

Fair Electronic Cash Based on a Group Signature Scheme^{*}

Greg Maitland and Colin Boyd

Information Security Research Centre
Queensland University of Technology
Brisbane, Australia.
{g.maitland,c.boyd}@qut.edu.au

Abstract. Several new group signature schemes have been proposed in recent years. In addition, several applications for group signatures (including electronic cash) have been suggested.

A new cash scheme based on a recent group signature by Ateniese, Camenisch, Joye and Tsudik is presented. Its construction uses a general framework suitable for a number of group signature schemes. We also identify the challenges faced by such schemes.

1 Introduction

Unlike ordinary signatures, group signatures allow a group member to create anonymous (and unlinkable) signatures. Upon verifying a signature, the verifier does not learn the identity of the group member that created the signature. However, should the need arise, a group signature can be ‘opened’ by a trusted party and the identity of the member who created the signature will be revealed.

Several proposals [3, 6, 4] have introduced group signatures into electronic cash schemes. The anonymity and unlinkability afforded by group signatures suggests that they may have a role to play in anonymous electronic cash scheme design. The existing proposals have utilised group signatures in different roles, where the group has been formed from the banks that issue the electronic coins [3], the customers that spend the electronic coins [3, 6] and indeed the coins themselves [4].

A general structure for using group signatures to form a ‘group of customers’ has been developed but, due to the limited amount of space available, this framework will not be described here. Instead, a new cash scheme based on a recently proposed group signature scheme is described in order to illustrate the construction. The main benefits of the new cash scheme compared to [6] relate to the underlying group signature scheme’s improved efficiency and provable security.

^{*} This research is part of an ARC SPIRT project undertaken jointly by Queensland University of Technology and Telstra

Main Contribution: We focus on the ‘group of customers’ model for applying group signatures to electronic cash scheme design and illustrate a general construction for these schemes. A new scheme is presented and the properties of the scheme are analysed with a view to identifying key unresolved issues. In particular, withdrawal protocol diversion and additional-overspending framing are discussed.

2 A New Offline Fair Cash Scheme

This section presents a new offline fair cash scheme based on the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [1]. This group signature scheme is provably coalition-resistant and quite efficient.

Setup: Let $\epsilon > 1$, k , and ℓ_p be security parameters. Let λ_1 , λ_2 , γ_1 , and γ_2 denote lengths satisfying $\lambda_1 > \epsilon(\lambda_2 + k) + 2$, $\lambda_2 > 4\ell_p$, $\gamma_1 > \epsilon(\gamma_2 + k) + 2$, $\gamma_2 > \lambda_1 + 2$. Define the integral ranges $\Lambda =]2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}[$ and $\Gamma =]2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}[$. Finally, let \mathcal{H} be a collision-resistant hash function $\mathcal{H} : \{0, 1\}^* \rightarrow \{0, 1\}^k$. (The parameter ϵ controls the tightness of the statistical zero-knowledgeness and the parameter ℓ_p sets the size of the modulus to use.)

The Group Manager: The initial phase involves the group manager (*GM*) setting the group public and his secret keys, \mathcal{Y} and \mathcal{S} , as follows:

- Select random secret ℓ_p -bit primes p' , q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are prime. Set the modulus $n = pq$.
- Choose random elements $a, a_0, g, h \in_R \mathbb{Q}_n$ where \mathbb{Q}_n is the group of quadratic residues in \mathbb{Z}_n^* and is of order $p'q'$.
- The group public key is: $\mathcal{Y} = (n, a, a_0, g, h)$.
- The corresponding secret key (known only to GM) is: $\mathcal{S} = (p', q')$.

The Revocation Manager: The revocation manager (*RM*) chooses a random secret element $x \in_R \mathbb{Z}_{p'q'}^*$ and publishes $y = g^x \bmod n$.

The Bank: The bank selects an appropriate set of parameters to support the chosen blind signature scheme for issuing authorities.

The Customer: Each customer \mathcal{C}_i who wishes to join the customer group interacts with the group manager in order to acquire:

- A private key x_i known only to the user such that $x_i \in \Lambda$. The associated public key is $C_2 = a^{x_i} \bmod n$ with $C_2 \in \mathbb{Q}_n$.
- A membership certificate $[A_i, e_i]$ where e_i is a random prime chosen by *GM* such that $e_i \in_R \Gamma$ and A_i has been computed by the *GM* as $A_i := (C_2 a_0)^{1/e_i} \bmod n$.
- *GM* creates a new entry in the membership table for $[A_i, e_i]$.

Withdrawal: The withdrawal process involves the customer and bank completing the following tasks.

- The customer completes the commitment phase of the signing process.
 - Generate a random value $w \in_R \{0, 1\}^{2\ell_p}$.
 - Compute: $T_1 = A_i y^w \bmod n$; $T_2 = g^w \bmod n$; $T_3 = g^{e_i} h^w \bmod n$.
 - Randomly choose:

$$r_1 \in_R \pm\{0, 1\}^{\epsilon(\gamma_2+k)}, \quad r_2 \in_R \pm\{0, 1\}^{\epsilon(\lambda_2+k)},$$

$$r_3 \in_R \pm\{0, 1\}^{\epsilon(\gamma_1+\ell_p+k+1)}, \quad r_4 \in_R \pm\{0, 1\}^{\epsilon(2\ell_p+k)}.$$
 - Compute:

$$d_1 = T_1^{r_1} / (a^{r_2} y^{r_3}) \bmod n; \quad d_2 = T_2^{r_1} / d^{r_3} \bmod n;$$

$$d_3 = g^{r_4} \bmod n; \quad d_4 = g^{r_1} h^{r_4} \bmod n.$$

The result is the commitment values $\{T_1, T_2, T_3, d_1, d_2, d_3, d_4\}$.

- The customer obtains an authority $Auth(T_1, T_2, T_3, d_1, d_2, d_3, d_4)$ from the bank via a blind signature protocol. The message which is signed is a pre-determined set of values chosen from the set $\{T_1, T_2, T_3, d_1, d_2, d_3, d_4\}$. For instance, the authority could be a signature on the message $(T_1 \parallel T_2)$. In this way, the customer's identity is bound to the authority because (T_1, T_2) is a modified ElGamal encryption of the customer's membership certificate and uniquely identifies the customer.

Payment: During the payment process, the payment transcript msg is signed using the group member's signing keys.

- The customer retrieves the previously calculated values $T_1, T_2, T_3, d_1, d_2, d_3$ and d_4 along with the previously obtained authority $Auth$.
- The customer uses the values $T_1, T_2, T_3, d_1, d_2, d_3, d_4$ and the message msg to complete the challenge and response phases of the signing process.
 - *Challenge Phase:* Calculate

$$c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel msg)$$

- *Response Phase:* Compute

$$s_1 = r_1 - c(e_i - 2^{\gamma_1}), \quad s_2 = r_2 - c(x_i - 2^{\lambda_1}),$$

$$s_3 = r_3 - ce_i w, \quad s_4 = r_4 - cw. \quad (\text{all in } \mathbb{Z})$$

The resulting group signature is $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$.

- The customer sends the merchant the group signature signature on the payment transcript msg plus the corresponding authority $Auth$.
- The merchant verifies the group signature $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ of the payment transcript msg as follows:

1. Compute:

$$d'_1 = a_0^c T_1^{s_1 - c2^{\gamma_1}} / (a^{s_2 - c2^{\lambda_1}} y^{s_3}) \bmod n,$$

$$d'_2 = T_2^{s_1 - c2^{\gamma_1}} / g^{s_3} \bmod n,$$

$$d'_3 = T_2^c g^{s_4} \bmod n,$$

$$d'_4 = T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4} \bmod n.$$

$$c' = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d'_1 \parallel d'_2 \parallel d'_3 \parallel d'_4 \parallel msg)$$

2. Accept the group signature if and only if $c = c'$ and
 - $s_1 \in \pm\{0, 1\}^{\epsilon(\gamma_2+k)+1}$
 - $s_2 \in \pm\{0, 1\}^{\epsilon(\lambda_2+k)+1}$
 - $s_3 \in \pm\{0, 1\}^{\epsilon(\gamma_1+2\ell_p+k+1)+1}$
 - $s_4 \in \pm\{0, 1\}^{\epsilon(2\ell_p+k)+1}$
- The merchant confirms that the attached authority $Auth$ is correct with respect to the pre-determined set of values from $\{T_1, T_2, T_3, d'_1, d'_2, d'_3, d'_4\}$.

Deposit: The deposit process proceeds as follows:

- The merchant sends to the bank the group signature on the payment transcript msg plus the authority i.e. $[msg, (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3), Auth]$.
- The bank verifies the group signature and the authority using the same operations as the merchant. If this is successful, the bank checks for double-spending by searching its list of previously used authorities. If the authority is not found, the authority is added to the list and the payment is accepted as valid. If the authority has been previously used, the bank sends both transcripts to the revocation manager RM and requests that the identity of the customer be revoked.

Identity Revocation: To open a signature and reveal the identity of the actual customer who created a given signature, RM executes the following procedure:

1. Check the signature's validity as per the merchant's verification procedure.
2. Recover A_i (and thus the identity of C_i) as $A_i = T_1/T_2^x \bmod n$.
3. Generate a proof that $\log_g y = \log_{T_2}(T_1/A_i \bmod n)$

3 Observations

The 'group of customers' offline model was first proposed by Lysyanskaya and Ramzan [3] and subsequently expanded upon by Traoré [6]. The structure of the new scheme follows that of Traoré [6] and hence it has the same general security properties. The weaknesses described previously by Traoré [6] have their origins in the level of coin transfer-resistance that is achieved.

The group signature signing process binds a customer's identity to the signature during the commitment phase by encrypting the customer's identity under T_1 and T_2 . Therefore, it is not possible for any other customer to spend the 'coin'. In this sense, the 'coin' is bound to the identity of a particular customer. Whether or not this customer is the withdrawing customer depends on the blind signature used to create the authority. In Brands' cash [2], the restrictive blind signature used to create the authority achieves tight binding and prevents the withdrawal protocol from being diverted. As a result, the signing keys of customer withdrawing the 'coin' must be known in order to spend the 'coin'.

The exact details of the commitments used in creating an authority have not been specified. Different choices can provide different properties. If all the

values in the set $\{T_1, T_2, T_3, d_1, d_2, d_3, d_4\}$ are signed when forming an authority, the knowledge extraction process for the group signature scheme will reveal the customer's private key and group membership certificate in the event that the customer overspends. As has been previously noted by Nyang and Song [5] in connection with Brands' cash scheme [2], the bank can then falsely accuse the customer of additional overspending.

If the values T_1, T_2, d_3 are used in forming the authority, the customer's A_i can be extracted if double-spending occurs. This allows the bank to independently identify the customer but the bank can not create false payment transcripts. If the values T_1, T_2 are used, the bank can still detect the double-spending event. The revocation manager can open the offending transcripts and identify the overspending customer – the reason for using group signatures to begin with.

4 Conclusions and Further Work

We have presented a new offline cash scheme based on an efficient and provably coalition-resistant group signature scheme. The group signature properties are used to deliver anonymity, unlinkability and revocation services. A blindly signed authority from the bank is used to detect double-spending. The exact nature of this authority has been left as flexible.

The scheme discussed in this paper is susceptible to diversion and this can lead to perfect crimes [7] such as blackmailing and money laundering. Designing an authority mechanism which is resistant to diversion is an open problem with respect to the underlying group signature scheme used in this paper.

References

1. Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Advances in Cryptology—CRYPTO 2000*, LNCS 1880, pages 255–270. Springer-Verlag, 2000.
2. Stefan Brands. Untraceable off-line cash in wallets with observers. In *Advances in Cryptology—CRYPTO '93*, LNCS 773, pages 302–318. Springer-Verlag, 1993.
3. A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In *Financial Cryptography: Second International Conference, FC '98*, LNCS 1465, pages 184–197. Springer-Verlag, 1998.
4. Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama. Unlinkable electronic coupon protocol with anonymity control. In *International Workshop on Information Security (ISW'99)*, LNCS 1729, pages 37–46, 1999.
5. DaeHun Nyang and JooSeok Song. Preventing double-spent coins from revealing user's whole secret. In *Second International Conference on Information Security and Cryptology (ICISC'99)*, LNCS 1787, pages 13–20. Springer-Verlag, 1999.
6. Jacques Traoré. Group signatures and their relevance to privacy-protecting off-line electronic cash systems. In *Australasian Conference on Information Security and Privacy (ACISP'99)*, LNCS 1587, pages 228–243. Springer-Verlag, 1999.
7. S. von Solms and D. Naccache. Blind signatures and perfect crimes. *Computers and Security*, 11:581–583, 1992.