On the use of continued fractions for electronic cash

Amadou Moctar Kane amadou-moctar.kane.1@ulaval.ca
Département de Mathématiques et de Statistiques
Université Laval
Québec G1V 0A6 Canada.

Abstract

This paper presents an electronic cash scheme using the theory of continued fractions. Continued fractions have already some utilities in cryptography such as in the cryptanalysis of RSA ***[17]*** or in the design of some stream ciphers ***[9]***. In order to achieve our prepaid e-cash scheme, we will use the continued fraction expansion of some irrationals numbers, although the same scheme can be obtain with a block cipher algorithm like AES or with some pseudo-random generators. Our e-cash scheme has two aims: the first one is to create a payment system independent of current constraints such as the revocation of anonymity (in the double spending case) or the obligation for those who want to use the e-cash, to have a bank account.
The second aim is to propose here a solution which prevents the copy of our e-coins and allows if necessary the reimbursement of the user with e-cash.

Keywords: continued fractions, cryptography, electronic commerce, electronic cash, prepaid card.

1. INTRODUCTION

The electronic cash aim is to permit an efficient trade in a total anonymity over networks. In the e-cash system, the user withdraws electronic coins from a bank, and pays a merchant using these coins. During the transaction, the merchant can verify the authenticity of the electronic coins (in some protocols the merchant does not need to interact with the bank before accepting a coin from the user); collects multiple coins spent by users and deposits them later at the bank. In our case the scheme is a bit different because the bank makes a prepaid card and the user buys this card in a shop.

The e-commerce is widely developed today, unfortunately many transactions are done with credit cards. And as we know it, making a transaction with a credit card can be dangerous when the web merchant is not well protected or when the web merchant is cheating. Recently, information from more than 130 million credit and debit cards was stolen in some big company in North America ***[2]***. Because of the increasing number of frauds, it is likely that holders of credit and debit cards will suffer the consequences of these frauds in the future.
We can list in the following some reasons which delay the emergence of the e-cash system in the world.

- People do not know how it is dangerous to use a credit card on-line.
- E-cash are often produced for holders of bank accounts.
- The existence of the e-cash is only known by passionate people.
- E-cash are accepted by a small number of traders.
- The e-cash cost is quite expensive.

- E-cash are produced by very few banks.
- There exists some fears regarding the traceability of e-cash.
- …

To correct these mistakes, we believe that the e-cash must be done in such a way as to be easy to get and to use. Unfortunately up to now, all the solutions given in the e-cash system are difficult to implement for a large public. Since the introduction of the e-cash by Chaum ***[3]*** in 1982, a lot of others protocols have been proposed. Among these protocols Okamoto and Ohta ***[6]*** have proposed the six desirables properties for an electronic currency system:

I. Hardware independence:
   The cash can be sent securely through computer networks.
II. Security:
   The ability to copy (reuse) and forge the cash must be prevented.
III. Anonymity:
   The identity of the user should be protected, but for some transactions weaker forms of anonymity should be use ***[1]***.
IV. Off-line:
   The transaction can be done off-line, meaning no communication with the bank is needed during the transaction.
V. Transferability:
   The e-cash can be transferred to others users.
VI. Dividability:
   A piece of cash can be divided into smaller amounts.

We can add to these six properties two new ones. The first one is: to be efficient, the transaction must be quick in some phases. The second one is the reimbursement of the user, which must be available if the client is not satisfied by goods or services.

To ease the use and the acquisition of the e-cash, we propose to increase the use of prepaid cards. In this paper the prepaid card is a piece of paper contending some hidden codes. This card can create some security issues because of the total anonymity which it gives. Hence, it will depend on each issuer to limit the value of the prepaid card or to forbid the use of the e-cash in the sale of some dangerous products. In some countries, some studies on prepaid cards have already been done ***[15]***, and some prepaid cards already exist.

In the e-cash area there exists now some efficient schemes such as the compact e-cash ***[4]*** which permits the withdraw of 2^lcoins in a short time. And more recently some news schemes can use the compact e-cash without the trusted third party ***[5]***.
Up to now, a lot of solutions such as the hash function, the random oracle model, the cut-and-choose technique, and the blind signature have been used in e-cash schemes. Our approach in the e-cash system is different, because of these following points.

I. We want to introduce the use of continued fractions in e-cash protocols.
II. In order to avoid some burdens imposed by the banks, we want to reduce their influence on the e-cash system.
III. We want to prevent the copy of the e-cash.
IV. As noticed previously, we believe that the reimbursement is important to solve in all e-cash schemes, because sending back the e-coin is not a solution.
V. Like the traditional cash, we want to create an e-cash which will be difficult to trace.
VI. We aim to present a very simple e-cash scheme.
VII. …

For the security aspect, we aim to cover these three issues, unforgeability, stating that valid coins can only be issued by the bank or an authorized entity; anonymity, ensuring that a user stays anonymous even if the complete system conspires against him; and exculpability, a malicious bank should not be able to conspire with malicious merchants to frame an honest user for double-spending.

Here we present an algorithm based on the difficulty of retrieving an irrational number from the sole knowledge of a part of its continued fraction expansion. As proved in ***[9]***, the continued fraction expansion can produce a pseudo-random sequence, hence our e-cash scheme is built around a pseudo-random sequence.

We recall that the use of pseudo-random function is already effective in some e-cash scheme like ***[4]***.

Continued Fractions: An expression of the form

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots}}}$$

is called a generalized continued fraction. Typically, the numbers $a_1, , b_1, \ldots$ may be real or complex, and the expansion may be finite or infinite.

We will avoid the use of the continued fraction expansions involving $b_i = 1$ for most i's. However, in order to simplify our explanation we will use in some cases the classical continued fraction expansion, namely $b_i = 1$ for any i:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

$$\alpha := a_0, a_1, a_2 \ldots$$

In this paper we denote by Γ the combined sets of algebraic irrationals of degree greater than 2 and transcendental numbers. Our algorithm, will use the irrational numbers which are in Γ, but we will avoid the use of transcendental numbers having a predictable continued fraction expansion (some examples of irrationals numbers given a predictable continued fraction expansion are presented in ***[7]***,***[10]***).

To calculate the classical continued fraction expansion of a number α, write down the integer part of α. Subtract this integer part from α. If the difference is equal to 0, stop; otherwise find the reciprocal of the difference and repeat. The procedure will halt if and only if α is rational.

We can enumerate some continued fractions properties:

I. The continued fraction expansion of a number is finite if and only if the number is rational.
II. The continued fraction expansion of an irrational number is unique.
III. Any positive quadratic irrational number α has a continued fraction which is periodic from some point onward, namely a sequence of integers repeat. (Lagrange Theorem)
IV. The knowledge of the continued fraction expansions of α and β cannot determine simply those of $\alpha + \beta$, or $\alpha\beta$.

Continued fractions were widely studied by C. Olds ***[13]*** and O. Perron ***[14]***, but cryptographic views are not explored by number theory specialists except in some fields like RSA cryptanalysis.

This paper is organized as follows. In section 2 we will propose and demonstrate some results concerning continued fractions; in section 3, we will introduce our e-cash scheme. Section 4 prove the security given by our scheme, and before the conclusion, we will study the efficiency of our design.

2. RESULTS

In order to show that the merchant or the user will not be able to make e-coins, we will prove the result 1 and 3. The result 2 will help us to exhibit an example of irrational number which we can use in our e-cash scheme.

Definition 1. An electronic cash scheme is secure if it has the unforgeability, the anonymity, the exculpability, and if the e-cash can not be copied.

Notation
Let $\alpha \epsilon \Gamma$ such that $a_1, \dots, a_m, \dots, a_{m+n}, \dots$ is the continued fraction expansion of α; m and n are two integers such that $m > 20, n \geq 1$. We denote by δ the vector made with the n partial quotients following the m first partials quotients in the continued fraction expansion.

Remark
The choice of $m > 20$ does not have a real influence on the security of this algorithm.

Result 1. *It is not possible to find α out of the knowledge of δ.*

Proof. Let $\alpha \epsilon \Gamma$. We suppose that we know a given part $a_{m+1}, \dots, a_{m+n}$ of α's continued fraction expansion. Can we find α with the knowledge of these n partial quotients?
The answer is negative, because there exists an infinite number of irrationals with these same partial quotients.
For instance we can exhibit infinitely many irrational numbers α_ρ which are different from α and which have the property that $a_{m+1}, .., a_{m+n}$ appears as a sequence of n consecutive partial quotients. As a matter of fact, when θ is an irrational number, it suffices to consider any sequence of m integers $(r_1, r_2, \dots, r_m)$ and to define α_ρ to be

$$\alpha_\rho = r_1 + \cfrac{1}{\ddots_{r_m} + \cfrac{1}{a_{m+1} + \cfrac{1}{\ddots_{a_{m+n-1}} + \cfrac{1}{a_{m+n} + \frac{1}{\theta}}}}}$$

Result 2. *For an integer r such that $r \geq 3$ and a real algebraic number A ($A \neq 0, 1$), the number $\sqrt[r]{log\ (A)}$ is transcendental.*

Proof. Assume that A is a real algebraic number such that $A \neq 0, 1$, then $\log(A)$ is transcendental number by Corollary 3.6 of ***[8]***.
If we suppose that $X = \sqrt[r]{\log(A)}$ is an algebraic number, then X^r is a algebraic number, which is absurd because $X^r = log(A)$ and $log(A)$ is transcendental.

Remark
The irrational number $\sqrt[r]{\log(A)}$ used in this paper is not a standard which we impose. It is an example which we choose in order to illustrate our scheme.

Result 3. *Let $\beta \epsilon \Gamma$ and let $a = [a_m, \dots, a_{m+n}]$ be a part of the continued fraction expansion of β. The knowledge of a does not allow to know any other partial quotient of continued fraction expansion.*

Proof. From the proof of *Result 1*, we can deduce the proof of *Result 3.*

For instance we can exhibit infinitely many irrational numbers γ such that the partial quotients of the continued fraction expansion of γ ($[u_0, u_1, u_2, \dots]$) verify $u_t \neq a_t$ for any $t \geq m+n+1$, $u_i \neq a_i$ for any $i < m$, and $u_j = a_j$ for any $m \leq j \leq m+n$.

3. DESIGN

Definitions
In this design, we have four entities the bank (***{B}***), the user (***U***), the merchant (***M***) and the trusted third party (***{TTP}***). We denote the concatenation by ||, and the hash function by h.

Remark
In order to reduce the influence of banks, the banking entity could be replaced in this scheme by a person who have a public key, a credit card and who is permitted to sell e-cash prepaid cards.

3.1 Design

We suppose that all communications between the protagonists are secure, we assume that the bank public key, the merchant public key, and the ***{TTP}*** public key are available for all entities. The integer e is fixed arbitrarily for all entities ($e = 7$). The solution proposed in this paper can be divided in five parts.

I. The bank preparation

a. ***{B}*** chooses randomly a number $z \in N^* \backslash \{1\}$ and computes the irrational number $\alpha = \sqrt[e]{\log(z)}$.
b. ***{B}*** computes the first partial quotients of α. For example if the price of the prepaid card is ten dollars, then the bank will compute the 1020 first partial quotients of the irrationals numbers α. In the following, ***{B}*** will ignore the 20 first partial quotients.
c. ***{B}*** chooses x_1 and q which are the prepaid card number.
d. The bank writes q and x_1 in the prepaid card.
e. The bank hides q.
f. ***{B}*** sends to the ***{TTP}*** z, q and x_1.
g. The bank sells the prepaid card to a shop.

II. The user preparation
We suppose that the user has already downloaded the software managing the prepaid card.
a. Before buying a prepaid card, the user and the seller ask to the ***{TTP}*** if the card number x_1 is already allocated?
b. If the ***{TTP}*** response is negative, the seller asks to the ***{TTP}*** to activate the prepaid card.
c. The ***{TTP}*** activates the card, chooses randomly a number $q_1 \in N^* \backslash \{1\}$ and sends q_1 to the user.
d. The vender sells the card to the user.
e. The user scratches the card and recovers q.
f. When the user connects the software, he chooses randomly a number $x \in N^* \backslash \{1\}$ and sends x, x_1, q_1 and q to the ***{TTP}***.

III. The ***{TTP}*** preparation
a. The ***{TTP}*** verifies if x_1, q and q_1 match.
b. If the verification is conclusive, the ***{TTP}*** computes y= $\sqrt[e]{\log(x)}$ and $\alpha = \sqrt[e]{\log(z)}$.
c. The ***{TTP}*** computes the first partial quotients of y and α. For example if the price of the prepaid card is ten dollars, then the ***{TTP}*** will compute

the 1020 first partial quotients of the irrationals numbers y and α. In the following, the ***{TTP}*** will ignore the 20 first partial quotients.

d. For all $i's$ (21 to 1020), let c_i be the concatenation of i-th partial quotient of y which is y_i and the i-th partial quotient of α which is α_i, hence $c_i = y_i \,||\alpha_i$.
e. The ***{TTP}*** computes the hash of the 100 first c_i's namely h_1, before computing it for the 100 c_i's following until the end of the c_i's.
f. The ***{TTP}*** sends the ten hash $\{h_1, h_2, \dots, h_{10}\}$ to the bank.
g. From the ten hash, the bank produces ten signatures $\{s_1, s_2, \dots , s_{10}\}$ with its private key.
h. The bank sends the signatures to the ***{TTP}***.
i. The ***{TTP}*** sends the signatures $\{s_1, s_2, \dots , s_{10}\}$ to the user.

IV. The Spending.
a. The user visits the merchant website and chooses for example a product which price is 3 dollars and 11 cents.
b. For the payment, the web merchant transfers the user to the ***{TTP}*** website.
c. The ***{TTP}*** asks to the user x_1, the 311 first useful partial quotients and the three first signatures mainly s_1, s_2, s_3.
d. The user ignores the 20 first partial quotients, sends the 311 following, x_1 and the signatures s_1, s_2, s_3.
e. The ***{TTP}*** rebuilds the c_i's after the calculation of the 420 first partial quotients of α.
f. The ***{TTP}*** verifies the validity of signatures and partial quotients. He generates with its private key s which is the signature of the 11 last partial quotients if all signatures and partial quotients are valid.
g. The ***{TTP}*** sends to the merchant the signatures s, s_1, s_2, s_3, the 311 partial quotients and x_1.
h. The merchant verifies the validity of the signatures received with public keys.
i. The merchant sends the product to the user if the partial quotients are valid.

V. The deposit
a. The merchant sends to the bank x_1, the signatures s, s_1, s_2, s_3 and the 311 partial quotients.
b. The bank verifies the validity of the partial quotients received.
c. If all the partial quotients are valid, the bank sends 3 dollars and 11 cents to the merchant.
d. When the bank is replaced by a person who sells prepaid cards, the person will pay the merchant with his credit card.

3.2 Remark

I. The order of the partial quotients is important to respect.
II. We suppose that the hash function used in this scheme is a collision resistant hash function.
III. In order to be effective, the bank signs by hundred partial quotients. But if the bank computing possibilities are high, the bank can sign by ten partial quotients (or less).
IV. In our scheme we assume that the smallest coin value is one cent, but depending on the value of the prepaid card the partial quotient value can for example correspond to 10 cents, 1 dollar…
V. For example in the case where a partial quotient value is one dollar, the ***{TTP}*** can divide the partial quotient. If we assume that c_1 is partial quotient to divide,

the ***{TTP}*** computes the partial quotients of $c = \sqrt[e]{\log(10^{40}\log(c_1)}$. The ***{TTP}*** ignores the 20 first partial quotients and takes the 100 partial quotients following, each value of these new partial quotients is one cent.

VI. Due to the rounding errors, the use of continued fractions must obey some rules. For example the ***{TTP}***, the user, and the bank must agree on their multiple precision library, on the rounding error, on the software used and on the architecture.

3.3 Reimbursement

A lot of electronic cash schemes omit or neglect this functionality which is a serious issue for the development of the e-cash system. We suppose that the user buys some goods with e-cash coins and he is unsatisfied when he receives the product. As the law allows it, he asks for a reimbursement to the web merchant. The anonymity of the user must be protected and we do not want the merchant to see the e-cash that he has to send back to the user (reuse).
The user can recover his e-cash in these following steps.

I. The user chooses randomly a transaction number N_1 and sends to the merchant a file $fic\ (x_1, N_1)$ contending x_1 (his prepaid card number), and N_1.
II. The merchant signs the file $fic(x_1, N_1)$ with his private key and sends to the user the signed file denoted by $fic_M\ (x_1, N_1)$.
III. The user verifies the validity of the merchant signature with the merchant public key. If the signature is valid, the user sends back to the merchant the goods with a system of acknowledgment of receipt (the user will receive a proof showing that he has sent the goods and the merchant has received it).
IV. The merchant sends the file $fic_M\ (x_1, N_1)$ to the bank as soon as he receives the goods.
V. The bank signs the file $fic_M\ (x_1, N_1)$ with its private key and sends to the merchant the signed file denoted by $fic_{MB}\ (x_1, N_1)$.
VI. The merchant verifies the validity of the bank signature with the bank public key. If the signature is valid, the merchant sends to the bank an signed order to debit the amount on his account.
VII. The bank sends to the ***{TTP}*** x_1, N_1, and the number of partial quotients needs for the reimbursement (for example 311).
VIII. The ***{TTP}*** computes the partial quotients from 1021 to 1332 of y and α which are $y_{1021}, \dots, y_{1332}$ and $\alpha_{1021}, \dots, \alpha_{1332}$. For all i's from 1021 to 1332, let c_i be the concatenation of i-th partial quotient of y which is y_i and the i-th partial quotient of α which is α_i, hence $c_i = y_i \,||\alpha_i$.

From $i = 1021$, the ***{TTP}*** computes the hash of the hundred first c_i's before computing it for the hundred c_i's following until the last bloc of hundred c_i's. The ***{TTP}*** computes the hash of 11 c_i's remaining.

The ***{TTP}*** writes in the same file, the four hash produced $(h_{11}, h_{12}, h_{13}, h_{14})$, x_1 and N_1. The ***{TTP}*** signs the file and sends to the bank the signed file denoted by f_{TTP}.

IX. ***{B}*** signs the four hash $(h_{11}, h_{12}, h_{13}, h_{14})$ with its private key, sends the four signatures produced $\{s_{11}, s_{12}, s_{13}, s_{14}\}$ and the file f_{TTP} to the web merchant.
X. The web merchant sends $\{s_{11}, s_{12}, s_{13}, s_{14}\}$ and the file f_{TTP} to the user.
XI. The user verifies the bank signature, verifies the ***{TTP}*** signature and recovers the four signatures required for his future transaction.

4. SECURITY ANALYSIS

Result 4. *According to definition 1 the e-cash scheme proposed in this paper is secure:*

- *The e-cash is unforgeable.*

- *The e-cash user is anonymous.*
- *The e-cash scheme has an exculpability property.*
- *The user is unable to copy the e-cash.*

Proof. In the following, we will prove that our scheme respect these four properties. We suppose that we have four potential attackers in this scheme. This attack can be tried by the user, by the merchant, by the bank or by someone else who is completely outside the scheme.

4.1 Unforgeability

The unforgeability is effective for someone who is outside the e-cash scheme under the assumption that the bank signature is unforgeable and the communication between the protagonists is secure.

If we assume that the user is not able to forge the bank signature, the unforgeability is effective for the user because of the following reasons.

- The user does not know the bank partial quotients which are α_i, so he will not be able to send corrects c_i's to a web merchant without the help of the ***{TTP}***.
- The user can not forge e-coins in addition to the good e-cash that he already has, because he needs the bank signature for these new partial quotients.

Due to the following points the merchant can not forge a valid e-cash.

- The merchant is not able to find the partial quotients corresponding to the signatures sent by the bank (in the case of a reimbursement).
- Assuming that the merchant knows the $c_i = y_i||\alpha_i$, can he guess the y_i and the α_i? The answer is negative because the number of digits of partial quotients is not fixed. In some cases a probability attack can find some y_i and α_i.
- Assuming that the merchant knows a lot of y_i (or α_i) can he find y (or α)? The answer is negative (proved in result 1).
- Assuming that the merchant knows y_i, can he find y_{i+1}? The answer is negative (proved in result 3).
- Even if we suppose that the merchant can find $y_{i+1}, y_{i+2}, \ldots, y_{i+100}$, he will not be able to forge the bank signature.

If we assume that the merchant and the user are accomplice.

- The user sends to the ***{TTP}*** his partial quotients and the bank signatures.
- The ***{TTP}*** computes α_i's, concatenates partial quotients, verifies bank signatures and sends signatures and c_i's to the merchant.
- The merchant sends to the user the c_i's.
- Since the user knows c_i he can find the α_i used but he can not find α (proved in result 1) and he can not find more α_i's (proved in result 3).
- The user and the merchant can not swindle the bank.

If we assume that the bank tries to swindle the user.

- The bank receives from the merchant the c_i's.
- Since the bank knows c_i he can find the y_i used but he can not find y(proved in result 1) and he can not find more y_i's (proved in result 3).
- The bank can not swindle the user.

4.2 Anonymity

The prepaid card is bought somewhere in the world, then the anonymity of the user is total. Even in the case of a reimbursement his anonymity is protected.

4.3 exculpability

The double spending is not feasible for the user, then the exculpabilty is effective in this scheme.

4.4 The e-cash can not be copied

The e-cash can not be copied by the user because of the ***{TTP}*** participation. If we suppose that the user sends these 400 partial quotients of y which are $y_{21}, \dots, y_{420}$ to the ***{TTP}***. The ***{TTP}*** computes the partial quotients corresponding which are $\alpha_{21}, \dots, \alpha_{420}$. When the user tries to send again the same 400 partial quotients, the ***{TTP}*** will assume that the user is sending the rest of his continued fraction expansion, then the ***{TTP}*** computes the 400 partial quotients following which are $\alpha_{421}, \dots, \alpha_{820}$. Hence, the signatures will not match with the partial quotients and this payment will be rejected.

If we suppose that the merchant copies the e-cash which he has received from the ***{TTP}***, and deposits it twice to the bank. The bank can easily find the cheater and refuses to send the concerned money twice. If the merchant copies the e-cash and gives the copy to another merchant, the ***{TTP}*** can show who had received in the first time the partial quotients which he sent.

4.5 Reimbursement security

Due to the total anonymity given in this scheme, the reimbursement must obey to some proprieties.

I. While protecting his anonymity, we must be sure that the user will receive his money back if he returns the undesirable product to the merchant.
II. We must be sure that the reimbursement can not be returned to someone else (someone who has stolen the product for example).
III. We must be sure that the seller has received its products and the condition of the product is good.
IV. We must be sure that the e-cash refunded is secure in the sense of *result 4*.

The first property is satisfied in our scheme, because to ensure that the user will receive his money back if he sends the goods to the merchant, the user has the file signed by the merchant $fic_M\ (x_1, N_1)$ and the acknowledgment of receipt.

To ensure that the bank will provide e-coins to the merchant, the merchant has the statement of his account showing that the money has been debited.

If after receiving the e-coins, the merchant denies and argues that he has not received the e-cash, the bank will send back the e-coins through the ***{TTP}***.

If after receiving the e-coins, the user denies and argue that he has not received the e-cash, the merchant will send back the e-coins through the ***{TTP}***.

If the bank tries to scam the user by sending an old refund where the user had chose (x_1, N), the merchant will exhibit $fic_{MB}\ (x_1, N_1)$ in order to prove to the bank that the user had sent (x_1, N_1).

If the merchant attempts to scam the user by sending to the user an old refund where the user had chose (x_1, N), the user will exhibit $fic_M\ (x_1, N_1)$ in order to prove that he had sent (x_1, N_1).

The second condition is solved by the fact that the user and the ***{TTP}*** are the only ones who know y, so if someone else return the merchandise to the merchant, he will not be able to use the signatures sent by the bank without knowing the partial quotients of the irrational number y.

The third condition is solved, since the acknowledgment of receipt allows the merchant to refuse the goods if it comes in a bad condition.

Finally, the fourth issue is resolved because the refunded e-cash is a part of the e-cash investigated in *result 4*.

Remarks
We recommend the use of the generalized continued fraction instead of the classical continued fraction, because the classical continued fraction produces a several partial quotients with only one digit ***[12]***. Even if the classical continued fraction is used, guessing 100 partial quotients in the right order will be very difficult. Another solution is to concatenate the partial quotients before the use.

5. EFFICIENCY ANALYSIS

We largely draw our inspiration from the evaluation method used in ***[11]*** in order to perform our critical discussion. We prove in this section that our scheme satisfy the specific characteristics from usability points of view, we compare our scheme with other e-cash models and with the traditional cash.

5.1 Usability

P2P Transferability: Our e-coin is transferable between users. If we suppose that user1 transfers 50cts to user2, then user1 has to send the 50 partial quotients concerned and the copy of the bank signature to user2. Hence user2 will not be able to spend more than 50cts because he can not guess the rest of the partial quotients (proved in result 3) and this transfer does not need the intervention of any authority (***{TTP}***, bank).

Interoperability: The use of continued fractions needs some precautions, so it can be difficult to inter-operate with e-cash using other formats.

Applicability and Cost: This scheme is very affordable because protagonists needs are: a simple calculator in order to compute the partial quotients; a connection between them (for example internet); and one software in order to manage the signatures. We recall that they need to agree on some rules in order to have the same partial quotients.

Ease of use: stages of preparation, expense and deposit are relatively short. The only point which could be cumbersome is the ***{TTP}***, however we believe that the ***{TTP}*** could be a server managed by the government. The ***{TTP}*** should not require an human intervention except during its audit or maintenance.

Efficiency: The time need for computing the partial quotients is low ***[9]***, and the time need for computing (verifying) the signature and the hash is low. We can add that the storage need is not important because it consists on storing approximately 1000 numbers for each user. The ***{TTP}*** capacities must be important because he plays a central role in this scheme.

Scalability: This system is scalable even for the ***{TTP}***.

Off-line usage: The system works in one-line mode because we need to prevent the copy of the partial quotients and to protect the anonymity of the user.

Mobility: The important things are bank signatures and integers (z, x), and they have the property of mobility.

5.2 Comparison

If we compare our solution to other existing e-cash schemes, we find that we meet the usual criteria such as security, mobility, portability, dividability, scalability, and P2P transferability. We

exceed by far these criteria with the introduction of the reimbursement that we have not seen yet in an e-cash scheme, and we prevent the copy of e-cash where most of the existing schemes break the anonymity of the user in a case of a double spending ***[3]***. The element that might play against our scheme would be the off-line use because we have reintroduced the ***{TTP}*** which most of the new schemes remove. The first reason which motivates the reintroduction is: the absence of the ***{TTP}*** in e-cash models is often offset by the introduction of a smart card ***[11]*** or an RFID tag. We have avoided the use of these cards because we have designed this e-cash scheme for internet transactions and using these cards on the Internet is often difficult, expensive and as dangerous as the traditional credit cards. The second reason is: we reintroduced the ***{TTP}*** entity because we take our inspiration from traditional cash where the bank distributes just the ticket which it has received from the central bank. We consider here the ***{TTP}*** as a sort of a central bank.

In Table 1 we compare our e-cash with the traditional cash

Characteristics	Our e-cash	Traditional cash
Verifiable origin and unforgeability	- Knowledge of the partial quotients. - Order of the partial quotients. - Authenticity of digitally signed.	Authenticity by means of material secure characteristics
Anonymity	- E-coins are anonymous. - Prepaid card is anonymous. - User anonymity can not be cancel.	Regular coins are anonymous. Payee is normally identifiable.
Untraceability	Serial numbers of prepaid cards can be recorded	Serial numbers of notes though, can be recorded
divisibility	Partial quotients are divisible.	Change can be done.
Mobility	Partial quotients and signatures have the property of mobility.	The paper is easy to transport.
Scalability	Everything can be extended in this scheme.	Only physical constrains of production, storage and transfer.
P2P Transferability	- Exchange of partial quotients and signatures. - No intermediate entities. - The merchant is able to exchange his partial quotients and signatures.	Physical objects exchange.
Off-line	One-line	No reference to authority while circulating
Life-cycle	- Coin expiration to reduce the ***{TTP}*** storage.	Material physical deterioration and destruction
Openness	-Open protocols (Continued Fraction Algorithm & Public Key	No infrastructure needed on the

	cryptography) - Common hardware (Calculator, Internet)	user's side
Reimbursement	The merchant sends back the e-coins to user The anonymity of the user is protected even in this case.	Physical objects can be given back.
Copy	The e-coin can be copied by the user but the presence of the ***{TTP}*** prevents the use of the copied e-coin. The e-coin can be copied by the merchant but bank will not send the concerned amount twice.	The cash can be copied by the user but the merchant and the bank are able to detect fake cash.

TABLE 1: Comparison between the designed e-cash (for Internet user) and the traditional cash.

6. CONCLUSION

We introduced in this paper an e-cash scheme using a prepaid card system, in summary the scheme presented here looks like a counter.
Assuming that it is the e-cash which has to adapt to users and not the opposite, we have designed a low cost system (scratch card) accessible to those who had not a bank account (prepaid card). At the same time, we have avoided to the Internet users some congestions such as readers of smart cards, and we have incorporated in our system most of the features existing in other e-cash models. On the other hand we have improved the patterns of existing e-cash, by proposing the use of the reimbursement, which is closer to reality since when a user buys something, he may have to return the thing purchased at the store if it does not suit him.
Finally, we introduced the use of continued fractions in order to create an alternative to mechanisms already used in the e-cash schemes (for example hash function and random oracle model).

Due the computer limits, the use of irrational numbers can be theoretical, but as proved in ***[9]***, we can use an approximation of irrational numbers.

It could be interesting in future research to find a prepaid card off-line without the ***{TTP}*** and where the communication between protagonists is not secure.

7. REFERENCES

1. E. Brickell, P. Gemmell, D. Kravitz, “Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change” In Proc. 6th Annual ACM-SIAM Symposium on Discrete Algorithms, 1995.
2. TJX suspect indicted in Heartland “Hannaford breaches” http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect.
3. D. Chaum, “Blind Signatures for Untraceable Payments.” In Proceedings of CRYPTO 82, 1983, Plenum, New York.
4. J. Camenisch, S. Hohenberger, and A. Lysyanskaya, “Compact e-cash” In EUROCRYPT, 2005, pages 302-321.
5. Man Ho Au, Willy Susilo and Yi Mu, “Practical Anonymous Divisible E-Cash From Bounded Accumulators.” In Proceedings of Financial Cryptography and Data Security 2008 (FC 2008).
6. T. Okamoto, K. Ohta, “Universal Electronic Cash.” In Proceedings of Crypto 91, 1992.
7. Beeler M., Gosper R.W., and Schroeppel, R. Hakmen, “MIT Artificial intelligence memo 239”, Feb. 29, 1972.
8. E.B. Burger and R. Tubbs, “Making transcendence transparent: An intuitive approach to classical transcendental number theory”, Springer-Verlag, 2004.
9. Amadou Moctar Kane, “On the use of Continued Fractions for Stream Ciphers” In Proceedings of Security and Management 2009, Las Vegas, USA.
10. Donald E. Knuth, “The art of computer programming Volume 2: Seminumerical algorithms (3rd Edition)”, Addison-Wesley, 1997.
11. Dimitrios Lekkas and Diomidis Spinellis. “Implementing regular cash with blind fixed-value electronic coins”. Computer Standards & Interfaces, 29(3), March 2007, 277–288.
12. P. Levy, “Sur les lois de probabilité dont dépendent les quotients complets et incomplets d'une fraction Continue”, Bull. Soc. Math. 57 (1929) 178-194.
13. C. D. Olds, “Continued Fractions”, Random House, 1963.
14. Oskar Perron, “Die Lehre Von Den Kettenbrüchen”, 3rd ed. (1954).
15. Report to the Council of The European Monetary Institute on PREPAID CARDS by the Working Group on EU Payment Systems, May 1994.
16. Sattar J Aboud "Secure E-payment Protocol". International Journal of Security,Volume 3, Issue 5:85-92, 2009.
17. Bruce Schneier, “Applied cryptography (2nd ed.): protocols, algorithms, and source code in C”, John Wiley & Sons, Inc., (1995).
18. G. Skinner. "Multi-Dimensional Privacy Protection for Digital Collaborations". International Journal of Security,Volume 1, Issue 1:22-31, 2007.
19. Michael J. Wiener, “Cryptanalysis of short RSA secret exponents”, IEEE Transactions on Information Theory, 36, 553-558, 1990.
20. A.Chandrasekar, V. Vasudevan, V.R. Rajasekar "Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography" International Journal of Computer Science and Security,Volume 3, Issue 4:272-333, 2009.