A new public key cryptography system based on hyperbolic curve over finite field

Xiaoqin Liu[1] Qi Zheng Jianhua Yang Lu Wang Tong Zhang Tao Li Rui Wang

Abstract. In this paper, we propose a new technology that improves Diffie-Hellman's safeness and keeps its good property.The technology is called "Hyperbolic Curve Cryptography System" (HCCS) which is designed on hyperbolic curve over finite filed. HCCS has a solid Abel group structure whose order is diverse over finite field and the system is secure which is mainly based on discrete logarithm problem (DLP) and hardness of solving fundamental solution. Compared with Diffie-Hellman, HCCS has the same calculation complexity, but it has excellently flexible. Therefore, HCCS can improve information technology's safeness.

Keywords: HCCS. Abel group. DLP. fundamental solution. flexible

1.1 Introduction

Since Diffie and Hellman [1] invented the concept of public key cryptography in 1976, a lot of public key cryptographic algorithms had been put forward all over the world. RSA [2] was developed to implement public key algorithm firstly. Its security is based on the hardness of solving factoring problem (FAC).In 1985 Elgamal [3] proposed his new cryptosystem based on discrete logarithm problem (DLP).Later, Victor Miller [4] and Neal Koblitz [5] independently put forward cryptosystem based on elliptic curve discrete logarithm problem (ECDLP).The elliptic curve cryptosystem is still in use. However, many researchers began to decipher the encryption algorithm based on the theory of elliptic curve and had made great achievements [6-7]. Afterwards, many researchers are proposing cryptosystems based on multiple hard problems [8-10].As above, the common point of most existing cryptosystems is that the security of the system is based on cryptographic assumptions, such as FAC or DLP or ECDLP. Enhancing the security and validity is the major objective for public key cryptosystems. In this paper, we develop a new public key cryptosystem based on hyperbolic curve over

[1] Xiaoqin Liu(✉)
School of Information Science and Engineering, Yunnan University. 650091 Kunming, China
e-mail: qin.le11@163.com

finite field. Not only the security of system is improved, but also the system can implement algorithms efficiently.

1.2 Preliminaries

In this section, a new public key cryptosystem mainly set up by hyperbolic curve related to pell's equation.The order of Abel group is discussed in detail.

1.2.1 Hyperbolic curve

Pell's equation is any Diophantine equation of the form, $x^2-Dy^2=1$, where D is a non-square integer. From the following Figure 1.1, we can see that Pell's equation has the form of hyperbola in Cartesian coordinates. And Joseph Louis Lagrange proved [11] that, as long as D is not a perfect square, Pell's equation has infinite distinct integer solutions.

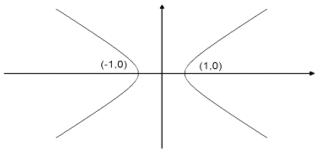

Fig. 1.1 Pell's equation

Let h_i/k_i denote the sequence of convergent to the continued fraction for $\sqrt{D}$ .The pair(x_0,y_0) solving Pell's equation and minimizing x satisfies $x_1=h_i$, $y_1=k_i$ for some i, which is called the fundamental solution of Pell's equation. As Lenstra describes [12],the time for finding the fundamental solution using the continued fraction method, with the aid of the Schonhage-Strassen algorithm for fast integer multiplication, is within a logarithmic factor of the solution size, the number of digits in the pair(x,y). As we known, the main feature of Pell's equation is the difficulty of finding a accurate fundamental solution and the coordinate values of which may be larger integers. The another feature of Pell's equation is that once the fundamental solution is found, the pair(x_k,y_k) on hyperbolic curve except for trivial solutions(1,0),(-1,0) may be calculated as

$$x_k + y_k\sqrt{D} = \pm\left(x_0 + y_0\sqrt{D}\right)^k \quad k > 1 \tag{1.1}$$

Equivalently, we may calculate subsequent solution (x_{k+1}, y_{k+1}) via the recurrence relations as below.

$$\begin{cases} x_{k+1} = x_1 x_k + y_1 y_k D \\ y_{k+1} = x_1 y_k + y_1 x_k \end{cases} \tag{1.2}$$

According to the features of Pell's equation mentioned above, we can obtain a hyperbolic curve related to Pell's equation. A hyperbolic curve denoted as $H(F_n)$ over finite field F_n in a general form is given by:

$$x^2 - Dy^2 = 1 \quad D \in F_n \tag{1.3}$$

where D is a non-square integer over finite field F_n. Clearly, the hyperbolic curve not only has much in common with Pell's equation, but also gets its features. Firstly, the set of solutions are never empty, at least two pairs (1,0),(-1,0). Secondly, hyperbolic curve's equation has finite distinct integer solutions over finite field F_n. Likewise, finding a accurate fundamental solution is very difficult. Thirdly, all nontrivial solutions can be calculated from formula (1.1) and subsequent solutions via the recurrence relations like formula (1.2). Finally, owing to the difference of algebraic structure, we might think whether other solutions exist except for solutions generated from fundamental solution. Although the question cannot prove theoretically, a lot of experimental datas fully demonstrate that there is not other solutions.

The operation of points on $H(F_n)$ mainly is multiplication •. $H_n(D)$ denotes as the set of points on hyperbolic curve.

$$H_n(D) = \{(x, y) \mid x < n, y < n \ and \ x, y \in \mathbb{Z}\}$$

Definition 1. (binary operation).Function f: $H_n(D) \bullet H_n(D) \rightarrow H_n(D)$.f is called binary operation. For example,

$$\begin{aligned} f(< P, Q >) = P \bullet Q &= (x_1, y_1) \bullet (x_2, y_2) = (x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) \\ &= (x_1 x_2 + y_1 y_2 D) + (x_1 y_2 + x_2 y_1)\sqrt{D} = (x_3, y_3) = R \end{aligned} \tag{1.4}$$

From the properties, features, definition 1 and algebraic structure of hyperbolic curve, all solutions of hyperbolic curve's equation can consist of an Abel group. Assume a trivial point E=(1,0). Now, the proofs in details are as follows.

Theorem 1. $<H_n(D), \bullet>$ is an Abel group.

Proofs. ①Closure.

$$P \bullet Q = (x_1, y_1) \bullet (x_2, y_2) = (x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = R \in H_n(D).$$

②Commutative law.

$$P \bullet Q = (x_1, y_1) \bullet (x_2, y_2) = (x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = Q \bullet P.$$

③Associative law.

$$(P \bullet Q) \bullet R = (x_1, y_1) \bullet (x_2, y_2) \bullet (x_3, y_3) = P \bullet (Q \bullet R).$$

④Existing an unit element E=(1,0). If $\forall$ P=(x,y) $\in$ $H_n(D)$, then

$$P \bullet E = (x + y\sqrt{D})(1 + 0\sqrt{D}) = P$$

⑤Existing an inverse element for every point. If ∀ P=(x,y) ∈ $H_n(D)$,then its inverse element P^{-1} =(x,-y) satisfy

$$P^{-1} \bullet P = (x + y\sqrt{D})(x - y\sqrt{D}) = E$$

$<H_n(D),\bullet>$ satisfies 5 properties of an Abel group. As a result, $<H_n(D),\bullet>$ is an Abel group.

Therefore, it is very difficult to find an integer r such that G•G•••G(r times)=G^r=E. The security of the proposed system finally can be ascribed to the reasonable order of Abel group.

1.2.2 The Order of $<H_n(D),\bullet>$

In order to ensure the security of the proposed scheme, it is necessary to discuss the order of $<H_n(D),\bullet>$.The order of $<H_n(D),\bullet>$ depends on different finite fields. In the following discuss, finite field is discussed in three situations: a large prime, a non-prime and an extension field.

- A large prime

If n is a large prime, F_n={0,1,⋯n-1} and F_n^* express as multiplicative groups, the number of solutions to $H(F_n)$ over F_n denotes as $N(x^2-Dy^2=1)$.

Definition 2. Feature χ over F_n is defined as a mapping from F_n^* to complex field and satisfies:

$$\chi(ab) = \chi(a)\chi(b), \chi(1) \neq 0 \ \forall a, b \in F_n^* \tag{1.5}$$

If a∈F_n^* make the formula χ(a)=1 established, then feature χ is a trivial feature χ_0.

Definition 3. Assume χ, λ are two features over F_n, $J(\chi,\lambda)$ is called Jacobi's sum, just like

$$J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b) \ a, b \in F_n \tag{1.6}$$

Theorem 2. If n is a large prime, then the number of solutions to $H(F_n)$ is n+χ(-1).

Proof.

$$N(x^2 - Dy^2 = 1) = \sum_{\substack{a+b=1 \\ a,b \in F_n}} (x^2 = a)(-Dy^2 = b)$$

$$= \sum_{\substack{a+b=1 \\ a,b \in F_n}} \sum_{i=0}^{1} \chi^i(a) \sum_{j=0}^{1} \chi^j(-\frac{b}{D}) = \sum_{\substack{a+b=1 \\ a,b \in F_n}} (1 + \chi(a))(1 + \chi(-\frac{b}{D}))$$

$$= n + 0 - \sum_{a+b=1} \chi(bD^{-1}) - \sum_{a+b=1} \chi(a)\chi(bD^{-1})$$

$= n - J(\chi, \chi^{-1}) - J(\chi_0, \chi^{-1}) = n + \chi(-1)$.

From above mentioned definitions, we can calculate $\chi(-1)$ whose value depends on n, $\chi(-1)=1$ or -1.

Thus, $N(x^2 - Dy^2 = 1) = \begin{cases} n-1, \ if\ p = 4n+1 \\ n+1, \ if\ p = 4n-1 \end{cases}$.

- A non-prime

Assume n is a non-prime and n=p×q, where p and q are two large primes. Solving the congruence $x^2-Dy^2 \equiv 1 \pmod n$ is equivalent to find the simultaneous solutions to the system of congruence $x^2-Dy^2 \equiv 1 \pmod p$ and $x^2-Dy^2 \equiv 1 \pmod q$.Thus, the number of solutions to $H(F_n)$ over F_n is shown as follows:

$$N(x^2 - Dy^2 = 1) = \begin{cases} (p-1)(q-1), \ if\ p = 4k+1\ and\ q = 4k+1 \\ (p-1)(q+1), if\ p = 4k+1\ and\ q = 4k-1 \\ (p+1)(q-1), if\ p = 4k-1\ and\ q = 4k+1 \\ (p+1)(q+1), if\ p = 4k-1\ and\ q = 4k-1 \end{cases}$$

- An extension field

Assume p is a large prime and F_n is an extension field over prime field F_P. Form the formula (1.3),$x \in F_p$, $y \in F_p$, elements of field are usually expressed via a polynomial basis.The operations of addition and multiplication for every element expressed as polynomial are also very simple. However, the order of Abel group might not be estimated.The challenge in calculating the order of Abel group over extension field is always worth trying.

The security of the proposed scheme is ensured by fundamental solution and order of Abel group. Firstly, there is not a polynomial time algorithm to find the fundamental solution. Secondly, assume the fundamental solution is found, the imprecise fundamental solution will further strengthen the difficulty of solving the order. Finally, solve order of points is to answer DLP.As we known, DLP is an intractable computational problems. Therefore, the situation discussed above, I think, can guarantee system security.

1.3 The proposed scheme

With the study of hyperbolic curve, we propose a new public key cryptosystem based on hyperbolic curve. It is called Hyperbolic Curve Cryptography System (HCCS).The scheme consists of three phases between two users (Alice and Bob), initialization, encryption, decryption. Now the descriptions for each phase are shown.

1.3.1 Initialization

1. Chooses coefficients to define hyperbolic curve x^2-Dy^2=1 over finite field F_n.
2. Picks a based point G=(x_0,y_0) with a large order r and this gives us G^r=E.
3. Selects an integer m and m<r.
4. Computes B=G^m mod q.

The public keys of the system are formed by (G,B) and can be publicly in open channel while the private key of HCCS is given by m and kept by the receiver.

1.3.2 Encryption

To encrypt any message w to Alice, Bob does the following:

1. Randomly chooses the secret integer k.
2. Computes H=G^k mod n and T=B^kw mod n.
3. Produces the cipher text (H,T).
4. Sends (H,T) to Alice.

1.3.3 Decryption

To decrypt the cipher text (H,T), Alice needs to do the following:

1. Computes R=H^m mod n.
2. Recovers w=T/R mod n.

1.3.4 Example

According to the public key encryption scheme described previously, the operation of the example is as follows:

Set p=19 and consider the hyperbolic curve H(F_{19}):x^2-$2y^2$=1 defined over F_{19}. Hyperbolic curve H(F_{19}) has an order r=18. H(F_{19}) is an Abel group and all point is generated from fundamental solution G=(3,2).The following Table shows that the multiple operation of G generates all the points on H(F_{19}).

Table 1.1 Points on Hyperbolic Curve H(F_{19})

(-17,12)	(-16,2)	(-15,3)	(-12,9)	(-7,9)	(-4,13)	(-3,2)
(-2,12)	(-1,0)	(0,3)	(0,-3)	(1,0)	(3,2)	(2,12)
(4,13)	(7,9)	(12,9)	(15,13)	(16,2)	(17,12)	–

Assume plaintext w=11 and calculate $B=G^3=(12,12)$,then m=3.Alice selects parameters (B,G)=((12,12),(3,2)) as public keys. Then Bob chooses randomly the secret integer k=2 and computes $H=G^2=(17,12)$,$T=B^2w=(25,7)$.Bob publics (H,T) in open channel. Only Alice, knowing the private key m=3 and computing $R=H^m=H^3=(26,27)$, can recover the plaintext message: w=T/R=11.

1.4 Evaluation of HCCS

The abovementioned three algorithms complete the newly developed cryptosystem.We now evaluate HCCS according to efficiency performance and flexibility.

1. Efficiency performance

In general, the efficiency performance of a cryptosystem is evaluated by the amount of time needed to compute and number of keys used for each algorithm. So we can measure the efficiency performance of HCCS as mentioned above and use the following notations to analyze efficiency performance:

- SK and PK denote the number of private and public keys respectively.
- T_{exp} is the time complexity taken for a modular exponentiation.
- T_{mul} is the time complexity taken for a modular multiplication.
- |x| denotes the bit length of x.

We hypothesize the time complexity for modular addition or substraction is negligible. So SK=2 and PK=2. The time complexity for encryption is given by $2T_{exp}+T_{mul}$ and the decryption is $T_{exp}+T_{mul}$. The communication costs of HCCS is only 4|n|. We use the conversions $T_{exp}=240T_{mul}$ given by Koblitz et al [13] to measure the performance in terms of T_{mul}. Then the time complexity of encryption is $481T_{mul}$ and the decryption is $241T_{mul}$.As we can see, HCCS can implement efficiently and the communication costs is very less.

Based on the Abel group structure and the discrete logarithm problem, it is not difficult to come up with time complexity which is the same to DLP in sub-exponential time $O(\exp(1+O(1)\sqrt{\ln n \ln(\ln n)}))$. Moreover, applying DLP encryption/decryption requires O(n) finite field grouping, using O(n) multiplication operations on hyperbolic curve $H(F_n)$. Therefore, the performance of HCCS yields the total running time O(n).

2. flexibility

HCCS owns flexible parameters: D,n,p Different coefficient D will constitute different hyperbolic curves. Compared with ECCS, hyperbolic curve can be easily chosen and effectively avoids algebraic attacks caused by improper selection of hyperbolic curve. Finite field F_n can be divided into many situations which will strengthen the selectivity of the order.

1.5 Conclusion

Enhancing security is the major objective for public key cryptosystem on the basis of the hardness of the intractable mathematic problems. In this paper, we have proposed a public key cryptosystem designed on hyperbolic curve. One who hopes to break HCCS must consider to solving DLP in a polynomial time. Moreover, with the complexity of solving fundamental solutions, the imprecise fundamental solutions have enhanced security of system further. From the above analysis, we can see that HCCS implements efficiently for each encryption and decryption phrase and has low costs, high flexibility in mobile communication environment.Therefore, HCCS is secure, flexible, efficient and feasible in theory.

1.6 References

[1]Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inform Theory, 22(6):644-54.

[2]Rivest, R. L., Shamir, A., & Adleman, L (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[3]ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on, 31(4), 469-472.

[4]Miller, V. S. (1986, January). Use of elliptic curves in cryptography. In Advances in Cryptology—CRYPTO'85 Proceedings (pp. 417-426). Springer Berlin Heidelberg.

[5]Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[6]Akishita, T., & Takagi, T. (2005). Zero-value register attack on elliptic curve cryptosystem. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 88(1),s 132-139.

[7]Eicher, J., & Opoku, Y. (1997). Using the Quantum Computer to Break Elliptic Curve Cryptosystems.

[8]Ismail E S, Hijazi M S. New cryptosystem using multiple cryptographic assumptions[J]. Journal of Computer Science, 2011, 7(12): 1765.

[9]Su, P. C., & Tsai, C. H. (2009). New cryptosystems design based on hybrid-mode problems. Computers & Electrical Engineering, 35(3), 478-484.

[10]Su, S., & Lü, S. (2012). A public key cryptosystem based on three new provable problems. Theoretical Computer Science, 426, 91-117.

[11]Yan, S. Y. (2002). Number theory for computing. Springer.

[12]Lenstra Jr, H. W. (2002). Solving the Pell equation. Notices of the AMS, 49(2), 182-192.

[13]Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. In Towards a Quarter-Century of Public Key Cryptography (pp. 103-123). Springer US.