BabyPRNG writeup

本题主要考查椭圆曲线幂乘发生器（Elliptic Curve Power Generator，ECPG）[1] 的截断比特序列预测问题。

题目描述

首先选取了一个素域$\mathbb{F}_p$上的常规椭圆曲线

$$E_{\mathbb{F}_p} : y^2 = x^3 + ax + b\ ,$$

其中a, b为未知的秘密参数。

接着，随机选取曲线上的一点$G \in E_{\mathbb{F}_p}$，每个随机数r按照如下流程生成：

$$\begin{gathered} G \leftarrow 1337 \cdot G \\ r_i \leftarrow G.x >> 32 \\ r_{i+1} \leftarrow G.y >> 32 \end{gathered}$$

本题中上述步骤共进行了三次，即提供该发生器输出的连续6个随机数$r_0, r_1, \ldots, r_5$。同时，给出了 `flag` 类RSA加密后的结果$c = (a^{3371} * \mathtt{flag} + b^{3713})^{1337} \mod p$以及1024比特的素数$p$。

解题思路

显然，要想求解 `flag` ，恢复出a, b即可。通过一番搜索，可以找到一篇基于Coppersmith方法对ECPG攻击的论文 [2] ，该文章的第5节中给出了攻击，但该攻击适用于a, b已知的情况，这并非本题的场景。事实上，该文章第4节给出了在a, b未知情况下，针对另一类随机数发生器ECLCG的攻击，但此攻击同样适用于本题中的ECPG发生器： 不妨假设迭代三次时对应的椭圆曲线点分别为$G_0 = (x_0, y_0), G_1 = (x_1, y_1), G_2 = (x_2, y_2)$，则有下列式子成立：

$$\begin{aligned} y_0^2 &= x_0^3 + ax_0 + b \\ y_1^2 &= x_1^3 + ax_1 + b \\ y_2^2 &= x_2^3 + ax_2 + b \end{aligned}$$

虽然a, b未知，但恰好可以将他们消去，最后得到一个关于$x_0, x_1, x_2, y_0, y_1, y_2$的六元四次等式

$$f = (y_0^2 - y_2^2 - (x_0^3 - x_2^3)) * (x_0 - x_1) - (y_0^2 - y_1^2 - (x_0^3 - x_1^3)) * (x_0 - x_2)$$

而本题中给出了这六个变量的大部分比特，仅低位32比特被舍弃，因此我们可以将它们写成形如$x_0 = x_0^* + x_0'$的形式，其中x_0^*表示题目给出的部分，而x_0'表示未知的部分。如此一来，f可以看作关于$x_0', x_1', x_2', y_0', y_1', y_2'$的方程，且注意到这六个变量的取值都非常小，不超过$2^{32}$。而论文 [2] 使用Coppersmith方法来求解此方程，但实际复杂度非常高，在笔记本电脑上无法完成。故本题需要选手对攻击的原理有一定理解，从而进行优化。

实际上，一个更简单的方法是直接使用LLL归约算法，为了便于理解，下面通过一个简单的例子进行描述。考虑多项式$h = Ax^2y + Bxy + Cy + Dx + E \in \mathbb{F}_p[x, y]$，现在我们想找出$f$的一组小值根$(x', y')$，其中满足$x' < U, y' < U$，而$S$是一个远大于$p$的数 。考虑构造下面的格：

$$\mathbf{L} = \begin{bmatrix} S*p & & & & & \\ S*A & 1 & & & & \\ S*B & & U & & & \\ S*C & & & U^2 & & \\ S*D & & & & U^2 & \\ S*E & & & & & U^3 \end{bmatrix}$$

显然，该格中包含了向量$\mathbf{v} = (0, x'^2y', Ux'y', U^2y', U^2x', U^3)$，即存在某个向量$\mathbf{u}$满足$\mathbf{uL} = \mathbf{v}$。而$\mathbf{v}$中每个分量都非常小，意味着可以通过格归约的方法将$\mathbf{v}$找出，进而恢复出$(x', y')$。

回到本题，即构造一个对应于f的格，然后通过格归约算法即可还原出$x_0', x_1', x_2', y_0', y_1', y_2'$，进而算出$a, b$解密 `flag` 。题目中截断了32比特，LLL算法可能无法求解，故可以考虑对每个变量枚举2比特，一共是2^{12}种可能。

参考文献

[1] Lange T, Shparlinski I E. Certain exponential sums and random walks on elliptic curves[J]. Canadian Journal of Mathematics, 2005, 57(2): 338-350.

[2] Mefenza T, Vergnaud D. Inferring sequences produced by elliptic curve generators using Coppersmith's methods[J]. Theoretical Computer Science, 2020, 830: 20-42.