Some group theoretical aspects of block cipher security

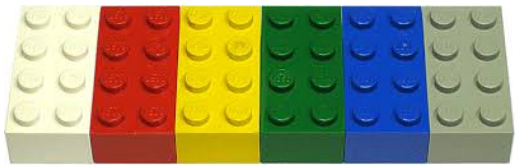
Roberto Civino

roberto.civino@univaq.it

∂cifris meets Rome
October 4, 2018

Block ciphers

Parameters



block size n

key size κ

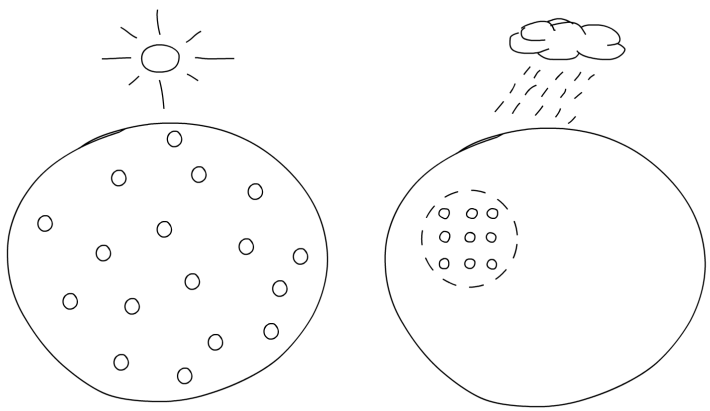
Spaces

- $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ the message space
- $\mathcal{K} \approx (\mathbb{F}_2)^\kappa$ the key space

An injective correspondence

$$\begin{array}{rccc} \Phi: & \mathcal{K} & \to & \mathrm{Sym}(V) \\ & K & \mapsto & \varphi_K \end{array}$$

The permutations induced by the 2^κ keys should look like being chosen uniformly from the set of all the permutations on V



representation of the cipher in $\mathrm{Sym}(V)$

Pick them at random?

$$2^{64} \times 2^{64} \text{ bit } \sim 2^{85} \text{ TB}$$

gotta find a more clever way

Shannon's principles

Idea

Iterate simple functions!

Two necessary properties to guarantee security against cryptanalysis:

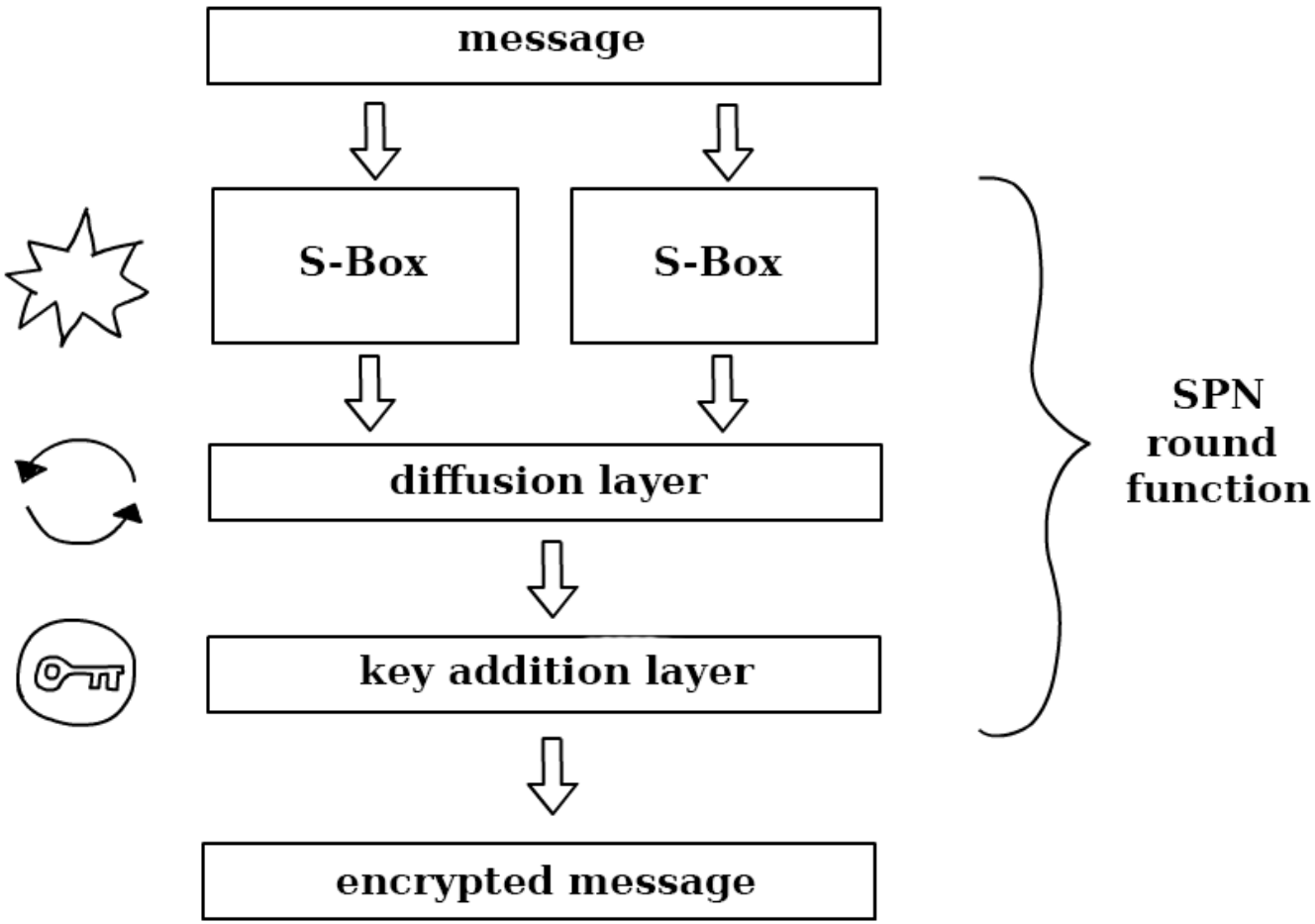
- confusion

  $$\texttt{123123123}_{\text{x}} \mapsto \texttt{f5bb0c8de146c67b44babbf4e6584cc0}_{\text{x}}$$

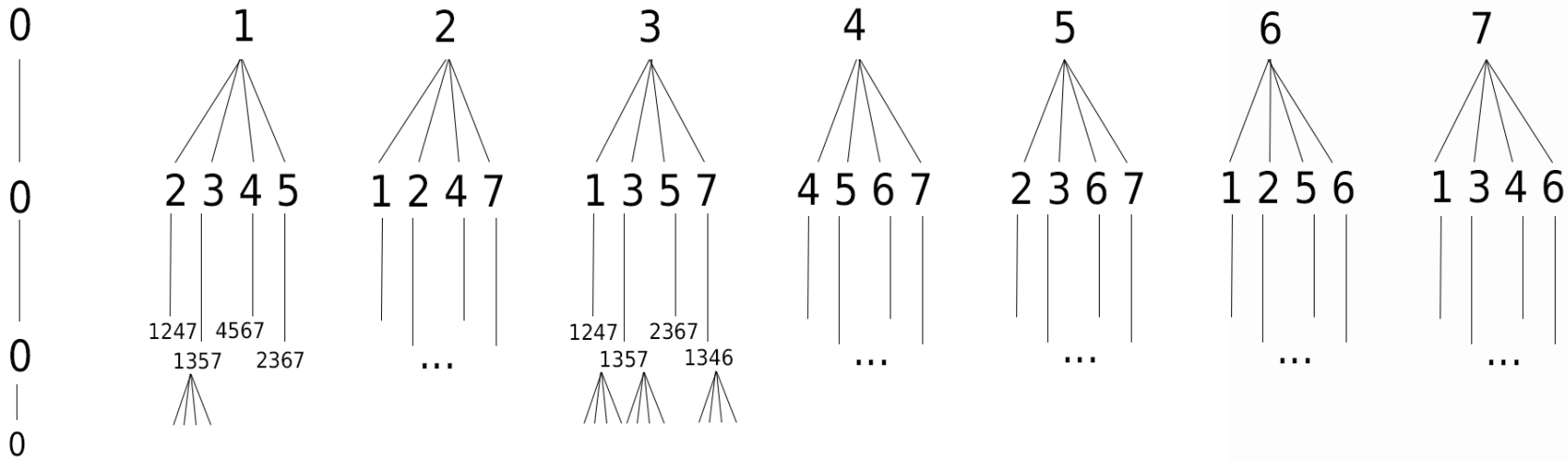
- diffusion

  $$\texttt{123113123}_{\text{x}} \mapsto \texttt{a335ab839b7164e878d9eae58a015ede}_{\text{x}}$$

Substitution-Permutation Networks



Non-linearity of a harmless 3-bit S-box



$\sim$ 7000000 leaves after 10 round, for a single and small S-Box

Another operation

If T_+ is the translation group on V, $T_+ \stackrel{\text{def}}{=} \{\sigma_b \mid b \in V, x \mapsto x + b\}$, then

$$a + b = \sigma_b(a)$$

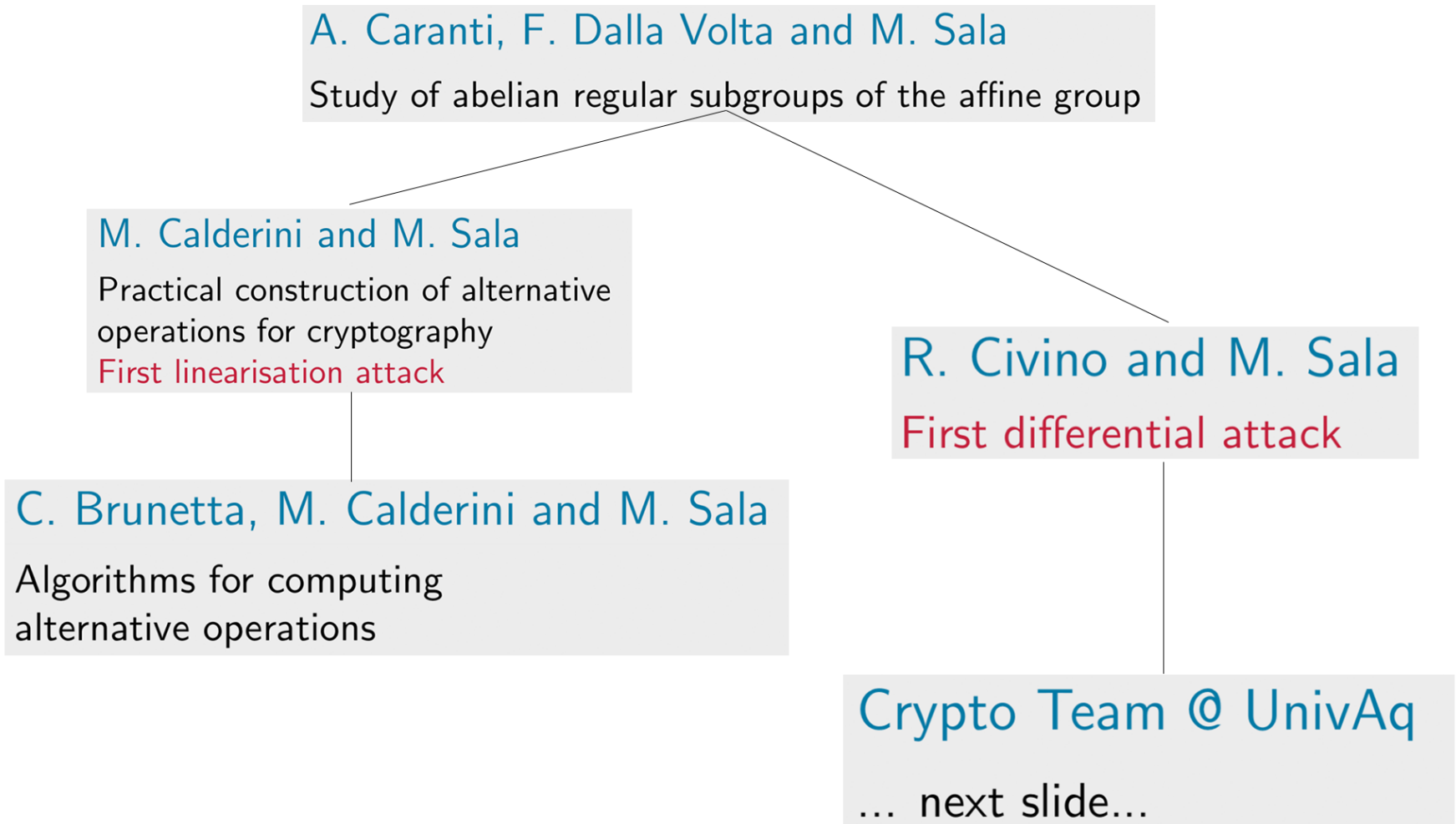
Analogously, if $T_\circ < \mathrm{Sym}(V)$ is a 2-elementary abelian regular group isomorphic to T,

$$T_\circ = \{\tau_b \mid b \in V\},$$

where τ_b is the unique element in T which maps 0 into b, then another operation is defined as

$$a \circ b \stackrel{\text{def}}{=} \tau_b(a)$$

People and things they've done



Crypto Team @ UnivAq...

... is R. Aragona, R. Civino, N. Gavioli and C. Scoppola

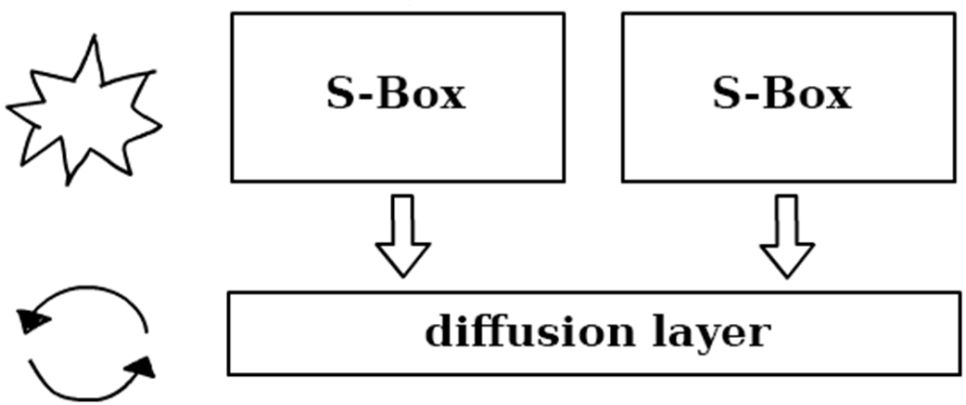
- properties of $T_\circ$ as a permutation group
- measuring non-linearity with respect to $T_\circ$

Crypto Team @ UnivAq...

... is R. Aragona, R. Civino, N. Gavioli and C. Scoppola

- properties of $T_\circ$ as a permutation group
- measuring non-linearity with respect to $T_\circ$
- the BIG alternative-operation problem:

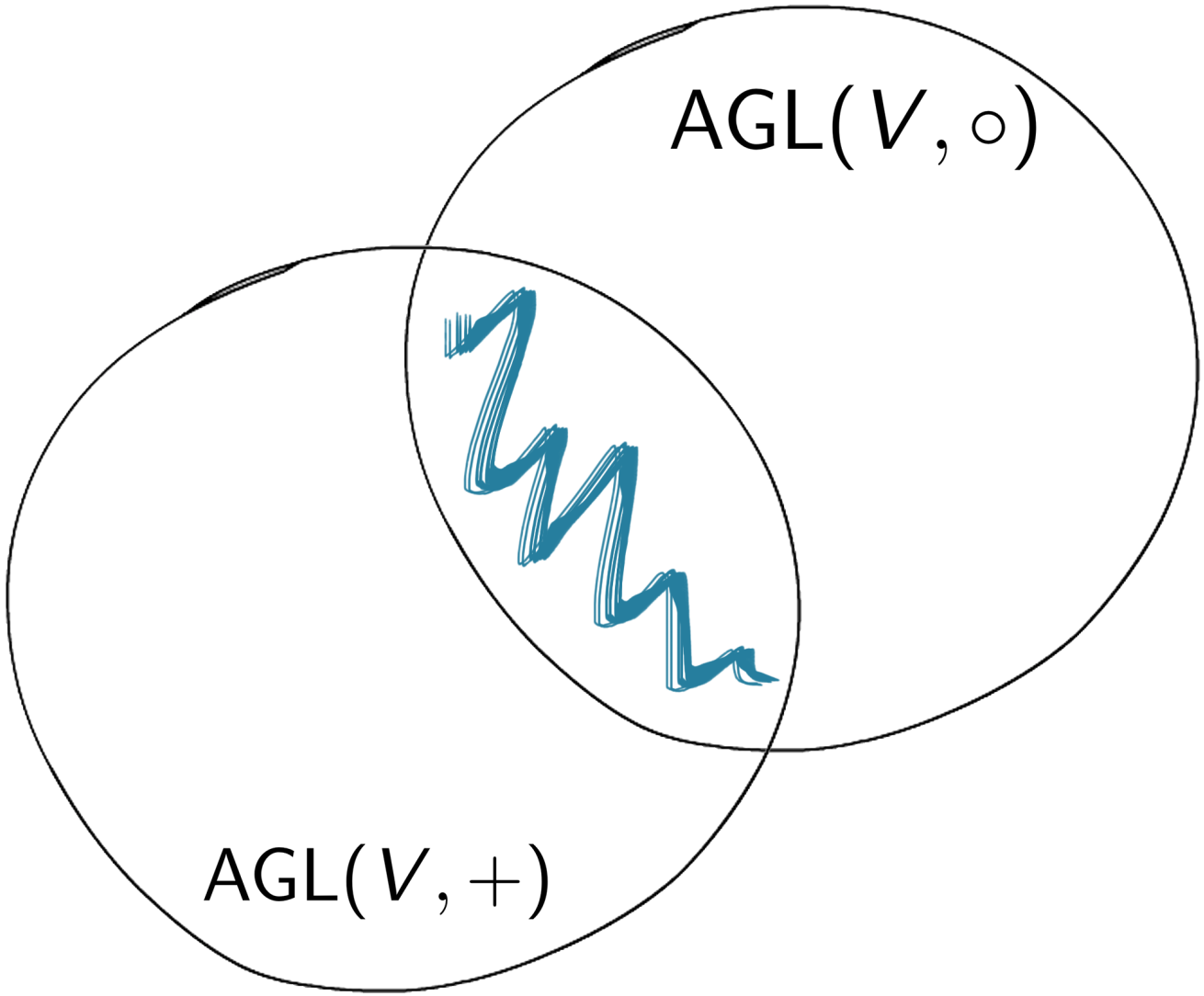
$$\mathrm{AGL}(V,+) \cap \mathrm{AGL}(V,\circ)$$



highly non-linear

completely linear

The Big Problem: $\#\mathrm{AGL}_+ \cap \mathrm{AGL}_\circ$



¿Questions?