, Proc. of Crypto '95 (Lecture Notes in Computer Science 963)*, pages 438–451. Springer-Verlag, 1995. Santa Barbara, California, U.S.A., August 27–31.

[OO92] T. Okamoto and K. Ohta. Universal electronic cash. In *Advances in Cryptology — Crypto '91 (Lecture Notes in Computer Science)*, pages 324–337. Springer-Verlag, 1992.

[Pai93] J. C. Pailles. New protocols for electronic money. In *Proceedings of Ausicrypt '92*, pages 263–274, 1993.

[PW92] B. Pfitzmann and M. Waidner. How to break and repair a 'provably secure' untraceable payment system. In J. Feigenbaum, editor, *Advances in Cryptology, Proc. of Crypto '91 (Lecture Notes in Computer Science 576)*, pages 338–350. Springer-Verlag, 1992.

[Sch91] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[Sim84] G. J. Simmons. The prisoners' problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology. Proc. of Crypto 83*, pages 51–67. Plenum Press N.Y., 1984. Santa Barbara, California, August 1983.

[Sim96] D. Simon. Anonymous communication and anonymous cash. In Neal Koblitz, editor, *Advances in Cryptology, Proc. of Crypto '96 (Lecture Notes in Computer Science 1109)*, pages 61–73, Santa Barbara, California, August 1996. Springer-Verlag.

[SPC95] M. Stadler, J. M. Piveteau, and J. Camenisch. Fair blind signatures. In *Advances in Cryptology, Proc. of Eurocrypt '95*, pages 209–219. Springer-Verlag, 1995.

[Sta95] Utah State. Digital signature act. Utah code ann. tit. 46, ch. 3, 1995. Amended in 1996. Digital Signature Act Amendments, 52nd

Leg., Gen. Sess., 1996 Utah Laws 188 (to be codified at Utah Code Ann. tit. 46, ch. 3). History and Current Status are available online at http://www.state.ut.us/ccjj/digsig/dsut-int.htm.

[Sta96] M. Stadler. Publicly verifiable secret sharing. In *Advances in Cryptology, Proc. of Eurocrypt '96*, pages 190–199. Springer-Verlag, 1996.

[Tsi97] Y. Tsiounis. *Efficient Electronic Cash: New Notions and Techniques*. PhD thesis, College of Computer Science, Northeastern University, Boston, MA, 1997. See http://www.ccs.neu.edu/home/yiannis for information on availability.

[vSN92] B. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers and Security*, 11(6):581–583, October 1992.

This article was processed using the LaTeX macro package with LLNCS style