International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **1**, January **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 459–469

COMPACT *k*-SPENDABLE E-CASH WITH ANONYMITY CONTROL BASED OFFLINE TTP

Qian Wang

School of Business
Sun Yat-Sen University
No. 135, Xingangxi Road, Guangzhou 510275, P. R. China
mnswq@mail.sysu.edu.cn

Received August 2009; revised December 2009

Abstract. *As known, compact e-cash schemes are constructed from signature schemes with efficient protocols and verifiable random functions, allowing a user to withdraw a wallet containing 2^l coins, which can be spent by the user unlinkably. However, the main drawbacks of the compact e-cash scheme are that anonymity control is insufficient, and the method does not address the issue of preventing crime. This paper presents an efficient and practical e-cash scheme that provides anonymity control and a valid date based on an offline trusted third party (TTP). By constructing a coin tag and two tracing tags, the new scheme allows for protecting the anonymity of honest users and can revoke anonymity protocols when dishonest users attempt to cheat the system. The wallet's withdrawal date is incorporated into the e-cash so that it captures the valid date, which makes it easier to control the size of the bank's database. In fact, compared with previous schemes, the complexity of the withdrawal and spend protocols remains $O(\lambda + \log(k))$, and 2^l coins can be stored in $O(\lambda + \log(k))$ bits. The security of our scheme is illustrated in the random oracle model.*

Keywords: Compact e-cash, Anonymity, Coin tracing, Owner tracing

1. **Introduction.** With the exponential increase in the number of Internet users and growing shift of the marketplace to the Internet, electronic payment systems play an increasingly crucial role. Electronic cash (e-cash) – regarded as an equivalent of coins in the physical world – could play an important role in the realization of fully online commerce. However, an important difference between e-cash and physical cash is that e-cash is represented by electronic bit strings. Because e-cash is easy to duplicate, it may facilitate fraud and other criminal acts such as money laundering, offline spending and double spending. Therefore, a practical electronic cash system must be secure and anonymous to effectively emulate the properties of physical cash transactions [1].

Security of e-cash refers to the fact that only the bank can produce a coin. For offline schemes, honest users should not be falsely accused of double spending, dishonest users who have double spent should be identified. Additionally, e-cash should provide users with anonymity from both the bank and the merchant during a purchase. As long as the spender is honest and uses the system properly, when merchants deposit the transacted money, the bank should not be able to trace who the actual spender was.

Many e-cash schemes that match the properties of the physical coin have been proposed in the recent past, and many of these have proven to be useful methods for paying electronically. The principal idea of anonymous electronic cash was invented by D. Chaum [2]. However, this solution lacks efficiency due to the use of expensive "cut-and-choose" methods. In the past few years, many scholars have made great efforts to improve upon the efficiency and the anonymity of e-cash schemes. There are essentially two approaches to