Group Theory for Cryptology

Carlo Maria Scoppola

October 22, 2019
Group Algebras, Representations and Computation
International Centre for Theoretical Research - Bengaluru
(joint work with R. Aragona, R. Civino and N. Gavioli)

Block ciphers consist of:

A *text space* (which is also the ciphertext space): $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$.

Block ciphers consist of:

A *text space* (which is also the ciphertext space): $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$.

A set of *keys*: $\mathcal{K}(\subseteq V)$.

Block ciphers consist of:

A *text space* (which is also the ciphertext space): $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$.

A set of *keys*: $\mathcal{K}(\subseteq V)$.

An (injective) map:

$$\begin{array}{rccc} \Phi: & \mathcal{K} & \to & \operatorname{Sym}(V) \\ & k & \mapsto & E_k \end{array}$$

Block ciphers consist of:

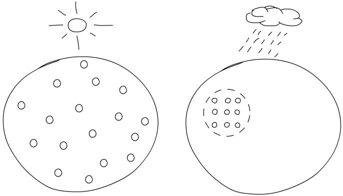
A *text space* (which is also the ciphertext space): $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$.

A set of *keys*: $\mathcal{K}(\subseteq V)$.

An (injective) map:

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

The permutations corresponding to the keys, called the *encryption functions*, should appear uniformly spread through the set of all the permutations on V.



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

The homomorphism

$$\begin{array}{rccc} \sigma: & V & \to & \mathrm{Sym}\,(V) \\ & v & \mapsto & \sigma_v : x \mapsto x + v \end{array}$$

is a *regular* representation of V:
it is transitive, and all the stabilizers are trivial.

The homomorphism

$$\begin{array}{rccc} \sigma: & V & \to & \mathrm{Sym}\,(V) \\ & v & \mapsto & \sigma_v : x \mapsto x + v \end{array}$$

is a *regular* representation of V:
it is transitive, and all the stabilizers are trivial.

$T = \{\sigma_v | v \in V\}$ is the group of the translations. It is well known that $N_{Sym(V)}(T) \cong V \rtimes GL(V) = AGL(V)$.

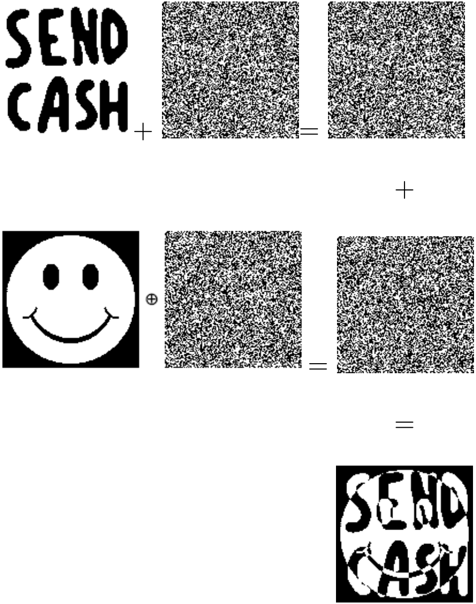
The homomorphism

$$\begin{array}{cccc} \sigma: & V & \rightarrow & \mathrm{Sym}\,(V) \\ & v & \mapsto & \sigma_v : x \mapsto x + v \end{array}$$

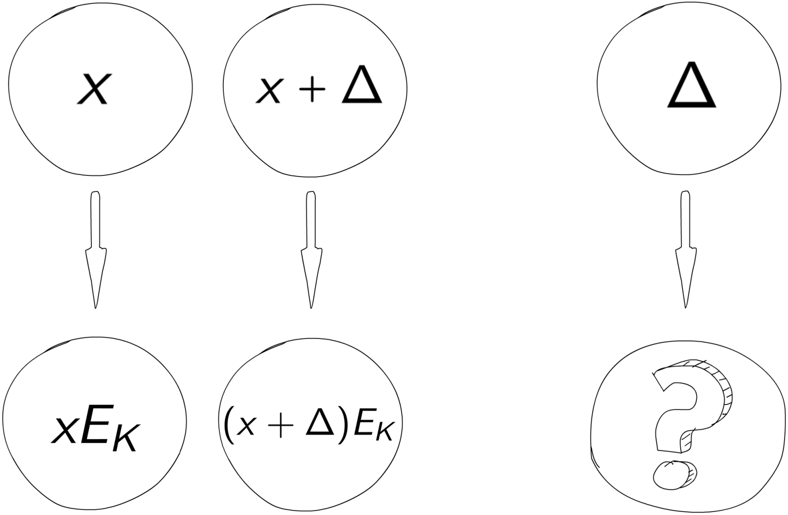
is a *regular* representation of V:
it is transitive, and all the stabilizers are trivial.

$T = \{\sigma_v | v \in V\}$ is the group of the translations. It is well known that $N_{Sym(V)}(T) \cong V \rtimes GL(V) = AGL(V)$.

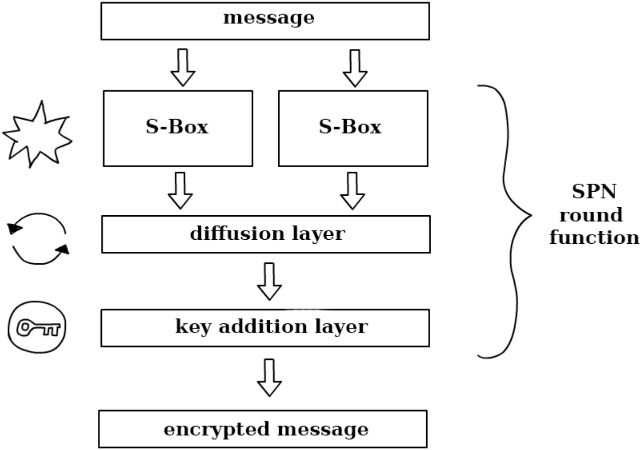
In our choice of the encryption functions, we would better STAY AWAY from $N_{Sym(V)}(T)$. Here is a problematic example in which σ was used to choose our encryption function.


SEND
CASH

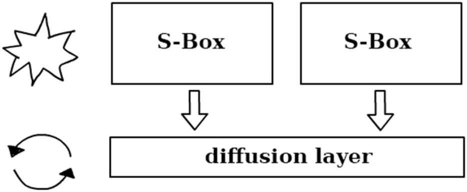
Differential attack



Substitution-Permutation Networks



Confusion and diffusion



highly non-linear

completely linear

There are many regular subgroups of $Sym(V)$, and many of them are isomorphic to V.

There are many regular subgroups of $Sym(V)$, and many of them are isomorphic to V.

Lemma (John D. Dixon, *Maximal abelian subgroups of the symmetric group*, Can. J. Math. XXIII, 3 (1971), 426-438.)

If G is a finite group any two regular representations of G in $Sym(G)$ are conjugate.

Proof.

Let $\sigma : G \to Sym(G)$ be the right regular representation of the finite group G, and let $\tau : G \to Sym(G)$ any regular representation of G. We indicate by g^σ, g^τ the images of $g \in G$ under σ, τ. Let 1 indicate the identity of G.
Now we define a map $\phi : G \to G$ by $g\phi = 1g^\tau$. The map ϕ is easily seen to be a permutation of G, because τ is a regular representation.
Any cycle of g^σ has the form $(x\ xg\ xg^2\ \ldots\ xg^{o(g)-1})$, and conjugating it by ϕ, and remembering that τ is an isomorphism, we obtain $(1x^\tau\ 1x^\tau g^\tau\ 1x^\tau (g^\tau)^2\ \ldots\ 1x^\tau (g^\tau)^{o(g)-1})$, which is a cycle of g^τ.

$\square$

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

$$a + b = a\sigma_b$$

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

$$a + b = a\sigma_b$$

analogously, if $T^g = T_\circ < \mathrm{Sym}(V)$ is conjugated to T in $\mathrm{Sym}(V)$,

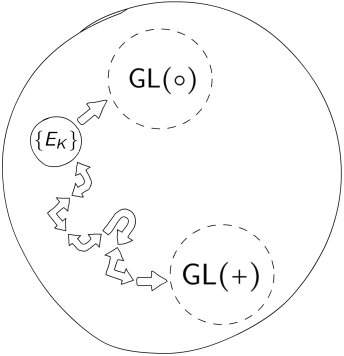
$$T_\circ = \{\tau_b \mid b \in V\},$$

where τ_b is the unique element in $T_\circ$ which maps 0 into b, then another operation is defined on V as

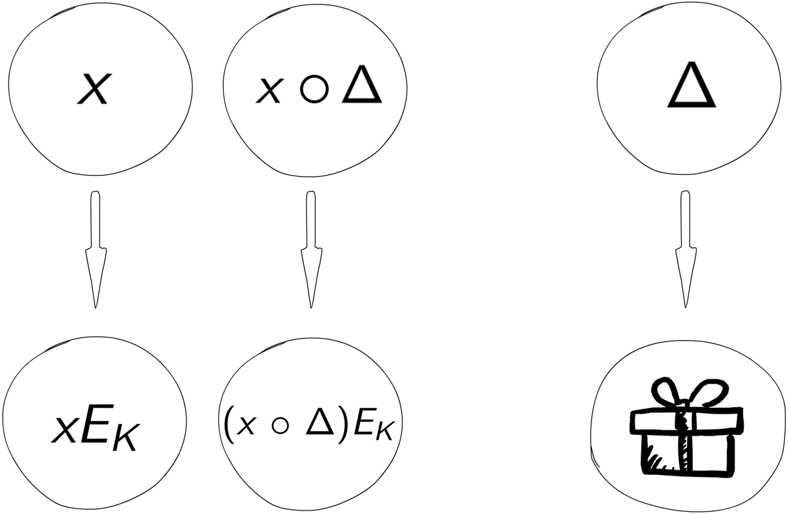
$$a \circ b \stackrel{\text{def}}{=} a\tau_b$$

It is easy to prove that $(V, \circ)$ is an elementary abelian group, thus isomorphic to $(V, +)$.

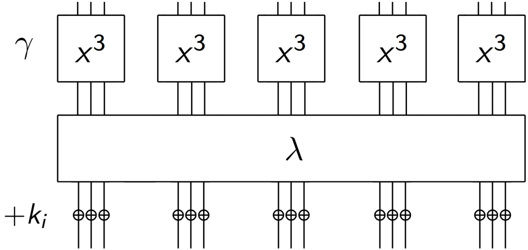
Is it possible that the encryption functions are "less non-linear" with respect to $\circ$ than they are with respect to $+$? In other words, should we "stay away" also from the conjugates of $AGL(V)$, when choosing our encryption functions?



Differential attack revisited



A successful example on a toy SPN*



- distinguishing attack based on classical differences fails
- distinguishing attack based on alternative differences succedes

*R. Civino, C. Blondeau, and M. Sala. *Differential attacks: using alternative operations*. **Designs, Codes and Cryptography**. 2019, 87.2-3: 225-247

Weak-key subspace

$$W_\circ \stackrel{\text{def}}{=} \{k \mid k \in V, \forall x \in V \;\; x \circ k = x + k\} \cong T \cap T_\circ$$

Weak-key subspace

$$W_\circ \stackrel{\text{def}}{=} \{k \mid k \in V, \forall x \in V \;\; x \circ k = x + k\} \cong T \cap T_\circ$$

- consider $T_\circ < \mathrm{AGL}(V)$

$$\downarrow^{*}$$

$$1 \leq d \stackrel{\text{def}}{=} \dim(W_\circ) \leq n - 2$$

*A. Caranti, F. Dalla Volta and M. Sala, 2006; M. Calderini and M. Sala, 2017

Weak-key subspace

$$W_\circ \overset{\text{def}}{=} \{k \mid k \in V, \forall x \in V \;\; x \circ k = x + k\} \cong T \cap T_\circ$$

- consider $T_\circ < \mathrm{AGL}(V)$

$$\downarrow^{*}$$

$$1 \leq d \overset{\text{def}}{=} \dim(W_\circ) \leq n - 2$$

- assume $d = n - 2$

$$\downarrow$$

  - $(x + k) \circ ((x \circ \Delta) + k) = \Delta$ half of the times
  - we can exhibit matrices that are linear with respect to $\circ$ as well

*A. Caranti, F. Dalla Volta and M. Sala, 2006; M. Calderini and M. Sala, 2017

Is the case $d = n - 2$ special?

apparently, yes[**]!

[*] R. Aragona, R. Civino, N. Gavioli, C.M.S., *Regular subgroups with large intersection*. **Annali di Matematica Pura ed Applicata**. 2019

Is the case $d = n - 2$ special?

apparently, yes[**]!

Theorem (R. Aragona, R. Civino, N. Gavioli, C.M.S.)

If $T_\circ < \mathrm{Sym}(V)$ *is such that* $\dim(W_\circ) = n - 2$*, then* $T_\circ < \mathrm{AGL}(V)$

- groups conjugated to T such that $\dim(W_\circ) = n - 2$ are called second-maximal intersection subgroups (2MI)
- possible construction of cyphers that are secure with respect to many different $\circ$ -differential attacks

---

[*] R. Aragona, R. Civino, N. Gavioli, C.M.S., *Regular subgroups with large intersection*. **Annali di Matematica Pura ed Applicata**. 2019

Sketch of proof: we show first that if an involution $\phi \in Sym(V)$ does not fix any of the cosets of a subgroup $W \leq V$ of index 4, and centralizes σ_W, then $\phi \in AGL(V)$. We then observe that $T_\circ$ is generated by $T \cap T_\circ$ and two such commuting involutions.
But we were also able to write those involutions in matrix form. This turned out to be crucial in the proof of our next result:

Theorem (A,C,G,S)

Every Sylow 2*-subgroup* Σ *of* $\mathrm{AGL}(V)$ *contains exactly one 2MI subgroup* T_Σ *which is normal in* Σ

$$\begin{tikzcd} \mathrm{AGL}(V) \arrow[d, dash] \\ \Sigma \arrow[d, dash, "\trianglelefteq"] \\ T_\Sigma \end{tikzcd}$$

Theorem (A,C,G,S)

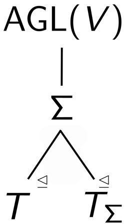
If $\bar{T}$ *is a 2MI subgroup, then there exists a Sylow* 2*-subgroup* Σ *of* $\mathrm{AGL}(V)$ *such that* $\bar{T} = T_\Sigma \trianglelefteq \Sigma$

Our next result is certainly the most technical of the whole paper. The proof is based on two basic ideas, namely:

- the fact that the Sylow 2-subgroups of $\mathrm{AGL}(V)$ are all isomorphic to the semidirect product of T with the group U_n of the unitriangular matrices, and therefore that they stabilize a flag in T;
- the canonical embedding of $\mathrm{AGL}(V)$ in $GL(n+1,2)$.

Theorem (A,C,G,S)

Let $\bar{T}$ be an elementary abelian regular subgroup of a Sylow 2-subgroup Σ of $\mathrm{AGL}(V)$. Then $\bar{T}$ is normal in Σ if and only if $\bar{T} \in \{\, T, T_\Sigma \,\}$



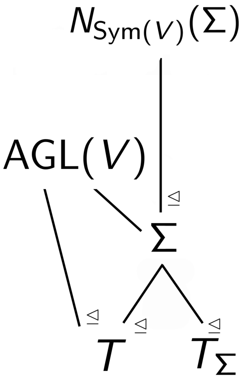
The proof consists essentially in showing that $\bar{T}$ is a 2MI subgroup.

Corollary

Every $g \in N_{\mathrm{Sym}(V)}(\Sigma) \setminus \mathrm{AGL}(V)$ interchanges by conjugation T and T_Σ

Corollary

If Σ is a Sylow 2-subgroup of $\mathrm{AGL}(V)$, *then* $[N_{\mathrm{Sym}(V)}(\Sigma) : \Sigma] = 2$



The fact that the Sylow 2-subgroups of $\mathrm{Sym}(V)$ are self-normalising was already known to P. Hall. Similarly:

Corollary

If Σ is a Sylow 2-subgroup of $\mathrm{AGL}(V)$, then $N_{\mathrm{AGL}(V)}(\Sigma) = \Sigma$. In particular,

$$[\mathrm{AGL}(V) : \Sigma] = \prod_{j=0}^{n-1} \left(2^{n-j} - 1\right).$$

is the number of distinct Sylow 2-subgroups of $\mathrm{AGL}(V)$

Next?

- 2MI subgroups $\rightleftharpoons$ normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$

Next?

- 2MI subgroups $\rightleftharpoons$ normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$
- 3MI subgroups

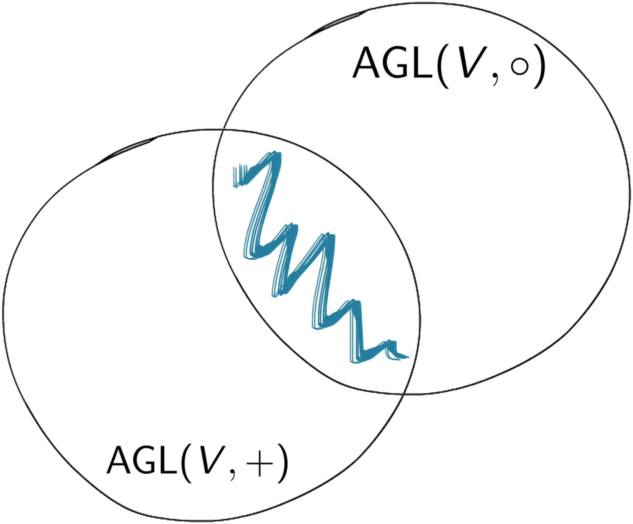
Next?

- 2MI subgroups $\rightleftharpoons$ normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$
- 3MI subgroups $\rightleftharpoons$ normalisers of normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$

Next?

- 2MI subgroups $\rightleftharpoons$ normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$
- 3MI subgroups $\rightleftharpoons$ normalisers of normalisers of Sylow 2-subgroups of $\mathrm{AGL}(V)$
- bring this back to crypto again

The Big Problem




Thank
You!