

Discrete Logarithm

HONGBO KANG, CSD THU

Additional Key Words and Phrases: Discrete Log, ElGamal, IND-CPA, DDH

ACM Reference Format:

Hongbo Kang. 2021. Discrete Logarithm. *Proc. ACM Meas. Anal. Comput. Syst.* 37, 4, Article 111 (August 2021), 1 page. <https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>

1 THE SECURITY OF ELGAMAL

在本章节中，我们分析 ElGamal 公钥加密算法的 IND-CPA 安全性，并说明直接在模 P 循环群上使用 ElGamal 公钥加密算法将导致不安全。最后我们将提出一种方式使得 ElGamal 公钥加密算法满足 IND-CPA 安全性。

1.1 IND-CPA 安全性

除了“直接获得明文”或者“直接获得密钥”的攻击之外，一种更弱的攻击是，虽然攻击者不能直接获得明文或密钥，但能获得一些关于他们的信息，从而可以通过某些统计学方法破译明文。

IND-CPA 是一种对加密算法安全性的描述，满足 IND-CPA 要求的加密算法应该在攻击者选择明文的基础上，产生攻击者无法获得信息的密文。其测试方法包括一个“攻击者”和一个“挑战者”，攻击者将给出两个明文，并从挑战者算出的密文中判断其产生自哪个明文。具体流程如下

- (1) 挑战者基于某些秘密参数 k 生成公私钥 (P_k, S_k) ，并将公钥 P_k 发给攻击者
- (2) 攻击者进行多项式级别的计算
- (3) 攻击者向挑战者发送 M_0, M_1 两条明文
- (4) 挑战者等概率随机选择两条明文中的一条，记作 M_b ，将加密后的串 $C_b = E(P_k, M_b)$ 发回给攻击者。
- (5) 攻击者进行任意多次计算，并给出对 b 的猜测

因为挑战者收到了密文 M_b ，与随机猜测 b 相比，他将获得一些优势。记其猜对的概率为 $\frac{1}{2} + \epsilon(k)$ ，若 $\epsilon(k)$ 并非是一个可以忽略的小量，则该算法不是 IND-CPA 安全的。

1.2 DDH 问题

1.3 ElGamal 公钥加密算法的 IND-CPA 攻击

1.4 改进的 ElGamal 公钥加密算法

Author's address: Hongbo Kang, khb20@mails.tsinghua.edu.cn, CSD THU.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2021 Association for Computing Machinery.

2476-1249/2021/8-ART111 \$15.00

<https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>