

## 17-round differential Distinguisher of probability 2^-45.49 $R24 \ \, \tiny{ 0\ \,$ **3** <<< 8 $R25 \ \ \, {\scriptstyle 1\ \, 0$ 0</t -0 0 0 0 0 0 ? 0 0 0 0 ? ? 0 0 ? 0 1 ? ? 0 0 ? L27 <<< 1 (h) **<<<** 2 L28 ? ? ? 1 ? ? 0 1 0 0 0 ? ? 0 0 ? 0 ? ? 0 <<< 1 **<<<** 2 0 ? ? 0 0 ? 0 ? ? ? 0 ? ? 1 ? ? ? 1 ? 7 0 1 : This key bit is guessed by the upper part of the attack ■ : This state bit can be computed by the upper part of the attack : This state bit is guessed by the upper part of the attack : This key bit is guessed by the lower part of the attack ■ : This state bit can be computed by the lower part of the attack : This state bit is guessed by the lower part of the attack ①: The difference on this bit is 0 1: The difference on this bit is 1 ?: The difference on this bit can be 0 or 1 P: The difference on this bit is considered 0 by probabilist propagation ■ : This bit takes all possible values : The value of this bit is fix for a specific structure