Future Generation Computer Systems 37 (2014) 252–258

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

New and efficient conditional e-payment systems with transferability

Xiaofeng Chen [a,*], Jin Li [b], Jianfeng Ma [a], Wenjing Lou [c], Duncan S. Wong [d]

[a] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, PR China
[b] School of Computer Science and Educational Software, Guangzhou University, Guangzhou, PR China
[c] Department of Computer Science, Virginia Polytechnic Institute and State University, USA
[d] Department of Computer Science, City University of Hong Kong, Hong Kong

HIGHLIGHTS

- We propose a new conditional e-payment scheme with transferability.
- Our scheme allows the coin to be transferred anonymously by a chain of payees.
- Our scheme does not require inefficient cut-and-choose techniques.
- Our scheme has lower computation and communication complexity.

ARTICLE INFO

Article history:
Received 28 March 2013
Received in revised form
16 June 2013
Accepted 17 July 2013
Available online 7 August 2013

Keywords:
Conditional e-payment
Blind signatures
Transferability
Bilinear pairings

ABSTRACT

Conditional e-payments (or e-cash) allow the user to anonymously cash a bank-issued e-coin at a future time if and only if a certain agreed-upon public condition is satisfied, which are useful in plenty of applications such as prediction markets, anonymous online betting, and securities trading. In this paper, we propose a new and efficient conditional e-payment system based on Chen et al.'s restrictive partially blind signature scheme. Compared to the existing conditional e-payment schemes [2,5,6], our construction requires neither the inefficient cut-and-choose techniques nor the complicated knowledge proof protocols and thus has lower computation and communication complexity. Another significant contribution of this paper is a conditional e-payment system with transferability which allows the coin to be further transferred anonymously by a chain of payees.

1. Introduction

The primitive of e-payments (or e-cash), introduced by Chaum [1], is arguably one of the most significant applications of modern cryptography. After its invention, plenty of research work has been done in the past three decades. There are two types of e-cash schemes namely on-line and off-line. Trivially, an on-line e-cash scheme can provide a good solution to the most serious problem in e-cash systems, i.e., the double-spending problem. However, it requires that the payee must contact the bank during each transaction and thus the bank must be on-line at any time. That is, the bank will soon become the bottleneck of the systems. Therefore, the off-line approach is more appealing to construct efficient e-cash systems.

Shi et al. [2] first introduced a new primitive named conditional e-payments. Compared with the traditional e-payment schemes, conditional ones allow the user to anonymously cash a bank-issued e-coin at a future time if and only if a certain agreed-upon public condition is satisfied. Besides, the coin in conditional e-payment systems is not bound to the identity of payees during the transferring (i.e., spending) and thus the payees remain anonymous all the time. Conditional e-payments are useful in plenty of secure (financial) big-data science applications such as prediction markets, anonymous online betting, securities trading, and outsourcing computations [3,4].

Shi et al. [2] also presented a concrete construction for conditional e-payments. However, the scheme is very inefficient due to the use of expensive cut-and-choose protocols and secret sharing techniques. Besides, the conditional transfer protocol requires participation of the bank (i.e., the bank needs to be on-line). Though Carbunar [5] later presented an off-line version of conditional e-payments based on oblivious transfer techniques, it still used inefficient cut-and-choose protocols and secret sharing techniques. Blanton [6] presented an improved conditional e-payment (with transferability) based on CL-signatures [7]. The scheme is off-line and does not use cut-and-choose protocols. Therefore, it has a lower computation and communication overload than [2].

* Corresponding author. Tel.: +86 2988204749.
E-mail address: xfchen@xidian.edu.cn (X. Chen).

0167-739X/$ – see front matter
http://dx.doi.org/10.1016/j.future.2013.07.015

However, it requires some complicated zero-knowledge proofs due to the use of CL-signatures. It is still an interesting problem to seek for more efficient constructions for conditional e-payments (with transferability).

Our contribution. In this paper we propose a new and efficient conditional e-payment system based on Chen et al.'s restrictive partially blind signature scheme from bilinear pairings. Compared to the existing conditional e-payment schemes [2,5,6], our construction requires neither the inefficient cut-and-choose techniques nor the complicated knowledge proof protocols and thus has lower computation and communication complexity. Similar to [6], we also eliminate the need for the bank to be involved in all conditional transfer protocols, *i.e.*, off-line bank. Another significant contribution of this paper is a conditional e-payment system with transferability which allows the coin to be further transferred anonymously by a chain of payees.

1.1. Related works

It is considered to be the most suitable solution to design an e-cash scheme using blind signatures [1,8–18]. Actually, the various security problems of (traditional) e-cash systems result in different types of blind signatures as shown below.

Chaum [10] proposed the first off-line e-cash scheme which can solve the double-spending problems. However, it is very inefficient due to the cut-and-choose protocol. Therefore, Brands [9,19] introduced a new primitive named restrictive blind signatures and used it to design a highly efficient e-cash system. Besides, since the bank can ensure that the user is restricted to embed his identity in the resulting blind signature, the double-spending can be detected undoubtedly. Partial blind signatures [8,20], which allow a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process, also play an important role in designing an efficient e-cash system. For example, the bank does not require different public keys for different coin values. On the other hand, the size of the database that stored the previously spent coins to detect double-spending would not increase infinitely over time. Maitland and Boyd [21] first incorporated these two blind signatures and proposed a provably secure restrictive partially blind signature scheme, which satisfies the partial blindness and restrictive blindness. Later, Chen et al. [13] proposed a restrictive partially blind signature scheme from bilinear pairings, which does not require some inefficient zero-knowledge proof and thus has the advantages of shorter signature length and lower communication complexity. On the other hand, Lysyanskaya and Ramzan [22] firstly combined the properties of group signatures and blind signatures and presented the notion of group blind signatures, which is useful to construct hierarchical e-cash systems. In order to prevent criminals from misusing the anonymity in e-cash systems, Stadler et al. [23] introduced the notion of fair blind signatures, where the blindness could be revoked by a trusted trustee in case of emergency.

Shi et al. [2] first introduced the notion of conditional e-payments which is different from traditional e-cash systems. However, the construction is very inefficient due to the use of expensive cut-and-choose protocols. Blanton [6] presented an improved conditional e-payment with transferability based on CL-signatures. The above conditional e-payment schemes [2,5,6] only support a same condition. Li and Chen [24] first presented a construction for multi-conditional e-payments. On the other hand, Carbunar and Tripunitara proposed fair conditional payments for outsourcing computation in order to solve the trust problem of the outsourcers, while it never considered the anonymity of the payees. Later, Carbunar and Tripunitara [25] proposed a new fair payment for outsourced computations that can be viewed as an instance of conditional e-cash. Nevertheless, the solution also uses the inefficient cut-and-choose protocol. Recently, Chen et al. [26] proposed a new conditional payment scheme for outsourcing computation in the rational lazy-and-partially-dishonest workers model, and the outsourcer pays the worker only under the condition that the worker indeed has completed his job before the deadline. However, the scheme is based on traditional e-cash systems and thus the anonymity of workers cannot be ensured (this is the same as [27]).

1.2. Organization

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. The security model and definition for conditional e-payment systems are introduced in Section 3. The proposed new conditional e-payment system and its security analysis are given in Section 4. The proposed conditional e-payment system with transferability is given in Section 5. Finally, conclusions will be made in Section 6.

2. Preliminaries

In this section, we will briefly describe the basic definition of bilinear pairings [28–31] and then introduce the verifiable encryption for discrete logarithms [32,33]. Finally, we present Chen et al.'s restrictive partially blind signatures from pairings [13].

2.1. Bilinear pairings

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic multiplicative groups of prime order q. Let g be a generator of $\mathbb{G}_1$. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

(1) Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q^*$.
(2) Non-degenerate: $e(g, g) \neq 1$.
(3) Computable: There is an efficient algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}_1$.

The examples of such groups can be found in supersingular elliptic curves or hyperelliptic curves over finite fields, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [28–31].

2.2. Verifiable encryption for discrete logarithms

The concept of verifiable encryption was first introduced by Stadler [34] in the context of publicly verifiable secret sharing schemes. Asokan et al. [35] extended the notion in a more general form for fair exchange and then Camenisch et al. [33] presented a formal definition for verifiable encryption.

Suppose Alice and Bob agree on a common value α^x, where α is a generator in a cyclic group $\mathbb{G}$. Alice wants to generate a verifiable encryption for x under the public key of a trusted third party T. Trivially, we assume that it is intractable to compute x from α^x in $\mathbb{G}$. Ateniese [32] presented a simple method of verifiable encryption for discrete logarithms as follows.

Consider the Naccache–Stern cryptosystem [36], let $n = pq$ be an RSA modulus which is generated by T along with a small integer B. Let σ be a square-free odd B-smooth integer such that it divides $\phi(n)$ and is prime to $\phi(n)/\sigma$ (a suggested size is $\sigma > 2^{160}$). Let g be an element whose multiplicative order modulo n is a large multiple of σ. A message $x < \sigma$ is encrypted by $g^x \mod n$. Decryption is performed using the prime factors of σ, getting x by the Chinese remainder theorem: Let p_i $(1 \leq i \leq k)$ be the prime factors of σ. Given the ciphertext $c = g^x \mod n$, compute $c_i = c^{\frac{\phi(n)}{p_i}} = g^{\frac{x_i\phi(n)}{p_i}} \mod n$, where $x_i = x \mod p_i$ can be computed by