On Anonymous Electronic Cash and Crime

Tomas Sander and Amnon Ta–Shma

International Computer Science Institute
1947 Center Street, Berkeley, CA 94704, USA
{sander,amnon}@icsi.berkeley.edu

Abstract. Anonymous electronic cash systems can be vulnerable to criminal abuse. Two approaches were suggested for solving this problem. In an escrowed cash system users are given anonymity which can be lifted by trustees. In an amount–limited system each user enjoys unconditional anonymity but only for payments up to a limited amount during a given time-frame. In this paper we discuss the two approaches.

1 Introduction

The Problem. In 1982 David Chaum [3] showed how to build an anonymous electronic cash system by devising blind signature schemes. Chaum's scheme is provably anonymous: even an all powerful agent that collaborates with the bank and any coalition of the users can not link payments to withdrawals, i.e. payers enjoy unconditional anonymity. In 1992 van Solms and Naccache [13] discovered a serious attack on Chaum's payment system. Blackmailers could commit a "perfect" blackmailing crime by using anonymous communication channels and anonymous ecash. Following that, further concerns were raised, e.g., it was argued that the ability to move money around anonymously at the speed of light may facilitate money laundering activities and tax evasion.
Escrowed Cash. These concerns stimulated a whole line of research of, so called, escrowed cash systems In escrowed systems payment transactions look anonymous from the outside (to users, merchants, banks), while Trustees are able to revoke the anonymity of each individual payment transaction.
Does Escrowed Cash Solve the Problem? We describe several weaknesses of escrowed cash in Section 2. We demonstrate that using some simple tricks criminals may still be able to hide their suspicious activities in an escrowed system in a way that is hard to detect. We further argue that escrowed cash is not a natural solution to some of the major attacks on electronic cash systems (blackmailing and bank robbery) that, in our opinion, are caused *not* by the anonymity feature but rather stem from the fact that most anonymous cash systems are implemented using signature based schemes. Finally, from the honest user's point of view escrowed cash might be undesirable, as no user can ever be sure of his privacy.
An Alternative Approach. We then discuss in Section 3 a different approach that was suggested by us in [11, 10]. We conclude in Section 4.

M. Mambo, Y. Zheng (Eds.): ISW'99, LNCS 1729, pp. 202–206, 1999.

2 Weaknesses in Escrowed Cash Systems

Revoking Anonymity Only Under Suspicion. In the U.S. the banking system has to report any cash transaction above $10,000 to law enforcement agencies. These high value payment activities are then monitored for "suspicious" transactions. According to FinCEN monitoring high volume transactions is an important and essential tool for *triggering suspicion* and fighting crime. On the other hand, in escrowed cash systems anonymity should be revoked only under suspicion and thus the order of suspicion and monitoring is reversed. It seems that the current proposed schemes for escrowed cash are in this respect much weaker then techniques currently used in fighting financial crimes today.

Issuer Attacks. In many offline or escrowed cash systems a payee can deposit received coins only back into the bank, unless he has some additional knowledge of a secret known to the payer (e.g. double spending related). We give an example of an issuer related attack in which a bank cooperates with a drug dealer L. L has received a large amount of electronic money (e.g. stemming from drug sales) in a currency issued from this bank that he does not want to deposit into his bank account to avoid being questioned about its origin by agencies monitoring account activities. Instead of depositing the payment transcripts into his account he exchanges the payment records secretly against fresh, unreported coins of the electronic cash issuer. Thus L has received spendable electronic money in return for his payment transcripts. From the bank's point of view the balance is preserved. In (non-escrowed) offline systems the transaction is almost riskless for the bank [1]. Such transactions become more risky and difficult if the bank has to keep a publicly verifiable and complete whitelist of withdrawal transcripts [2].

Blackmailing and Signature-Based Systems. In the blackmailing attack [13], the attacker forces the bank to issue valid coins via anonymous communication channels that are indistinguishable from valid coins, and thus can not be later recognized by the bank as stemming from a crime. In the bank robbery attack [7], the secret key the bank uses for signing coins is stolen, and the attacker issues valid unreported money. While the attacks use the anonymity feature of the system, the anonymity feature by itself is not enough for the attacks to work. This is obvious, e.g., with the bank robbery attack, where the attack assumes the bank has a secret key for signing coins. We believe that these attacks show the vulnerability of blind-signature based schemes, rather than of anonymous schemes in general.

Some papers [7, 4, 9, 6] suggested to use the escrow features for detecting such an attack when it goes on, or for fixing it later on, but not for preventing it efficiently altogether. However, even detection is not easy in escrowed cash systems, and [6] claim to be the first(!) to provide detection at a very early stage

[1] Even double spending risks are small, as the bank can always move some of the payment transcripts received from L into its official database, and then the double spender can be detected as usual.

[2] See [1, 5] for reports on laundering activities that involved the (sometimes unintentional) cooperation of financial institutions.

that a bank key has been compromised. Fixing the situation usually requires the system to move to an on-line mode and many times requires rebuilding of the whole system. Many systems (but not e.g. [6]) also have the additional unpleasant feature that fixing the system requires lifting the anonymity of all users and coins. Instead of seeing this as a motivation for escrowed cash one may conclude that blind–signature based techniques might not be well suited for anonymous electronic cash.

The Colombian Black Market Exchange. Here we describe a weakness that is due to the fact that money is *transferable*. The attack already exists in completely non-anonymous systems. It seems also to exist in escrowed cash systems.

The so called "Colombian Black Market Peso Exchange" is described in the FATF 1997-1998 Report on Money Laundering Typologies [2] as an "example of a widely used money laundering technique". Its goal is that drug traffickers in the U.S. want to transfer profits from drug sales to Colombia. Simplified it can be described as follows [3]. Colombians residing in or visiting the U.S. open several personal check accounts at U.S. banks. The customers sign blank checks for these accounts and give them to the drug cartels. Then drug money in low amounts is transferred to these accounts. Later a dollar amount is entered into the check but the name of the payee is left blank. These checks are later sold in Colombia to Colombian business men who need dollars to conduct business in the U.S. at a discounted rate for Pesos. The Colombian businessman fill in the payees name and can use the checks for payment. It is important to notice that the attack works even in a completely non-anonymous environment, like checks and U.S. bank accounts. The crux of the attack is that the checks can be made *transferable*.

3 An Alternative Approach

A different approach to limit potential abuses of anonymous electronic cash systems was suggested by the authors in [11, 10]. We observe:

- Financial transactions that use the banking system as an intermediary are easier to monitor. This monitoring has been described as an important tool against money laundering. Banks are closely and regularly monitored to ensure safety and soundness of the financial system.
- Law enforcement agencies are interested in large value transactions. Small value transactions are usually not monitored.

We define the following (technical) requirements for electronic cash systems:

1. **Amount-Limited Anonymity.** [11] Each user can anonymously spend only a fixed amount, say $ 10,000 a year, and transactions exceeding this amount do not enjoy the anonymity protection.
2. **Non-transferability.** [11] Only the user who withdraws a coin can make a payment with it. The payee can only deposit the coin back into the bank.

[3] cf also [12] for a detailed presentation of this attack.

3. **Auditability**. [10] There should be a one-to-one correspondence between withdrawal records and valid coins.

Non-transferability. The example of the "Colombian Black Market Peso Exchange" attack makes direct use of checks with blank payee that can be obtained by one person and used for payment by another, i.e. of the transferability feature of checks (resp. electronic cash). It seems that a non-transferable system is not vulnerable to this attack. [4]

Amount–Limited Anonymity. Financial crimes typically involve large amounts of money. Thus, it is a natural approach to limit the amount of anonymous electronic cash that users (and criminals) can obtain. This can be achieved by limiting the amount of anonymous electronic cash each user can obtain in a *non-transferable* system. We observe that the non-transferability requirement is essential; in a transferable system criminal organizations may obtain electronic cash in large amounts by buying it from other users.

Auditability. To protect against issuer related attacks it is desirable to have an electronic cash system in which the *money supply* can be closely monitored, and issuers can not secretely issue electronic coins. The auditable system in [10] is not based on "blind signatures" but on the primitive of "blind auditable membership proofs". In this system, the security of the system does not rely on the secrecy of secret keys of the bank, but on the bank's ability to maintain the integrity of a *public* database. As a result, it is no longer vulnerable to the bank robbery attack. Furthermore, there is no way to force the bank to issue coins in the system [10], that can not be invalidated, a property that is important for defending against blackmailing of the bank.

4 Conclusions

Starting with [13] several potential abuses of completely anonymous electronic cash systems were found. Escrowed cash was introduced to solve this problem. We believe that escrowed cash systems, at least partially, do not live up to this goal. We have pointed out several weaknesses in escrowed cash systems.

- Escrowed cash systems are hard to secure against the blackmailing and the bank robbery attack.
- Escrowed cash systems do not per se address issuer related attacks.
- Black markets and exchanges may effectively circumvent tracing.
- Escrowed cash does not effectively *find* suspicious activities and law enforcement may be harder than today.

One way to solve these problems is, in our opinion, by using auditability to solve issuer related attacks, blackmailing and bank robbery, and non-transferability and amount-limitedness to address money-laundering and tax evasions. Furthermore, our solution guarantees users provable, unconditional

[4] Another case where non-transferability can be useful is for the implementation of the so called Geographic Targeting Order. See [1, 8].

anonymity. Yet, users are limited in the amount of anonymous electronic coins they can use per time frame and they can not transfer their anonymous money.

Chaum showed that modern cryptography makes unconditionally anonymous electronic cash possible. On the other hand, completely anonymous electronic cash systems might be abused for unlawful activities. Thus, one should first determine whether he/she finds these abuses threatening enough to require a solution. It seems that if one wants to address these possible abuses, one needs to make some kind of a compromise. This raises two questions. First, do we prevent these abuses by making the compromise? and second, what is the price we pay for the compromise? Comparing the escrowed cash approach and our approach with regard to the second question, one could ask oneself what is better: "unlimited amounts of money with revokable anonymity" or "limited amounts of money with unconditional anonymity".

Some aspects of the solution we suggest in [10] are only theoretically efficient but not yet practical. It would be interesting to see a practical and privacy friendly implementation of these ideas.

References

[1] FATF-VII report on money laundering typologies, August 1996. http://www.treas.gov/fincen/pubs.html.
[2] FATF-IX report on money laundering typologies, Febuary 1998. http://www.ustreas.gov/fincen/typo97en.html.
[3] David Chaum. Blind signatures for untraceable payments. In *Crypto 82*, pages 199–203, 1982.
[4] E. Fujisaki and T. Okamoto. Practical escrow cash system. *Lecture Notes in Computer Science*, 1189, 1997.
[5] General Accounting Office (GAO). Private banking: Raul Salinas, Citibank, and alleged money laundering. GAO/OSI-99-1, December 1998. http://www.gao.gov/monthly.list/dec98/dec9811.htm.
[6] M. Jakobsson and J. Muller. Improved magic ink signatures using hints. In *Financial Cryptography*, 1999.
[7] M. Jakobsson and M. Yung. Revokable and versatile electronic mony. In *3rd ACM Conference on Computer and Communications Security*, pages 76–87, 1996.
[8] R.C. Molander, D.A. Mussington, and P. Wilson. Cyberpayments and money laundering. RAND, 1998. http://www.rand.org/publications/MR/MR965/MR965.pdf/.
[9] H. Peterson and G. Poupard. Efficient scalable fair cash with off-line extortion prevention. *Lecture Notes in Computer Science*, 1334, 1997.
[10] T. Sander and A. Ta-Shma. Auditable, anonymous electronic cash. In *Crypto*, 1999.
[11] T. Sander and A. Ta-Shma. A new approach for anonymity control in electronic cash systems. In *Financial Cryptography*, 1999.
[12] Bonni G. Tischler. The Colombian black market Peso exchange. Testimony before the Senate Caucus on International Narcotics Control, June 1999. http://jya.com/bmpe062199.htm.
[13] S. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers and Security*, 11(6):581–583, October 1992.