# An Algebraic Approach to the Design of Block Ciphers

José Valença　　Óscar Pereira　　Tiago Oliveira

{ jmvalenca, oscar, tfaoliveira }@di.uminho.pt

**HASLab, INESC TEC & Univ. of Minho (PT)**

Mathematical Methods for Cryptography

Svolvær, Lofoten, Norway

September 2017

# In the beginning. . .

## . . . there was Óscar’s MSc thesis

Wanted to build a (symmetric) cipher, using:

- **APNL** (Almost Perfect Non-Linear) functions
- **CRT** (Chinese Remainder Theorem)

**GOAL: simple algebraic description**

# And speaking of GOALs. . .

## We also aim to. . .

- **Being able to formally reason about security**
- Have a reasonably efficient implementation

On the latter goal, we're not quite there yet. . .

# Cipher structure

- **Confusion-Diffusion Permutation (CDP)**
- **Round (basically a keyed CDP)**
- Substitution-Permutation Network (SPN) — iterated round

# CDP version 1

$$\mathcal{X}_q \xrightarrow{\quad \text{mod}_q \quad} \Pi_q \xrightarrow{\quad \mathcal{S} \quad} \Pi_q \xrightarrow{\quad \text{crt}_q \quad} \mathcal{X}_q$$

- $\mathcal{X}_q \rightarrow$ ring $GF(2)[x]/\langle\Phi_{257}\rangle$, where $\Phi_{257} = 1 + x + x^2 + \ldots + x^{256}$
- $\Pi_q \rightarrow$ product ring
$$\prod_{i=0}^{15} GF(2)[x]/\langle q_i\rangle$$
where each $q_i$ is ***irreducible*** and with degree 16
- $\mathcal{S} \rightarrow$ layer of Sboxes, aligned with the $q_i$'s

# CDP version 1

$$\mathcal{X}_q \xrightarrow{\mathsf{mod}_q} \Pi_q \xrightarrow{\mathcal{S}} \Pi_q \xrightarrow{\mathsf{crt}_q} \mathcal{X}_q$$

## Problems:

- “good” sbox layer requires prod. ring with ***odd degree*** factors
- key mixing also in $\mathcal{X}_q$ ($\cong \Pi_q$) → hence it is ***block-wise*** op, i.e. little actual mixture

# CDP version 2

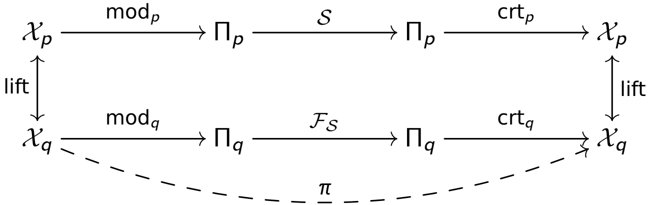
$$\mathcal{X}_p \xrightarrow{\text{mod}_p} \Pi_p \xrightarrow{\mathcal{S}} \Pi_p \xrightarrow{\text{crt}_p} \mathcal{X}_p$$

- $\Pi_p \rightarrow$ prod. ring, with $p_i$ ***irreducible*** and of deg 9 or 11 $[(11 \times 5 + 9) \times 4 = 64 \times 4 = 256]$
- $\mathcal{X}_p \rightarrow$ ring over $GF(2)$, with modulus $\prod p_i$

**This is what is really implemented**

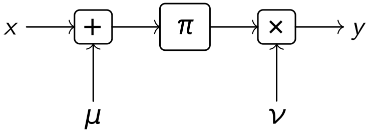
# CDP: two views

$\mathcal{F}_\mathcal{S}$ is such that makes the diagram commute




***Goal:*** reduce analysis to studying $\mathcal{F}_\mathcal{S}$

# Round




- Most operations can be stored as pre-computed matrices
- ***Multiplicative key***: op. done in $\mathcal{X}_q$ (not $\mathcal{X}_p$)
- ***MK***: increases the ***algebraic degree*** of equations? (i.e. increases resistance to algebraic cryptanalysis?)

# Is it secure?

## A tentative argument. . .

- APNL / AB strengthens differential immunity
  - And to some extent, linear immunity. . .
- Niho exponents (APNL power functions) increases algebraic immunity

  (cf. J. Cheon and D.H. Lee, ***"Almost Perfect Nonlinear Power Functions and Algebraic Attacks"***, 2004)

# Three ending notes

- More of a “***framework for ciphers***” than a cipher per se

- Diffusion matrices

- A (**tentative**) lattice-based attack

# Diffusion matrices

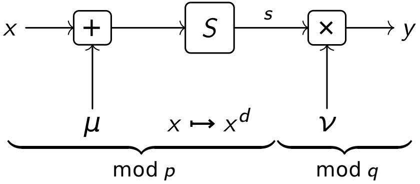
## Prob. of output weight $r$, when input has weight $\ell$?

- $\|F\| = Prob[F \neq 0]$
- $\psi_r(x) = 1$ iff $hw(x) = r$

$$DM_{\ell,r} = \|(\psi_r \circ F) \times \psi_\ell\| / \|\psi_\ell\|$$

- Spheres not centered in **0**: flipping bits in arbitrary vectors
- Size is $(n+1) \times (n+1)$!

# The lattice attack (KPA)




$$\begin{cases} s = (x + \mu)^d \pmod{p} \\ y = s \times \nu \pmod{q} \end{cases}$$

- Resembles Coppersmith ($deg(s, \mu, \nu) < blocksize$)
- Extends Cohn & Heninger (2013)

# So to conclude. . .

## Feedback is welcome:

- Efficiency improvements
- ***The algebraic aspects*** (starting with the mult. keys)

# Questions. . .