Turning Online Ciphers Off

FSE 2018, Bruges, Belgium

Elena Andreeva[1], Guy Barwell[2], *Ritam Bhaumik*[3], Mridul Nandi[3], Daniel Page[2] and Martijn Stam[2]

[1] ESAT/COSIC, KU Leuven

[2] Department of Computer Science, University of Bristol

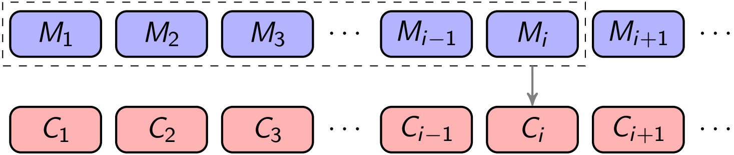
[3] Indian Statistical Institute, Kolkata

7 March 2018

Introduction

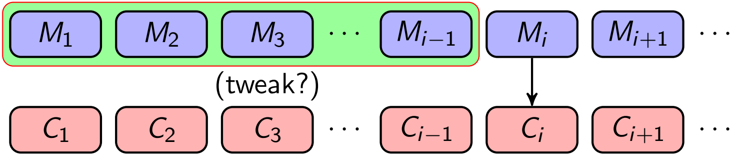
Encryption: Online and Offline

When is a permutation online?



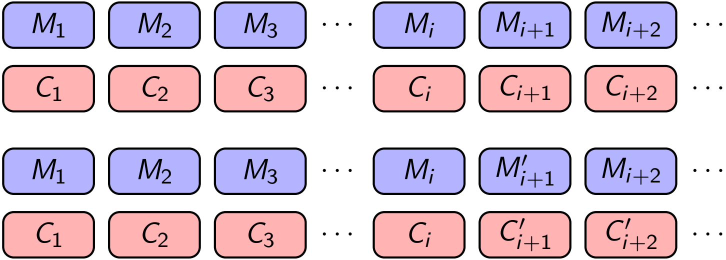
C_i is a function of $M_1, \ldots, M_i$ alone (not of $M_{i+1}, \ldots$)

Connection with a tweakable blockcipher



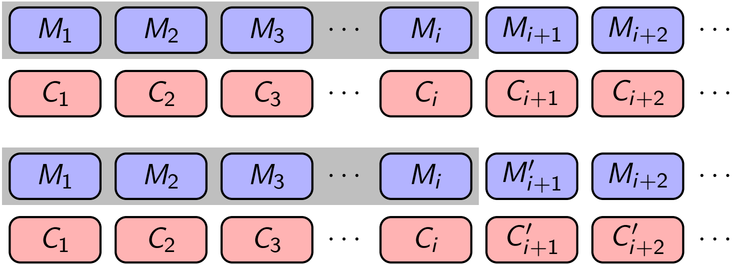
Can be thought of as a TBC with variable-length tweak

Shows common prefix



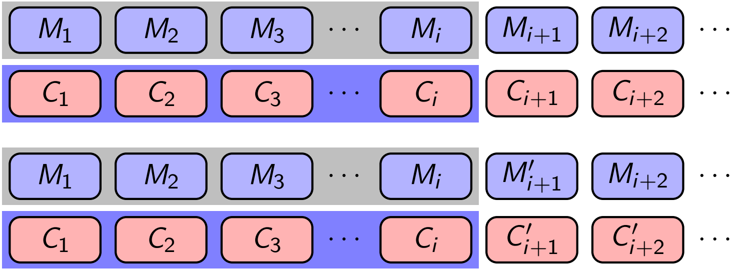
M_1	M_2	M_3	$\cdots$	M_i	M_{i+1}	M_{i+2}	$\cdots$
C_1	C_2	C_3	$\cdots$	C_i	C_{i+1}	C_{i+2}	$\cdots$
M_1	M_2	M_3	$\cdots$	M_i	M'_{i+1}	M_{i+2}	$\cdots$
C_1	C_2	C_3	$\cdots$	C_i	C'_{i+1}	C'_{i+2}	$\cdots$

Shows common prefix



M_1	M_2	M_3	$\cdots$	M_i	M_{i+1}	M_{i+2}	$\cdots$
C_1	C_2	C_3	$\cdots$	C_i	C_{i+1}	C_{i+2}	$\cdots$
M_1	M_2	M_3	$\cdots$	M_i	M'_{i+1}	M_{i+2}	$\cdots$
C_1	C_2	C_3	$\cdots$	C_i	C'_{i+1}	C'_{i+2}	$\cdots$

Shows common prefix



M_1 M_2 M_3 $\cdots$ M_i M_{i+1} M_{i+2} $\cdots$

C_1 C_2 C_3 $\cdots$ C_i C_{i+1} C_{i+2} $\cdots$

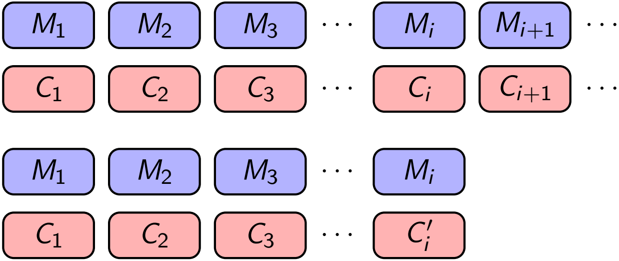
M_1 M_2 M_3 $\cdots$ M_i M'_{i+1} M_{i+2} $\cdots$

C_1 C_2 C_3 $\cdots$ C_i C'_{i+1} C'_{i+2} $\cdots$

Pros and Cons

- **Advantage:**
  - Single-Pass encryption
  - Fast
  - Efficient
  - Lightweight
- **Disadvantage:**
  - Changing plaintext suffix does not affect ciphertext prefix
  - Leaks information on shared prefix
  - Cannot be SPRP secure

Online-but-last



$M_1 \quad M_2 \quad M_3 \quad \cdots \quad M_i \quad M_{i+1} \quad \cdots$

$C_1 \quad C_2 \quad C_3 \quad \cdots \quad C_i \quad C_{i+1} \quad \cdots$

$M_1 \quad M_2 \quad M_3 \quad \cdots \quad M_i$

$C_1 \quad C_2 \quad C_3 \quad \cdots \quad C_i'$

Last block does not have online property

Ensures at least one block of randomness for every new query

The Problem

Going from Online to Offline

What we want to do

Question

Can we build an *offline cipher* using online ciphers as primitives?

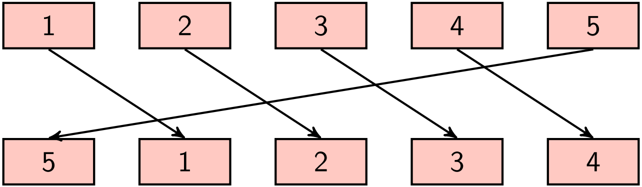
Other components:

Linear mixing layers

Linear layers considered

Three linear mixing layers:

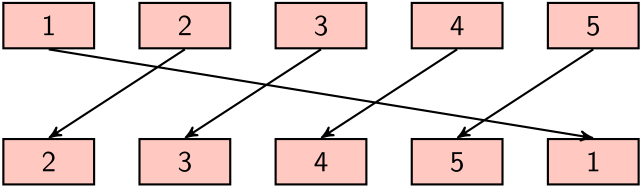
- **Right block-shift**
- Left block-shift
- Blockwise reverse



Linear layers considered

Three linear mixing layers:

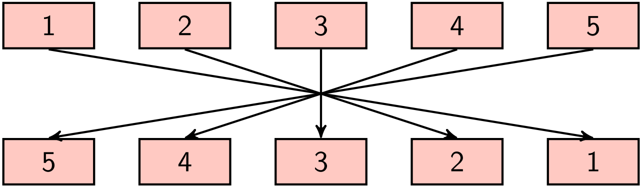
- Right block-shift
- **Left block-shift**
- Blockwise reverse



Linear layers considered

Three linear mixing layers:

- Right block-shift
- Left block-shift
- **Blockwise reverse**



Constructions Proposed

The generic structure

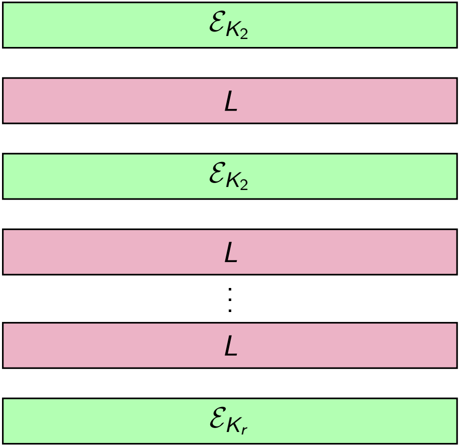
$\mathcal{E}$: ideal online cipher

L: linear mixing layer

Design Idea:
Interleave calls to $\mathcal{E}$ and L

r layers

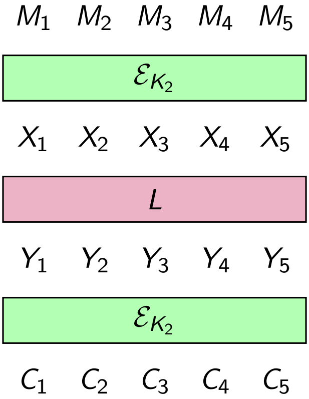
$K_1, \ldots, K_r$ independent



Generic birthday attack on 2-layer constructions

Two cases:

- Y_1 has no linear dependence on X_5:
    - Two-query attack
    - Only vary M_5
    - C_1 remains same
- Y_1 has a linear dependence on X_5:
    - Birthday attack
    - Keep varying M_5
    - All C_1's distinct


M_1 M_2 M_3 M_4 M_5
$\mathcal{E}_{K_2}$
X_1 X_2 X_3 X_4 X_5
L
Y_1 Y_2 Y_3 Y_4 Y_5
$\mathcal{E}_{K_2}$
C_1 C_2 C_3 C_4 C_5

Security of 2-layer constructions

At most birthday bound (from previous slide)

2-layer with left-shift:

- Y_1 independent of X_5
- insecure

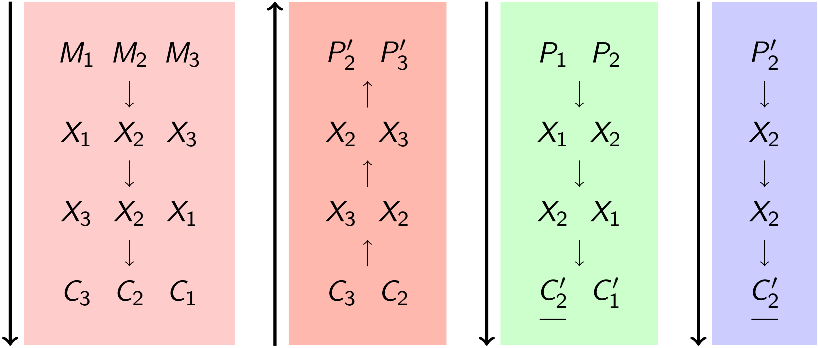
2-layer with right-shift:

- inverse is 2-layer with left-shift
- insecure in CCA setting
- birthday-secure prp

2-layer with reverse:

- insecure in CCA setting (attack on next slide)
- birthday-secure sprp when $\mathcal{E}$ is online-but-last cipher

4-query CCA attack on 2-layer with reverse



$$\begin{array}{ccc} M_1 & M_2 & M_3 \\ & \downarrow & \\ X_1 & X_2 & X_3 \\ & \downarrow & \\ X_3 & X_2 & X_1 \\ & \downarrow & \\ C_3 & C_2 & C_1 \end{array}$$

Query 1

$$\begin{array}{cc} P'_2 & P'_3 \\ \multicolumn{2}{c}{\uparrow} \\ X_2 & X_3 \\ \multicolumn{2}{c}{\uparrow} \\ X_3 & X_2 \\ \multicolumn{2}{c}{\uparrow} \\ C_3 & C_2 \end{array}$$

Query 2

$$\begin{array}{cc} P_1 & P_2 \\ \multicolumn{2}{c}{\downarrow} \\ X_1 & X_2 \\ \multicolumn{2}{c}{\downarrow} \\ X_2 & X_1 \\ \multicolumn{2}{c}{\downarrow} \\ \underline{C'_2} & C'_1 \end{array}$$

Query 3

$$\begin{array}{c} P'_2 \\ \downarrow \\ X_2 \\ \downarrow \\ X_2 \\ \downarrow \\ \underline{C'_2} \end{array}$$

Query 4

Security of 3-layer constructions

3-layer with left-shift:

- still insecure (a similar attack works)

3-layer with right-shift:

- inverse is 3-layer with left-shift
- as before insecure in CCA setting
- n-bit-secure prp

3-layer with reverse:

- n-bit-secure sprp for fixed arbitrary-length messages
- Variable input lenght - *Still open*
- (Probably) easy to prove for online-but-last ciphers

More layers?

Natural question:
Does adding more layers improve things?

Finding

Adding more layers does not change the security of this construction, except for the constant factors.

Open problem: *Can right-shift with enough layers become sprp?*

Thank you for your attention.

Judge a man by his questions rather than his answers. [Voltaire]