ID-Based Fair Off-Line Electronic Cash System with Multiple Banks

Chang-Ji Wang¹,²,³ (王常吉), Yong Tang¹ (汤 庚), and Qing Li¹ (李 琴)

¹Department of Computer Science, Sun Yat-Sen University, Guangzhou 510275, China
²Guangdong Province Information Security Key Laboratory, Guangzhou 510275, China
³The State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049 China

E-mail: isswchj@mail.sysu.edu.cn
Received May 8, 2006; revised January 12, 2007.

Abstract ID-based public key cryptography (ID-PKC) has many advantages over certificate-based public key cryptography (CA-PKC), and has drawn researchers’ extensive attention in recent years. However, the existing electronic cash schemes are constructed under CA-PKC, and there seems no electronic cash scheme under ID-PKC up to now to the best of our knowledge. It is important to study how to construct electronic cash schemes based on ID-PKC from views on both practical perspective and pure research issue. In this paper, we present a simpler and provably secure ID-based restrictive partially blind signature (RPBS), and then propose an ID-based fair off-line electronic cash (ID-FOLC) scheme with multiple banks based on the proposed ID-based RPBS. The proposed ID-FOLC scheme with multiple banks is more efficient than existing electronic cash schemes with multiple banks based on group blind signature.

Keywords electronic cash, restrictive partially blind signature, ID-based cryptography

1 Introduction

The first electronic cash scheme was put forward by Chaum[1] in 1982, and the concept of blind signature was used to guarantee the privacy of users. A blind signature protocol allows a recipient to get a signature from a signer, but the signer can learn neither the messages he/she signs nor the signatures the recipient obtains afterwards. To prevent users from double-spending electronic coins in anonymous electronic cash system, a low efficient cut-and-choose technique was applied. To improve the efficiency of anonymous off-line electronic cash scheme, Brands[2] proposed the concept of restrictive blind signature (RBS), together with an efficient single-term electronic cash scheme where the bank ensures that the user is restricted to his identity to be embedded in the resulting blind signature. An RBS scheme is virtually a protocol that allows a signature requestor to obtain a blind signature in a message from a signer, but the choice of messages is restricted and must conform to certain rules.

In 1992, Solms and Naccache[3] pointed out that this complete anonymity of electronic cash could be used for criminal activities, such as money laundering or illegal purchase etc. For this reason, Stadler et al.[4] proposed the concept of “Fair Blind Signatures” in 1995. Frankel et al.[5] provided a fair off-line electronic cash (FOLC) scheme with revocable anonymity based on “indirect discourse proof”, and they made further improvements in [6]. Since then, the design of FOLC scheme has become an active research field in the application of cryptography[7].

To embed the expiry date and denomination information into the electronic coins that are blindly signed by the bank, Abe and Fujisaki[8] introduced the concept of partially blind signature (PBS). In a PBS scheme, a receiver receives a signature $\sigma(\text{msg, info})$ in $\text{msg}$ and $\text{info}$, but the signer does not get any such information in $\text{msg}$ or in the resulting signature $\sigma(\text{msg, info})$. The $\text{info}$-part is called the clear part, which is agreed on prior to the signature generation, while the $\text{msg}$-part is called the blinded part of the message. This signature allows both a signer and a recipient to agree upon some information that will be included in the blinded signature. Because of the particular property of PBS, many PBS schemes have been proposed in succession since the concept was presented[8~11].

Maitland and Boyd[12] first integrated restrictive blindness property into the PBS scheme, and presented a provably secure restrictive partially blind signature (RPBS) scheme, which satisfies the partial blindness and restrictive blindness. Recently, Chen et al.[13] proposed an ID-based RPBS scheme and an off-line anonymous electronic cash scheme based on the proposed ID-based RPBS.

The concept of the group signature was first introduced by Chaum and Heyst[14]. In a group signature scheme, any member of the group can sign messages on behalf of the entire group and the receiver can verify that it is a valid group signature with the single public key of the group. The first efficient group signature, whose group public key and signatures have length independent of the number of group, was proposed by Camenisch and Stadler[15]. Then Lysyanskaya and Ramzan[16] proposed the concept of group blind signature, together with an efficient electronic cash
scheme with multiple banks based on group blind signature. The existent electronic cash schemes with multiple banks are all based on group signature. However, there remain some open problems in group signature, such as member revocation and low efficiency.

Shamir[17] proposed the concept of ID-PKC in 1984. In ID-PKC, the user’s public key is derived from its identity information, such as email address or IP address etc., and the corresponding private key is generated by a trusted third party named as private key generator (PKG). The private key is transferred from PKG to the user through a secure channel. ID-PKC has many advantages over CA-PKC, and has drawn researchers’ extensive attention, in recent years, more and more applications under ID-PKC have appeared[18]. However, current electronic cash schemes are still constructed under CA-PKC, and there are no electronic cash schemes under ID-PKC up to now. It is important to study how to construct electronic cash schemes under ID-PKC from views on both practical perspective and pure research issue.

In this paper, we present a simpler and provably secure 1D-based RPBS scheme, and then propose an 1D-based FOLC (ID-FOLC) scheme with multiple banks based on the proposed 1D-based RPBS. The proposed ID-FOLC scheme with multiple banks is more efficient than previous electronic cash schemes with multiple banks based on group blind signature. Other than the ideas of Maitland and Boyd’s RPBS in [12] and Chen et al.’s RPBS in [13], where a specialized hash function is used, to map the agreed common information into the public key of the Schnorr proof of knowledge, we integrate the idea of partial blindness in Abe et al.’s PBS[8] into the Brand’s RBS[3]. To achieve partial blindness, Abe et al.[9] replace the signer’s private key d with dH1 (info). In the proposed 1D-based RPBS scheme, we use the same technique to replace SID with SIDH1 (info), and the corresponding public key QID with QIDH1 (info).

This paper is organized as follows. Some preliminaries are described in Section 2. A simpler 1D-based RPBS scheme and the security analysis are presented in Section 3, and an ID-FOLC scheme with multiple banks based on the proposed 1D-based RPBS are presented in Section 4. Finally, we draw conclusions in Section 5.

2 Preliminaries

2.1 Bilinear Pairings and Diffie-Hellman Problems

Let (G1,+) and (G2,·) be two cyclic groups of the same prime order q. A bilinear pairing is a map e: G1 × G1 → G2 with the following properties:

- **Bilinear**: e(aP,bQ) = e(P,Q)ab for all P,Q ∈ G1 and a,b ∈ Z∗q.
- **Non-degenerate**: There exists P, Q ∈ G1 such that e(P,Q)  1.

- **Computable**: There exists an efficient algorithm to compute e(P,Q) for all P,Q ∈ G1.

Typically, the map e will be derived from either Weil or Tate pairing on an elliptic curve over a finite field.

**Definition 1.** Given a generator P of a group (G1,+) and a 2-tuple (aP,bP), where a,b ∈ Z∗q, the Computational Diffie-Hellman Problem (CDHP) is to compute abP.

**Definition 2.** Given a generator P of a group (G1,+) and a 3-tuple (aP,bP,cP), where a,b,c ∈ Z∗q, the Decisional Diffie-Hellman Problem (DDHP) is to decide if c ≡ ab.

**Definition 3.** If G1 is a group such that DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial-time, then we call G1 a Gap Diffie-Hellman group.

Throughout the rest of this paper, we let (G1,+) be a gap Diffie-Hellman group of prime order q, (P,P1,P2,P3) be independent generators of G1, (G2,·) be a group of the same prime order, e: G1 × G1 → G2 be an admissible bilinear pairing and k is a security parameter. Define five cryptographic secure hash functions H : {0,1}∗ × G1 → Z∗q, H0 : {0,1}∗ → G1, H1 : {0,1}∗ → Z∗q, and H2 : {0,1}∗ × G1 × Z∗q3 → Z∗q.

2.2 1D-Based Cryptography

ID-PKC setting from bilinear pairings can be implemented as follows.

- **Setup.** This algorithm is executed by PKG. On an unary string input 1k, it produces the public parameters \( \{G_1,G_2,e,q,P,P_{pub},H_0\} \) and the master-key s, where \( P_{pub} = sP \) and s is only known to PKG.

- **Extract.** A user submits his/her identifier ID to PKG. PKG computes the user’s public key as \( Q_{ID} = H_0(\text{ID}) \), and then returns \( S_{ID} = sQ_{ID} \) to the user as his/her private key.

2.3 Signature of Proof of Knowledge

The signature of proof of knowledge (SPK) allows a prover to demonstrate knowledge of a secret with respect to some public information such that no other information is revealed in this process. Various SPKs have been proposed and have proved secure in the random oracle model[6,15,16].

**Definition 4.** A tuple \((d,r)\) satisfying \( d = H(\zeta,P,P_1,A_1,rP + dA_1) \) is an SPK of the discrete logarithm of A to the base P equalling that of A1 to the base P1 on message \( \zeta \in \{0,1\}^* \), denoted as SPK[\( \{aA = aP \cap A_1 = aP_1\} \zeta \)].

**Definition 5.** A tuple \((d,r_1,r_2)\) satisfying \( d = H(\zeta,P,P_1,P_2,A_1,r_1P + dA_1,r_1P_1 + r_2P_1) \) is an SPK of the P1-part of A1 to the bases P1 and P2 equalling the discrete logarithm of A to the base P on message \( \zeta \).