Curves in Cryptography*

R. Athale & F. Winkler
Research Institute for Symbolic Computation
Johannes Kepler University
Linz, Austria.
Email: athale,winkler@risc.uni-linz.ac.at

Abstract

Here, we give two examples of ElGamal cryptosystem, one of which uses the group of rational points on an elliptic curve. We mention the possible research problems.

1 Historical development

Since ancient times people have strived hard to secure secret and important transactions. Today with the increase in the usage of the Internet, cryptography has become a necessary part of everyday life for most of the people. We give here the Shanon's description of a conventional cryptosystem. Alice wants to send a very important message to Bob. There is a possibility, because of the importance of the message, that some eavesdropper, say Eve, would like to steal it in the middle of the transaction. Therefore Alice needs a secure transaction. We show this with the help of Figure 1, where m is the message, E_k is an encryption function using the key k and D_k denotes the decryption function using the key k.

In 1985, Neal Koblitz proposed to use the group of rational points on elliptic curves over finite fields in developing more secure cryptosystems, see [5]. We will demonstrate by example how these cryptosystems work. In 1989, Koblitz generalized the above stated concept to hyperelliptic curves [3, 4]. The topic is still in the research phase and people are still trying to tune algorithms and different methods to make the computations faster. It is not yet clear till now whether the hyperelliptic cryptosystems are more secure or not than elliptic ones, [7, 2].

*The original version of this paper was presented as a poster in ISSAC 2001.

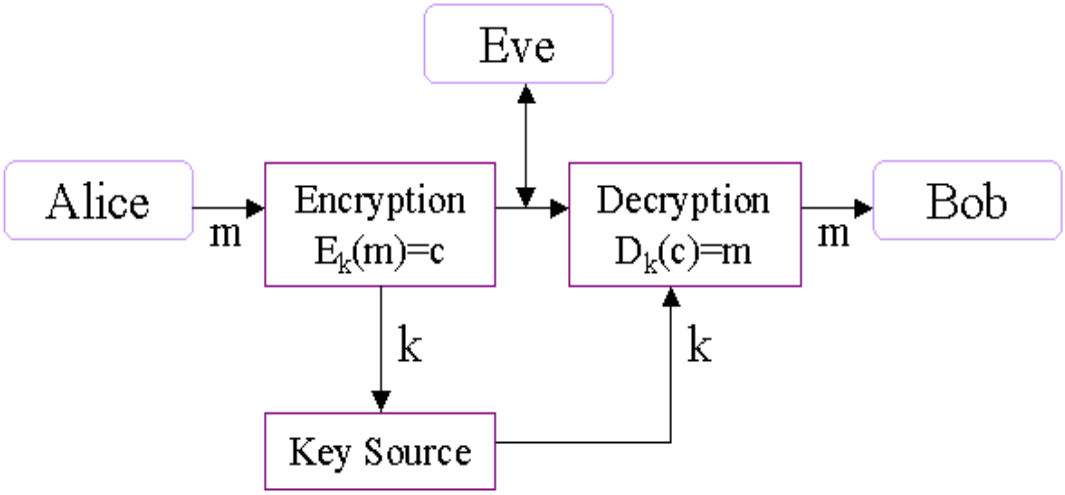

Figure 1: Shannon's description of a conventional cryptosystem

2 ElGamal Cryptosystem

Many protocols have been suggested and used for the encryption and decryption, like RSA, ElGamal, etc [5, 8]. We state here the steps carried out to encrypt and decrypt a message in ElGamal cryptosystem.

ElGamal Cryptosystem
Given: **Alice**(sender), **m**(message), **Bob**(receiver)
Step I: Setup

1. Choose a finite group G and choose $\alpha \in G$.
2. Each user picks a random integer l, the private key, and makes public $\alpha * l$, the public key.

Step II: Message transfer

1. Alice converts the message into an element of G.
2. Alice generates a random integer k and computes $\alpha * k$.
3. Alice looks up Bob's public key $\alpha * b$, and computes $(\alpha * b) * k$ and $m + \alpha * (bk)$.

4. Now Alice transmits the pair of group elements $(\alpha * k, m + \alpha * (bk))$ to Bob.

5. Bob computes $(\alpha * k) * b$ with his private key b.

6. Bob inverts $\alpha*(kb)$ and adds it to $m+\alpha*(bk)$ to recover the original message.

Example of ElGamal Cryptosystem (using the group of positive integers modulo a prime number under multiplication)
Given: **Alice**, **m** = ISSAC, **Bob**
Step I: Setup

1. Choose the group G formed by the positive integers modulo the prime 33554467 under the operation of multiplication, usually denoted by $\mathbb{Z}_{33554467}$. Let $\alpha = 4 \in G$.

2. Bob picks $b = 68$, the private key, and makes public $\alpha^b = 10821202$, the public key.

Step II: Message transfer

1. To convert ISSAC into element of G, Alice uses the following method. She uses the position of the letter in the English alphabet and converts it into binary equivalent in 5 digits. She then writes the binary numbers one after the other to make it a 25 digit binary number. Consider $I = 9 = 01001_2$, $S = 19 = 10011_2$, etc. She gets $m = 01001\ 10011\ 10011\ 00001\ 00011_2 = 10079267$. Now consider 10079267 as an element of G.

2. Alice picks $k = 264$ and computes $\alpha^k = 11190892$.

3. Alice looks up Bob's public key α^b, and computes $(\alpha^b)^k = 15956816$ and $m * \alpha^{(bk)} = 6145208$, say c, and sends (α^k, c) to Bob.

4. Bob inverts $\alpha^{(kb)}$ to get $\alpha^{-(kb)} = 14480096$ and multiplies it with c to get $c * (\alpha^{-(bk)}) = 10079267$ to recover the original message m. Bob then writes it in binary notation to get back the message ISSAC.

3 Introduction to Elliptic Curves

Let K be a finite field and let $\overline{K}$ denote its algebraic closure.

Definition 1. *An* **elliptic curve***, denoted by E, is an affine non-singular curve defined over K by an equation of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$*, together with the point at infinity,* O*.*

Now let us define a rational point on an elliptic curve. For details please see [6].

Definition 2. *A point* $P = (x, y)$ *satisfying the equation (1) is called a* **rational point** *on the elliptic curve if* $x, y \in K$*.*

The set of rational points forms a group, denoted by $E(K)$, with O as the identity, under the addition operation. One should note that, by a change of coordinates any rational point on E can be moved to the line at infinity, that is, every point of E could act as the identity of the group $E(K)$. We pictorially show how the addition operation works in the case of addition of two distinct points on the elliptic curve and addition of the point to itself, in Figures 2 and 3 respectively. We have shown in the figures the curves defined over the field of real numbers but in cryptographic applications we use curves defined over finite fields.

Example of ElGamal Cryptosystem(using the group of rational points on an elliptic curve)
Given: **Alice**, **m** = ISSAC, **Bob**
Step I: Setup

1. Choose the group G of rational points on the elliptic curve $E : y^2 = x^3 - 5x + 3$ defined over $\mathbb{Z}_{33554467}$. Let $\alpha = (2, 1) \in G$.

2. Bob picks $b = 68$, the private key, and makes public $\alpha * b = (31922274, 27324960)$, the public key.

Step II: Message transfer

1. To convert ISSAC into element of G, Alice uses the following method. She uses the position of the letter in the English alphabet and converts it into binary equivalent in 5 digits. She then writes the binary numbers one after the other to make it a 25 digit binary number. Consider $I = 9 = 01001_2$, $S = 19 = 10011_2$, etc. She gets $m = 01001\ 10011\ 10011\ 00001\ 00011_2 = 10079267$. She substitutes m in E as x-coordinate to get the two values for the y-coordinate, $y = 31266460$, $y = 2288007$. She chooses the smaller value of y. Now our $m = (10079267, 2288007)$.

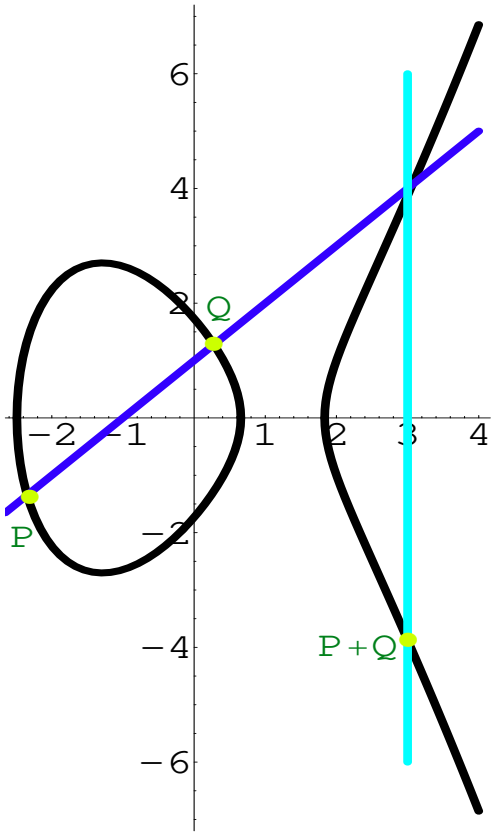

Figure 2: Addition of two distinct points on an elliptic curve $E : y^2 = x^3 - 5x + 3$ defined over the field of real numbers $\mathbb{R}$

2. Alice picks $k = 264$ and computes $\alpha * k = (23185761, 8227820)$.

3. Alice looks up Bob's public key $\alpha * b$, and computes $(\alpha * b) * k = (11242539, 28443674)$ and $m + \alpha * (bk) = (19389891, 13204812)$, say c, and sends $(\alpha * k, c)$ to Bob.

4. Bob inverts $\alpha * (kb)$ to get $-\alpha * (kb) = (11242539, 5110793)$ and adds it to c to get $c + (-\alpha * (bk)) = (10079267, 2288007)$ to recover the original message m. Bob then uses the x-coordinate of m to get back ISSAC.

4 Advantages of elliptic curve cryptosystems

In this section, we note the advantages of using the group of rational points on an elliptic curve for building a cryptosystem, over the conventionally used group, the

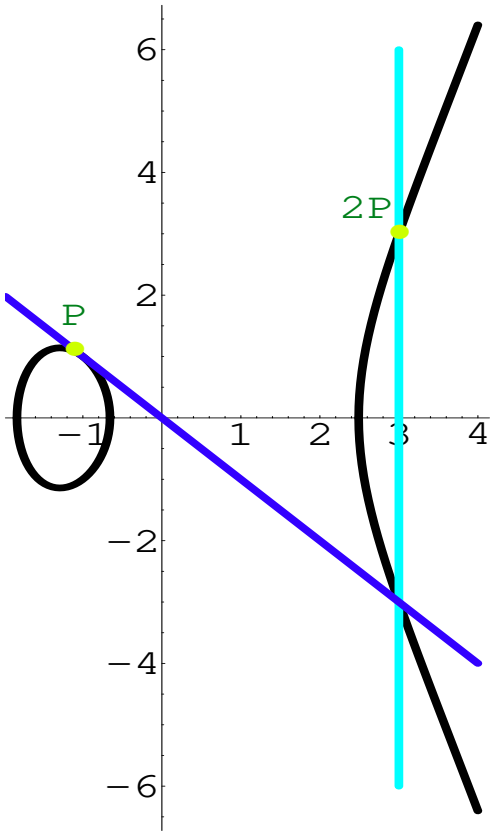

Figure 3: Computing $2P$ for a point P on an elliptic curve $E : y^2 = x^3 - 5x - 3$ defined over the field of real numbers $\mathbb{R}$

group of numbers modulo a prime, $\mathbb{Z}_p$. More detailed discussion can be found in [1].

- The discrete logarithm problem in the group $E(K)$ is believed to be very difficult, in particular, harder than the discrete logarithm problem in finite fields of the same size as K. Therefore these systems potentially provide the equivalent security as the existing public key schemes, but with shorter key lengths.
- The shorter key lengths require smaller bandwidth and memory requirements.
- Elliptic curves can be changed periodically without changing the basic field to give the greater security.

5 Benefits of using good computer algebra system

One has to do a lot of computational work to build a cryptosystem and then to tune it one needs many desirable properties from software. Computer algebra systems like *MATHEMATICA*®, Maple and number theory software and libraries like PARI, NTL provide necessary software tools for further research into tuning different algorithms. We state here some of the benefits of using a good computer algebra system in enhancing the research in this area.

- Availability of fast field arithmetic makes point addition on an elliptic curve very fast.
- Ability to solve equations is used to get the y-coordinate for a given x-coordinate of a point.
- Fast generation of huge prime numbers.

6 Generalisation to hyperelliptic curves

Koblitz [3, 4] generalised the concept of using the group of rational points on an elliptic curve to divisors of a hyperelliptic curve. We first state the definition of hyperelliptic curve.

Definition 3. *A* **hyperelliptic curve** *C of genus g ($g \geq 1$), is an affine non-singular curve defined over K by an equation of the form*

$$C \quad : \quad v^2 + h(u)v = f(u) \text{ in } K[u, v],$$

where $h(u) \in K[u]$ is a polynomial of degree at most g, $f(u) \in K[u]$ is a monic polynomial of degree $2g + 1$.

A curve C defined in definition (3) is non-singular if and only if there are no solutions $(u, v) \in \overline{K} \times \overline{K}$ which simultaneously satisfy the equations $v^2 + h(u)v = f(u)$ and the partial derivative equations $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$. From the Definition 3, it is clear that a hyperelliptic curve of genus $g = 1$ is an elliptic curve.

7 Why hyperelliptic curves?

The elliptic curve based cryptosystems are still new in the market. So why do we want to consider hyperelliptic curves of higher genus? The elliptic curve based

cryptosystems are new so people have not yet developed sophisticated attacks on them but with time we expect that this will not be the case. We summarize the reasons for considering hyperelliptic curve based cryptosystems.

- Hyperelliptic curves are a natural generalisation of the curves, namely the Jacobian of a hyperelliptic curve plays the same role as group of rational points on an elliptic curve, for the construction of a cryptosystem. In fact, the Jacobian of a elliptic curve is isomorphic to its group of rational points.
- Current cryptosystems are getting prone to attack by hackers so new concepts are needed in order to build more secure systems.

8 Problems and research work

In the previous section, we gave some reasons for considering hyperelliptic curve based cryptosystems. We would like to do theoretical as well as experimental work in this direction during the thesis work of the first author. Here, we give some specific points for further research. As many people are working in this area, present problems are solved and new problems evolve, so the points noted below should only be considered as a guideline, for more details consult [2, 5].

- Researchers have till now used only specific classes of hyperelliptic curves which give the equivalent security to corresponding elliptic curves under certain mappings. Investigate whether some other classes of hyperelliptic curves provide better security or not.
- An efficient implementation of the addition rule in the Jacobian is needed. Some work has been done for $g = 1, 2$ but no general fast method is available.
- The projective representation of points is used to speed up the computation in the case of elliptic curves. There is no parallel work done for the curves with genus more than one.

References

[1] R. ATHALE. *Counting number of points on elliptic curves over $\mathbb{F}_{2^m}$ fields. M.Sc.(Engg.) thesis,* Department of Computer Science and Automation, Indian Institute of Science, Bangalore, India, 2000.

[2] F. HESS, G. SEROUSSI, N. SMART. *Two Topics in Hyperelliptic Cryptography. Technical Report HPL-2000-118*, 2000.

http://www.hpl.hp.com/techreports/2000/
HPL-2000-118.html

[3] N. KOBLITZ. *Hyperelliptic cryptosystems. J. Crypto.,* 1, 139-150, 1989.

[4] N. KOBLITZ. *Algebraic Aspects of Cryptography.* Springer, 1999.

[5] E. MENEZES. *Elliptic Curve Public Key Cryptosystems.* Kluwer Academic Publishers, 1993.

[6] J. H. SILVERMAN, J. TATE. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[7] N. SMART. *On the Performance of Hyperelliptic Cryptosystems. Advances in Cryptology, EUROCRYPT '99,* Springer-Verlag, LNCS 1592, 165-175, 1999.

[8] H. C. A. VAN TILBORG. *Fundamentals of Cryptology : A Professional Reference and Interactive Tutorial.* Kluwer International Series in Engineering and Computer Science, 1999.