An Anonymous and Undeniable Payment Scheme

Liqun Chen[†1] and Chris J. Mitchell[‡]
[†] Hewlett-Packard Labs. Bristol, UK. liqun@hplb.hpl.hp.com
[‡] Royal Holloway, University of London, UK. cjm@dcs.rhbnc.ac.uk

Abstract. At Asiacrypt 1996, M'Raihi presented an electronic payment scheme using a blinding office to achieve anonymity. This scheme allows both a bank and blinding office to impersonate a user without being detected. It may result in a denial problem where the user can deny his bad behaviour by suggesting that either the bank or the blinding office did wrong. This paper proposes a variant of the M'Raihi scheme to prevent the bank and blinding office from impersonating the user, so that the user cannot deny it if he abuses a coin himself.

1 Introduction

In electronic payment systems there are likely to be two contradictory Requirements. On the one hand users want to have *anonymous* electronic cash, and on the other hand banks have requirements to ensure the electronic cash cannot be misused. For instance, if abuse (e.g. over-spending) is suspected, the related user's identity should be *traceable*. Some recent research has made use of blind signature and escrow-like techniques to design a payment scheme, which meets the requirements of both the users and banks, e.g. [4, 5].

M'Raihi [7], at Asiacrypt 1996, presented a payment scheme using a Blinding Office (BO) as a pseudo-identity escrow agency. This protocol relies on the assumption of strong trust relationships among a User (U), Bank (BA) and BO, because both BA and BO can impersonate U without being detected. A potential problem resulting from these trust relationships is that U can deny his bad behaviour by claiming no longer to trust either BA or BO. In this case it is difficult for an impartial Judge (J) to arbitrate amongst the three parties.

In this paper we introduce an extra requirement in the M'Raihi scheme: *non-denial*, which, if it holds, will enable J to determine who is lying: U, BA or BO. This requirement has been met in a number of other payment schemes, e.g. [3]. We then present a modification of the M'Raihi scheme to offer the three properties of *anonymity*, *traceability* and *non-denial*. The main advantage of the new scheme is in preventing BA and BO from impersonating U, so that U cannot deny that he has misused a coin himself.

2 An electronic payment model

In this section we describe a general electronic payment model which is suitable for both the M'Raihi scheme and our modified one. It consists of five participants, i.e., U, BA, BO, a Shop (S) and J.

Briefly, this electronic payment model works as follows. U gets a coin (C) blindly signed by BA. BA retains a relationship-proof between U's real identifier

[1] Part of the first author's work was funded by the European Commission under ACTS project AC095 (ASPeCT) when she worked in Royal Holloway, University of London.

(ID) and pseudo identifier (PID). BO, involved in the blind signature, maintains another relationship-proof between PID and C. To spend C, U proves to S that he has knowledge of a private key x corresponding to C. If C is abused, e.g. if it is over-spent, BA and BO will collaborate to build a link between ID and C. J will be involved in this tracing procedure to arbitrate.

We suppose that both BA and U have public-key based signature schemes, respectively named (S_{BA}, V_{BA}) and (S_U, V_U), where V_{BA} is known to U, BO and S, and V_U is known to BA. We also suppose that BO has a public-key based encryption scheme, named (E_{BO}, D_{BO}), where E_{BO} is known to U and BA. All the schemes can be verified by J. A possible implementation for these asymmetric cryptographic schemes is RSA [8].

We assume that the coin C consists of three components. The first is the public verification key y for a public-key based signature scheme, where the corresponding private signature key is denoted by x. The second is a data field D containing certain relevant information about C, such as its expiry date and value. The third is BA's signature on both y and D. There are two different ways of including D in BA's signature. Firstly D can be concatenated with y by BO, prior to computing a blinded public key denoted by $\hat{y}$. Secondly D can be 'added' by BA by using a different signature key depending on the data which is to be indicated. In the subsequent discussion in this paper we ignore this distinction, and assume that either may be used.

We actually require the signature scheme of the bank to have certain special property, i.e., $S_{BA}(z_1)S_{BA}(z_2) = S_{BA}(z_1 z_2)$, which holds for RSA. Of course this is normally a most undesirable feature for a signature scheme, and is one reason why RSA should, in normal circumstances, always be used in conjunction with a one-way hash-function or a special 'redundancy' function (such as that specified in ISO/IEC 9796 [2]). In our case, we either explicitly specify the use of a one-way hash-function (denoted by $H(z)$ for message z) with S_{BA}, or prevent frauds resulting from the use of 'straight' RSA by other means. We denote a blinding function by F, and let it be an 'inverse' of the signature function, so that $S_{BA}(F(z_1)z_2) = z_1 S_{BA}(z_2)$ for any z_1, z_2. If BA's signature scheme is RSA, then F is simply exponentiation using the public verification exponent.

Note also that we do not make a similar assumption for the user's signature scheme used in spending a coin. In fact, if DSA, [1], is used for this signature scheme, the user's computational load can be significantly reduced through pre-computations.

3 Outline of the M'Raihi scheme

The M'Raihi scheme works as follows. U and BA first establish a shared secret s. BA then signs a collision-free one-way function of s, i.e. $S_{BA}(H(s))$, which is used to construct PID by concatenating with $E_{BO}(s)$. BA also retains a relationship-proof between ID and s, which we denote by $\{ID, s\}$. It, for example, is a signature on $H(s)$ using S_U. To withdraw C, U shows BO both PID and x which is generated by U. BO computes a corresponding y and a set of pre-computed values (which is used for reducing the computation of U's

signature used in spending C). BO then blinds y with a random blinding factor v to obtain $\hat{y} = F(v)y$. BA signs $\hat{y}$ without knowing y and withdraws a real coin from U's account. BO derives C from BA's signature on $\hat{y}$ and gives it to U. BO maintains a relationship-proof between PID and C, which we denote by $\{PID, C\}$. To spend C, U signs a message, which is generated by S as a challenge, to prove U knows x. S claims a real coin back from BA later. If C is over-spent, BA will ask for a tracing procedure in which BA and BO collaborate to build a link between C and ID, based on $\{ID, s\}$ and $\{PID, C\}$.

As mentioned earlier, this scheme relies on strong trust relationships amongst U, BA and BO. Both BA and BO must be trusted not to impersonate U to obtain and spend C, since they are capable of doing so if they wish. During a tracing procedure, U can make one or more of the following claims to J to suggest that BA and/or BO has been impersonating U.

Claim 1. *BA can impersonate U to BO to obtain C, and is then able to impersonate U to S to spend C.* This holds because BA knows s.

Claim 2. *BO can impersonate U to spend C.* It holds because BO knows x.

Claim 3. *BO can cheat BA and U to obtain more than one coin from a single delegating blind signature.* It can be shown in the following one possible implementation example.

Suppose that BA's signature scheme is RSA, in which BA's private signature key is d and public verification key is (e, n). That is, BA's signature on a message z is defined as $S_{BA}(z) = z^d \bmod n$, and the corresponding blinding function of the blinding factor v is $F(v) = v^e \bmod n$. Suppose also that the signature scheme used in spending C is DSA, in which the private signature key is x and its corresponding public verification key is $y = g^x \bmod p$. The meaning of d, e and n in RSA and x, y, g and p in DSA follows [8] and [1] respectively.

If BO wants to obtain m different coins from one blind signature, he chooses $v = v_1(g^{m-1} \bmod p)$, where v_1 is a random number, and computes

$$\hat{y} = (v_1^e \bmod n)((g^{m-1} \bmod p)^e \bmod n)y.$$

After obtaining $S_{BA}(\hat{y})$, he unblinds it by using different blinding factors $(v_1 \cdot g^{m-1-i} \bmod p,\ i = 0, 1, ..., m-1)$ as follows:

$$\begin{aligned} S_{BA}(\hat{y}) &= v_1(g^{m-1} \bmod p)((g^x \bmod p)^d \bmod n) \\ &= v_1(g^{m-1-i} \bmod p)((g^{(x+ie)} \bmod p)^d \bmod n). \end{aligned}$$

Following the M'Raihi scheme, U obtains one pair of private and public keys $(x, y = g^x \bmod p)$, and BO obtains a set of key pairs $(x_i = x + ie,\ y_i = g^{x+ie} \bmod p,\ 0 \le i \le m-1)$. Each key pair is relevant to a valid coin.

4 A new scheme

The new scheme has the following three differences from the M'Raihi one.

- $\diamond$ BO does not know x, and hence is not able to spend C.
- $\diamond$ U and BO jointly generate a random v. It ensures that neither U nor BO can individually control the value of v, and hence neither U nor BO can obtain more than one coin from a single blind signature.
- $\diamond$ BA retains U's signature on $\hat{y}$ as a relationship-proof between ID and $\hat{y}$, denoted by $\{ID, \hat{y}\}$. It ensures that BA and U cannot dispute whom x was

issued by. Note that in the M'Raihi scheme, although BA can record ID with $\hat{y}$, it is still possible for U to refuse the responsibility for C because he has no idea about the relationship between y and $\hat{y}$ when making a contribution to this record, in other words, because he was blinded as well.

In the new scheme, the procedure of withdrawing a coin works as follows, where all messages exchanged between U and BO are assumed to be encrypted with s if the communication channels between them are unprotected.

1. U randomly chooses x, computes y, and then sends $E_{BO}(y)$ to BO.
2. U and BO establish a shared v, e.g. using Diffie-Hellman algorithm [6].
3. BO then computes $\hat{y} = F(v)y$ and sends it to U.
4. U verifies $\hat{y}$, and then sends BA a message signed using S_U. This message is made up of s, $\hat{y}$, BO's name and (possibly) other application data, such as a nonce and/or a time-stamp, to ensure that the uniqueness and freshness of the signature is verifiable.
5. BA retains the U's signature, withdraws a real coin from U's account, and then replies to U with $T = E_{BO}(S_{BA}(\hat{y}))$.
6. U passes T to BO.
7. BO decrypts T to obtain $S_{BA}(\hat{y})$, unblinds $S_{BA}(y)$ to construct C, and then sends C to U. After that, BO stores $\{PID, C\}$, which consists of a record of PID and two encryption values, i.e. the encryption of $E_{BO}(y)$ with s and the encryption of T with s.

We now sketch the proofs that the new scheme holds the following security properties. Unless giving a specific indication, we suppose that all participants, U, BA, BO, S and J, do not collude with each other.

Theorem 1. *U cannot obtain C without the involvement of BA and BO.*

Proof sketch. In order to obtain C without BA and/or BO being involved, U must invert either BA's signature function S_{BA} or BO's decryption function D_{BO}, both of which are assumed to be infeasible. □

Theorem 2. *A valid coin relevant to a private key x can only be spent by the participant who is the issuer of x.*

Proof sketch. Assume that given y and other related public information, it is computationally infeasible to recover x, e.g. based on the discrete logarithm problem. Following the scheme, x is known only to its issuer and is not revealed to anyone else. Thus, the issuer of x is the only person able to spend C. □

Theorem 3. *BO cannot impersonate U to either BA or S.*

Proof sketch. To impersonate U to BA, BO must invert U's signature function S_U, which is assumed to be infeasible. To impersonate U to S for spending C, BO must know both C and x. Since U is able to verify $\hat{y}$, BO cannot blind U and then obtain BA's signature on $\hat{y}$ with his own x. Therefore, it is infeasible for BO to obtain C and its corresponding x. □

Theorem 4. *If BA impersonates U to obtain and to spend a coin, he cannot claim that the coin was issued by U.*

Proof sketch. It holds because if U was not involved in the coin generation, whether colluding with BO or not, BA cannot prove $\{ID, \hat{y}\}$. □

We conclude the analysis of security properties of this scheme by the following final theorem.

Theorem 5. *If a coin, with a relationship-proof of* $\{ID, C\}$*, is misused,* U *cannot deny responsibility for this abuse.*

Proof sketch. Based on Theorems 2, 3, and 4, a valid coin, C, with a relationship-proof of $\{ID, C\}$, maintained jointly by BA and BO, must be related to a private key, x, issued by U, and then U is the only person able to spend the coin. The theorem follows. □

5 Conclusions

This paper discussed a potential denial problem in the M'Raihi payment scheme and proposed a variant scheme to overcome the problem. The main advantage of the new scheme is that neither BA nor BO can impersonate U to obtain and spend a coin without being detected, so that if U abuses the coin, he cannot deny it by suggesting that it was done by either BA or BO. This advantage is at the cost that the user computational requirements are more onerous than for the M'Raihi scheme, because the user himself needs to do precomputations of the signature (if using DSA) for spending a coin.

Acknowledgment

The authors would like to thank Wenbo Mao for pointing out a weakness in an earlier version of the paper.

References

1. U.S. Department of Commerce/National Institute of Standards and Technology, *Digital Signature Standard*. Federal Information Processing Standard Publication (FIPS BUB) 186, May 1994.
2. ISO/IEC 9796: 1991. *Information technology — Security techniques — Digital signature scheme giving message recovery.*
3. S. Brands. Untraceable off-line cash in wallet with observers. In *Advances in Cryptology – CRYPTO '93, Lecture Notes in Computer Science 773*, pages 302–318. Springer-Verlag, Berlin, 1993.
4. E. Brickell, P. Gemmel, and D. Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Proceedings of 6th Annual Symposium on Discrete Algorithm (SODA)*, pages 457–466. ACM Press, 1995.
5. J. Camenisch, U. Maurer, and M. Stadler. Digital payment systems with passive anonymity-revoking trustees. In *Computer Security – ESORICS 96, Lecture Notes in Computer Science 1146*, pages 33–43. Springer-Verlag, Berlin, 1996.
6. W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, November 1976.
7. D. M'Raihi. Cost-effective payment schemes with privacy regulation. In *Advances in Cryptology – ASIACRYPT '96, Lecture Notes in Computer Science 1163*, pages 266–275. Springer-Verlag, Berlin, 1996.
8. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:294–299, 1978.

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