MULTI-BANK ELECTRONIC CASH SCHEME BASED ON ELLIPTIC CURVE CRYPTOSYSTEM

Daxing WANG[1], Leying XU[2]

The payment system based on e-cash electronic is the core of e-commerce, but it is still in research stage. Elliptic curve cryptography has the advantages of short key size and fast implementation speed. We use the superiority of Elliptic Curve Cryptosystems to design an efficient e-cash scheme with many issuing banks. This scheme combines the divisibility of electronic cash, so it can better meet actual needs. The core idea of our scheme comes from the resistant Schnorr blind signature in Brands' scheme, and its security is based on the elliptic curve discrete logarithm problem. The analysis results of the scheme show that the new scheme has good properties, high security and efficiency.

Keywords: electronic cash, multi-bank, elliptic curve, divisibility

1. Introduction

Compared to regular cash, electronic payment systems offer greater convenience, but usually at the cost of a loss in terms of privacy. As an important means of payment, electronic cash (e-cash) not only has the security requirement like credit cards and electronic checks, but also has the advantages of independence, off-line payment and private ownership. The first e-cash system [1] was introduced by Chaum in 1982. To make better use of e-cash, the research of e-cash agreement is generally carried out from four characteristics, namely: conditionality, divisibility, transferability and multi-banking. The conditionality allows users and merchants to make the final cost based on the condition of an unknown result. Divisibility guarantees the user's spending on any denominations smaller than the electronic cash withdrawn. The transferability ensures that when the merchant receives the electronic cash spent by the user, it can directly spend the electronic cash without depositing it in the bank. Multi-banking imitates the situation of real money, allowing electronic cash to be circulated among multiple banks. The above four characteristics are all to expand the electronic cash protocol under the premise of ensuring the offline and anonymity of electronic cash, so that electronic cash can better realize the function of real currency. In 2015, in the

[1] School of Mathematics and Finance, Chuzhou University, China,
e-mail: daxingwang@chzu.edu.cn

[2] School of Mathematics and Finance, Chuzhou University, China,
e-mail: 305878321@qq.com

standard model, Canard et al. constructed an effective scalable and divisible electronic cash protocol and a practical divisible electronic cash protocol [2]. In 2016, Yang et al. constructed a practical, anonymous, and divisible e-cash protocol suitable for mobile devices. This protocol uses a trusted third party to build a divisible e-cash protocol that has a relatively high cost protocol [3]. In 2017, Haddad et al. constructed a conditional multi-payment protocol, which considered the user's consumption plan and used conditions to meet the user's personal consumption plan [4]. In some later studies, transferable electronic cash [5, 6] and multi-bank electronic cash protocol have also been proposed in recent days [7, 8]. However, most of these electronic cash schemes are provably security under the random oracle model [9] and are not practical in practice. In particular, the computational cost and time cost of a multi-bank electronic cash scheme using a complex group signature is too expensive. Since electronic coins are just digital data, they can easily be duplicated, and hence spent several times, which is called double-spending. Thus, an e-cash system needs a mechanism to detect such a double-spending and to identify the defrauder afterwards.

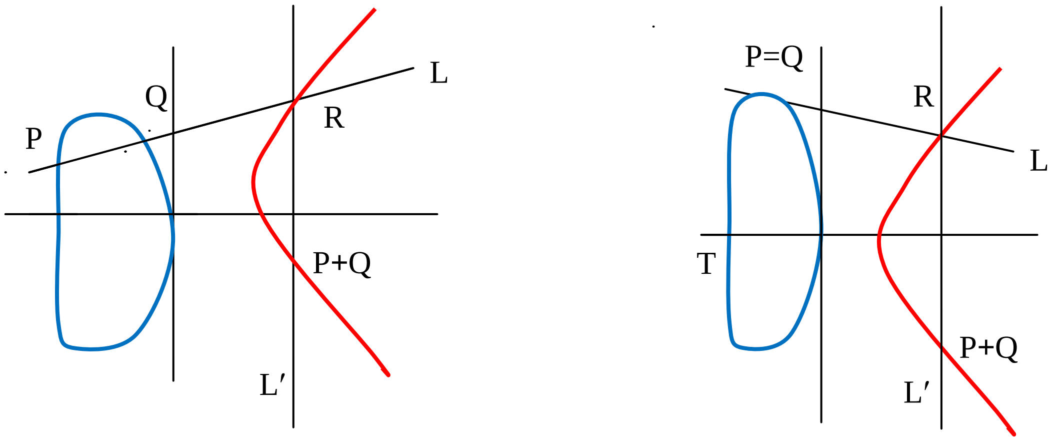
The key technology of e-cash is the blind digital signature algorithm [10] of cryptography. Elliptic curve cryptosystem [11] has the characteristics of “short key, high security”. We extended the Brands scheme [12] to the multiple banks e-cash model by using the Schnorr restricted blind signature [13] based on elliptic curve and proposed an efficient multi-bank e-cash scheme. Compared to the existed scheme [6, 7, 8], the new scheme has the advantages of short signature length, high efficiency, divisibility and detecting double spending.

2. Preliminaries

To discuss the research work of this paper in more detail, we must give the elliptic curve algorithm and the general electronic cash model. Elliptic curve cryptography is a method of public key cryptography based on elliptic curve mathematics. In 1985, Neal Koblitz and Victor Miller proposed the elliptic curve cryptosystem independently, which was based on the intractability of the discrete logarithm problem defined on elliptic curve point groups. Generally, when designing an electronic cash system, it is necessary to avoid fraudulent behaviors of users, banks and merchants. At the same time, it is also necessary to prevent trusted third parties from engaging in frauds similar to banks.

2.1 Elliptic curve discrete logarithm

To find the k-th power of an element in a finite field, we can use the "repetition-square multiplication" method to calculate it. Similarly, finding the point $kP \in E$ of a point $P \in E$ on the elliptic curve can also be calculated by the method of "repeated doubling and addition". We know that all point-by-point addition rules in an elliptic curve $E(F_q)$ form a finite commutative group. Therefore, there is also a discrete logarithm problem similar to the finite multiplicative group on elliptic curves. New scheme's security is based on the intractability of the elliptic curve discrete logarithm problem (abbreviated as ECDLP). The addition operation on the elliptic curve is shown in Fig. 1. Among them, addition operation of different point is shown in Fig.1(a), while Fig.1(b) shows addition operation of same point.



(a) Addition operation of different point (b) Addition operation of same point

Fig. 1. Addition operations on elliptic curves

Let $E(F_q)$ be an elliptic curve defined over a finite field F_q, and let $P \in E(F_q)$ be a point of order n. Given $Q \in <P>$, the elliptic curve discrete logarithm problem (ECDLP) is to find the integer x, $0 \le x \le n-1$, such that $Q = xP$. We choose a set of base points of the same order $P_1, P_2, \mathrm{L}\ , P_m \in E$, whose order is L. Then $a \in E$ can be expressed as an m-tuple $(x_1, x_2, \mathrm{L}\ , x_m)$ for all $1 \le i \le m$ and $0 \le x_i \le L$, we have:

$$a = x_1P_1 + \mathrm{L}\ + x_iP_i + \mathrm{L}\ + x_mP_m \qquad (1)$$

For any element $a \in E$, there are L^{m-1} m-tuple $(P_1, P_2, \mathrm{L}\ , P_m)$ representations of a. The discrete logarithm representation problem on elliptic curves is a generalization of the discrete logarithm problem of elliptic curves, that is, if the base point is randomly selected, finding two different representations of the same element is as difficult as solving the discrete logarithm of elliptic curves.

2.2 E-cash model

Electronic cash is a cash currency that exists in a digital form, and there is no clear physical form. It converts the cash value into a series of encrypted serial numbers, which represent the currency value of various amounts in reality through these serial numbers. After a user opens an account in a bank that develops electronic cash services and deposits money in the account, they can shop at merchants that accept electronic cash. In the general electronic cash payment system, at least three aspects of participation are required:

(1) Bank: Issue electronic cash.

(2) User: Withdrawal, payment and recipient of electronic cash.

(3) Merchant: Accept the user's electronic cash and send the goods.

(4) Trusted third party: To prevent fraud by criminals, users of specific electronic cash and electronic cash of specific users can be tracked when necessary.

In the typical electronic cash life, the interaction between customers, merchants and banks is shown in Fig. 2.

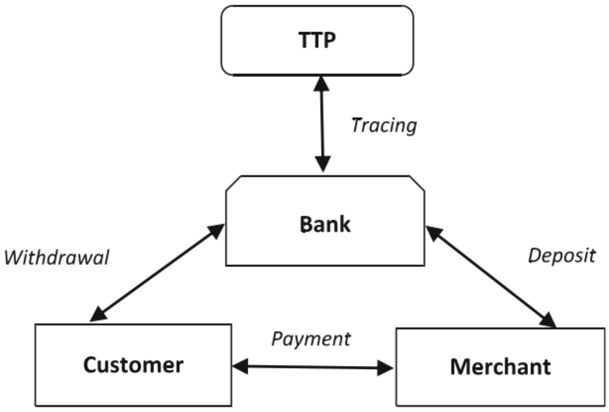


Fig. 2. Model of e-cash payment

The whole process is that the customer withdraws cash from the bank firstly, then the customer pays the electronic cash to the merchant, and the merchant deposits the electronic cash to the bank, and finally the customer deposits the unused electronic cash into the bank. The working process of multi bank e-cash model is as follows, shown in Fig. 3.

Step1. Registration.

The user U establishes linkages between the true identity and the anonymous identity through the trusted third party (TTP), which makes the TTP to revoke the user's anonymity later, and the TTP sends the registered certificate to the user.

Step2. Open an account.

The user U has his own account in his bank B_i .

Step3. Withdraw.

The user U withdraws an electronic cash from his bank B_i .

Step4. Spend.

The user U bought something at the shop S and paid the e-cash to the shop.

Step5. Deposit.

Upon receiving the data, the shop S verifies correctness of the signatures, and deposit the e-cash into bank B_j 's account.

Step6. Trace.

Once it is discovered that electronic cash is involved in fraud, the bank B_j submit it to the central bank which could find the bank B_i , and then traced it to the user U with the help of the TTP.

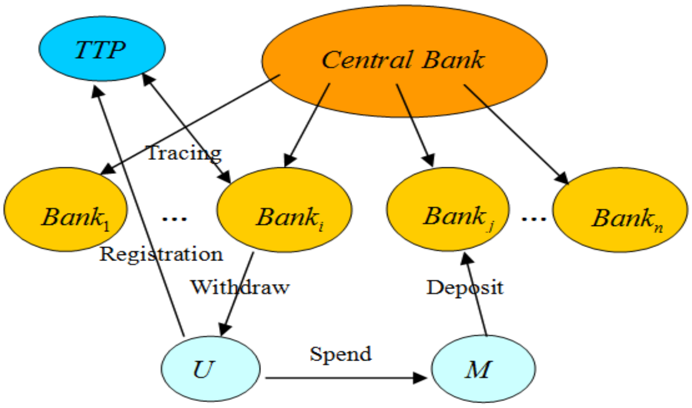


Fig. 3. Multi-bank e-cash model

3. Multi-bank e-cash scheme

The design idea of the multi-bank electronic cash solution is that each bank uses a different signature mechanism, uses its own private key to sign, and independently issues electronic cash coupons. If the number of banks in the system is small, the public key tables corresponding to all banks can be stored in each user's local database. When there are many banks, public key certificate technology can be used. In this way, each store can verify the validity of all electronic cash issued by banks. To solve the fund settlement between multiple banks, a settlement center is needed, and the design of the settlement center can replicate the real-life transaction system. The multi-bank electronic cash model based on the elliptic curve cryptographic algorithm we proposed is described as follows.

3.1 Initialization of the system

Elliptic curves $E(GF(q))$ is defined on finite field $GF(q)$, The number of rational points $\#E(GF(q))$ can be divisible by a big prime number n. The character of $GF(q)$ is p, and the base point $G, G_1, G_2 \in E(GF(q))$, $q = p$ or $q = 2^m$. Let $a, b \in GF(q)$, Elliptic curves $E(GF(q))$ is defined as follows:

$$y^2 = x^3 + ax + b, p > 3; \quad y^2 + xy = x^3 + ax^2 + b, p = 2. \tag{2}$$

Many banks choose $x_1, x_2, \cdots, x_n$ as their respective private keys to issue electronic cash. The corresponding public key is $h_1 = x_1 G,\ h_2 = x_2 G, \ldots h_n = x_n G$, and calculate $h = h_1 + h_2 + \cdots + h_n$ as public key for all banks. $H(\cdot)$ is a public one-way function, $\parallel$ shows connected operation of character string.

Each bank $Bank_i\ (1 \le i \le n)$ has a database that stores accounts. When the user U opens an account in bank $Bank_1$, the bank asks U to prove his identity. U selects u_1 randomly, and calculate $I = u_1 G_1$, then send it to $Bank_1$. The bank stores the identification information of user and I in the account database. At the same time, $Bank_1$ selects $e\ (0 \le e \le p)$ randomly, and calculate $E = e(I + G_2), z_1 = x_1 E$, then send E to $Bank_2, \cdots, Bank_n$ who calculate $z_2, \cdots, z_n$ and return them to $Bank_1$. $Bank_1$ calculates $z = e^{-1}\sum_{i=1}^{n} z_i$, and send it to U.

3.2 Withdrawal protocol

Before executing the withdrawal agreement, the user has to prove to the bank that he is the holder of the legal account. In fact, without revealing the private key, the user's identity information can be proved through a cryptographic protocol.

Step1. $Bank_1$ generates a pair of random numbers k, w_1 ($0 < k, w_1 \le p$), and calculate $a_1 = w_1 G$, $K = k(I + G_2),\ b_1 = w_1 K$, then send k to other banks $Bank_2, \cdots, Bank_n$ who calculate a_i, b_i and return it to $Bank_1$. $Bank_1$ calculates

$$a = a_1 + a_2 + \cdots + a_n, \tag{3}$$

$$b = k^{-1}(b_1 + b_2 + \cdots + b_n) \tag{4}$$

And sends a, b to the user U.

Step2. The user U chooses s, x_1', x_2' randomly, and calculates

$$A = s(I + G_2),\ z' = sz,\ B = x_1' G_1 + x_2' G_2 \tag{5}$$

Subsequently, U generates two numbers u and v of coprime, and calculates

$$a' = ua + vG, \quad b' = sub + vA, \tag{6}$$

$$c' = H(A_x \parallel B_x \parallel z_x' \parallel a_x' \parallel b_x'), c = c'/u \bmod n, \tag{7}$$

then sends c to $Bank_1$. A_x represents the x coordinate of point A.

Step3. $Bank_1$ calculates $r_1 = cx_1 + w_1 \bmod n$, and send c to $Bank_i$ $(2 \le i \le n)$, $Bank_i$ calculates r_2,L ,r_n respectively and send these numbers to $Bank_1$. $Bank_1$ calculates $r = \sum_{i=1}^{n} r_i \bmod n$, and send r to the user U, then deduct the Corresponding amount of deposit M_T from her account.

Step4. The user U checks whether the following two equations are valid:

$$rG = a + ch\ ,\quad r(I + G_2) = b + cz \tag{8}$$

If they holds, U calculates $r' = ru + v \bmod n$.

Finally, the signature obtained by U is $Sig(A,B) = (z', a', b', r', M_T)$, and save e-cash balance M_T. The entire withdrawal protocol is shown in Fig. 4.

U		$Bank_1$
$s, x_1', x_2' \in_R Z_n^*$		$k, w_1 \in_R Z_p^*$
$A = s(I + G_2), z' = sz, B = x_1' G_1 + x_2' G_2$.		$a_1 = w_1 G, K = k(I + G_2), b_1 = w_1 k$
$u, v \in_R Z_n^*$		send k to other $Bank_i$, $Bank_i$, and calculate a_i, b_i
$a' = ua + vG, b' = sub + vA$.		$a = a_1 + a_2 + \cdots + a_n$, $b = k^{-1}(b_1 + b_2 + \cdots + b_n)$
$c' = H(A_x \Vert B_x \Vert z_x' \Vert a_x' \Vert b_x')$	$\xleftarrow{a,\ b}$	
$c = c' / u \bmod n$	$\xrightarrow{c}$	$r_1 = cx_1 + w_1 \bmod n$
$rG \overset{?}{=} a + ch$		send c to other $Bank_i$, $Bank_i$, and calculate r_i
$r(I + G_2) \overset{?}{=} b + cz$		$r = r_1 + r_2 + \cdots + r_n \bmod n$
$r' = ru + v \bmod n$	$\xleftarrow{r}$	
Final signature $Sig(A,B) =$ (z', a', b', r' , M_T).		

Fig. 4. Withdrawal protocol

Only the user U knows a representation of the e-cash $(A, B, Sign(A, B))$, which is an effective e-cash. From the withdrawal protocol, we know that the protocol is a blind signature protocol, so that users can spend money anonymously.

3.3 Spend protocol

Step1. The user U sends the e-cash $(A, B, Sign(A, B))$ to the store S. S verifies whether the following equation is true:

$$r'G = H(A_x \Vert B_x \Vert z_x' \Vert a_x' \Vert b_x') \cdot h + a'\ ,\quad r'A = H(A_x, B_x, z_x', a_x', b_x') \cdot z' + b' \tag{9}$$

If the equation does not hold, the transaction will be terminated immediately. Suppose that the user U wants to pay the e-cash amount of M_p to the store, S tests if $M_T > M_p$ firstly, Otherwise the agreement is terminated. The store

S calculates $d = H(A_x \,\mathrm{P} B_x \,\mathrm{P} I_s)$, and send it to the user U, I_s stands for the account number of the store S in his bank.

Step2. The user U calculates:

$$r_1 = d(u_1 s) + x_1' \bmod n\,,\ r_2 = ds + x_2' \bmod n \tag{10}$$

and send (r_1, r_2) to the store S.

Step3. The store S checks whether the following equation are valid: $r_1 G_1 + r_2 G_2 = dA + B$. If it holds, S accepts the payment of U, otherwise he will reject it.

Step4. The store S saves the payment information, while the user U saves his balance $M_T - M_p$. The entire spend protocol shown in Fig. 5.

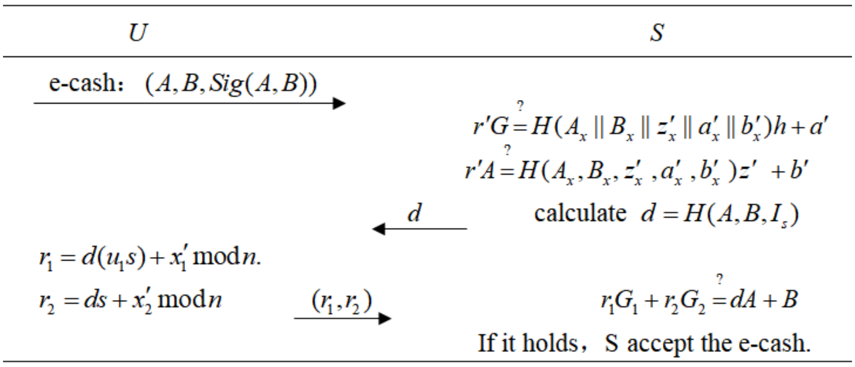

U
S
e-cash: $(A, B, Sig(A, B))$
$r'G \overset{?}{=} H(A_x \| B_x \| z_x' \| a_x' \| b_x')h + a'$
$r'A \overset{?}{=} H(A_x, B_x, z_x', a_x', b_x')z' + b'$
d
calculate $d = H(A, B, I_s)$
$r_1 = d(u_1 s) + x_1' \bmod n.$
$r_2 = ds + x_2' \bmod n$
(r_1, r_2)
$r_1 G_1 + r_2 G_2 \overset{?}{=} dA + B$
If it holds, S accept the e-cash.

Fig. 5. Spend protocol

3.4 Deposit protocol

All banks have an online database in which a list of e-cash that are spent has been saved, which can be published by the central bank. The store S sends the e-cash and payment information to the $Bank_2$, and $Bank_2$ checks whether the electronic cash is overdue and exceeds the balance. Expired electronic cash can be deleted from the bank database periodically. Then, $Bank_2$ finds A in its database, and there are two kinds of cases.

Case1. The search failed. There is no such electronic cash in the bank database, which indicates that the current electronic cash must be spent for the first time. The bank stores (A, r_1, r_2, I_s) in the database and adds the corresponding amount to the account of the store S.

Case2. The search was successful. At this point, one of the users U and the store S must be cheaters. Compare the e-cash records that have just been received and the existing e-cash records in the database. If I_s is the same, it means that the store S tries to store the same e-cash twice in the bank. Otherwise, it means the user U duplicates the same electronic cash copy. The bank can calculate the identity of the illegal user U who spends electronic cash twice. Because of the three tuple (d,r_1,r_2) corresponding with A recorded in the database, and the three tuple (d,r_1,r_2) which have just been received, we obtain two equations.

$$\begin{cases} r_1 = d(u_1 s) + x_1' \bmod n \\ r_1' = d'(u_1 s) + x_1' \bmod n \end{cases}, \tag{11}$$

$$\begin{cases} r_2 = ds + x_2' \bmod n \\ r_2' = d's + x_2' \bmod n \end{cases} \tag{12}$$

Obviously, we have

$$r_1 - r_1' = (d-d')u_1 s \text{ and } r_2 - r_2' = (d-d')s, \tag{13}$$

so,

$$((r_1 - r_1')/(r_2 - r_2'))\cdot G_1 = u_1 \cdot G_1 = I \tag{14}$$

The bank identifies the user's actual identity information corresponding to the account I in its account database, and finds the users who are trying to duplicate the same e-cash.

4. Analysis of scheme

We propose a new multi bank e-cash scheme, which embeds the balance information of the currency into the e-cash, and directly represents the amount of the e-cash in clear text, so that the bank does not need to maintain different signature keys for different currencies. Therefore, the scheme reduces the complexity of bank key management. In this section, we further analyze the correctness, security and operation efficiency of the scheme.

4.1 Correctness analysis

Theorem 1 In the spend protocol, if the electronic cash transmitted by the customer is legal, then the merchant's equation for verifying the digital signature must be satisfied.

Proof. We have to prove that:

$r'G = H(A_x \| B_x \| z_x' \| a_x' \| b_x')\cdot h + a'$ and $r'A = H(A_x \| B_x \| z_x' \| a_x' \| b_x')\cdot z' + b'$

We have:

$$\begin{aligned}
&H(A_x \| B_x \| z_x' \| a_x' \| b_x')\cdot h + a' \\
&= c'h + a' \\
&= cuh + ua + vG \\
&= cu(h_1 + h_2 + \cdots + h_n) + u(a_1 + a_2 + \cdots + a_n) + vG \\
&= cu(x_1 G + x_2 G + \cdots + x_n G) + u(w_1 G + w_2 G + \cdots + w_n G) + vG \\
&= (((cx_1 + w_1) + (cx_2 + w_2) + \cdots + (cx_n + w_n))u + v)G
\end{aligned}$$

$$
\begin{aligned}
&=((r_1+r_2+\cdots+r_n)u+v)G\\
&=(ru+v)G\\
&=r'G\\
&H(A_x \,\|\, B_x \,\|\, z'_x \,\|\, a'_x \,\|\, b'_x)\cdot z'+b'\\
&=c'sz+sub+vA\\
&=cus\cdot e^{-1}(z_1+z_2+\cdots+z_n)+su\cdot k^{-1}(b_1+b_2+\cdots+b_n)+vs(I+G_2)\\
&=cus\cdot e^{-1}(x_1E+x_2E+\cdots+x_2E)+su\cdot k^{-1}(w_1K+w_2K+\cdots+w_nK)+vs(I+G_2)\\
&=cus\cdot e^{-1}(x_1e(I+G_2)+\cdots+x_ne(I+G_2))+su\cdot k^{-1}(w_1k(I+G_2)+\cdots+w_nk(I+G_2))+vs(I+G_2)\\
&=cus(x_1+x_2+\cdots+x_n)(I+G_2)+su(w_1+w_2+\cdots+w_n)(I+G_2)+vs(I+G_2)\\
&=(((cx_1+w_1)+(cx_2+w_2)+\cdots+(cx_n+w_n))u+v)s(I+G_2)\\
&=((r_1+r_2+\cdots+r_n)u+v)s(I+G_2)\\
&=(ru+v)A\\
&=r'A
\end{aligned}
$$

4.2 Security analysis

In the phase of withdrawal, the bank uses the blind signature algorithm to issue electronic cash, which protects the privacy of the users. The difficulty of counterfeiting electronic cash is equivalent to solving the problem of elliptic curve discrete logarithm. The electronic cash containing the amount of money and the validity period can easily satisfy the divisibility of e-cash, and avoid the complex binary tree principle. In addition, in the deposit phase, banks can find out illegal sellers and users, and carry out the detection of double spending.

4.3 Efficiency analysis

The computational complexity of the elliptic curve discrete logarithm problem is currently completely exponential, while RSA/DSA are sub-exponential. This shows that ECC has higher security per bit than RSA/DSA. On the other hand, under the equivalent security strength, the key size required by ECC is shorter. Fig. 6 reflects the comparison of the attack resistance of several public key cryptosystems. The scheme we proposed is based on elliptic curve cryptosystem. Compared with the same scheme, the modulus is reduced from 1024 bits to 160 bits. That is to say, the new scheme guarantees higher security through shorter keys, and the signature length is only 121KB, which is suitable for smart wallet based electronic wallet. Moreover, the whole scheme is realized by the elliptic curve scalar multiplication and point addition, compared with the modular multiplication and modular exponentiation, the computational complexity is greatly reduced.

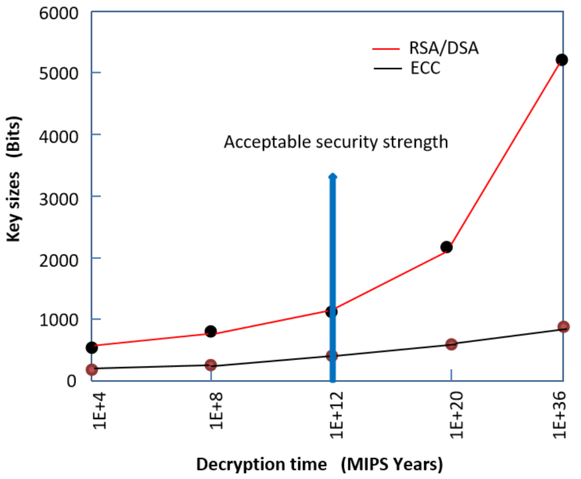


Fig. 6. The comparison of several public key cryptosystems

5. Conclusion

E-commerce is becoming a hot topic of research and application. As one of the key technologies in the field of e-commerce, the electronic cash system is worth studying. Although different electronic cash experimental systems are running in various countries, due to security and efficiency for various reasons, real and practical large-scale electronic cash systems are rare. In real life, electronic cash issued by multiple banks is more suitable than electronic cash issued by a single bank. Therefore, the scheme proposed in the paper has more practical significance. The research of electronic cash system is also very necessary. And there is not much research in this area. In order to improve the efficiency of electronic cash system and realize quick payment, a new e-cash scheme is proposed in this paper. The new scheme satisfies the anonymity of the user, the unforgeability of e-cash, and the property of preventing double spending. Furthermore, the whole scheme is implemented on elliptic curve cryptosystem, and the cost of computation and communication are greatly reduced compared with RSA/DSA cryptosystem.

REFERENCES

[1]. *Chaum D.* Blind Signatures for Untraceable Payments, Advances in Cryptology. Springer US, 1983: 199-203.

[2]. *Canard S, Pointcheval D, Sanders O, et al.* Divisible E-Cash Made Practical, LNCS 9020: Proceedings of the 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, Mar 30-Apr 1, 2015. Berlin, Heidelberg: Springer, 2015: 77-100.

[3]. *Yang B, Yang K, Zhang Z, et al*. AEP-M: Practical Anonymous E-Payment for Mobile Devices Using ARM Trust Zone and Divisible E-Cash, Information Security. Springer International Publishing, 2016: 130-146.

[4]. *Haddad G E, Hage H, Aïmeur E*. E-Payment Plan: A Conditional Multi-payment Scheme Based on User Personalization and Plan Agreement, International Conference on E-Technologies. Springer, Cham, 2017: 285-299.

[5]. *Baldimtsi F, Chase M, Fuchsbauer G, et al*. Anonymous Transferable E-Cash, IACR International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2015: 101-124.

[6]. *Zhang Jiangxiao, Feng Chunhui*, Transferable E-Cash System with Arbitrarily Spending Order, Transaction of Beijing Institute of Technology, 2019, 39(3): 283-289 .

[7]. *Zhang Jiangxiao, Li Zhoujun*, Guo Hua. Multiple Bank E-Cash without Random Oracles, LNCS 8300: Proceedings of the 5th International Symposium on Cyberspace Safety and Security, Zhangjiajie, China, 2013: 40-51.

[8]. *Li Y, Zhou F, Xu Z.* A fair offline electronic cash scheme with multiple-bank in standard model. Journal of the Chinese Institute of Engineers, 2019, 42(1):87-96.

[9]. *Xiao-Ying J, Bao L I, Ya-Min L*. Random Oracle Model. Journal of Software, 2012, 23(1):140-151.

[10]. *Schröder D, Unruh D*. Security of Blind Sig -natures Revisited. Journal of Cryptology, 2017, 30(2): 470-494.

[11]. *Kapoor, Abraham, Sonny V, et al*. Elliptic curve cryptography. Ubiquity, 2010, 2008(5): 291-328.

[12]. *Brands S A*. An Efficient Off-line Electronic Cash System Based On The Representation Problem. CWI, 1993. 94 (93) : 63–67.

[13]. *Gong Z, Li X, Chen K*. Efficient Partially Blind Signature Scheme with Provable Security, International Conference on Computing and Combinatorics. Springer-Verlag, 2006: 378-386.