关于 SPRING 算法中 SubRow 运算差分性质的进一步说明

田甜　戚文峰　叶晨东　谢晓锋

1. SubRow 运算的最大差分概率

在 SPRING 算法中，SubRow 运算是$\mathbf{F}_2^{32}$到$\mathbf{F}_2^{32}$的一个非线性置换，由非线性反馈移位寄存器 NFSR-SR 实现。我们利用太湖之光超级计算机穷尽了 SubRow 运算的差分分布表，得到 **SubRow 运算的最大差分概率等于**$\frac{152}{2^{32}} \approx 2^{-24.75}$，即

$$\max_{\alpha,\beta\in\mathbf{F}_2^{32},(\alpha,\beta)\neq(0,0)} \#\{x \in \mathbf{F}_2^{32}: \mathrm{SubRow}(x\oplus\alpha)\oplus\mathrm{SubRow}(x) = \beta\} = 152,$$

并且有且仅有一对差分(α,β)取到上述最大值，即

$$\alpha = 0\mathrm{x}07060106,\ \beta = 0\mathrm{x}509000\mathrm{f}4,$$

其中从高位到低位依次为寄存器

$$(\mathrm{A}_7,\mathrm{A}_6,\ldots,\mathrm{A}_0,\mathrm{B}_7,\mathrm{B}_6,\ldots,\mathrm{B}_0,\mathrm{C}_7,\mathrm{C}_6,\ldots,\mathrm{C}_0,\mathrm{D}_7,\mathrm{D}_6,\ldots,\mathrm{D}_0)$$

的差分。

2. SPRING 算法有效差分特征轮数的估计

根据我们得到的 SubRow 运算最大差分概率等于$2^{-24.75}$以及 SPRING 算法r轮最小活跃 S 盒个数等于r，128 比特分组长度的 SPRING 算法不存在大于 5 轮的有效差分特征；256 比特分组长度的 SPRING 算法不存在大于 10 轮的有效差分特征。