Generic DPA attacks: curse or blessing?

KU LEUVEN

Oscar Reparaz, Benedikt Gierlichs, Ingrid Verbauwhede

COSIC/KU Leuven

COSADE 2014, Paris

Original MIA

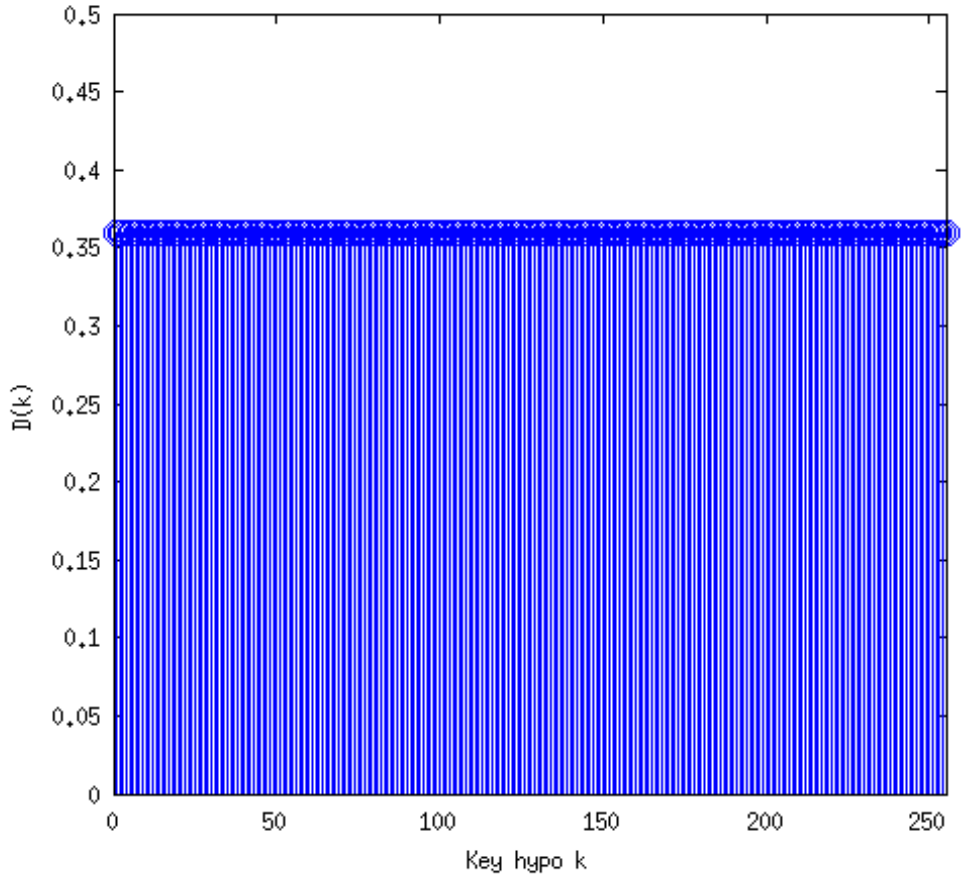
- Consider an sbox output $\mathbf{Z} = S(\mathbf{P} \oplus k)$
- In a typical DPA attack, we compare measurements vs. predictions

$$\mathbf{O} = \mathbf{L}_{\text{device}}(\mathbf{Z}) \qquad \mathbf{H} = \mathbf{L}_{\text{model}}(\mathbf{Z})$$

$$I(\mathbf{O};\mathbf{H})$$

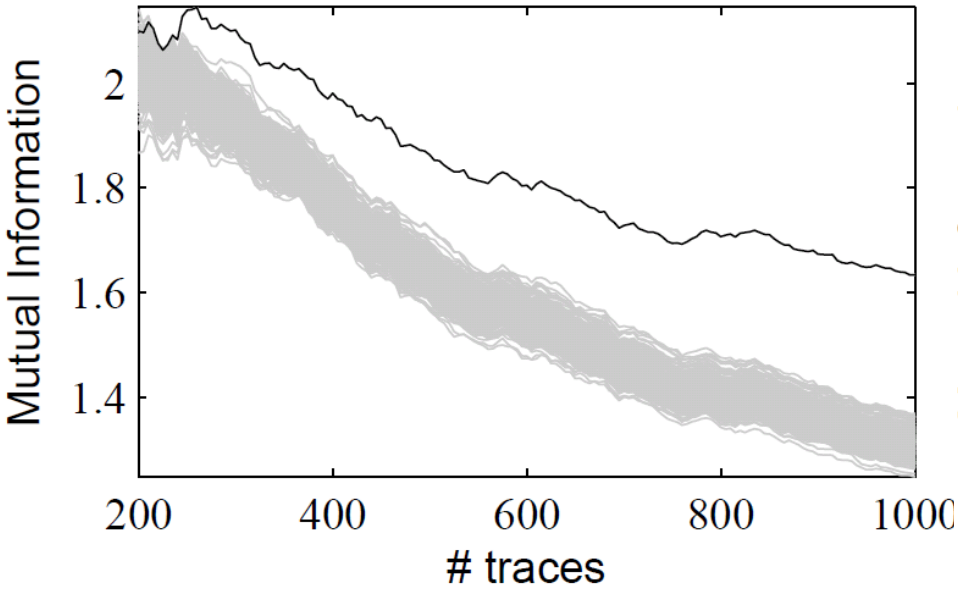
- Nice point of generic DPA attacks: we can skip the modeling: $\mathbf{H} = \mathrm{Id}(\mathbf{Z})$

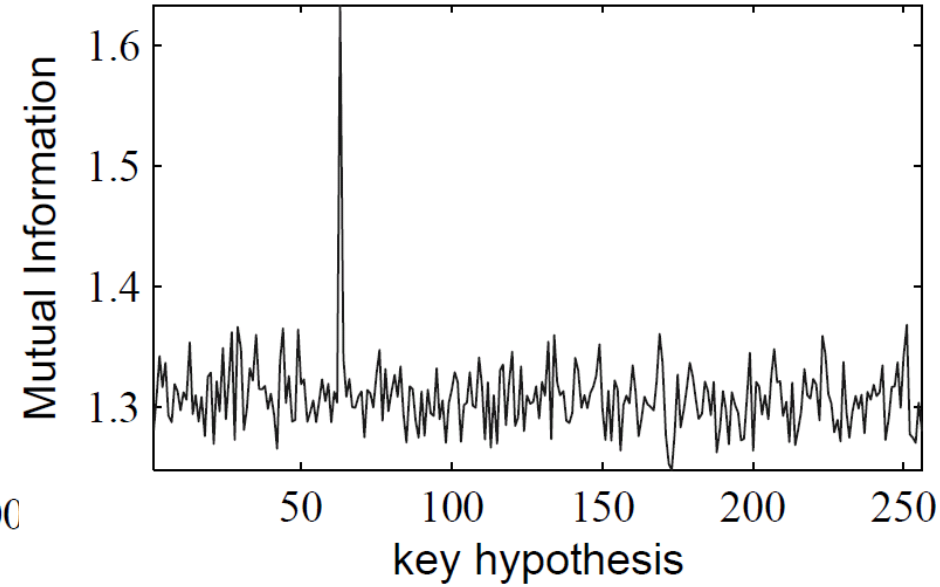
Injective targets with model skipped $\mathbf{H} = \mathrm{Id}(\mathbf{Z})$ AES Key addiiton, AES Sbox output



Disappointment: cannot distinguish the correct key hypothesis!

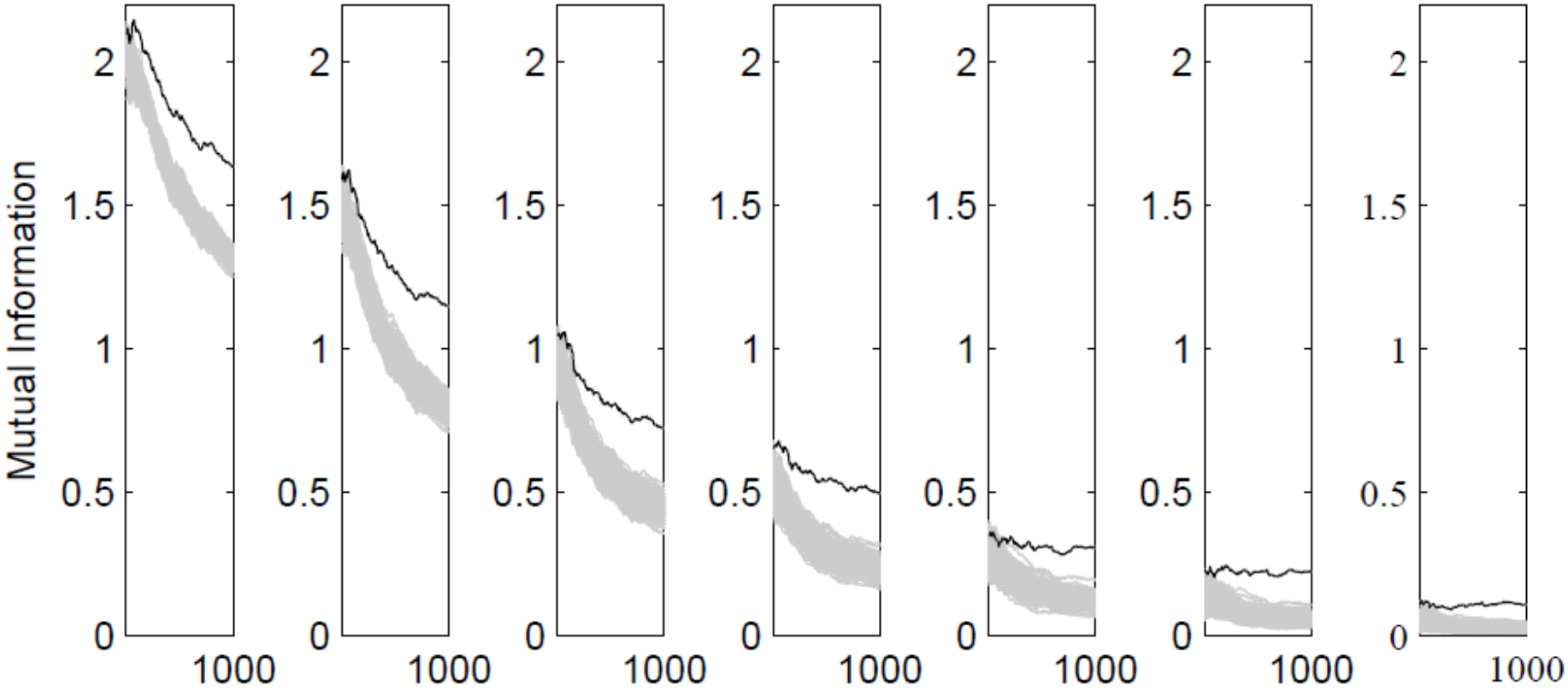
First solution: drop a bit on predictions





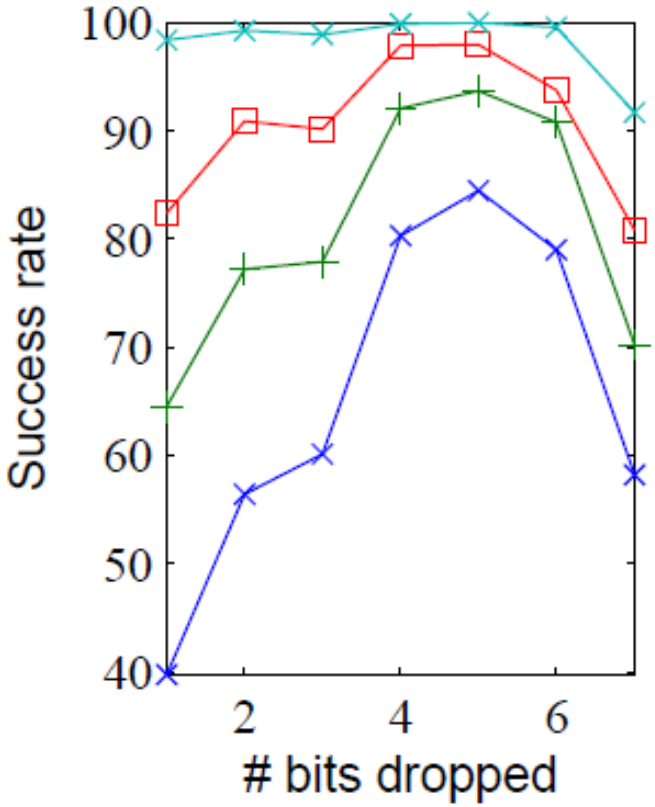
- Break the injectivity by dropping one bit on the predictions $\mathbf{H} = \mathrm{drop}_1(\mathbf{Z})$
- Experiments on 8-bit uC

Dropping 1, 2,…, 7 bits



x-axes: No. of traces

How many bits to drop?

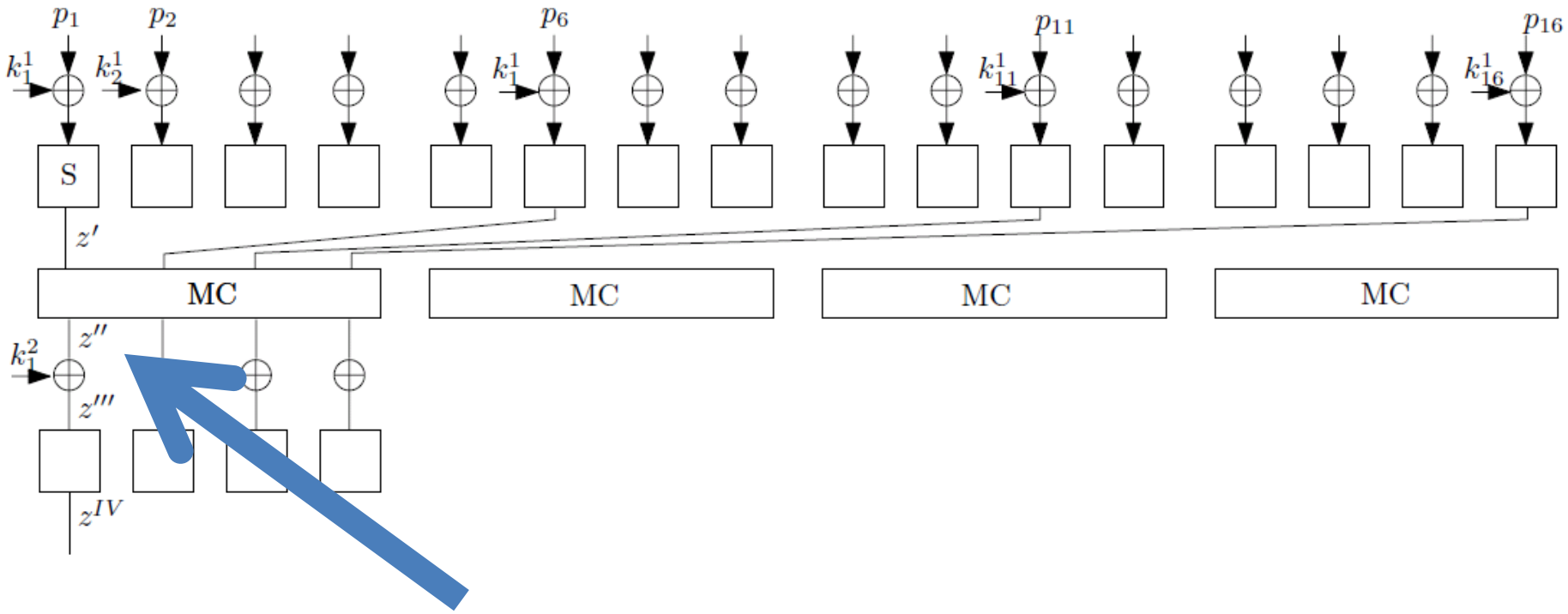


For details, see the paper. Each line on the left Indicates a fixed budget for number of traces.

We can see that dropping 5 bits consistently leads to best success rate, for any given (fixed) number of traces.

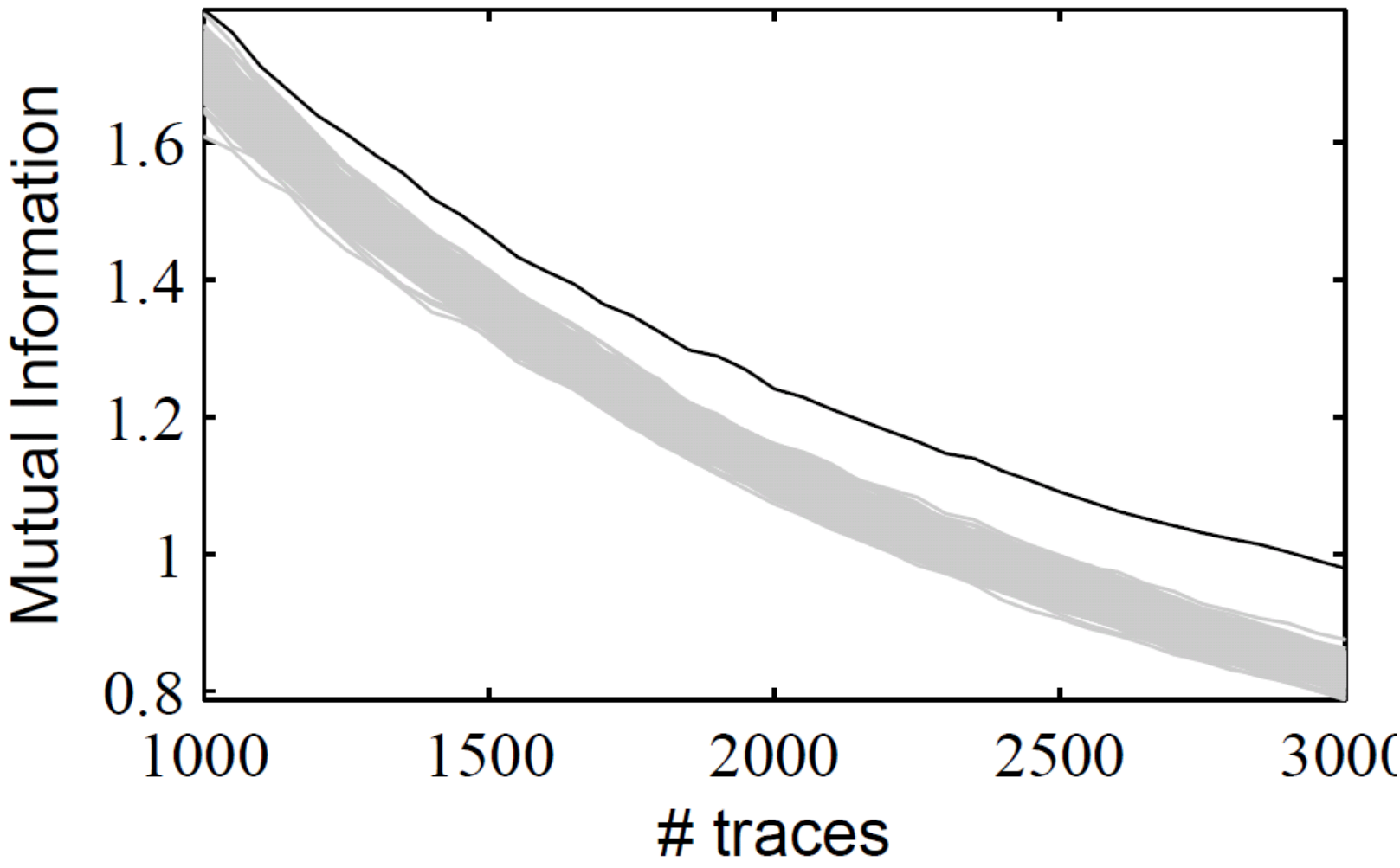
- Messerges said that predicing 3 out of 8 bits gave the best tradeoff between information and throwing away traces
- (we assume all bits leak similarly)

Second way: find non-injective targets

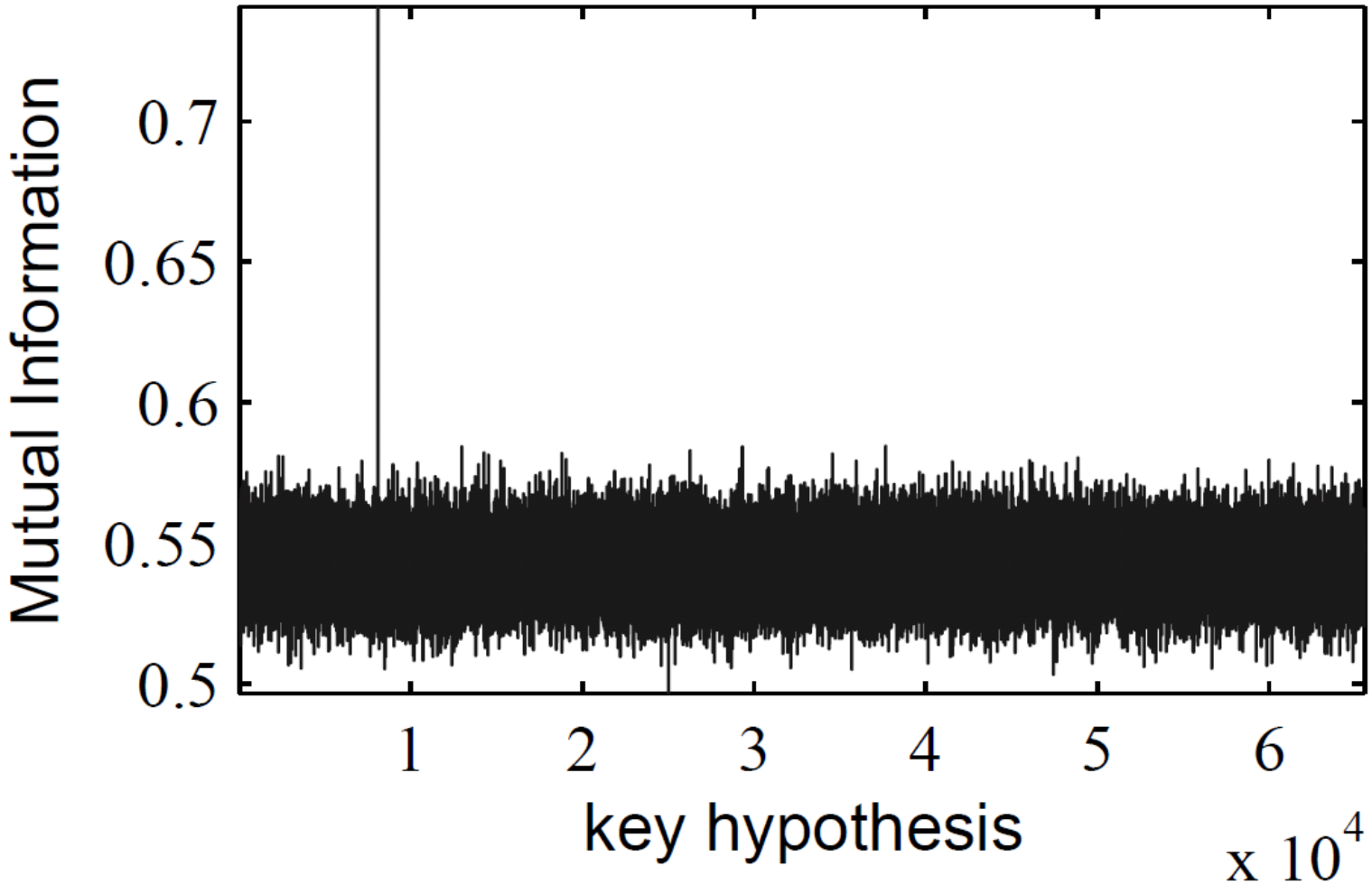


- The attacker has plenty of options to target

Attacking MixColumns in our device

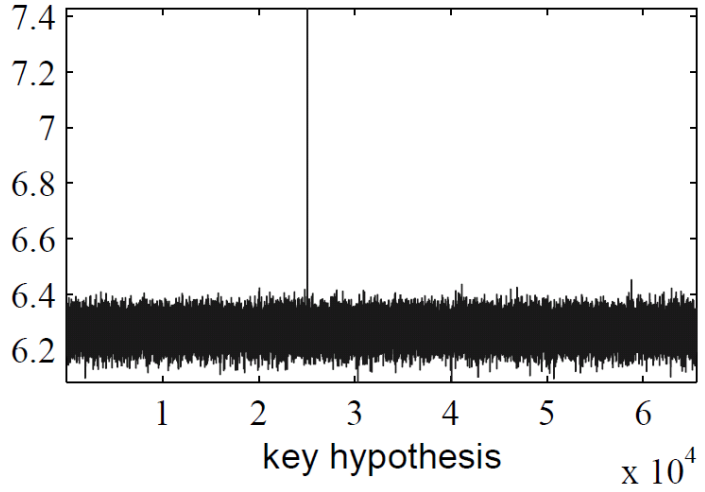


There are no equivalent keys

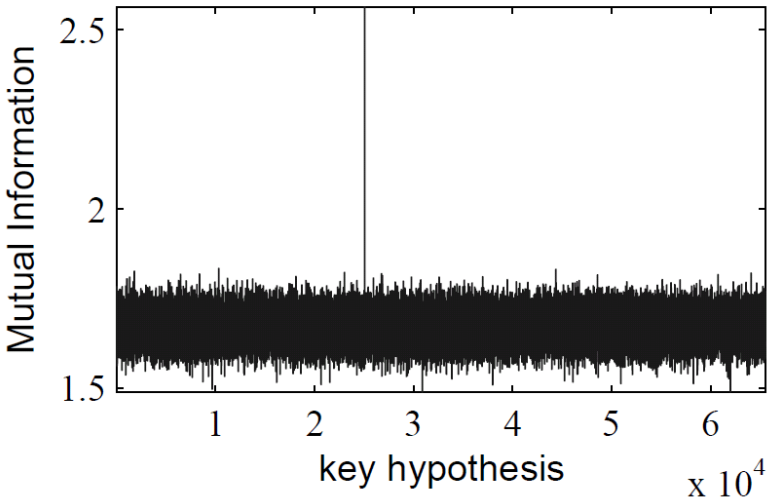


Arbitrary leakage functions

$\mathbf{L}_{\text{device}} = S_{\text{AES}}$



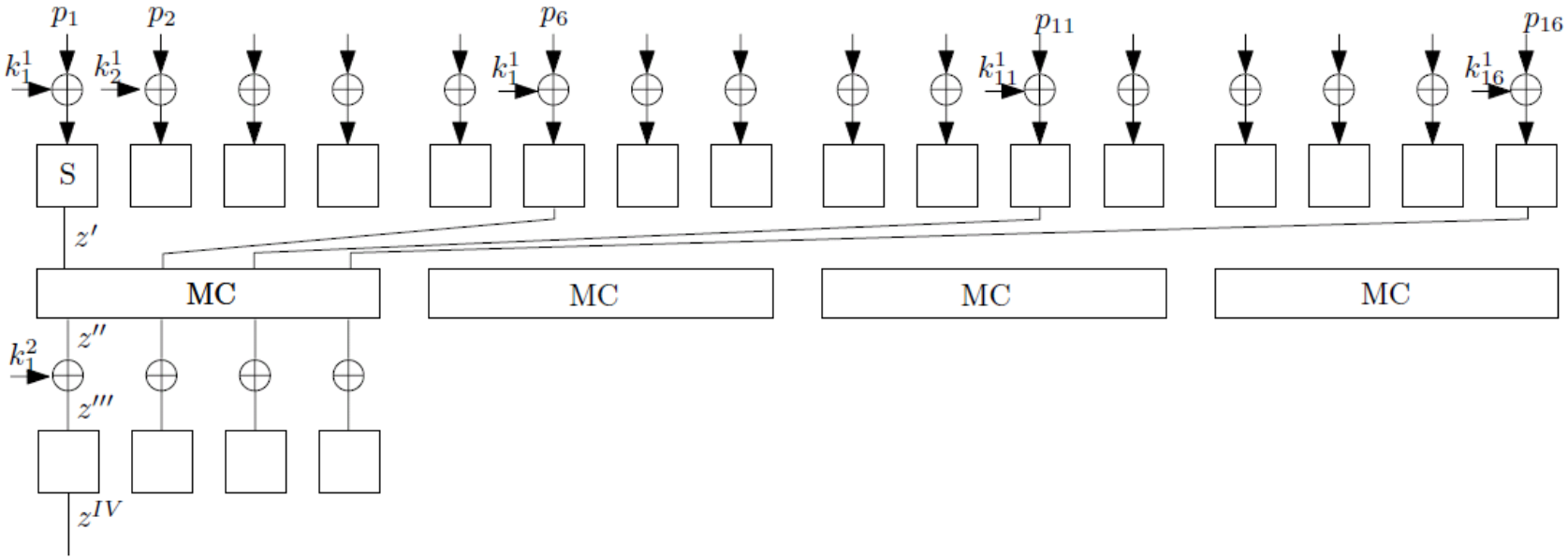
$\mathbf{L}_{\text{device}} = \mathrm{HW}(S_{\text{AES}})$



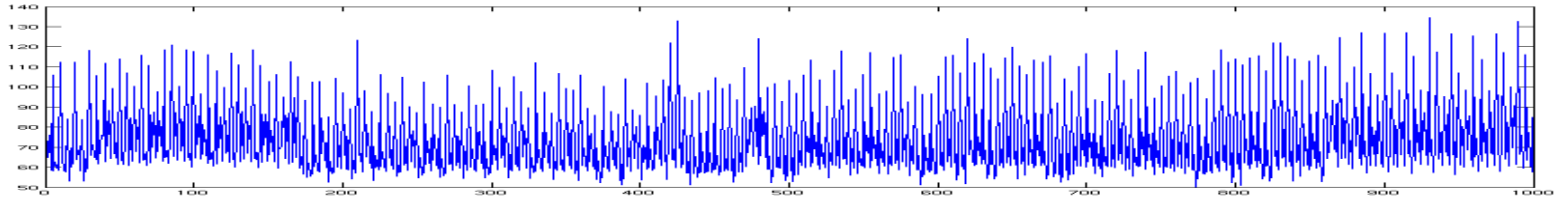
Bit-drop trick didn't work if L device is very nonlinear

On the other hand, attacking after MixColumns works even if we use a sophisticated bus scrambling mechanism

Leakage from further rounds



- If first round is masked --> exploit leakage z IV (second round) and get keys from first round



- Condition for the generic attack to succeed:

$$I(\mathbf{Z}; \mathbb{E}_{\mathbf{N}}[\mathbf{L}_{\text{device}}(\mathbf{Z}, \mathbf{N})]) > 0$$

Conclusions

- Generic attacks are endowed with two-sided properties – curse or blessing depending on the particular situation!
- More:

http://www.esat.kuleuven.be/~oreparaz/curseorblessing/