Construction of an Elliptic Curve over Binary Finite Fields to combine with LDPC Code in Mobile Communication

B.ONTIVEROS(1), I. SOTO(1), R. CARRASCO(2)
(1) Industrial Engineering Department
Universidad de Santiago de Chile, Chile
http://fermat.usach.cl/~ontivero
(2) School of Electrical, Electronic and Computer Engineering.
University of Newcastle upon Tyne, UK

Abstract:
In this paper we propose the construction of an efficient cryptographic system, based on the combination of the ElGamal Elliptic Curve Algorithm and Low Density Parity Check (LDPC) codes for mobile communication. When using elliptic curves and codes for cryptography it is necessary to construct elliptic curves with a given or known number of points over a given finite field, in order to represent the input alphabet. In this paper we develop algorithms to construct efficient elliptic curves over binary finite field for combination with LDPC codes. A list of the suitable elliptic curves and the study of time to construction elliptic curves is presented.

Keywords: elliptic curves, low density parity check, cryptography.

1. Introduction
In 1985, Koblitz [5] and Miller [8] independently proposed the implementation of a public key cryptosystem using elliptic curve groups over finite fields. The Elliptic curve discrete logarithm problem appeared to be much more difficult than above discussed algorithms [7]. The elliptic curve cryptosystems arise as an alternative to RSA because these curves offer key size smaller than RSA key. For example, a 160-bit elliptic curve cryptosystem key offers security equivalent to that of a 1024-bit RSA key [6]. In previous work we have presented the algorithms to construct efficient elliptic curves over prime finite fields for combination with convolutional codes [9]. In this paper we present the algorithms to construct efficient elliptic curves over binary finite fields to combine with LDPC codes [4] [10]. We propose the construction of a cryptographic system called LDPC_EGEC, based on the combination of the ElGamal [3] Elliptic Curve Algorithm and LDPC codes for mobile communication. In order to improve the LDPC_EGEC cryptosystem and reduce the size of the public keys we construct elliptic curves with a small class number using a new variant of the Complex Multiplication (CM) method [1]. This paper is organised as follows: Section 2 describes the flow of information for this new infrastructure. Section 3 presents the steps to construct elliptic curves over binary finite fields suitable for combination with LDPC codes. Section 4 describes how to work the validation of Elliptic Curve parameters. The results for this suitable method of construction are presented in Section 5. 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 elliptic 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_EGEC 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_EGEC Cryptosystem for encryption scheme is described using non-supersingular elliptic curve groups.

3. Construction of Elliptic Curve over Binary Finite Field
An elliptic curve $E$ defined over a binary finite field $F_{2^n}$, denoted by $E(F_{2^n})$, is the set of all points $(x,y)$, $x, y \in F_{2^n}$, which satisfies the equation $y^2 + xy = x^3 + ax^2 + b$ (1)
where \( a, b \in F_{2^n} \), and \( b \neq 0 \), together with special point \( O \) called the point at infinity. The curves of Equation (1) are called non-supersingular curves and are suitable for cryptographic applications [2]. The rules for arithmetic in \( F_{2^n} \) can be defined by either polynomial basis representation or by optimal normal basis representation [7]. For any negative integer \( D \) congruent to 0 or 1 mod 4, there exits, up to isomorphism, a unique imaginary quadratic order \( \mathcal{O} = \mathbb{Z}[\sqrt{D}/2] \). In the complex multiplication method a discriminant \( D \) of an imaginary quadratic order will be choosen and will find a finite field of \( q \) elements such that \( m^2.D = t^2 - 4q \) for integers \( t \) and \( m \) and such that \( q - t + 1 \) contains a large prime factor. The existence and construction of an elliptic curve with this discriminant \( D \) is given by the following conditions. For \( \mathcal{O} \) to be endomorphism ring of an elliptic curve \( E \) over \( k \) of characteristic \( p \), it is necessary and sufficient that \( D = \text{disc}(\mathcal{O}) \) satisfies \((D/p) = 1 \) and the order in the class group of a prime over \( p \) divides \( [k : F_p] \) in order to construct an elliptic curve with complex multiplication some classical constructions of class field theory will be used. Let \( \mathcal{O} \) be an imaginary quadratic order of discriminant \( D \) and class number \( h(\mathcal{O}) \). There exists a unique monic irreducible polynomial \( H_D (x) \) of degree \( h(\mathcal{O}) \) such that \( E \) is an ordinary elliptic curve over a field \( k \) of characteristic \( p \) with endomorphism ring \( \mathcal{O} \) if and only if \((D/p) = 1 \) and the \( j \)-invariant of \( E \) is a root of \( H_D (x) \mod p \) in \( k \).

Let \( k \) a field of \( q \) elements and let \( m \) be an integer coprime to \( q \). For any integer \( t \) such that \( t^2 = 4q \) (mod \( m^2 \)) with \( |t| \leq 2\sqrt{q} \), the integer \( D = (t^2 - 4q)/m^2 \) is the discriminant of the endomorphism ring of an ordinary elliptic curve over \( k \).

While this approach is constructive, using factorisation modulo the prime divisors of \( m \) and Hensel lifting, the problem remains that the computation of class polynomials appears to have exponential complexity, which effectively implies an absolute bound on the discriminant. Thus, in practice, it is necessary to choose \( m \) sufficiently large that \(|D|\) is of a prescribed size.

In order to pass from a class polynomial to an elliptic curve with a known number of points a construction is required for curves with given \( j \)-invariant. An elliptic curve, however, may have several nonisomorphic twists with the same \( j \)-invariant.

### 4. Validation of Elliptic Curve Parameters over Binary Finite Field \( F_{2^n} \)

There are several important details that have to be considered when setting up this new cryptosystem. The first consideration is how the elliptic curves are chosen in the underlying field. The second consideration is how the LDPC code parameters are chosen. In this new cryptosystem the following parameters can be set: Finite field, Elliptic curve, encoding algorithm, frame size, a parity matrix, maximum number of iterations, number of frame errors to terminate, signal to noise ratio \( E_b/N_0 \).

Elliptic curve parameters over \( F_{2^n} \) are a sextuple: \( T = (m, f(x), a, b, G, \pi, k) \) consisting of an integer \( m \) specifying the finite field \( F_{2^n} \), an irreducible binary polynomial \( f(x) \) of degree \( m \) specifying the representation of \( F_{2^n} \), two elements \( a, b \in F_{2^n} \) specifying the elliptic curve \( E(F_{2^n}) \) defined by the equation (1), a base point \( G = (x_G, y_G) \) on \( E(F_{2^n}) \), a prime \( n \) which is the order of \( G \), and an integer \( h \) which is the cofactor \( h = \#E(F_{2^n})/n \).

The approximate security level in bits required from the elliptic curve parameters — this must be an integer \( t \in \{56,64,80,96,112,128,192,256\} \) Elliptic curve parameters over \( F_{2^n} \):

\[
T = (m, f(x), a, b, G, n, h) \quad (2)
\]

such that taking logarithms on the associated elliptic curve requires approximately \( 2^t \) operations.

Generate elliptic curve parameters over \( F_{2^n} \) as follows:

1. Let \( t' \) denote the smallest integer greater than \( t \) in the set \( \{64,80,96,112,128,192,256,512\} \).

Select

\[
m \in \{113,131,163,193,233,239,283,409,571\}
\]
such that \(2t < m < 2t'\) to determine the finite field \(F_{2^m}\).

2. Select a binary irreducible polynomial \(f(x)\) of degree \(m\) to determine the representation of \(F_{2^m}\).

3. Select elements \(a, b \in F_{2^m}\) to determine the elliptic curve \(E(F_{2^m})\) defined by the Equation 1, a base point \(G = (x_G, y_G)\) on \(E(F_{2^m})\) a prime \(n\) which is the order of \(G\), and an integer \(h\) which is the cofactor \(h = \#E(F_{2^m})/n\), subject to the following constraints:
   - \(b \neq 0\) in \(F_{2^m}\)
   - \(\#E(F_{2^m}) \neq 2^m\)
   - \(2^{m.b} \neq 1 \mod n\) for any \(1 \leq B < 20\)
   - \(h \leq 4\)

4. Output \(T = (m, f(x), a, b, G, n, h)\)

5. For the LDPC we choose the Size of the Frame, a parity matrix, maximum number of iterations, number of frame errors to terminate and signal to noise ratio \(E_b/N_0\).

### 5. Evaluation of the Time to construct Elliptic Curve over \(F_{2^m}\).

In this section the performance of the time to construct elliptic curves over binary finite fields is evaluated using different discriminants and different field degree. Figure 2 shows the time spend to construct elliptic curves using Discriminants 19, 67, 71 and 163. From Figure 2 can be seen that the time increase when the field degree increases.

Table 1 shows some cases of constructing elliptic curves using different bit size for the binary finite fields. In this table the coefficients \(a\) and \(b\) of Elliptic curve according equation (1) are presented.

### 6. Conclusions

In this paper the construction of an efficient cryptographic system for mobile communication, based on the combination of the ElGamal Elliptic Curve Algorithm and LDPC codes has been presented. Our experimental results about constructing elliptic curves may be used as a guide for the selection of the most efficient elliptic curves to combine with LDPC code in applications residing in resource limited devices that support secure and efficient Public Key Infrastructure services.

### 7. Acknowledgements

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

### 8. References


Figure 1: The simulation infrastructure of LDPC_EGEC Cryptosystem

Figure 2: Time to construct elliptic curves versus Discriminant for different binary finite field size(in bytes)

<table>
<thead>
<tr>
<th>Field degree</th>
<th>field polynomial, coefficients of elliptic curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>$D = -22279$, Field polynomial = $[113,9,0]$</td>
</tr>
<tr>
<td></td>
<td>$a = 1$, $b = 4DE236AA2FE8E4249398F484F661$</td>
</tr>
<tr>
<td>163</td>
<td>$D = -57047$, Field polynomial = $[163,7,6,3,0]$</td>
</tr>
<tr>
<td></td>
<td>$a = 1$, $b = 13611854F001490402ECA0FF3EE5E4ED5768F6A9E$</td>
</tr>
<tr>
<td>163</td>
<td>$D = -99559$, Field polynomial = $[163,7,6,3,0]$</td>
</tr>
<tr>
<td></td>
<td>$a = 0$, $b = 48389E6C5E69D55D6CE1396B1326ACEED224CB079$</td>
</tr>
<tr>
<td>192</td>
<td>$D = -36095$, Field polynomial = $[192,7,2,1,0]$</td>
</tr>
<tr>
<td></td>
<td>$a = 0$, $b = 16C3117FF676EC50C2D6685FD2DF55A2D406E2A0D550259B$</td>
</tr>
<tr>
<td>245</td>
<td>$D = -184487$, Field polynomial = $[245,6,4,1,0]$</td>
</tr>
<tr>
<td></td>
<td>$a = 0$, $b = 3721073BACB1ED6234B6505C2E6D070B6E618EC11F13AF86673901895CA04A$</td>
</tr>
</tbody>
</table>

Table 1: Constructing elliptic curve using different field degree