A new cryptography algorithm using Cab curves an LDPC for wireless communication systems

B. ONTIVEROS(1), I. SOTO(1), R. CARRASCO(2)

(1) Industrial Engineering Department
Engineering Faculty
University of Santiago of Chile
Av. Ecuador 3769, Santiago
CHILE

(2) School of Electrical, Electronic and
Computer Engineering.
University of Newcastle upon Tyne
Merz Court Newcastle upon Tyne (NE1 7RU)
UNITED KINGDOM

Abstract:

In this paper we propose a new public key cryptographic system using Cab curves and Low Density Parity Check (LDPC) codes for mobile communication. This algorithm uses the Jacobian group of the Cab curves as a mathematical group to perform the encoder and space time operations. This paper offers an improved performance of 17.27 dB for BER = 10^{-5} against BPSK over a Fading channel.

Keywords: *Cab curves, low density parity check, cryptography.*

1. Introduction

In 1987 Koblitz [8] proposed the use of the group of an elliptic curve in cryptography, and again in 1989 he [7] proposed the use of the Jacobian of a hyperelliptic curve in cryptography. Later on the Jacobian of Picard curves [4], the Jacobian of superelliptic curves [5] and the Jacobian of *Cab*–curves [2] have been proposed. Because of some attacks [1] [6] on the DLP of hyperelliptic curves of large genus, the community is today looking at the Jacobian of curves curves of genus 1,2 and 3.
Nowadays elliptic curve cryptosystems are widely used, discrete logarithm based cryptosystem with Jacobian group of more general algebraic curves, such as hyperelliptic, superelliptic [5] and *Cab* curve [2], are not used. One of the main reasons for that is the heavy computational amount of addition in Jacobian of such non-elliptic curves.
In previous work we have been presented another cryptographic systems, which combined elliptic curves with LDPC codes [9] and elliptic curves with convolutional codes [10].
This paper presents a discrete-log based public key cryptosystem using the Jacobian group of Cab curves combined with LDPC for wireless communication systems.

This paper is organised as follows: Section 2 describes the flow of information for this new infrastructure. Section 3 presents the mathematical background of Cab curves. The performance is evaluated in terms of bit error rate in Section 4. Finally, conclusions are given in the last section.

2. System description

The construction of a new efficient cryptographic system is presented, based on the mapping of Cab curves and regular low-density parity check codes. The strength is based on the simplicity of performing the compression mapping before entering the LDPC encoder. Figure 1 shows the simulation infrastructure composed of a non-linear block that performs the encryption/decryption process and LDPC encoding/decoding process.
Figure 1 shows the LDPC_Cab cryptosystem composed by Encryption process (sender) in this case represented by Alice, and the other side of the channel the Decryption process (receiver) represented by Bob. LDPC_Cab Cryptosystem for encryption scheme is described using the Jacobian group of Cab curves

3. Mathematical Background

Cab curves constitute a wide class of algebraic curves including elliptic or hyperelliptic curves. In this paper we used C_{34} curve, which is a special case of *Cab* curve, is a non-singular plan curve defined by the following form of polynomial $F(X,Y)$.

$$F(X,Y) = Y^3 + a_0X^4 + a_1XY^2 + a_2X^2Y$$
$$+ a_3X^3 + a_4Y^2 + a_5XY + a_6X^2 + a_7Y + a_8X + a_9 \qquad (1)$$

where *ai*'s are elements of the definition field *k* and $a_0 \neq 0$.

C

C_{34} curve *C* has a unique point ∞ at the infinity. The function *Y* and *X* has the unique pole at ∞ of order four and three, respectively. We can see the gap sequence at ∞ is $N_0 - <3,4>= \{1,2,5\}$ and the genus of C_{34} is found to be three.

Let $D_C^0(k)$ denote the group of divisors of degree 0 on *C* defined over *k*, and $P_C(k)$ be the group of principal divisors on *C* defined over *k*. As well known, Jacobian group $J_C(k)$ on *C* is defined to be the factor:

$$J_C(k) = D_C^0(k)/P_C(k) \qquad (2)$$

On the other hand, let $\mathrm{R} = \mathrm{k}[\mathrm{X},\mathrm{Y}]/F$ be the coordinate ring of *C*. Since C_{34} curve *C* is nonsingular by the definition, *R* is integrally closed domain, so *R* is a Dedekind domain. Hence, all of the nonzero fractional ideals of *R* compose a group $I_R(k)$. Putting the group of principal ideals of *R* $P_R(k)$, the ideal class group $H_R(k)$ of *R* is defined to be the factor:

$$H_R(k) = I_R(k)/P_R(k) \qquad (3)$$

In general, for a nonsingular curve, we can identify divisors on the curve and ideals of the coordinate ring, and its Jacobian group $J_C(k)$ is naturally isomorphic to the ideal class group $H_R(k)$.

$$J_C(k) \approx H_R(k) \qquad (4)$$

In the below, we treat Jacobian group $J_C(k)$ as the ideal class group $H_R(k)$ of the coordinate ring *R*.

First, we compute f_J for the ideal product $J = I_1.I_2$. For that sake, it is sufficient to find Groebner base of ideal J, (for details see [3]) with respect to C_{34} order (f_J is the first element of it).

In this paper we deal with C_{34} curve $Y^3 + X^4 + 7X = 0$ on the prime field of characteristics $p = 1009$. Since the genus of C_{34} curves is three, types of ideals are either 11, 21, 22, 31 or 32. Here, we only discuss the case in which ideals I_1, I_2 are both of type 31. Another cases are dealt with similarly. Take the following two ideals of type 31:

$$I_1 = \left\{ \begin{matrix} X^2 + 726Y + 836X + 355, XY + 36Y + \\ 428X + 477, Y^2 + 746Y + 425X + 865 \end{matrix} \right\}$$

$$I_2 = \left\{ \begin{matrix} X^2 + 838Y + 784X + 97, XY + 602Y + \\ 450X + 291, Y^2 + 506Y + 524X + 497 \end{matrix} \right\}$$

We would like to compute Groebner base of $J = I_1.I_2$ to find f_J. By computing the remainder of each m_i in equation (3) modulo I_1 and I_2 respectively, we get the matrix M_C for I_1, I_2:

$$M_C = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 654 & 173 & 283 & 912 & 225 & 171 \\ 532 & 581 & 973 & 718 & 559 & 407 \\ 144 & 584 & 263 & 512 & 485 & 503 \\ 349 & 269 & 429 & 53 & 821 & 109 \\ 609 & 418 & 243 & 888 & 856 & 916 \\ 199 & 720 & 418 & 310 & 331 & 91 \\ 554 & 498 & 143 & 643 & 522 & 107 \end{pmatrix}$$

To obtain linear relations among rows of M_C, we connect M_C and 10-th unit matrix I_{10} to get $M_C^{''} = M_C : I_{10}$. Against $M_C^{''}$, we apply the row reduce procedure up to the sixth row.

The result in the Figure 2 showed the first six rows of M_C are linearly independent. This means monomials $1, X, Y, X^2, XY, Y^2$ are linearly independent in R/J and the product *J* is of type 61.

Moreover, the right 10 elements of the seventh, eighth and ninth rows of *m* represents liner expressions of the seventh, eighth and ninth rows of M_C by the first six rows of M_C, respectively. From this, we know linear expressions of X^3, X^2Y, XY^2 by $1, X, Y, X^2, XY, Y^2$ 1 in R/J, respectively, and we get the following Groebner base of *J*:

$$J = \left\{ \begin{array}{l} 28 + 132X + 31Y + 271X^2 + 469XY \\ +166Y^2 + X^3, \\ 856 + 618X + 747Y + 909X^2 + \\ 132XY + 636Y^2 + X^2Y, \\ 652 + 322X + 240Y + 978X^2 + \\ 826XY + 846Y^2 + XY^2 \end{array} \right\}$$

Hence, we have

$$f_J = 28 + 132X + 31Y + 271X^2$$
$$+469XY + 166Y^2 + X^3$$

4. Evaluation of the System

In this section the performance is evaluated in terms of bit error rate. The efficiency of the system have been evaluated by running of two simulations that simulate the combination of Cab curves and LDPC code in Gaussian and Fading environments.

Figure 3 shows that the combination LDPC_Cab achieves a signal to noise ratio of 17.27 dB for BER = 10^{-5} against BPSK over a Fading channel showed in Figure 1.

5. Conclusions

In this paper the construction of an efficient cryptographic system for mobile communication, based on the combination of the Cab Curve Algorithm and LDPC codes has been presented. This algorithm uses the Jacobian group of the Cab curves as a mathematical group to perform the encoder and space time operations. Our experimental results about the combination of C_{34} cab curves with LDPC may be used as a guide for the selection of another cab curves to combine with LDPC code in applications residing in resource limited devices.

This combination offers an improved performance of 17.27 dB for BER = 10^{-5} against BPSK over a Fading channel and -8 dB for BER = 10^{-5} against Shannon limit approximately.

Acknowledgements

The authors would like to thank PBCT/CONICYT ACT11/04 -Chile, for their financial support.

References

[1] L. M. Adleman, J. DeMarrais, and M.-D. Huang. *A sub exponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q).* Theoret. Comput. Sci., 226(1-2):7–18, 1999. Cryptography.

[2] S. Arita, *Algorithms for computations in Jacobian group of Cab curve and their application to discrete-log-based public key cryptosystems,* IEICE TRANS. FOUND., vol.J82-A, Nº.8, pp.1291–1299, 1999.

[3] D.Cox, J.Little, D.O'Shea, *Ideals,* V*arieties, and Algorithms,* Springer-Verlag, 1992.

[4] J. Estrada Sarlabous, E. Reinaldo Barreiro, and J. A. Piñeiro Barceló. *On the Jacobian varieties of Picard curves: explicit addition law and algebraic structure. Math. Nachr.,* 208:149–166, 1999.

[5] S. D. Galbraith, S. M. Paulus, and N. P. Smart. *Arithmetic on superelliptic curves. Math. Comp.,Vol.* 71(237), pp. 393–405, 2002.

[6] P. Gaudry. *An algorithm for solving the discrete log problem on hyperelliptic curves.* In Advances in cryptology—EUROCRYPT 2000 (Bruges), pages 19–34. Springer, Berlin, 2000.

[7] N. Koblitz. *Elliptic curve cryptosystems.* Math. Comp., 48(177):203–209, 1987.

[8] N. Koblitz. *Hyperelliptic cryptosystems.* J. Cryptology, 1(3):139–150, 1989.

[9] Ontiveros B., Soto I. ,Carrasco R.A. , "Construction *of an Elliptic Curve over Binary Finite Fields to concatenate with LDPC Codes in Wireless Communication",* WSEAS Transactions on Communications, Issue 9, Volume 5, pages 1758-1762, ISSN 1109-2742, 2006.

[10] Ontiveros B., Soto I. ,Carrasco R.A. , *Construction of an Elliptic Curve over Finite Fields to combine with Convolutional Code for Cryptography,* IEE Proc. Circuits, Devices & Systems, Vol. 153, No. 4, August 2006.

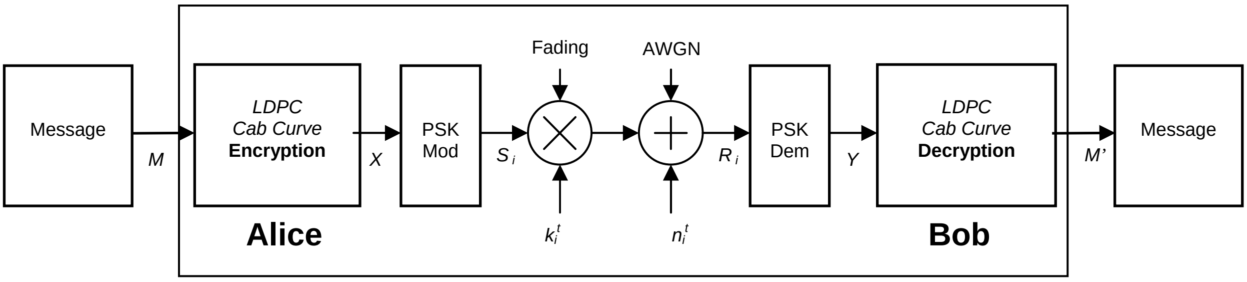

Figure 1: The simulation infrastructure of LDPC_Cab Cryptosystem

$$m = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 258 & 52 & 897 & 355 & 836 & 726 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 621 & 688 & 268 & 365 & 592 & 187 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 31 & 514 & 469 & 637 & 669 & 155 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 28 & 132 & 31 & 271 & 469 & 166 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 856 & 618 & 747 & 909 & 132 & 636 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 652 & 322 & 240 & 978 & 826 & 846 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 333 & 346 & 980 & 935 & 824 & 614 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Figure 2: Matrix m

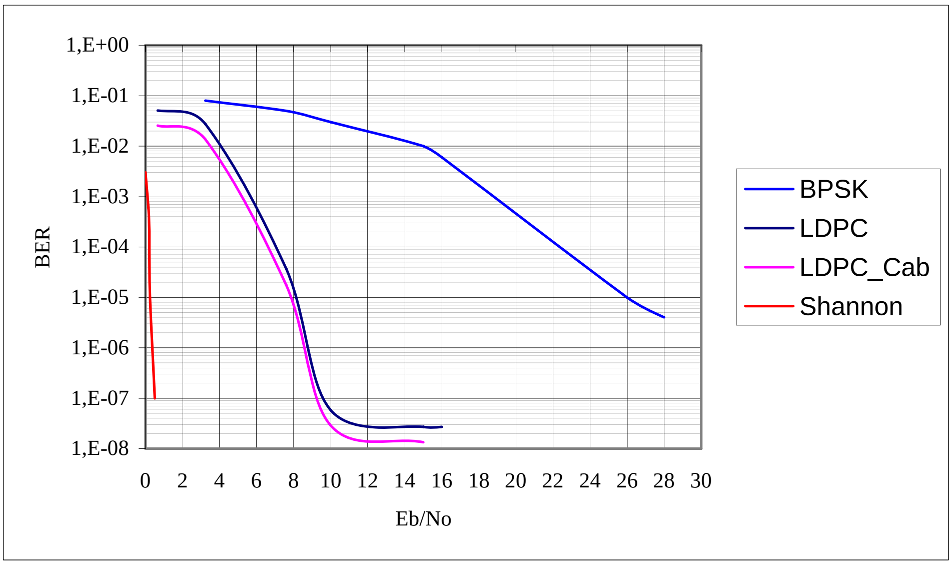

Figure 3: The benefit introduced by the LDPC-Cab system