Elgamal Encryption and its application to Ellicptic Curve Cryptography

Prof. Dr.- Ing. Ulrich Jetzek, David Kledtke
University of Applied Sciences Kiel
Germany

10th International Symposium on
Ambient Intelligence and Embedded Systems

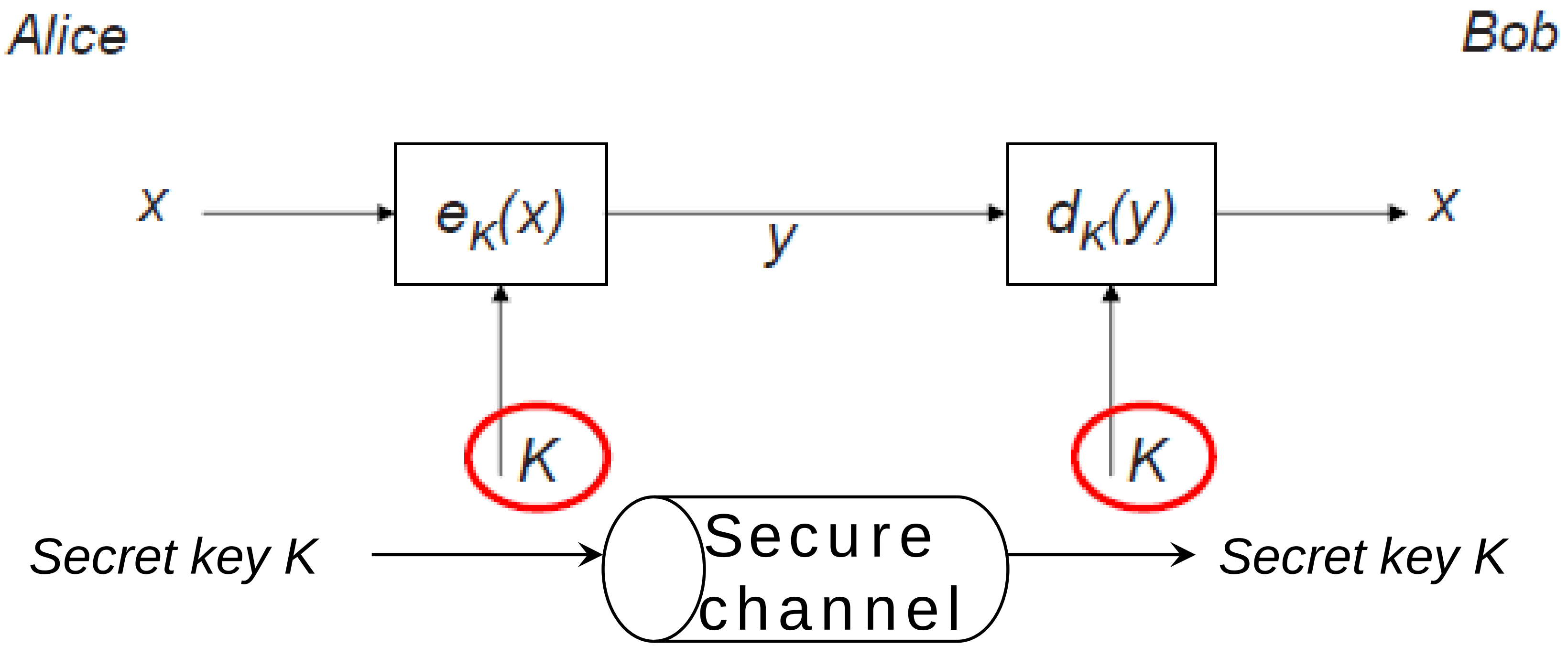
September 22nd – 24th, 2011

Chania, Crete, Greece

Overview

1. Introduction Public key cryptography
2. Idea of Diffie-Hellman Key Exchange
3. El Gamal Encryption
4. Elliptic Curve Introduction
5. El Gamal Encryption to Elliptic Curve Cryptography
6. Implementation of the El Gamal EC encoder
7. Conclusion

1. Symmetric Cryptography



- Major properties of symmetric cryptography:
  - **SAME secret key *K*** is used for encryption and decryption
  - **SAME secret key K** used by sender (Alice) and receiver (Bob)
- Disadvantage: **Key K** must be **transmitted** to receiver **over secure channel**!

1. Idea of Public Key Cryptography

- „Good old mailbox“ principle:
  - **Everybody** can drop a letter into the mailbox, i.e. **encrypt** a message
  - **ONLY the owner of the mailbox** can take out the letter, i.e. **decrypt** the message.

- 1976: first publication of such an algorithm by Whitfield Diffie, Martin Hellman and Ralph Merkle.

Source: Paar, Pelzl: *Understanding Cryptography, chapter 6*

1. Introduction Public Key Cryptography

- **Key** is split into **2 parts**:
  - Public key
    - known to everyone
    - allows to encrypt a message!
  - Private key
    - ONLY known by the receiver of the message
    - allows to decrypt a message!

Alice (Sender) — Bob (Receiver)

$$k = (k_{pub}, k_{priv})$$

$$\xleftarrow{\text{Publication of } k_{pub}}$$

$$y = e_{k_{pub}}(x)$$

$$\xrightarrow{\text{Sending cipher text } y}$$

$$x = d_{k_{priv}}(y)$$

Source: Paar, Pelzl: *Understanding Cryptography, chapter 6*

1. Discrete Logarithm Problem

Logarithm over real number arithmetic:

$$\beta = \alpha^x \qquad \Rightarrow x = \log_\alpha \beta$$

$$\beta = \alpha^x \bmod p \quad \Rightarrow x = ??$$

$\Rightarrow$ Discrete Logarithm Problem

- If prime p is sufficiently large (> 1000 bits in length), **exponentiation *modulo p*** forms **a one-way (or trapdoor-) function**

2. Idea of Diffie-Hellman Key Exchange (DHKE)

- If p is prime and α is generator (primitive element) of the finite field $Z_p^*=\{1,\ldots,p-1\}$, then the following identity holds:

$$
\begin{aligned}
&(\alpha^a \bmod p)^b \bmod p \\
&\equiv (\alpha^b \bmod p)^a \bmod p \\
&\equiv \alpha^{a \cdot b} \bmod p
\end{aligned}
$$

1.2 Algebraic Introduction: Cyclic Groups

- What happens if we multiply an element a of G k times with k= 1,2,3,…?
- Example: $a=3^k$, $a=2^k$ within Z_{11}^* with k=1,2,3,…?

$$
\begin{aligned}
a^1 &= 3 \\
a^2 &= a \cdot a = 9 \\
a^3 &= a^2 \cdot a = 27 \bmod 11 \equiv 5 \\
a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \bmod 11 \equiv 4 \\
a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \bmod 11 \equiv 1 \\
a^6 &= a^5 \cdot a = 1 \cdot 3 = 3 \\
a^7 &= a^6 \cdot a = 3 \cdot 3 = 9 \\
&\vdots
\end{aligned}
$$

Definition : Order of an element

The order *ord(a)* of an element *a* of a group $(G, \circ)$ is the smallest positive integer *k* such that

$$a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k \text{ times}} = 1$$

where $e = 1$ is the identity element of G.

Source: Paar, Pelzl: *Understanding Cryptography, chapter 8*

1.2 Algebraic Introduction: Cyclic Groups

- Example: What is the order ord(a=2) within Z_{11}^* ?

$$a^1 = 2$$
$$a^2 = a \cdot a = 4$$
$$a^3 = a^2 \cdot a = 8$$
$$a^4 = a^3 \cdot a = 16 \bmod 11 \equiv 5$$
$$a^5 = a^4 \cdot a = 5 \cdot 2 = 10$$
$$a^6 = a^5 \cdot a = 10 \cdot 2 = 20 \bmod 11 \equiv 9$$
$$a^7 = a^6 \cdot a = 9 \cdot 2 = 18 \bmod 11 \equiv 7$$
$$a^8 = a^7 \cdot a = 7 \cdot 2 = 14 \bmod 11 \equiv 3$$
$$a^9 = a^8 \cdot a = 3 \cdot 2 = 6$$
$$a^{10} = a^9 \cdot a = 6 \cdot 2 = 12 \bmod 11 \equiv 1$$

- Ord(a=2)=11-1=10 in Z_{11}^*!

Source: Paar, Pelzl: *Understanding Cryptography, chapter 8*

3. ElGamal Encryption

Domain parameters:

Large prime p

Primitive element α Î Z_p^*

Alice | **Bob** | DHKE

Alice		Bob
		choose random private key $k_{prB}=b \in \{2,\ldots,p-2\}$
choose random private key $k_{prA}=a \in\{2,\ldots,p-2\}$		
	$k_{pubB}= (p, \alpha, B)$ $\longleftarrow$	compute public key Bob $k_{pubB}= B = \alpha^b \bmod p$
compute public key Alice $k_{pubA}= A = \alpha^a \bmod p$	$\xrightarrow{A}$	
compute common secret key $k_{AB} = B^a \equiv (\alpha^b)^a \bmod p \equiv \alpha^{ba} \bmod p$		compute common secret key $k_{AB} = A^b = (\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$
Encrypt message m Î Z_p^*: $c = m \cdot k_{AB} \bmod p$	$\xrightarrow{c}$	Decryption: $m = c \cdot k_{AB}^{-1} \bmod p$

4. Motivation for Elliptic Curve Cryptography

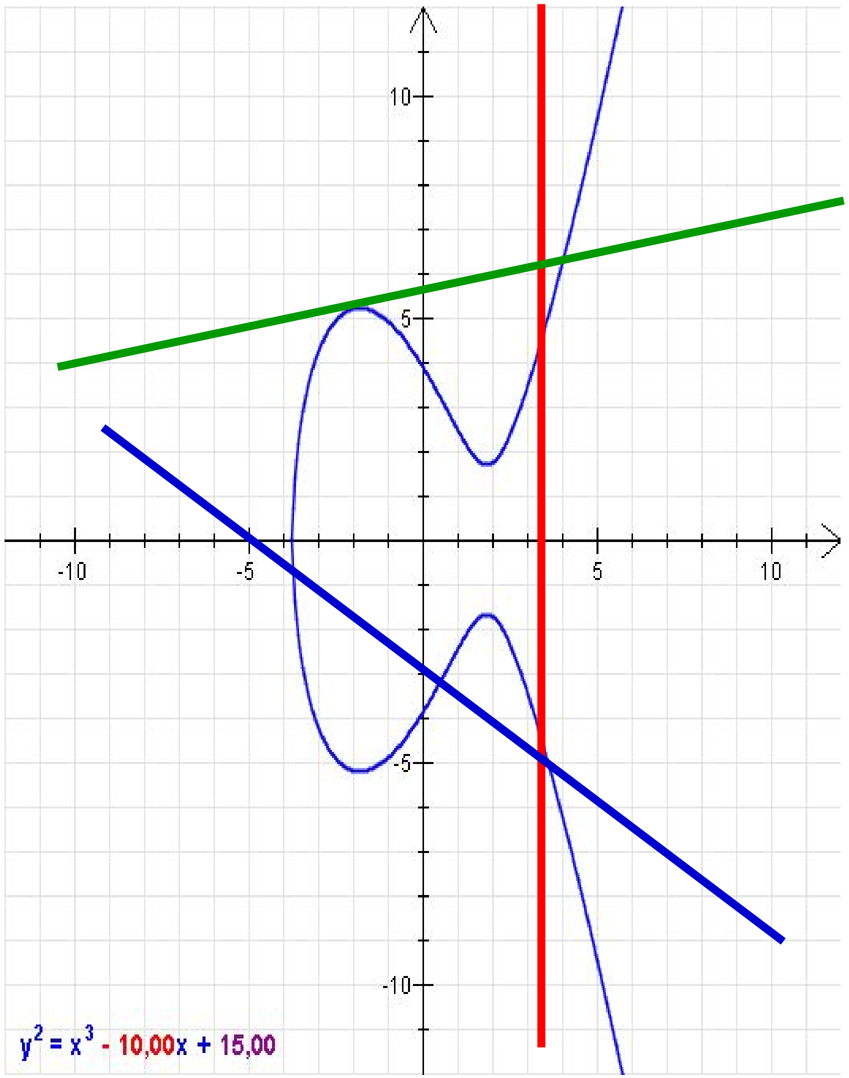
RSA key length / bit	ECC key length / bit	Ratio ECC/RSA key length	security-level (AES) bit
1024	160	1/6	80
3072	256	1/12	128
7860	384	1/20	192
15360	512	1/30	256

- Security level of n bits = best known attack requires 2^n steps.

- Advantage of ECC obvious: SAME security level with MUCH SHORTER key length!

Paar: Understanding Cryptography

4. Introduction to Elliptic Curves



- Generic expression:

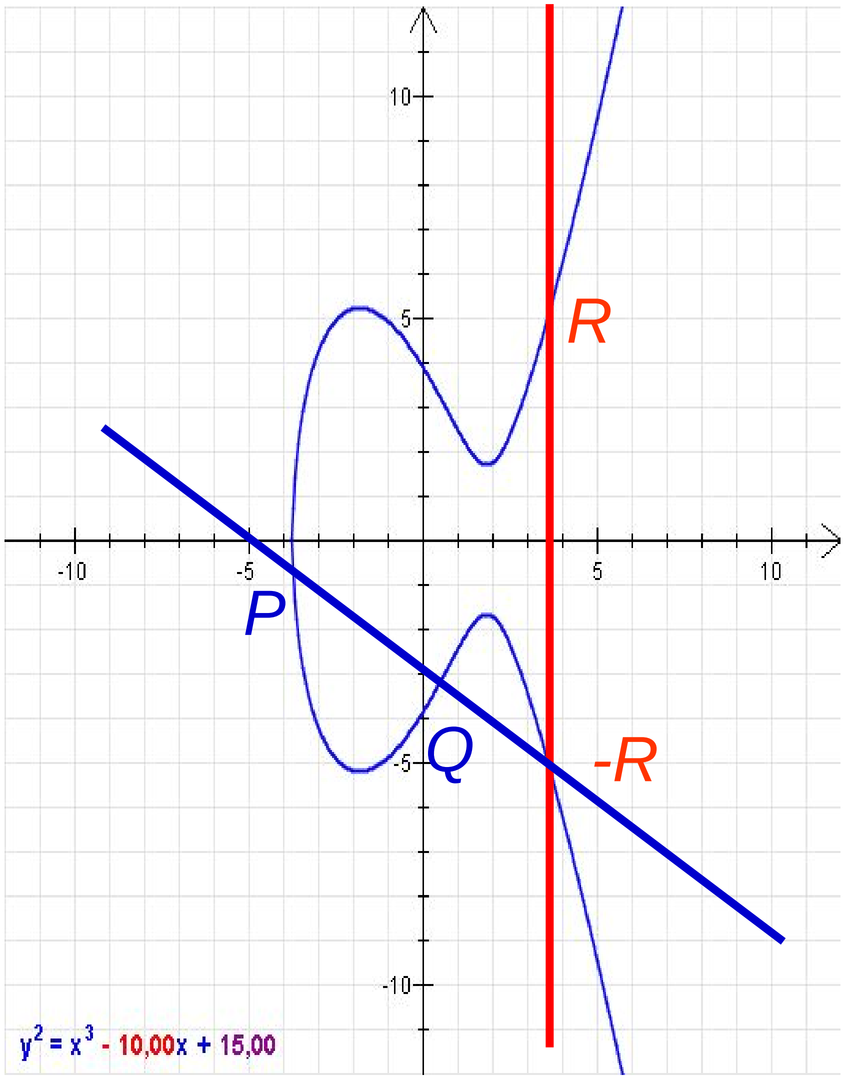
$$y^2 = x^3 + ax + b$$

- Special Elliptic Curve Property:

  A line through an Elliptic Curve always has 3 intersections with the Elliptic Curve.

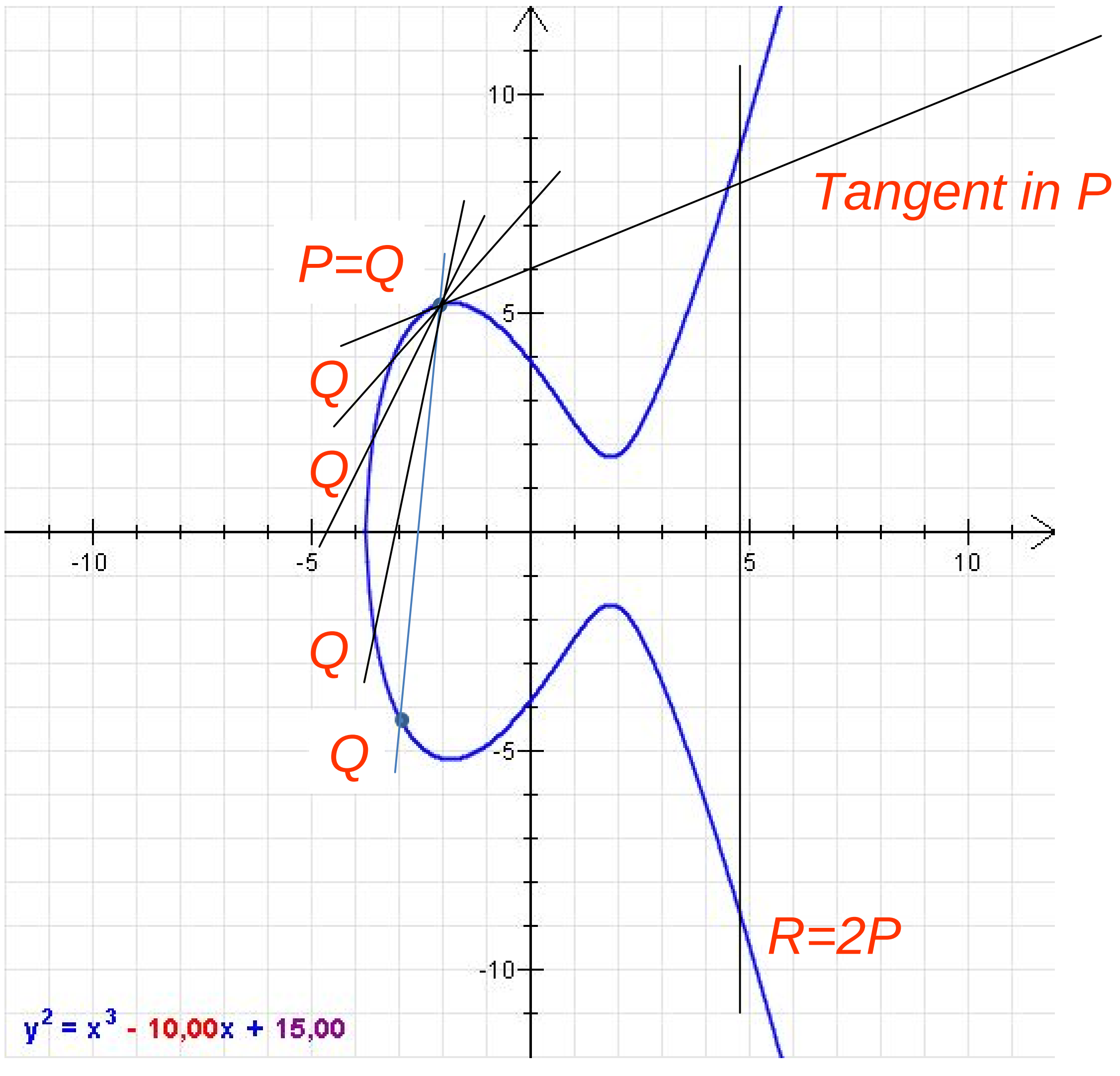
- Following cases do exist:
  - Line parallel to the y-axis: one of the 3 intersection points is the point at infinity *O.*
  - *Line is a tangent to the elliptic curve. The touch point is counted as 2 intersection points.*
  - *In other cases: 3 intersections obvious.*

4. Point Addition on Elliptic Curves



- *Definition of Point Addition on EC (geometric approach):*
  1. Draw a line through P and Q and obtain a 3rd point of intersection between this line and the elliptic curve E.
  2. Mirror the 3rd point at the x-Axis.
  3. The resulting point is the „sum“ R of the points P and Q.
- With this „Addition“ all points on an EC together with the point at infinity *O* form a group with the group operation „Addition“.
- Description by formulae possible as well.

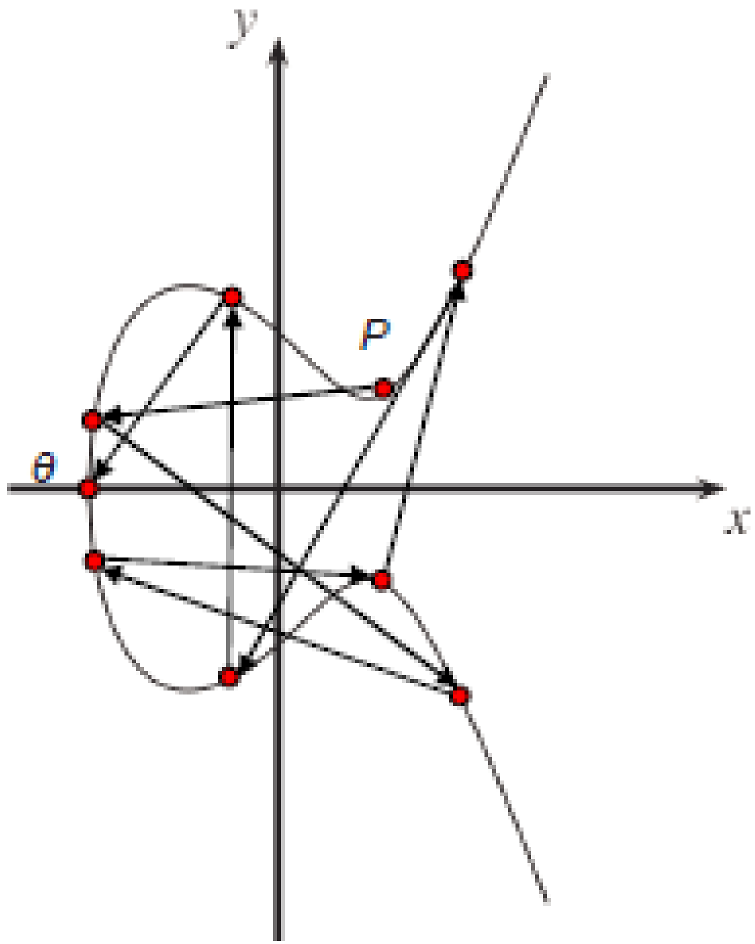
4. Point Doubling



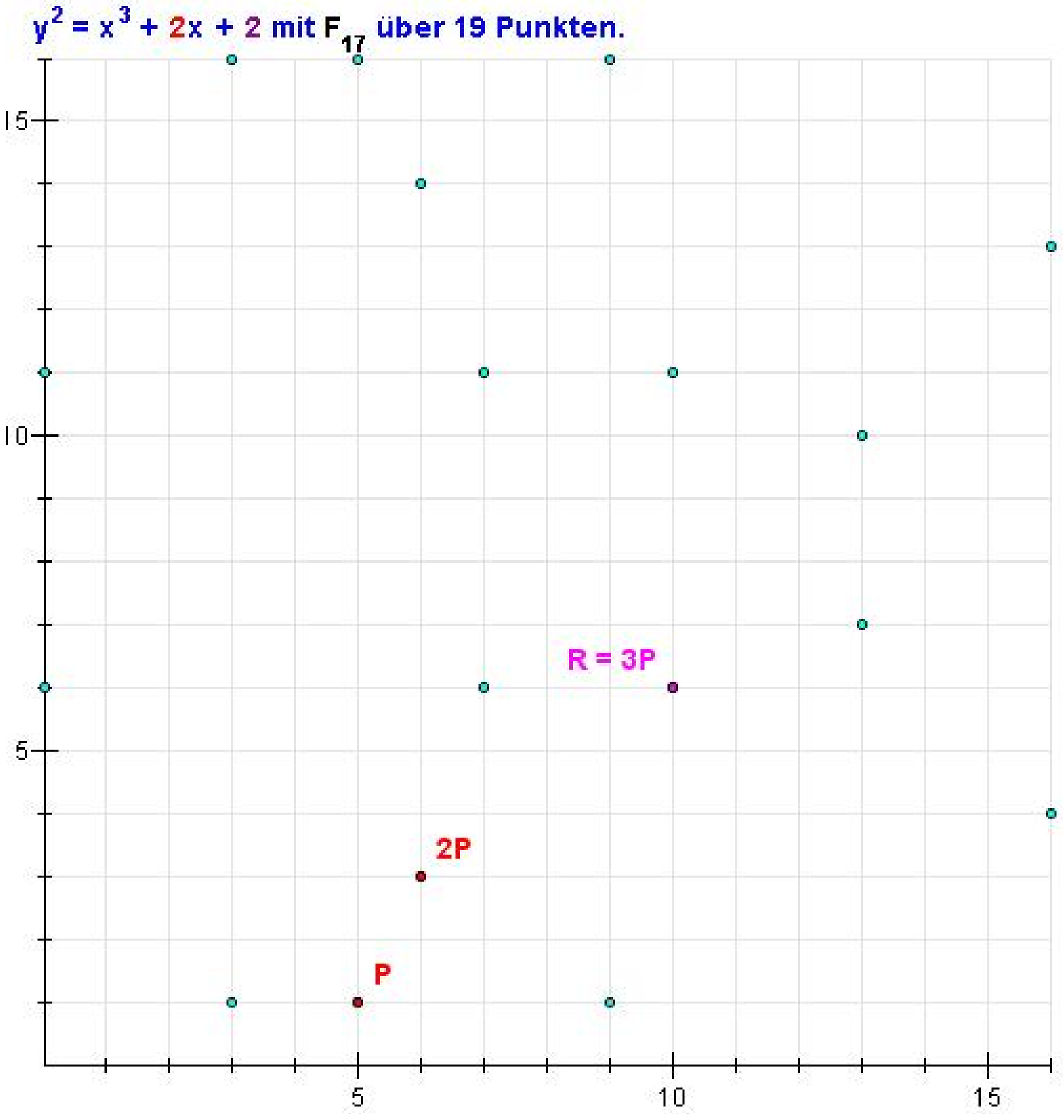
4. Point Multiplication and the DLP on Elliptic Curves

- If point P on an elliptic curve E with prime order p is a primitive element, ANY OTHER point Q of the EC can be reached by adding the point P to itself k times (multiplication of P with the factor k).
- If ONLY P and Q are given, finding the integer value k, this is called the DLP on Elliptic Curves.
- Since this problem – finding the value of k – is difficult to solve it is used in cryptography.

Point multiplication= „hopping on the EC“



4. Elliptic curves over Finite Fields



- **Point multiplication equals „hopping“ between points on the EC.**
- P is prime
- $F_p = \{0,1,\ldots,p-1\}$
- *All parameters x,y,a,b must be elements of* F_p
- à each combination which fulfills the condition $y^2=x^3+ax+b \bmod p$ is point on the EC.
- Advantages:
  - Calculations with positive integers only
  - Implementation in FPGA rather straightforward
  - No rounding errors

4. Point Addition on EC (algebraic approach)

Elliptic Curve Point Addition and Point Doubling

$$x_3 = s^2 - x_1 - x_2 \mod p$$

$$y_3 = s(x_1 - x_3) - y_1 \mod p$$

where:

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \mod p & \text{; if } \mathrm{P} \neq \mathrm{Q} \text{ (point addition) - slope of line defined P and Q} \\ \dfrac{3x_1^2 + a}{2y_1} \mod p & \text{; if } \mathrm{P} = \mathrm{Q} \text{ (point doubling) - slope of tangent defined by P} \end{cases}$$

slope of tangent in point P:

$$E\text{:}\ y^2 = x^3 + ax + b$$

$$\frac{dy^2}{dx} = \frac{dy^2}{dy} \cdot \frac{dy}{dx} \quad \text{(chain rule: outer * inner derivation)}$$

$$2\mathrm{y} \cdot \mathrm{y}' = 3 \cdot \mathrm{x}^2 + a \Rightarrow$$

$$y' = s = \frac{3 \cdot \mathrm{x}^2 + a}{2y}$$

4. Encryption over Z_p^* à Elliptic Curve Encryption over F_p

Item	Encryption over Z_p^*	Elliptic Curve Encryption over F_p
Dimensions	1-dimensional	2-dimensional
Group elements	Integers x Î Z_p^*	Points X Î F_p
Group Operation	Multiplication	Addition
Operation	Exponentiation mod p	Point Multiplication on Elliptic Curve E mod p

5. El Gamal Encryption on Elliptic Curves

Domain parameters:

Prime p

Elliptic Curve *E* over finite field F_p *(*incl. *O)*, with prime order *n*

Primitive Element of *E: P*

DHKE

Alice		Bob
		choose random private key $k_{prB}=b \in \{2,\ldots,p\text{-}2\}$
choose random private key $k_{prA}=a \in \{2,\ldots,p\text{-}2\}$		
compute public key Alice $k_{pubA}= A = a\cdot P$	$\xleftarrow{k_{pubB}= (p,E,n,P,Q)}$	compute public key Bob $K_{pubB}= Q = b\cdot P$
	$\xrightarrow{A}$	
compute common secret key $K_{AB} = a\cdot Q = a \cdot b \cdot P$		compute common secret key $K_{AB} = b\cdot A = b \cdot a \cdot P = a\cdot Q$
Encrypt plain text M Î F_p $C = M + a \cdot Q$	$\xrightarrow{C}$	Decrypt cipher text C: $M = C – K_{AB} = C - a\cdot Q$

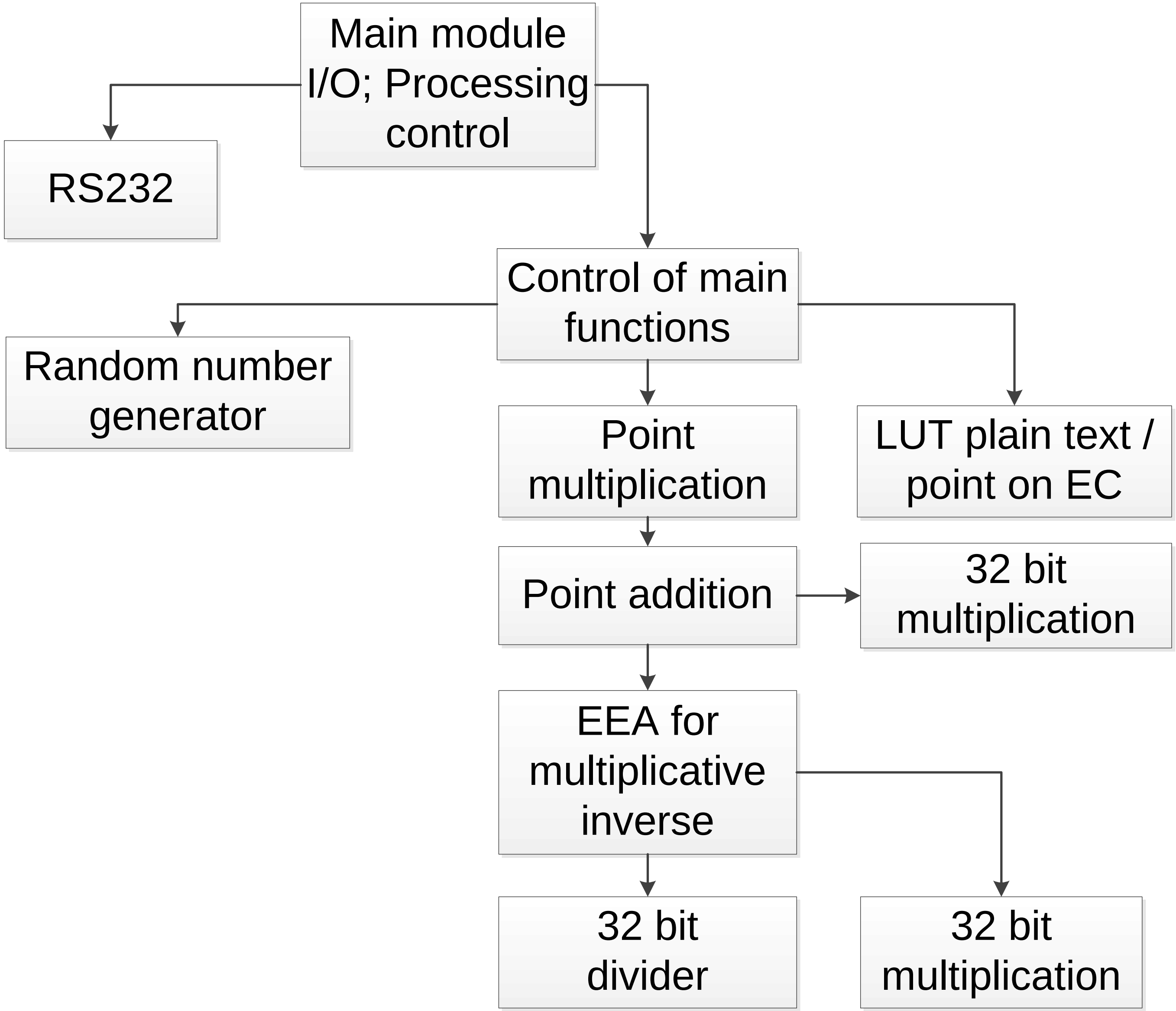
6. Needed arithmetic operations

- Operations to be implemented:

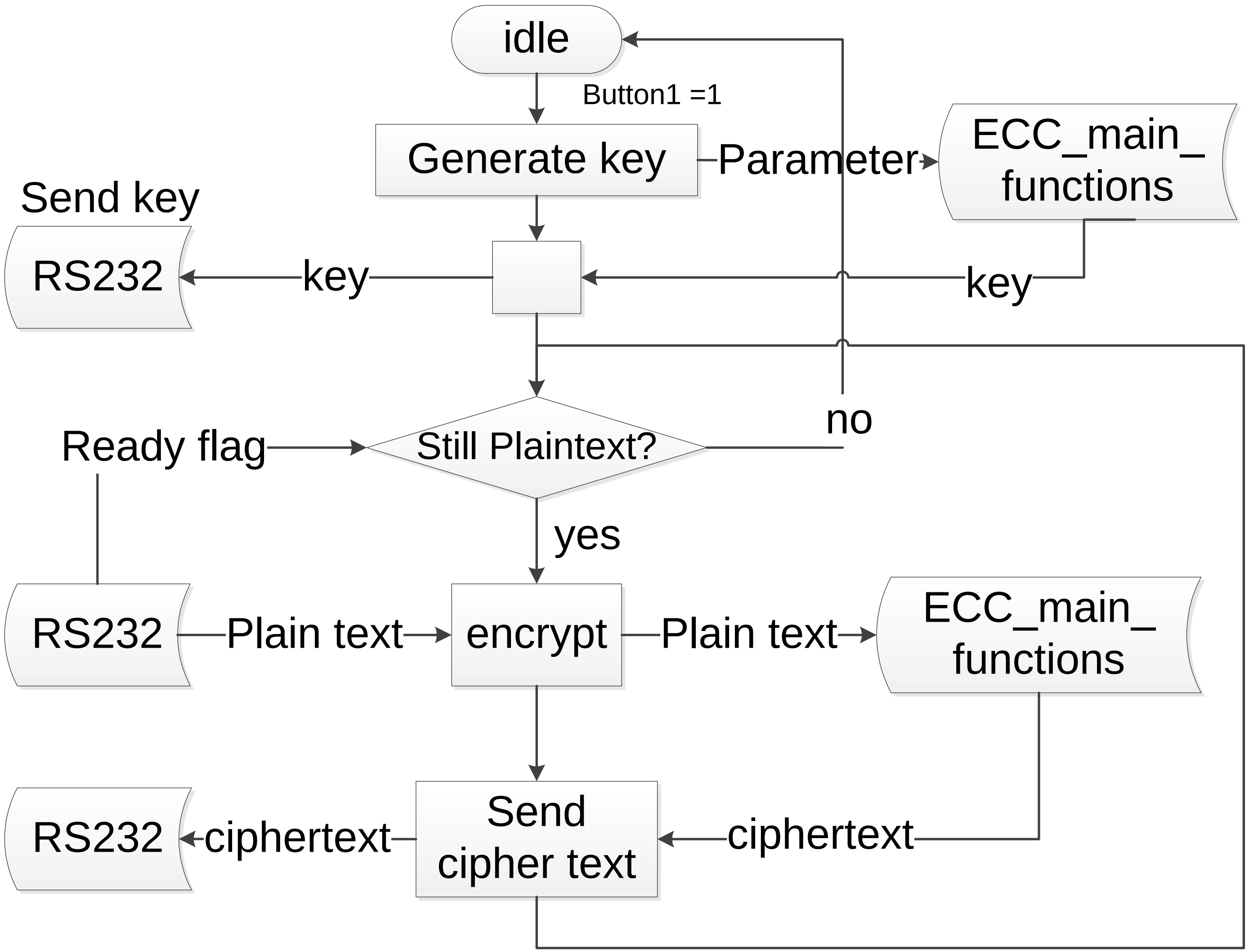
- Addition, Subtraction and Multiplication
  - Direct synthesis possible

- Modulo-operation and multiplication with multiplicative inverse (division):
  - Multiplicative inverse by Extended Euclidean Algorithm

6. Hierarchy of the ElGamal-EC-encoder



6. Finite State Machine for ElGamal-EC encryption



7. Conclusion

- ElGamal Encryption may be seen as an extension of the DHKE
- Elliptic Curves with corresponding „addition“ and „multiplication“ operation leads to **2-dimensional encryption.**
- ElGamal encryption can almost straightforward be applied to Elliptic Curves as well
- FPGA implementation of ElGamal EC-encoder mainly requires
  - EC operations
  - Extended Euclidean algorithm
  - Finite state machine to control the processing.