The ElGamal Cryptosystem

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@.unipi.it
Version: 30/03/25

1

The ElGamal Cryptosystem

INTRODUCTION

2

Introduction

extension to use DHKE as a cypher.
DH is only used for key establishment

- Taher ElGamal, 1985
- An "extension" of Diffie-Hellman Key Exchange
- One-way function: Discrete Logarithm
- Appliable in any cyclic group where DLP and DHP are intractable
- We consider the cyclic multiplicative group $\mathbb{Z}_p^*$

Mar-25 The ElGamal Cryptosystem 3

3

From DHKE to ElGamal encryption

Alice		Bob
		(a) choose $d = privK_B \in \{2, \ldots, p-2\}$
		(b) compute $\beta = pubK_B \equiv \alpha^d \bmod p$
		y_B
	< -------------- β -----------------	
(c) choose a new $i \in \{2, \ldots, p-2\}$		in DH it is the shared secret
(d) compute $k_E \equiv \alpha^i \bmod p$ (*ephemeral key*)		
y_A	------------------k_E------------------ >	
(e) compute $k_M \equiv \beta^i \bmod p$ (*masking key*)		(f) compute $k_M \equiv k_E^d \bmod p$
		y_A
(g) Encrypt $x \in Z_p^*$: $y \equiv x \cdot k_M \bmod p$		
	------------------y------------------ >	
x is plaintext		(g) decrypt $x \equiv y \cdot k_M^{-1} \bmod p$
So encryption is multiplication		

IDEA

Mar-25 The ElGamal Cryptosystem 4

4

From DHKE to ElGamal encryption

- On domain parameters and keys
- Domain parameters
  - Large p and primitive element α
- Keys
  - The public-private pair (d, β) does not change
  - The public-private pair (i, k_E) is generated for every new message (ephemeral)
  - k_E is called *ephemeral key*
  - k_M is called the *masking key*

Mar-25 The ElGamal Cryptosystem 5

5

From DHKE to ElGamal encryption

- Intuition
  - One property of cyclic groups is that, given $k_M \in \mathbb{Z}_p^*$, every message *x* maps to another ciphertext *y* if the two values are multiplied, $y = x \cdot k_M \bmod p$
  - If every k_M is randomly chosen from $\mathbb{Z}_p^*$ then every *y* in {1, 2, …, p – 1} is equally likely
- Remark
  - In the ElGamal encryption scheme we do not need a TTP which generates *p* and α

Trusted Third Party

Mar-25 The ElGamal Cryptosystem 6

6

The ElGamal encryption scheme

THE ELGAMAL ENCRYPTION SCHEME

Mar-25 The ElGamal Cryptosystem 7

7

Real encryption scheme

From DHKE to ElGamal encryption

UNIVERSITÀ DI PISA

Alice **Bob**

choose large prime p

choose primitive element α of (a subgroup of) Zp*

choose $d = privK_B \in \{2, \ldots, p-2\}$

compute $\beta = pubK_B \equiv \alpha^d \bmod p$

<-------------- $pubK_B = (p, \alpha, \beta)$ -----------------

choose a new $i \in \{2, \ldots, p-2\}$

compute *ephemeral key*: $k_E \equiv \alpha^i \bmod p$

compute *masking key*: $k_M \equiv \beta^i \bmod p$

encrypt $x \in Z_p^*$: $y \equiv x \cdot k_M \bmod p$

-------------------(y, k_E)------------------- >

compute masking key: $k_M \equiv k_E^d \bmod p$

decrypt $x \equiv y \cdot k_M^{-1} \bmod p$

Mar-25 The ElGamal Cryptosystem 8

8

Consistency property

UNIVERSITÀ DI PISA

- Proof of the consistency property consists in proving that: $x \equiv y \cdot k_M^{-1} \bmod p$
- Proof
  1. $y \cdot k_M^{-1} \equiv (x \cdot k_M) \cdot (k_E^{d})^{-1} \equiv (x \cdot (\alpha^{d})^{i}) \cdot ((\alpha^{i})^{d})^{-1} \equiv$
  2. $x \cdot \alpha^{d \cdot i - d \cdot i} \equiv x \bmod p$

Mar-25 The ElGamal Cryptosystem 9

9

ElGamal is probabilistic

UNIVERSITÀ DI PISA

- ElGamal encryption scheme is *probabilistic*
  - Encrypting two identical messages x_1 and x_2 with the same public key $pubK_B = (p, \alpha, \beta)$ results in two different ciphertext y_1 and y_2 (with high probability) (because you change ephemeral key
  - Masking key k_M is chosen at random for every new message
  - Brute force against *x* is avoided a priori

↑ $y \equiv x \cdot k_M \bmod p$: even if x is small, you get a random number (so it's hard to understand if you got it right)

Mar-25 The ElGamal Cryptosystem 10

10

Performance issues

- Communication issues
  - Cyphertext expansion factor is 2
    - The bit size of (y, k_E) is twice as the bit size of x (sizeof(x) ≃ sizeof(K_E))
- Computational issues
  - Key Generation
    - Generation of large prime p (at least 1024 bits)
    - privK is generated by a RBG → (d is private key)
    - pubK requires a modular exponentiation

Mar-25 The ElGamal Cryptosystem 11

11

Performance issues

- Computational issues
  - Encryption
    - Two modular exponentiations and a modular multiplication
      - Exponentiations are independent of plaintext ➔ Pre-computation of k_E and k_M
  - Decryption
    - A modular exponentiation, a modular inverse and a modular multiplication
      - EEA can be used for modular inverse, or
      - We may combine exponentiation and inverse together, so we just need an exponentiation and a multiplication (➔)

Decryption a bit more efficient than encryption

Mar-25 The ElGamal Cryptosystem 12

12

Computational issues

- How to combine exponentiation and inverse together
  - Proof
    - Recall Fermat's Little Theorem
      - Let a be an integer and p be a prime, $a^{p-1} \equiv 1 \bmod p$
    - Merge the two steps of decryption
      - $k_M^{-1} \equiv (k_E^{d})^{-1} \equiv (k_E^{d})^{-1}\, k_E^{p-1} \equiv k_E^{p-d-1} \bmod p$

13

ElGamal Cryptosystem

SECURITY ISSUES

14

Security against passive attacks

Public Key
cyphertext

- The ElGamal problem
  - Recovering x from (p, α , β) and (y, k_E) where $\beta \equiv \alpha^d$ mod p; $k_E = \alpha^i$ mod p, and y = x · β^i mod p → K_M
- The ElGamal Problem relies on the hardness of DHP*
  - Currently there is no other known method for solving the DHP than solving the DLP
  - The adversary needs to compute Bob's secret exponent *d* or Alice's secret random exponent *i* like in DH.
  - The Index-calculus method can be applied ➔ |p| = 1024+ → 1024 bits or more

* if you can derive i from K_E you can decrypt

Mar-25 The ElGamal Cryptosystem 15

15

Security against active attacks

- Active attacks
  - Bob's public key must be authentic: authenticity of Public key (MITM)
  - Secret exponent *i* must be not reused (➔)
  - ElGamal is malleable (➔) (Homomorphic)

Mar-25 The ElGamal Cryptosystem 16

16

Security against active attacks

UNIVERSITÀ DI PISA

- On reusing the secret exponent i
  - Alice uses the same i for x_1 and x_2, then
    - both the masking keys and the ephemeral keys would be the same
      - $k_E = \alpha^i \equiv \text{mod } p$
      - $k_M = \beta^i \equiv \text{mod } p$
    - She transmits (y_1, k_E) and (y_2, k_E)
  - The adversary
    - Can easily identify the reuse of i
    - If (s)he can guess/know x_1, then (s)he can compute $x_2 \equiv y_2 \cdot k_M^{-1} \text{ mod } p$ with $k_M \equiv y_1 \cdot x_1^{-1} \text{ mod } p$

Because two quantities are the same

Mar-25 The ElGamal Cryptosystem 17

17

Security against active attacks

UNIVERSITÀ DI PISA

- On malleability
  - The adversary replaces (k_E, y) by $(k_E, s \cdot y)$
  - The receiver decrypts $x' \equiv x \cdot s \text{ mod } p$ (if you make all the comput.)
  - Schoolbook ElGamal is often not used in practice, but some padding is introduced

Mar-25 The ElGamal Cryptosystem 18

18

Mar-25 The ElGamal Cryptosystem 19

19