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), 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 THE SECURITY OF ELGAMAL

在本章节中，我们首先介绍 IND-CPA 安全性，之后给出 ElGamal 的 IND-CPA 安全性的等价问题，并说明直接在模 P 循环群上使用 ElGamal 公钥加密算法将导致 IND-CPA 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

在 ElGamal 的 IND-CPA 证明中，攻击者可以获得的信息包括：$\{P_k, P_r, M_0, M_1, C_b\}$，其中 $P_k = \alpha^k$ 是公钥，$P_r = \alpha^r$ 是加密使用的随机幂。要判断 C_b 来自哪个明文，攻击者可以对两个密文分别计算 $M_x^{-1} C_b$ ，并判断其是否等于 α^{rk}，若等于则 $b = x$。我们将这个判断问题简化为下述 DDH 问题：

Theorem 1.1. 给定循环群 G 及其生成元 α。给出 $\alpha, \alpha^a, \alpha^b, \alpha^c$，其中 a, b 从 Z_t 中独立随机选择，c 通过下面两种方式产生：$c = ab$ 或从 Z_t 中随机选择。判断 c 是通过哪种方式产生的。

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/nnnnnnn.nnnnnnn

不难发现，如果我们可以以一定的概率估计 α^c 是否等于 α^{ab}，我们就能对 ElGamal 的 IND-CPA 安全性进行攻击。

1.3 模 P 循环群上 ElGamal 公钥加密算法的 IND-CPA 攻击

对模 P 循环群及其生成元 α，有下列引理存在：

Lemma 1.2. $(\alpha^i)^{(P-1)/2} \equiv \pm 1(modP)$

Proof. $((\alpha^i)^{(P-1)/2})^2 = (\alpha^{P-1})^i \equiv 1(modP)$。而 $X^2 \equiv 1(modP)$ 对质数 P 只有两个解，则他们是 ± 1。 □

由于上述引理存在，在判断 $\alpha^c = \alpha^{ab}$ 是否成立时，我们可以通过分别计算 $(\alpha^a)^{(P-1)/2}$, $(\alpha^b)^{(P-1)/2}$, $(\alpha^c)^{(P-1)/2}$ 获得 a, b, c 的奇偶性，从而对结果有所估计。

除了 $(P-1)/2$ 可以用于进行域的收缩外，对任意 $K \geq 2$，$(P-1)/k$ 均可以用于进行数域的收缩。

1.4 改进的 ElGamal 公钥加密算法

我们发现，上述对 ElGamal 公钥加密算法的安全性攻击基于 $(P-1)$ 的小质因子成立。首先我们可以尽量避免 $(P-1)$ 的小质因子：选择质数 q，另 $P = 2q+1$ 且也是质数，这样 $(P-1)$ 就只会有 $2, P$ 两个质因子。

我们接着解决质因子 2 带来的问题。值得注意的是，如果我们要求公钥 $P_k = \alpha^k$ 和随机幂 $P_r = \alpha^r$ 中的 k 和 r 均是偶数，上一章节中提到的 $(P-1)/2$ 幂次攻击将永远得到 c, ab 奇偶性相同的结论，从而无法进行攻击。这一防范方法的等价做法为：令 $\alpha' = \alpha^2$，则 α' 将生成子群 $\{\alpha^{2\cdot 1}, \alpha^{2\cdot 2}, ..., \alpha^{2\cdot q}$，我们可以基于这个循环子群进行加密：

(1) 选择大质数 q，使得 $P = 2q+1$ 也是质数
(2) 寻找大质数 P 的生成元 α，令 $\alpha' = \alpha^2$
(3) 在 Z_q 中选取私钥 $S_k = k$，公钥为 $\{P, \alpha', P_k = (\alpha')^k\}$