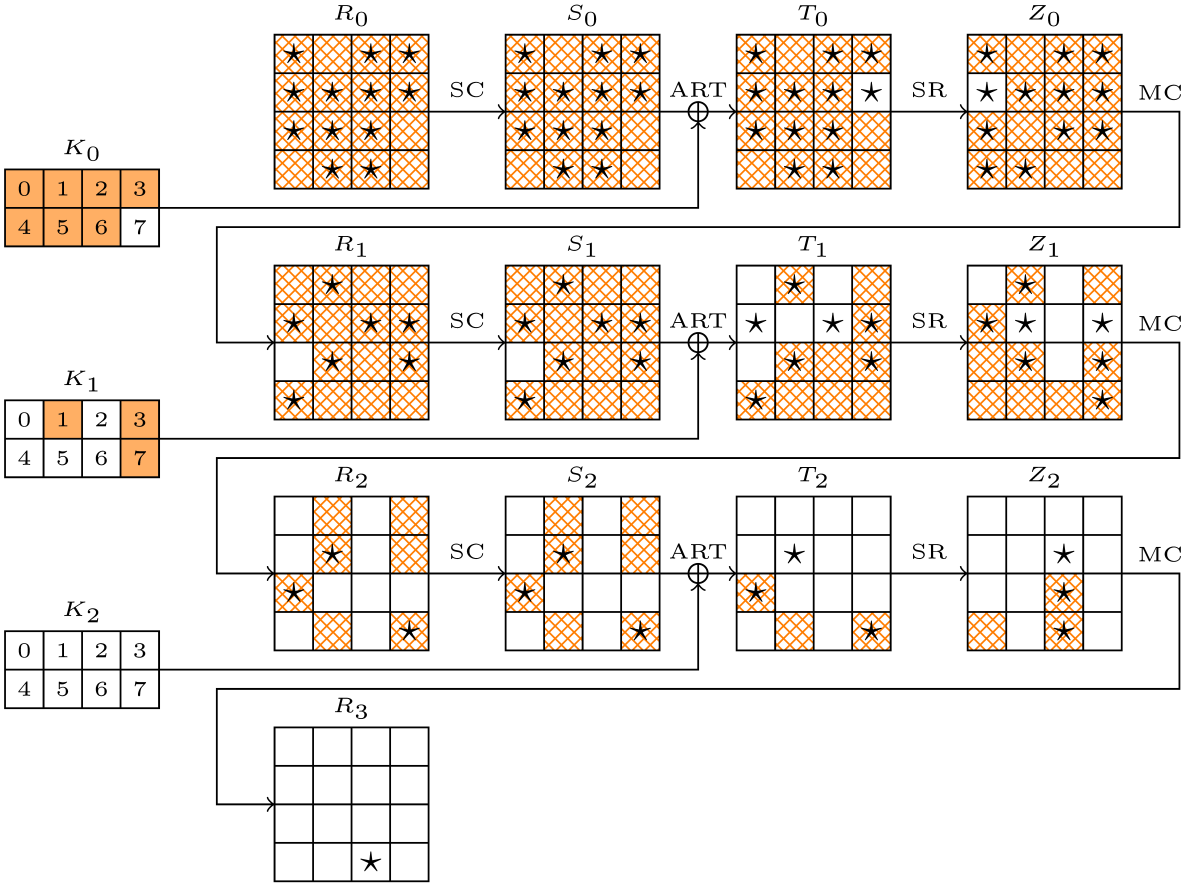
# DS-MITM攻击SKINNY的Online Phase：$k_{in}$的确定




如图，我们在$R_3[14]$建立一个$\delta$-set。我们想要确定$k_{in}$。

假设我们已经知道$k_{in}$就是$K_{0,1,2}$中橙色的部分，我们说明为什么这样可以确定$P$的Multiset——$\{P\}$。

常规的DS-MITM从一个随机的$P$出发，计算到$R_3$再回推得到$\{P\}$。

首先，state中橙色的crosshatch表示我们能计算出value的位置。

注意到我们无法计算出$R_3[14]$的value，但这没有关系，我们使用multiset而不是sequence来减少$k_{in}$。

假设$Z_2[6]=a, Z_2[10]=b, Z_2[14]=c$，那么固定剩余字节，
$Z_2[6]=a+x, Z_2[10]=b+x, Z_2[14]=c+x$，这里$x$取遍$0,1,\dots,256$将在$R_3$形成一个我们想要的multiset。所以不需要猜测任何$K_2$中的字节来计算$R_3$的value。

现在问题变成如何得到一个这样的$\{Z_2\}$。

我们观察$S_2$，在$S_2$中，三个有差分的位置的value我们都能计算，同样的，假设
$S_2[5]=a, S_2[8]=b, S_3[15]=c$，固定其他字节，
$S_2[5]=a+x, S_2[8]=b+x, S_2[15]=c+x$，这里$x$取遍$0,1,\dots,256$，会在$Z_2$得到我们想要的multiset。

注意这里$\{S_2\}$是可以继续推导到$\{R_2\}$的，因为我们同时知道value和差分。

**所以密钥恢复的第一步：随机选择一个$P$，猜测橙色部分的$k_{in}$，计算得到$S_2$，然后在三个有差分的字节处遍历相同的差分$x$，然后往回推导。**

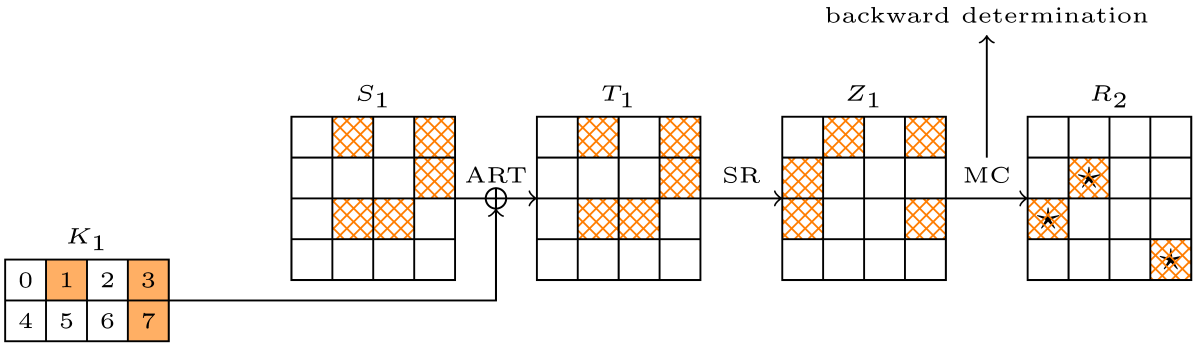
由于$S_2$往回算到$S_1$是完全线性的，所以$S_1$的所有差分我们都能算出来。注意到在有差分的位置，我们也知道value，那么继续算到$R_1$。

同理，得到$S_0$的所有差分，结合$S_0$的value，得到$\{P\}$。

我们发现，问题的关键在于状态$S_{0,1,2}$，我们需要在所有$S_{0,1,2}$差分不为零的位置知道value。

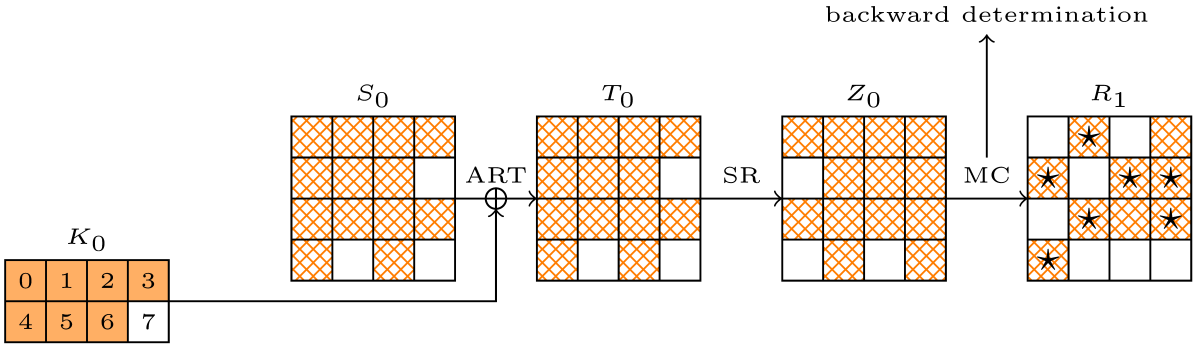
所以我们首先对$R_3[14]$求backward differential到$R_0$。（星号所在位置）

为了确定$S_2[\star]$的value，我们求backward determination，并求$SR^{-1}$得到：




若我们在$S_1$处橙色crosshatch的字节已知，且猜测$K_1$的橙色部分，则$S_1[\star]$的value可以计算。

我们下一步是要确定$S_1$处橙色crosshatch的字节和有差分的字节$S_1[\star]$（求并集）。




注意$R_1$处橙色crosshatch的部分是求并集后的结果。同样的方法我们就确定了$K_0$。

以上就是Online Phase中确定$k_{in}$的方法。