



现代密码学

第四十一讲 椭圆曲线密码学

信息与软件工程学院



椭圆曲线密码学



为了使用椭圆曲线来构造密码体制, 需要找到类似大整数因子分解或离散对数这样的困难问题。

定义1 椭圆曲线 $E_p(a, b)$ 上点 P 的阶是指满足

$$nP = \underbrace{P + P + \dots + P}_n = O$$

的最小正整数, 记为 $ord(P)$, 其中 O 是无穷远点。



椭圆曲线密码学



定义2 设 G 是椭圆曲线 $E_p(a, b)$ 上的一个循环子群, P 是 G 的一个生成元, $Q \in G$ 。已知 P 和 Q , 求满足

$$mP = Q$$

的整数 $m, 0 \leq m \leq \text{ord}(P) - 1$, 称为椭圆曲线上的离散对数问题 (elliptic curve discrete logarithm problem, ECDLP)。计算 mP 的过程称为点乘运算(Point multi-plication)。

椭圆曲线密码学

在使用一个椭圆曲线密码体制时,首先需要将发送的明文 m 编码为椭圆曲线上的点 $P_m = (x_m, y_m)$,然后再对点 P_m 做加密变换,在解密后还得将 P_m 逆向译码才能获得明文。下面对椭圆曲线上的 **ElGamal** 密码体制做一介绍。

1) 密钥生成(KeyGen)

在椭圆曲线 $E_p(a, b)$ 上选取一个阶为 n (n 为一个大素数) 的生成元 P 。随机选取整数 x ($1 < x < n$), 计算 $Q = xP$ 。公钥为 Q , 私钥为 x 。

2) 加密(Encrypt)

为了加密 P_m , 随机选取一个整数 k , $1 < k < n$, 计算

$$C_1 = kP, C_2 = P_m + kQ$$

则密文 $c = (C_1, C_2)$ 。



3) 解密(Decrypt)

为了解密一个密文 $c = (C_1, C_2)$, 计算

$$C_2 - xC_1 = P_m + kQ - xkP = P_m + kxP - xkP = P_m$$

攻击者要想从 $c = (C_1, C_2)$ 计算出 P_m , 就必须知道 k 。而要从 P 和 kP 中计算出 k 将面临求解椭圆曲线上的离散对数问题。



感谢聆听!

xionghu.uestc@gmail.com
