

1

The ElGamal Cryptosystem

INTRODUCTION

Mar-25

The ElGamal Cryptosystem

Introduction



extension to use OHKE as a cypher.

Off as 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}_n^*

Mar-25

The ElGamal Cryptosystem

From DHKE to ElGamal encryption



```
Alice
                                                                                   Bob
                                                                 (a) choose d = privK_B \in \{2, ..., p - 2\}
                                                                 (b) compute \beta = \text{pubK}_B \equiv \alpha^d \mod p
(c) choose a new i \in \{2, ..., p\}
                                                                     in DH at is the showed secret
(d) compute k_E \equiv \alpha^i \mod p (ephemeral key)
(e) compute k_M \equiv \beta^i \mod p (masking key)
                                                                 (f) compute k_M \equiv k_E^d \mod p
(g) Encrypt x \in Z_p^*: y \equiv x \cdot k_M \mod p
                                                                 (g) decrypt x \equiv y \cdot k_M^{-1} \mod p
                 So encryption is multiplication
                                                                                     l0ŧa
                                            The ElGamal Cryptosystem
```

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_F 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, $y = x \cdot k_M \mod p$
 - 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

Panky

Mar-25

The ElGamal Cryptosystem

6

The ElGamal encryption scheme

THE ELGAMAL ENCRYPTION SCHEME

Mar-25

The ElGamal Cryptosystem

7

7

From DHKE to ElGamal encryption



```
Alice
                                                                                Bob
                                                         choose large prime p
                                                         choose primitive element \alpha of (a
                                                         subgroup of) Zp*
                                                         choose d = privK_B \in \{2, ..., p-2\}
                                                         compute \beta = \text{pubK}_B \equiv \alpha^d \mod p
                          <----- pubK<sub>B</sub>= (p, \alpha , \beta) -----
choose a new i \in \{2, ..., p-2\}
compute ephemeral key: k_E \equiv \alpha^i \mod p
compute masking key: k_M \equiv \beta^i \mod p
encrypt x \in Z_p^*: y \equiv x \cdot k_M \mod p
                                -----> (y, k<sub>E</sub>)----->
                                                         compute masking key: k_M \equiv k_E^d \mod p
                                                         decrypt x \equiv y \cdot k_{M}^{-1} \bmod p
Mar-25
                                          The ElGamal Cryptosystem
```

Consistency property



- Proof of the consistency property consists in proving that: x ≡ y·k_M⁻¹ mod 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. $\mathbf{x} \cdot \alpha^{\mathbf{d} \cdot \mathbf{i} \mathbf{d} \cdot \mathbf{i}} \equiv \mathbf{x} \mod \mathbf{p}$

Mar-25

The ElGamal Cryptosystem

9

9

ElGamal is probabilistic



- ElGamal encryption scheme is probabilistic
 - Encrypting two identical messages x_1 and x_2 with the same public key pub K_B = (p, α, β) results in two different ciphertext y_1 and y_2 (with high probability) (because you sharp exhaust large y_1)
 - Masking key k_M is chosen at random for every new message
 - Brute force against x is avoided a priori

Mar-25

The ElGamal Cryptosystem

10

Performance issues



- Communication issues
 - Cyphertext expansion factor is 2
 - The bit size of (y, kE) is twice as the bit size of x (Size of (K) \$ Size of (KE)
- Computational issues
 - Key Generation
 - · Generation of large prime p (at least 1024 bits)
 - privK is generated by a RBG \Rightarrow (d vs provate heg)
 - 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 afficient than encryption

Mar-25

The ElGamal Cryptosystem

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, $a^{p-1} \equiv 1 \mod p$
 - Merge the two steps of decryption
 - $k_M^{-1} \equiv (k_E^d)^{-1} \equiv (k_E^d)^{-1} k_E^{p-1} \equiv k_E^{p-d-1} \mod p$



Mar-25

The ElGamal Cryptosystem

13

13

ElGamal Cryptosystem

SECURITY ISSUES

Mar-25

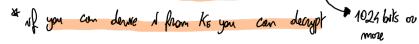
The ElGamal Cryptosystem

14

Security against passive attacks



- 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 $y = x \cdot \beta^i \mod p$
- 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 Am DH.
 - The Index-calculus method can be applied → |p| = 1024+



Mar-25

The ElGamal Cryptosystem

15

15

Security against active attacks



- Active attacks
 - Bob's public key must be authentic: authorizing of Public key (HITM)
 - Secret exponent i must be not reused (→)
 - ElGamal is malleable (→)

(Homomorphic)

Mar-25

The ElGamal Cryptosystem

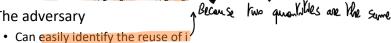
16

Security against active attacks



- 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 (y₁, k_E) and (y₂, k_E)

The adversary



• If (s)he can guess/know x₁, then (s)he can compute $x_2 \equiv y_2 \cdot k_M^{-1} \mod p$ with $k_M \equiv y_1 \cdot x_1^{-1} \mod p$

Mar-25

The ElGamal Cryptosystem

17

Security against active attacks



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

Mar-25

The ElGamal Cryptosystem

