小秘密

范浩强

IIIS, Tsinghua

阿米巴是谁?

得分分布

- 集训队中，得分的有9人，最高20分。
- 非集训队中，最高60分（杜瑜皓）。

题目描述

- $x=K_1$
- for i in InputData:
- 　o=w(f(x) and K_2) xor i
- 　output o
- 　x=2x+o
- 给1MB=8Mbit的输出，求K_2
- 10%数据$K_2<2^5$；10%数据b=0.5
  60%数据$K_2<2^{50}$；其他数据$K_2<2^{60}$
- $b\geq 0.12$

0.5-b的概率1，0.5+b的概率0的随机分布

问题的本质

- 解带噪声的线性方程组
- $Ax=b+\varepsilon$

碰撞攻击

- 两两配对
- $a_1^T x = b_1$

  $a_2^T x = b_2$

  $(a_1+a_2)^T x = b_1+b_2$
- 使得a_1+a_2末尾有很多的零。
- 建立一个从末尾映射到等式的查找表。

之后

- 进行一轮碰撞，我们可以得到限制在40个变量上的7M组等式。噪声从0.38扩大到0.4712。

然后

- 进行两轮碰撞，变量个数减少到20，b缩小到0.00166.
- 暴力枚举这20个变量的值
- 轮换变量的次序，求解另外40个。

枚举

- 使用高维FFT
- $B(x) = \sum_{y \in \{0,1\}^n} \prod_{i=0}^{n-1} (-1)^{x_i \cdot y_i} A(y)$

谢谢！