Rump Session 2016

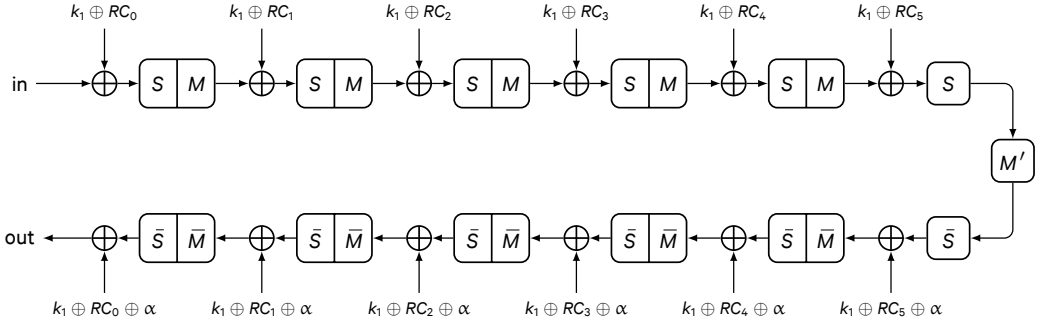
QARMA

Roberto Avanzi

Qualcomm

Memory Encryption: PRINCE, son of ENIGMA

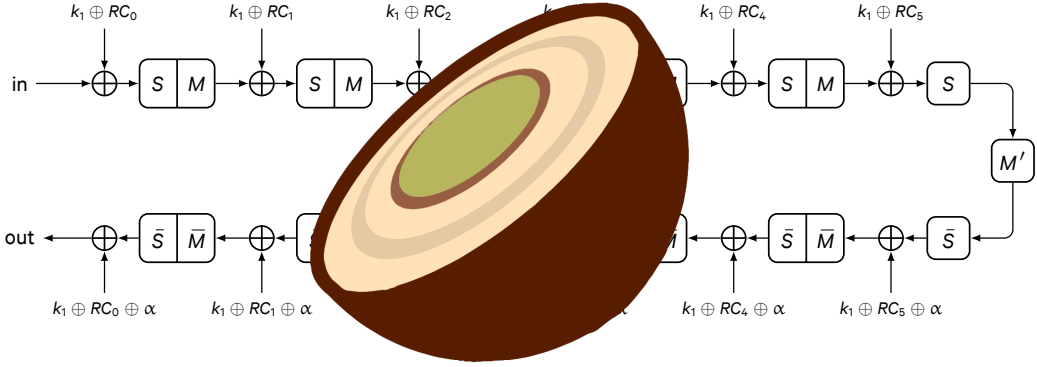
Yet another example of german technology inspired by austrian leadership!



Because it's a **Mozartkugel!** A (involutory) core surrounded by several symmetric layers, wrapped in a thin but opaque skin (the ~~brown~~whitening)
(Bar over function denotes inverse)

Memory Encryption: PRINCE, son of ENIGMA

Yet another example of german technology inspired by austrian leadership!



Because it's a **Mozartkugel!** A (involutory) core surrounded by several symmetric layers, wrapped in a thin but opaque skin (the ~~brown~~whitening)

(Bar over function denotes inverse)

Problem

Context: Memory encryption with no memory overhead

- ECB mode:

  Sadly, traces of Herr Drumpf left...

- XEX mode:

$$\text{encrypted block} = W \oplus \texttt{PRINCE}_k(\text{clear block} \oplus W)$$

  with W securely derived from address $\Rightarrow$ more latency

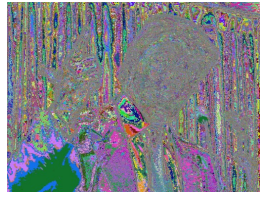
Idea:

- Use a *tweakable* cipher

$$\text{encrypted block} = \texttt{TWEAKABLE-PRINCE}_{K,T=addr}(\text{clear block})$$

Problem

Context: Memory encryption with no memory overhead



- ECB mode:

  Sadly, traces of Herr Drumpf left...

- XEX mode:

$$\text{encrypted block} = W \oplus \texttt{PRINCE}_k(\text{clear block} \oplus W)$$

  with W securely derived from address $\Rightarrow$ more latency

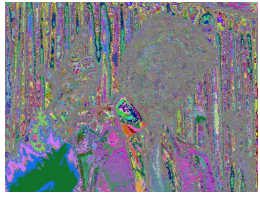
Idea:

- Use a *tweakable* cipher

$$\text{encrypted block} = \texttt{TWEAKABLE-PRINCE}_{K,T=addr}(\text{clear block})$$

Problem

Context: Memory encryption with no memory overhead



- ECB mode:

  Sadly, traces of Herr Drumpf left...

- XEX mode:

$$\text{encrypted block} = W \oplus \texttt{PRINCE}_k(\text{clear block} \oplus W)$$

  with W securely derived from address $\Rightarrow$ more latency

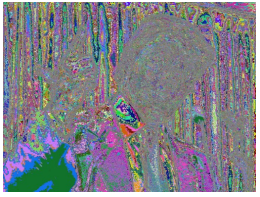
Idea:

- Use a *tweakable* cipher

$$\text{encrypted block} = \texttt{TWEAKABLE-PRINCE}_{K,T=addr}(\text{clear block})$$

Problem

Context: Memory encryption with no memory overhead



- ECB mode:

  Sadly, traces of Herr Drumpf left...

- XEX mode:

$$\text{encrypted block} = W \oplus \texttt{PRINCE}_k(\text{clear block} \oplus W)$$

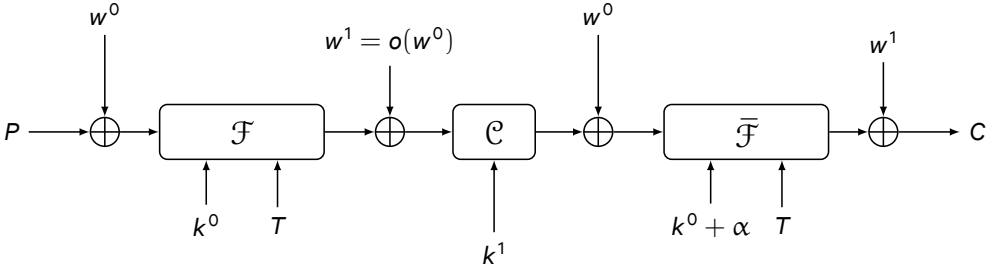
  with W securely derived from address $\Rightarrow$ more latency

Idea:

- Use a *tweakable* cipher

$$\text{encrypted block} = \texttt{TWEAKABLE-PRINCE}_{K,T=addr}(\text{clear block})$$

QARMA: Beyond the Mozart Ball

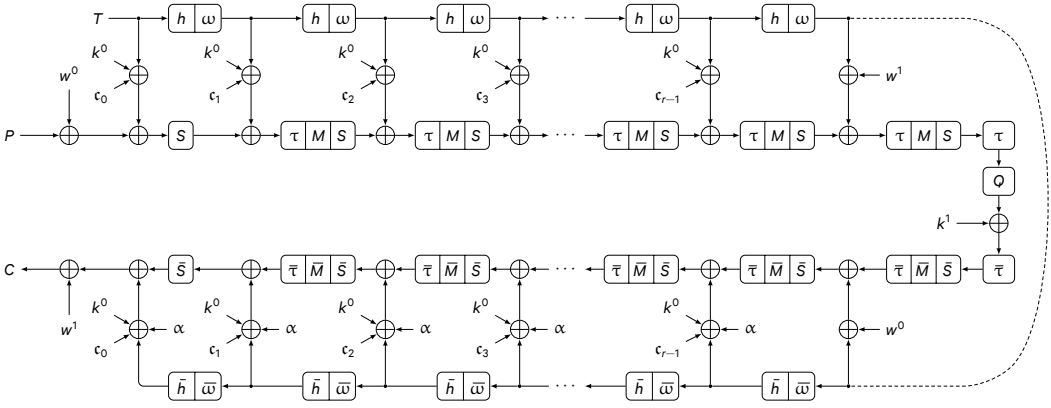


3-Round Even-Mansour with outer perms keyed & tweaked, middle perm $\mathcal{C}$ keyed, not involutory

Whitening key derivation $w^0 \mapsto w^1 = o(w^0)$ with $o(\cdot)$ orthomorphism (taken from PRINCE)

Crucial difference w.r.t. PRINCE: we use upper indexes (k^0) instead of lower indexes (k_0)!

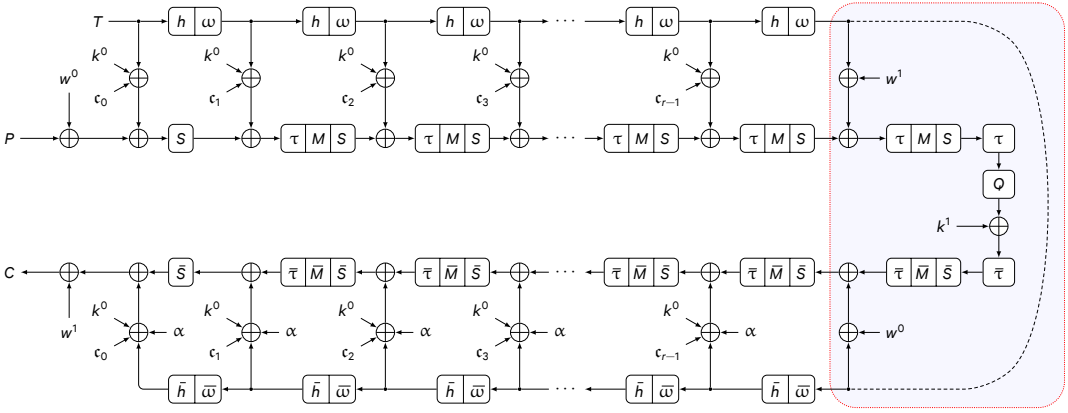
QARMA: Just Another Bricklayer in the Crypto Wall?



τ, h = Shuffles of the cells, M, Q = Almost MDS matrices, Q involutory, S = S-Box layer, ω = LSFR

Reuses tweak shuffle from `MANTIS` (a `PRINCE`-like FX construction with `MIDORI` round function)

QARMA: Just Another Bricklayer in the Crypto Wall?



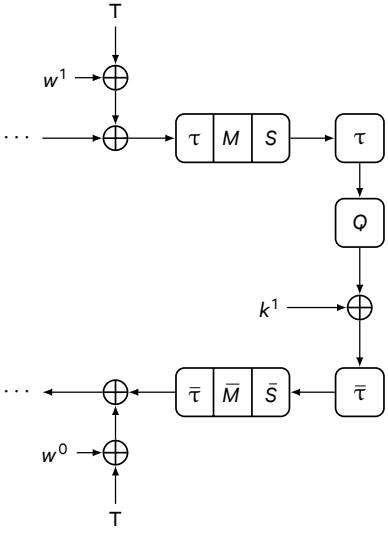
τ, h = Shuffles of the cells, M, Q = Almost MDS matrices, Q involutory, S = S-Box layer, ω = LSFR

Reuses tweak shuffle from `MANTIS` (a `PRINCE`-like FX construction with `MIDORI` round function)

New Central Construction

Properties of central rounds:

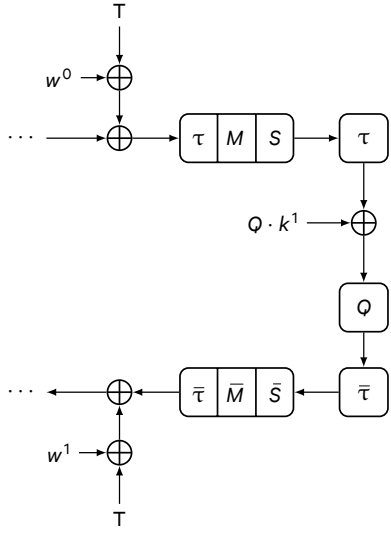
- Use whitening key(s) instead of core key
  - Thwarts reflection attacks
- Non involutory *Pseudo-Reflector*
  - Add key k^1, not tweak
  - Easy to invert
  - Also makes reflection attacks more difficult
- Chosen Q, M's have $\leqslant 2^{n/2}$ fixed points
  - The $\{0,1\}$ `MIDORI` circulant has $2^{3n/4}$!
  - New almost MDS family over $\mathbb{F}_2[\rho] = = \mathbb{F}_2[X]/(X^m+1)$ with optimal critical path (circulants, classification)
  - Also makes attacks more difficult



New Central Construction

Properties of central rounds:

- Use whitening key(s) instead of core key
  - Thwarts reflection attacks
- Non involutory *Pseudo-Reflector*
  - Add key k^1, not tweak
  - Easy to invert
  - Also makes reflection attacks more difficult
- Chosen Q, M's have $\leqslant 2^{n/2}$ fixed points
  - The $\{0,1\}$ `MIDORI` circulant has $2^{3n/4}$!
  - New almost MDS family over $\mathbb{F}_2[\rho] = = \mathbb{F}_2[X]/(X^m+1)$ with optimal critical path (circulants, classification)
  - Also makes attacks more difficult



Implementation

We consider here gate depth (and to a lesser extent, area)

σ_0, σ_2 different S-Boxes

Values are estimates

Details in tech report
`http://ia.cr/2016/444`

Cipher	Depth (GE)	Area (GE)
QARMA-64_5-σ_0	100	8971
QARMA-64_6-σ_0	117	10451
QARMA-64_7-σ_0	134	11929
QARMA-64_5-σ_2	107	9484
QARMA-64_6-σ_2	125	11048
QARMA-64_7-σ_2	143	12616
MANTIS_5	100	8703
MANTIS_6	117	10155
MANTIS_7	134	11605
PRINCE	114	7424

Implementation

We consider here gate depth (and to a lesser extent, area)

σ_0, σ_2 different S-Boxes

Values are estimates

Details in tech report
`http://ia.cr/2016/444`

Cipher	Depth (GE)	Area (GE)
QARMA-128_8-σ_0	152	26592
QARMA-128_9-σ_0	168	29521
QARMA-128_{10}-σ_0	185	32450
QARMA-128_{11}-σ_0	201	35379
QARMA-128_8-σ_2	164	28127
QARMA-128_9-σ_2	183	31228
QARMA-128_{10}-σ_2	201	34328
QARMA-128_{11}-σ_2	219	37429
AES-128	554	63234
(Encryption only)	294	143888

Implementation

We consider here gate depth (and to a lesser extent, area)

σ_0, σ_2 different S-Boxes

Values are estimates

Details in tech report
`http://ia.cr/2016/444`

Cipher	Depth (GE)	Area (GE)
QARMA-128_8-σ_0	152	26592
QARMA-128_9-σ_0	168	29521
QARMA-128_{10}-σ_0	185	32450
QARMA-128_{11}-σ_0	201	35379
QARMA-128_8-σ_2	164	28127
QARMA-128_9-σ_2	183	31228
QARMA-128_{10}-σ_2	201	34328
QARMA-128_{11}-σ_2	219	37429
AES-128	554	63234
(Encryption only)	294	143888