ElGamal on Elliptic Curve Cryptography

Grant McNaughton

29 March 2024

1 Introduction

Cryptography is the practice and study of making communications unintelligible to all except authorized parties. Naturally, we want to ensure the following:

- *Correctness*: The message sent by the sender is correctly received by the receiver.
- *Security*: The third party is prevented from eavesdropping the message. For this, the sender typically encrypts the message and the receiver decrypts. The encryption should be done in a way that the decryption is **extremely difficult** for the the third party.
- *Efficiency*: Encryption should be efficient for the sender and decryption should be efficient for the receiver.

In this paper, we will describe

1. a cryptosystem called "ElGamal", proposed by Taher ElGamal [1]. It is built on an group, say G.
2. a field called "Finite prime field".
3. a group called "Elliptic Curve Group". It is built on a field, say F.

2 Cryptosystem (ElGamal)

Algorithm 1 (ElGamal Scheme)**.**
Consider a situation where Alice (sender) wants to send a message to Bob (receiver).

1. *Bob does the following once.*
   (a) *Pick a group* $(G, \cdot)$*. For some prime number* p, $G = \{\mathbb{Z} \setminus 13\mathbb{Z}\}^* = \{1, 2, \ldots, p-1\}$ *and* $\cdot$ *represents multiplication modulo* p.
   (b) *Choose* $g \in G \setminus \{e\}$
   (c) *Choose* $k \in \mathbb{N}$ *such that* $k > 0$.
   (d) *Set* $h = g^k = g \cdot g \cdot \ldots \cdot g$.
   (e) *Publish* $(G, \cdot)$, g, *and* h.
2. *Alice does the following whenever she wants to send a message to Bob.*
   (a) *Encode her message* $m \in G$.

(b) *Choose* $s \in \mathbb{N}$ *such that* $s > 0$.

(c) *Calculate* $c_1 = g^s = g \cdot g \cdot \ldots \cdot g$ *and* $c_2 = h^s m = h \cdot h \cdot \ldots \cdot h \cdot m$.

(d) *Send* c_1 *and* c_2 *to Bob.*

3. *Bob does the following upon receiving series of* c_1, c_2 *from Alice.*

   (a) *Calculate* $m' = c_1^{-k} c_2 = m$.

Example 2.

1. *Suppose that* $G = (\mathbb{Z}/7\mathbb{Z})^*$, $g = 2$, $k = 5$, $m = 3$, $s = 4$. *Determine the values of* h, c_1, c_2 *and* m'.
   Note
   - $h = g^k = 2^5 = 4$
   - $c_1 = g^s = 2^4 = 2$
   - $c_2 = h^s m = 4^4 \cdot 3 = 5$
   - $m' = c_1^{-k} c_2 = 2^{-5} \cdot 5 = 4^5 \cdot 5 = 3$
2. *Suppose that* $G = (\mathbb{Z}/13\mathbb{Z})^*$, $g = 4$, $k = 5$, $m = 6$, $s = 2$. *Determine the values of* h, c_1, c_2 *and* m'.
   Note
   - $h = g^k = 4^5 = 10$
   - $c_1 = g^s = 4^2 = 3$
   - $c_2 = h^s m = 10^2 \cdot 6 = 2$
   - $m' = c_1^{-k} c_2 = 3^{-5} \cdot 2 = 9^5 \cdot 2 = 6$

Theorem 3. *The ElGamal scheme is correct, that is,* $m' = m$.

Proof. Set $g \in G$ and $k, s \in \mathbb{N}$ with $k, s > 0$. Note that because $\cdot$ represents multiplication modulo p, $\cdot$ is commutative and thus G is an Abelian group. Establish $h = g^k$, $c_1 = g^s$, $c_2 = h^s m$, and $m' = c_1^{-k} c_2$. From this we can derive that

$$
\begin{aligned}
h &= g^k \\
h^s &= {g^k}^s \\
h^s &= g^{sk} \\
1 = e &= g^{sk^{-1}} h^s \\
m = em &= g^{sk^{-1}} h^s m \\
m &= c_1^{-k} c_2 = m'
\end{aligned}
$$

Therefore $m' = m$. $\square$

Algorithm 4 (*gpow* : efficient algorithm for power)**.** *Let* G *be a group.*
Input: $g \in G, k \in \mathbb{N}$
Output: g^k

1. *If* $k = 0$ *then return* e.
2. *If* k *is even, then define* r *given by the output of* $gpow(g, \frac{k}{2})$ *and return* $r \cdot r$.
3. *If* k *is odd, then define* r *given by the output of* $gpow(g, \frac{k-1}{2})$ *and return* $r \cdot r \cdot g$.

3 Finite prime field

Definition 5 (Finite prime field)**.** *Let p be a prime number. Then the finite prime field structure is given by the following set F_p and two operations $+_p$ and $\times_p$ on it.*

1. $F_p = \{0, 1, \dots, p-1\}$
2. *Operation* $+_p : a +_p b$, *(addition mod p)*
3. *Operation* $\times_p : a \times_p b$, *(multiplication mod p)*

Example 6. $p = 5$

1. $F_5 = \{0, 1, 2, 3, 4\}$
2. $2 +_5 4 = 1$
3. $2 \times_5 4 = 3$

Theorem 7. *F_p is a field where 0 is the identity for $+_p$ and 1 is the identity for x_p.*

Proof. See any standard text book. □

Algorithm 8 (inverse for $\times_p$ using the extended Euclidean algorithm)**.**
Input: $a \in F_p \setminus \{0\}$
Output: a^{-1}

1. $r_0 \leftarrow p$
2. $r_1 \leftarrow a$
3. $t_0 \leftarrow 0$
4. $t_1 \leftarrow 1$
5. $r_{i-2} = q_i r_{i-1} + r_i$
6. $t_{i-2} = q_i t_{i-1} + t_i$
7. *Repeat while $r_i > 0$ and stop when $r_i = r_{\text{final}} = 0$.*
8. $a^{-1} = t_{\text{final}-1}$

Example 9.

1. *Find 4^{-1} in $\mathbb{Z}_7$ using the algorithm.*
   (a) *See the trace of the algorithm:*

i	q_i	r_i	t_i
0		7	0
1		4	1
2	1	3	6
3	1	1	2
4	3	0	

   (b) *Note that $r_4 = 0$. Thus $4^{-1} = t_3 = 2$.*

2. *Find 7^{-1} in $\mathbb{Z}_{13}$ using the algorithm.*

   (a) *See the trace of the algorithm:*

i	q_i	r_i	t_i
0		13	0
1		7	1
2	1	6	12
3	1	1	2
4	6	0	

   (b) *Note that $r_4 = 0$. Thus $7^{-1} = t_3 = 2$.*

Theorem 10. *The algorithm terminates.*

Proof. Immediate from $r_0 > r_1 > \cdots \geq 0$. □

Theorem 11. *The algorithm is correct.*

4 Group based on Elliptic curve

Definition 12 (Elliptic Curve Structure)**.** *Let F be a field and let $a, b \in F$. The elliptic curve structure is given by the following set E and an operation $+$.*

1. $E_{ab} = \left\{(x, y) \in F^2 : y^2 = x^3 + ax + b\right\} \cup \{\infty\}$
2. *Operation $+$:* $\quad C = A + B$

$$
\begin{array}{lll}
\textit{If} \quad A = \infty & : & C = B \\
\textit{Else if} \quad B = \infty & : & C = A \\
\textit{Else if} \quad x_A = x_B \ \textit{ and } y_A = -y_B & : & C = \infty \\
\textit{Else if} \quad x_A = x_B \ \textit{ (and } y_A = y_B\textit{)} & : & m = \frac{3x_A^2 + a}{2y_A} \\
 & & x_c = m^2 - 2x_A \\
 & & y_c = -m(x_C - x_A) - y_A \\
\textit{Else} \quad (x_A \neq x_B,\ \textit{generic case}) & : & m = \frac{y_B - y_A}{x_B - x_A} \\
 & & x_A = m^2 - x_A - x_B \\
 & & y_C = -m(x_C - x_B) - y_A
\end{array}
$$

Example 13.

1. *Let $F = (F_3, +_3, \times_3)$ and $a = 1$ and $b = 1$. (see below for the definition of the field.)*

   (a) *Find all the elements of the elliptic curve E.*

$$
\begin{aligned}
E &= \left\{(x, y) \in F_3^2 : y^2 = x^3 + x + 1\right\} \cup \{\infty\} \\
&= \{(0, 1), (0, 2), (1, 0), \infty\}
\end{aligned}
$$

(b) *Construct the operation table.*

oA	$(0,1)$	$(0,2)$	$(1,0)$	∞
$(0,1)$	$(1,0)$	∞	$(0,2)$	$(0,1)$
$(0,2)$	∞	$(1,0)$	$(0,1)$	$(0,2)$
$(1,0)$	$(0,2)$	$(0,1)$	∞	$(1,0)$
∞	$(0,1)$	$(0,2)$	$(1,0)$	∞

2. *Let* $F = (F_5, +_5, \times_5)$ *and* $a = 0$ *and* $b = 1$.

   (a) *Find all the elements of the elliptic curve* E.

$$\begin{aligned} E &= \left\{(x,y) \in F_5^2 : y^2 = x^3 + 1\right\} \cup \{\infty\} \\ &= \{(0,1), (0,4), (2,2), (2,3), (4,0), \infty\} \end{aligned}$$

   (b) *Construct the operation table.*

oA	$(0,1)$	$(0,4)$	$(2,3)$	$(2,3)$	$(4,0)$	∞
$(0,1)$	$(0,4)$	∞	$(2,3)$	$(4,0)$	$(2,2)$	$(0,1)$
$(0,4)$	∞	$(0,1)$	$(4,0)$	$(2,2)$	$(2,3)$	$(0,4)$
$(2,2)$	$(2,3)$	$(4,0)$	$(0,4)$	∞	$(0,1)$	$(2,2)$
$(2,3)$	$(4,0)$	$(2,2)$	∞	$(0,1)$	$(0,4)$	$(2,3)$
$(4,0)$	$(2,2)$	$(2,3)$	$(0,1)$	$(0,4),$	∞	$(4,0)$
∞	$(0,1)$	$(0,4)$	$(2,2)$	$(2,3)$	$(4,0)$	∞

Derivation 14.

- *We will derive the formulas for* m, x_C *and* y_C *for the generic case.*

  1. *Determine* $x_{C'}$ *and* $y_{C'}$.

     (a) *For this, we need to solve*

$$\begin{aligned} y &= y_A + m\,(x - x_A) \\ y^2 &= x^3 + ax + b \end{aligned}$$

     where

$$m = \frac{y_B - y_A}{x_B - x_A}$$

     (b) *Because* $y = m(x - x_A) + y_a$, *we know that* $y^2 = (m(x - x_A) + y_a)^2$, *which can be simplified as follows:*

$$\begin{aligned} y^2 &= (m(x - x_A) + y_a)^2 \\ &= (m(x - x_A))^2 + 2m(x - x_A)y_A + y_A^2 \\ &= (mx - mx_A)^2 + 2mxy_A - 2mx_Ay_A + y_A^2 \\ &= m^2x^2 - 2m^2xx_A + m^2x_A^2 + 2mxy_A - 2mx_Ay_A + y_A^2 \end{aligned}$$

$$= m^2x^2 + (-2m^2x_A + 2my_A)x + (m^2x_A^2 - 2mx_Ay_A + y_A^2)$$
$$= m^2x^2 + 2m(y_A - mx_A)x + (mx_A - y_A)^2$$

This result can then be used as the left-hand side of $y^2 = x^3 + ax + b$ *as follows:*

$$m^2x^2 + 2m(y_A - mx_A)x + (mx_A - y_A)^2 = x^3 + ax + b$$
$$0 = x^3 - m^2x^2 + (a - 2m(y_A - mx_A))x + (b - (mx_A - y_A)^2)$$

Using Vieta's formulas, we can say that $x_A + x_B + x_{C'} = -\frac{-m^2}{1}$ *and thus* $x_{C'} = m^2 - x_A - x_B$. *By definition,* $y_{C'} = m(x_C - x_A) + y_A$.

2. *Determine* x_C *and* y_C.
   $x_C = x_{C'} = m^2 - x_A - x_B$
   $y_C = -y_{C'} = -(m(x_C - x_A) + y_A) = -m(x_C - x_A) - y_A$.

- *Derive the formula for the slope* m *when* $x_A = x_B$ *and* $y_A = y_B$.

  1. *We can use implicit differentiation to find the derivative* $\frac{dy}{dx}$*:*

  $$y^2 = x^3 + ax + b$$
  $$2y\frac{dy}{dx} = 3x^2 + a$$
  $$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

  2. *We can then evaluate the derivative at point* A *to find* $m = \frac{2x_A^2 + a}{2y_a}$.

Theorem 15. $(E, +)$ *is is a group where* ∞ *is identity and the inverse of* A *is* ∞ *if* $A = \infty$ *and* $(x_A, -y_A)$ *if* $A = (x_A, y_A)$.

References

[1] Taher ElGamal A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms *IEEE Transactions on Information Theory*, 31(4), 1985.