Secure ECash Payment Method Based on Pseudo-Random Functions in Centralized and Decentralized Systems

Stefan Andonov
stefan.andonov@finki.ukim.mk

Jovana Dobreva
jovana.dobreva@students.finki.ukim.mk

Keti Isajloska
keti.isajloska@students.finki.ukim.mk

Lina Lumburovska
lina.lumburovska@students.finki.ukim.mk

Vesna Dimitrova
vesna.dimitrova@finki.ukim.mk

Faculty of Computer Science & Engineering
Ss Cyril and Methodius, University of Skopje
Skopje, North Macedonia

***Abstract*—One of the first online payment systems was eCash, which was discovered in the previous century and is still used worldwide. In this communication system, we are talking about more participants and contributors, but the main characters are the buyer and the seller. Their identity should stay anonymous and that is what this protocol can afford. Taking into consideration its advantages and disadvantages, the system works in real life centralized and decentralized systems and is spreading its usage to a higher level. Maintaining secure protocol must be obtained, so we discussed a few methods in order to achieve this property. We have also shown some basic principals for good implementation and what should be fulfilled in order to provide the best version of the eCash payment system. Basically, starting from the beginnings of eCash, we studied its implementation and design and then presented its security aspects and how this system works in real life examples in both centralized and decentralized systems.**

***Keywords* – eCash payment system, digital cash, pseudo-random functions, anonymity, (de)centalized systems**

I. Introduction

The emergence of electronic payment systems (EPS) revolutionized the way we buy and sell goods and services. As a result, we can say that global e-commerce is growing at an unprecedented pace. ECash is one of the first online payment systems. It is developed by the company DigiCash. Since it is based on the real money principle, it has changed the world of financial transactions. But, it seems unlikely that virtual money will ever completely replace conventional money. In comparison with conventional cash where the cash is spent many times by many people i.e it is completely transferable, eCash prevents double spending; it can be transferable only until it is spent. eCash payment system is mainly focused on electronic money anonymity assurance, and what is important is that the buyer and the seller must have an account opened at the same bank. [**?**]

A. Types of ECash

- Network type - supporting the electronic payment system using the value that is transmitted and stored to the PC from cyber bank and
- Smart card type - plastic cards embedding chips which involve the value and user's information [**?**]

B. How Does ECash Work?

In order to use eCash, every user needs to have an account. The bank provides and marks eCash in lieu of the user's conventional cash. Some protocols have been developed for ensuring that the system works seamlessly concerning account opening, withdrawal and payments. The end-user can download eCash from their bank account, and store them on a local hard drive. The same software provides taking amounts from their eCash wallet and adding it to the other's wallet. In order to verify the transaction, the eCash must go through the eCash bank. Transactions don't incur a fee except for a small amount charged by the eCash company. [**?**]

C. Advantages of ECash

- **Anonymity** - eCash system provides usage of the blind signatures in coin generating. In that way, the electronic money is impossible to trace them.
- **Security** - eCash uses secure protocol. The system uses the public cryptographic keys RSA that assure both the digital and blind signatures. In that way eCash is secure against the popular eaves-dropping attacks. The coin protection in the local machine can be improved by providing crypting and passwords.
- **Low cost** - in comparison to bank transactions which require huge amounts of infrastructures, eCash can use basic services such as the Internet to make the same transaction online, so it brings down the cost of the transaction.

- **Long Distance Transactions** - for long distance transactions, sending money with physical cash can be very expensive (paying fees), but eCash can be sent without too much of a hassle. [**?**]

D. Disadvantages of ECash

- **Spent coin database dimension** - since eCash system has very large database dimension for the signatures, and it is hard to manage with – this problem has been solved by using marked electronic tokens.
- **Standard** - many companies offer complete property on eCash so the system is not a standard one.
- **Not Traceable** - because eCash uses the Internet, traceability is getting difficult. This provides anonymity. The bad thing is that it can be susceptible to money laundering.
- **Forgery** - eCash system can be susceptible to forgery. There is a risk of breaking into the system, and making inappropriate actions - generating more coins on an inappropriate way - not paying anything to earn that cash. [**?**]

II. Implementation and Design of ECash

A. General Information About Good Implementation

In the following section, we will describe what are the key issues in order to provide good implementation of the eCash payment system. General implementation of the system is based on real money principle due to its primary usage described in the introduction part. Basically, this system uses cryptography with public keys in order to assure both the digital and the blind signatures. If we take a scenario from everyday life, for example a buyer and a seller trying to make a transaction or transfer money, the main point of this payment is keeping money anonymity assurance, which means both of them must have an account opened at the same bank as mentioned before. There are some essential requirements that must be accomplished for a successful implementation starting with its security. We researched more ways for establishing security, for example pseudo-random functions, more of which will be explained in the next section. [**?**]

We can discuss good implementation if the scalability of the system is at high point, because a stable system may support bigger number of users. What is more, if the system has an ability to transfer fast enough, the coins can be transfered directly to the user, without necessary verification of the coin issuer. Consequently, it leads to offline operability because the transfer is executed between two parts: the buyer and the seller, which means again there is no need of the coin issuer. It is one of the reasons why the security must be at the highest level and even when the transmission is not watched, the communication may happen without any problems. Since, the user interface is not a cryptographic problem and in most cases the user is a non-technical person, the system must be practical and easy to use. Last but not least, efficiency of the system is an important factor for all of the above, including the operations adding and deleting users from the system which also contribute to a better system implementation. [**?**]

B. Design of the Payment System

The system is designed with few participants. As mentioned, the transfer has an issuer (issues coins), user (uses e-coins to buy or sell merchandise), payer (uses e-coins to buy merchandise), payment beneficiary (receives e-coins in order to sell merchandise) and certification authority (certificates the public keys of the participants). The design of the whole protocol is described graphically in Figure 1 [**?**], where we can see the process in two directions which means it is a constant process and each element is connected and depends on others.

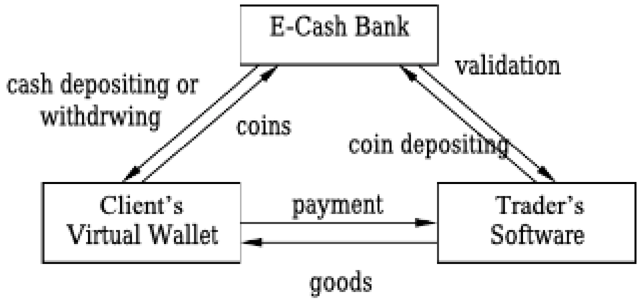

Fig. 1. ECash payment system [**?**]

The coins in eCash are pairs of two integers, first coordinate is the serial number of the coin and the second one is its value obtained during a calculation. For instance, the bank can use a private key from RSA algorithm to sign the second coin when the second value is being computed. If a is the first coordinate, $f(a)$ is the second one and f is a hash function.

Before the bank signs the coin, the user must prepare it. The user prepares a demand, for example 50 coins, 50$ for each. He requires the following information: sum (50$), serial number (the first coordinate) and identification number (11,12,13...), so that the serial number must be different for each coin. The identification number is a combination of two parts which are being generated using a different secret protocol. When the bank receives a request for transfer, it receives prepared money and uses the cut-and-choose protocol in order to open 40 from 50 coins and must verify if the sum is the same, but different serial number and valid identification number. After this, the next step is the signing process using the blind signature, which is introduced as the bling factor r. The bling factor is a random integer number which can be multiplied in coin before the bank signs it. After signing, the user can eliminate this random number. Instead of sending only $f(a)$, the user sends $f(a)*r$ to the bank. When the bank signs the coin, only the person knows what is the value after the factor r will be eliminated. [**?**]

C. Simple Example for Its Usage

The user A has some money and he wants that money to be signed from the user B using the blind signature. The user B has the public key e, the private key d and a public module n. The user A selects a random number k from 1 to n. After this, the user A blinds the value a, computing $t = a * k^e(modn)$. The user B signs t with his private key d, $t^d = (a * k^e)^d(modn)$. The user A can reveal the money when the previous result is divided by k. When the process is over, the user A has the money signed by user B, which was his primary goal and in this case the user B does not know what he or she has signed. The formula for this example is:

$$\frac{f^d}{k} = \frac{(a * k^e)^d(modn)}{k} = \frac{a^d * k(modn)}{k} = a^d(modn) \quad (1)$$

The process shown on Figure 2 [?] is described in five steps and all in all it is how the spending of eCash works.

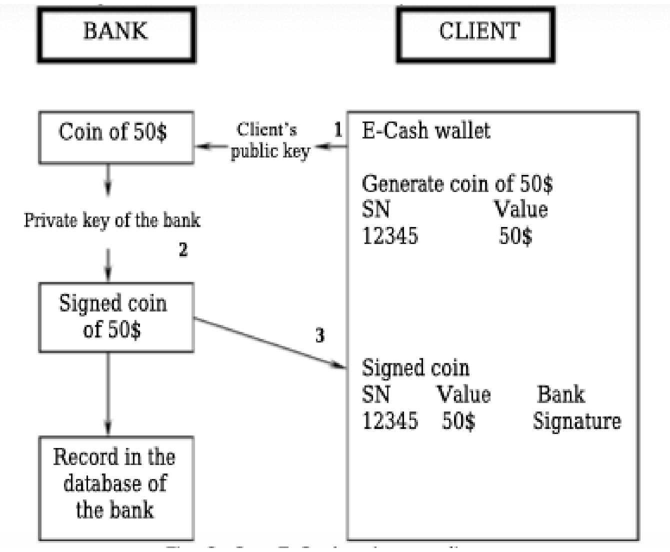

Fig. 2. Example for using eCash system [?]

1) the seller requires the payment – if the buyer agrees then the eCash coins are selected and erased from the buyer, invalidating the numerical series. Then, each coin is sent to the seller
2) the seller sends the coins to the bank to see if the coins were spent another time
3) the bank verifies the signature and informs the seller if the coins are valid
4) if the coins are valid, the seller receives a confirmation and the value of the coins is transferred in the seller's account
5) the goods are transferred to the buyer.

III. Security Aspects of ECash

A. Anonymous Compact ECash

Anonymous compact eCash was suggested by Camenisch, Hohenberger and Lysyanskaya [?], which was informally based on the following idea. Let N be the amount a user withdraws from a wallet. A consumer must then basically disclose $F_s(i)$, where F is a pseudo-random function with secret key s to spend the i-th coin and proof, in a zero-knowledge way, that it's well-formed. In other words, this must be certified and the serial number must be generated using F_s on the input belonging in the interval of $[1, N]$. All these proofs can be mounted easily in several settings. Anonymity stems from the zero-knowledge properties of the proofs and the properties of the pseudo-random function, since it is difficult to determine whether $F_s(i)$ and $F_s(j)$ were generated under the same secret key s.

B. Compact / divisible ECash systems

A system offering efficient storage is called compact and a system supporting both efficient storage and spending is called divisible [?]. It leads for more formal approach, turning the traditional concept into a structured architecture. A user receives a certificate on some hidden value s during a withdrawal that will be used as a seed for a pseudo-random function (PRF) F, thus specifying the serial numbers of the N coins as $F_s(i)$ for $i \in (1, N]$. For more than a decade, the above issue remained undetected, while all compact / divisible eCash systems are based on the same intuition. For example let we have €8.75 investment in case all of the coins are of the smallest possible size. That means the consumer no longer has an € 10 coin but has 1000 coins of €0.01. Such a device can manage any amount without change but must have an effective means of stocking and spending hundreds of coins at once.

C. Generic Frameworks

In this paper we introduce the first frameworks for divisible eCash systems that only use constrained PRFs and very standard cryptographic primitives. We use the proofs from the book Advances in Cryptology [?] for the security of the global constructions assuming that each of the building blocks achieve some properties that are identified. It presents this complex primitive in a new light, highlighting its strong relations with constrained PRFs.

D. Pseudo-Random Functions

Starting with Camenisch's work [?] defining the serial numbers as outputs of a PRF, the specifications on a divisible eCash framework are formalized as properties that the PRFs must achieve. Actually, the main requirements is that the serial numbers can be revealed by batches, which means that it must be possible to reveal some element k_s that allows to compute $F_s(i)$, for every i of S, where $S \in [1, N]$ and does not provide any information on the other serial numbers, i.e. on the outputs of the PRF outside S . This exactly matches the definition of constrained PRF. There are also several requirements that the restricted key k_s must implicitly fulfill for anonymity to hold, and especially non-linkability of transactions: different restricted keys created from the same master key must be unlinkable, which also requires k_s to hide any information on the subset S (besides its cardinality, which will reflect the amount).

E. Security model

The security models are basically based on the interests of the consumer and the bank. Indeed, the former must be able to anonymously invest their coins without being falsely accused of fraud, while the latter must be able to detect fraud and identify the perpetrators. This is formally defined by three security properties: anonymity (user spendings are anonymous, even with respect to the bank), exculpability (honest users cannot be falsely accused, even by the bank) and traceability (an author of overspending should be traced back). The framework [**?**] makes use of three standard cryptographic primitives, namely digital signature, commitment scheme and non-interactive zero-knowledge (NIZK) proofs along with their respective security properties.

- digital signature
  Given a security parameter $\lambda \in N$, the algorithm generates a digital signature key pair (pk, sk). To generate a private key for some user's identity ID, the PKG generates a fresh digital signature key pair.
  1) Keygen(1^λ): on input a security parameter λ, this algorithm outputs a pair of signing and verification keys (sk, pk)
  2) Sign(sk, m): on input the signing key sk and a message m, this algorithm outputs a signature σ
  3) Verify(pk, m,σ): on input the verification key pk, a message m and its alleged signature σ, this algorithm outputs 1 if σ is a valid signature on m under pk, and 0 otherwise
- commitment scheme
  1) Keygen(1^λ): on input a security parameter λ, this algorithm outputs a comitment key ck that specifies a message space M, a randomizer space R along with a commitment space C
  2) Commit(ck, m, r): on input ck, an element $r \in R$ and a message $m \in M$, this algorithm returns a commitment $c \in C$
- zero-knowledge proof systems
  1) completeness: if the statement is true, the prover should be able to convince the verifier.
  2) soundness: a malicious prover should not be able to convince the verifier if the statement is false.
  3) zero-knowledge: a malicious verifier learns nothing except that the statement is true

F. First Divisible ECash System Secure in the Standard Model

Finally, extensive evidence is given for the structures to demonstrate that the overall construction protection usually keeps each of the building blocks under the defense. In concrete terms, this means that a safe divisible eCash framework can be designed for any setting by essentially designing a restricted PRF which achieves some simple properties. To highlight this point, the first divisible eCash method in the standard model is protected by using this structure.

IV. Real Life Examples of ECash Paying Systems

Although eCash as a concept was invented in the previous century, it is still a huge inspiration for the modern electrical paying systems. In this part we will give an overview on some of the currently most used paying systems based on the eCash system. From 2015 the term eCash is used for the digital cash that can be transferred between entities and can be stored on electronic cards or some alternative online mobile or web platforms. [**?**]

Nowadays, the electronic payment systems are a very important part of our lives and we use them all the time. Based on the fact whether there is a central authority that controls the money flow, the payments systems can be classified as centralized or decentralized.

The centralized payment systems have a central authority (a bank, a nation) and therefore they are regulated by laws in specific countries. The centralized systems support cash transfer protocols (which have to be authorized by a bank), but they do not support in general the concept of digital currency. Also, nowadays the centralized systems are moving into the direction of digitalization of the transactions via creation of digital wallets where people can store different types of funds and make contactless transactions through one or multiple mobile devices. The first example of a digital wallet was the Mondex who introduced the so called electronic purse. Some of the most popular digital wallets that are being used nowadays are: PayPal, Google's Wallet, Apple Pay, Venmo, eWallet etc. Some of the digital wallets can work with digital currencies that are part of the decentralized systems. [**?**]

The decentralized payments systems do not have a central authority and mainly they are not regulated by laws. The main asset in the decentralized systems are the cryptocurrencies. The cryptocurrencies are dependent on the digital signatures for asset transfer, on peer-to-peer networkings and on proof-of-work and proof-of-stake schemes for management of the payment systems. The first published cryptocurrency was Bitcoin which is based on blockchain technology. After that over 6000 altcoins (alternative cryptocurrencies to Bitcoin) have been released. [**?**]

Acknowledgment

This work was partially financed by the Faculty of Computer Science and Engineering at the Ss. Cyril and Methodius University, Skopje, North Macedonia.

References

[1] Baddeley, Michelle. ”Using e-cash in the new economy: An economic analysis of micro-payment systems.” Journal of Electronic Commerce Research 5.4 (2004): 239-253.

[2] Fera, Leah, et al. ”Digital cash payment systems.” Dec 6 (1996): 1-21. APA

[3] https://due.com/blog/defining-ecash-and-calculating-its-benefits/

[4] Jing, Yang. ”On-line Payment and Security of E-commerce.” Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009). Academy Publisher, 2009.

[5] Srivastava, Lara and Robin Mansell. “Electronic Cash and the Innovation Process: A User Paradigm.” (1998).

[6] Marius, Popa, Calugaru, Adrian. (2009). On-line Payment System Survey–eCash. Journal of Mobile, Embedded and Distributed Systems. 1. 95-103.

[7] Boldyreva, Alexandra, and Daniele Micciancio, eds. Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings. Part III. Vol. 11694. Springer, 2019.

[8] Camenisch, Jan, Susan Hohenberger, Anna Lysyanskaya. ”Compact e-cash.” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2005.

[9] https://due.com/ecash/

[10] http://nearfieldcommunication.org/payment-systems.html

[11] Böhme, Rainer, et al. ”Bitcoin: Economics, technology, and governance.” Journal of economic Perspectives 29.2 (2015): 213-38.

[12] Bourse, Florian, David Pointcheval, and Olivier Sanders. ”Divisible e-cash from constrained pseudo-random functions.” International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2019.

[13] Camenisch, Jan, et al. ”Oblivious PRF on committed vector inputs and application to deduplication of encrypted data.” International Conference on Financial Cryptography and Data Security. Springer, Cham, 2019.