

A satellite view of Earth from space, showing the curvature of the planet and the glowing blue atmosphere. The surface is dark, with numerous bright yellow and orange lights representing cities and urban areas, primarily concentrated in the central and lower portions of the frame.

# Slide Attack on CLX-128

DEFENCE AND SPACE

Alexandre MÈGE, 2019-11-04

*Third Lightweight Cryptography Workshop at NIST*

**AIRBUS**

1. CLX algorithm description
2. Slide property of CLX permutation
3. Use of slide property to generate more online states
4. Extension of attack to other CLX family members
5. Slide property of Tiny JAMBU permutation

## Author and interest in LWC process

Interest in LWC for use in radiation hardened FPGA for space.


- Very small area : low datarate for Control/command, ~100 kbit/s
- Area and power efficient : ultra high rate for telecommunication, 10 Gbit/s to 100 Gbit/s



**Alexandre MÈGE**

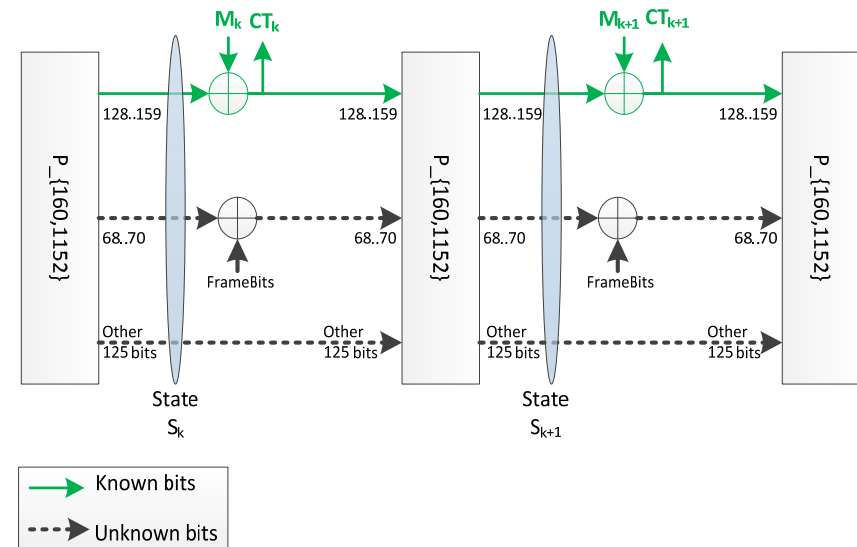
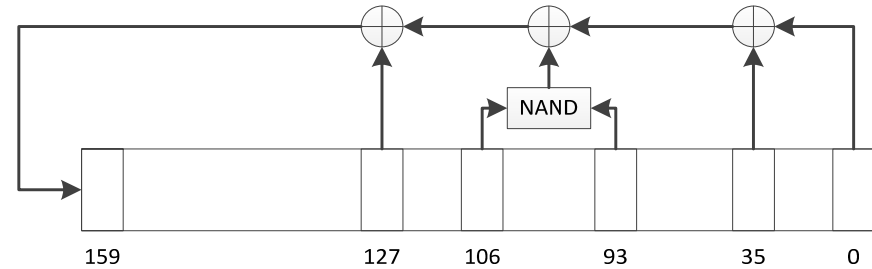
*Equipment Data Processing Expert*

**Airbus Defence and Space,**  
Spacecraft equipments



# CLX algorithm

- CLX-128 uses a 160 bits Nonlinear Feedback shift register as the permutation.
- This permutation is used to create an AEAD algorithm using a Sponge-like architecture
- FrameBits are added at the beginning of each full round to provide slide protection and domain separation



# CLX security goal and slide property impact

## CLX Security analysis

$2^{50}$  online Byte limit  $\Rightarrow 2^{48}$  online states

The 160 bit internal state guarantees that  $2^{112}$  offline states must be processed before a collision is found with the  $2^{48}$  online states.

## Slide attack impact

The slide attack is able to generate more online states (equivalent to  $2^{51.7}$  states) from  $2^{50}$  bytes of data.

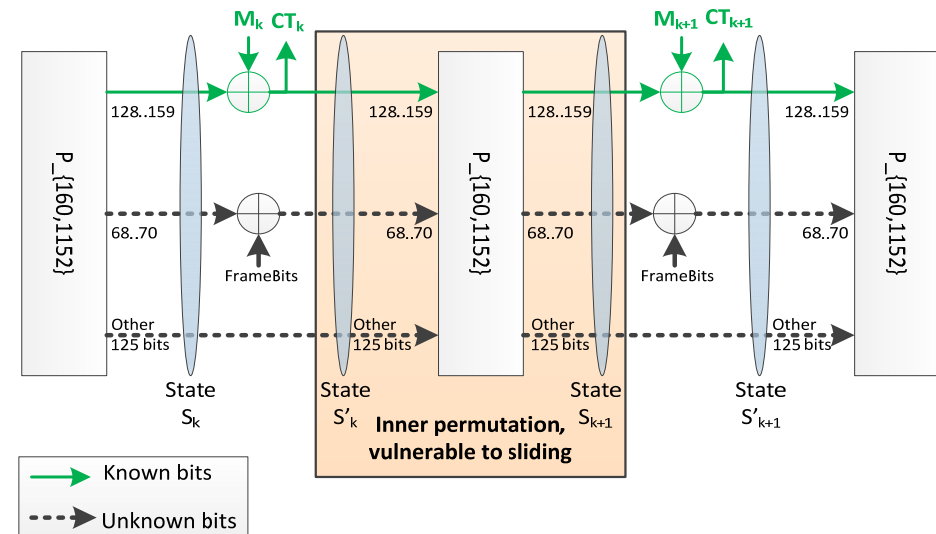
This reduces the number of online states to compute to  $2^{108.3}$  to find a collision.

The total complexity of the attack is  $2^{108.5}$ , *taking into account additional verification steps.*

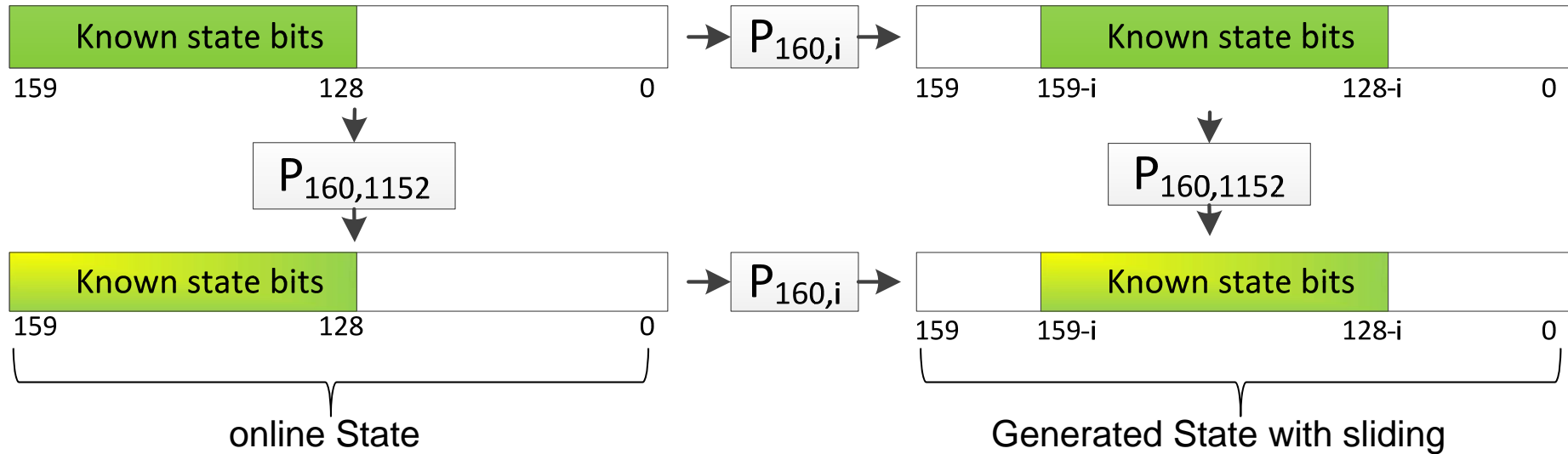
# CLX permutation analysis and slide property

- CLX uses the addition of Framebits to provide domain isolation and slide protection
- Framebits are only added once before the permutation
- No round constants are used during the 1152 iterations of the permutation

=> The inner permutation is vulnerable to sliding

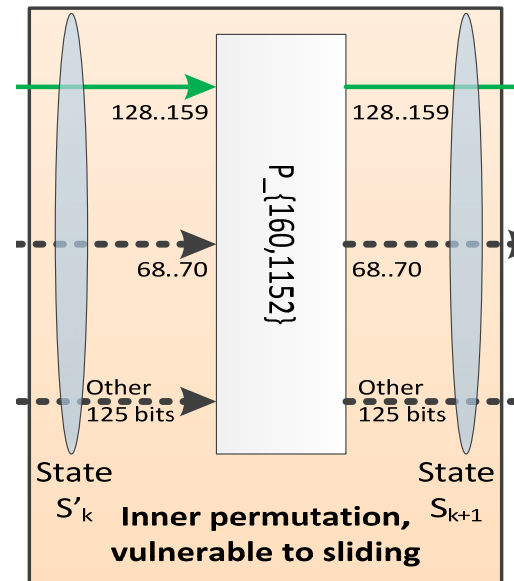


# Slide property of CLX



$$\text{StateUpdate}(\mathbf{P}_{160,1152}(\mathbf{S})) = \mathbf{P}_{160,1152}(\text{StateUpdate}(\mathbf{S}))$$

With this slide property, new states with known bits can be generated from online states



# Getting more pairs of consecutive states with known bits with the slide property

An online cipher calls gives

1 State with :

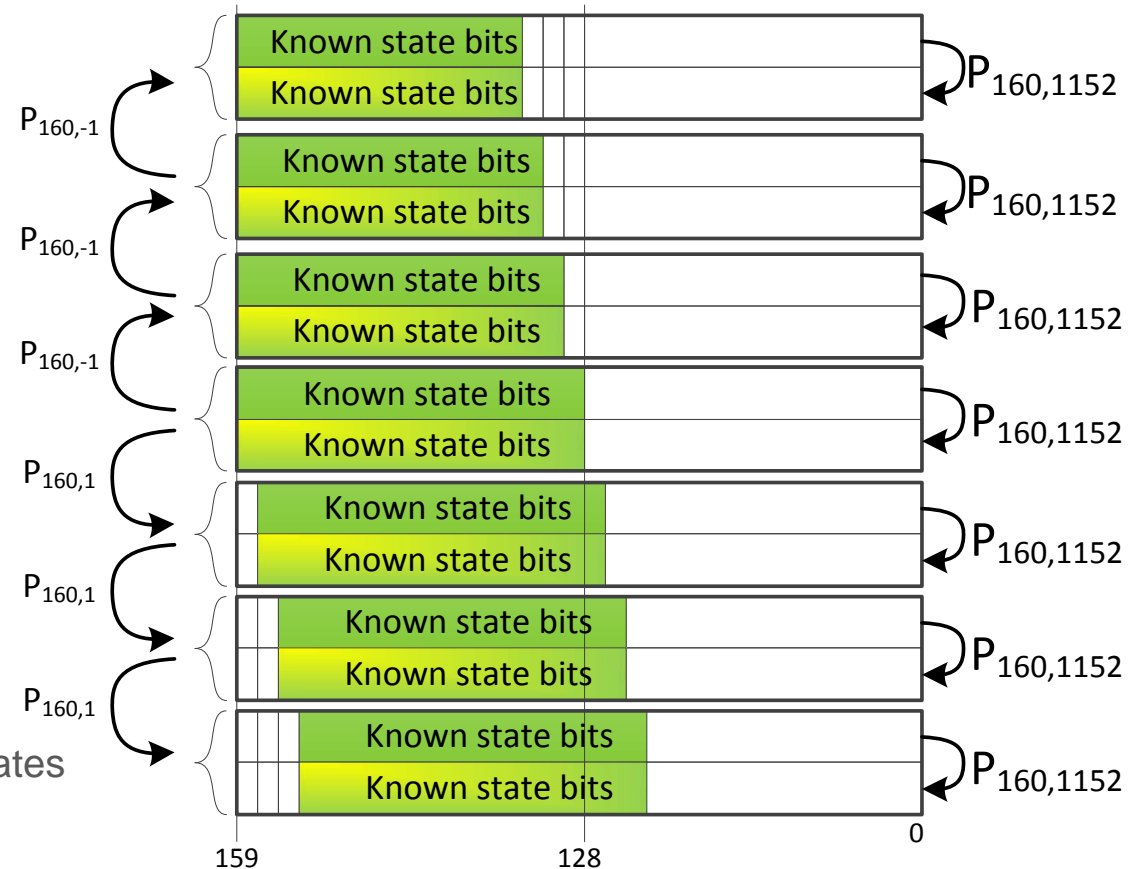
- 32 known bits at step K
- 32 known bits at step K+1.

Using a slide window of -6 to +6 gives 13 States with at least :

- 26 known bits at step K
- 26 known bits at step K+1.

This increases the number of online states with known bits from  $2^{48}$  to  $2^{51.7}$

This reduces the number of offline states to compute to find a collision from  $2^{112}$  to  $2^{108,3}$





## Extension of attack to other CLX family members

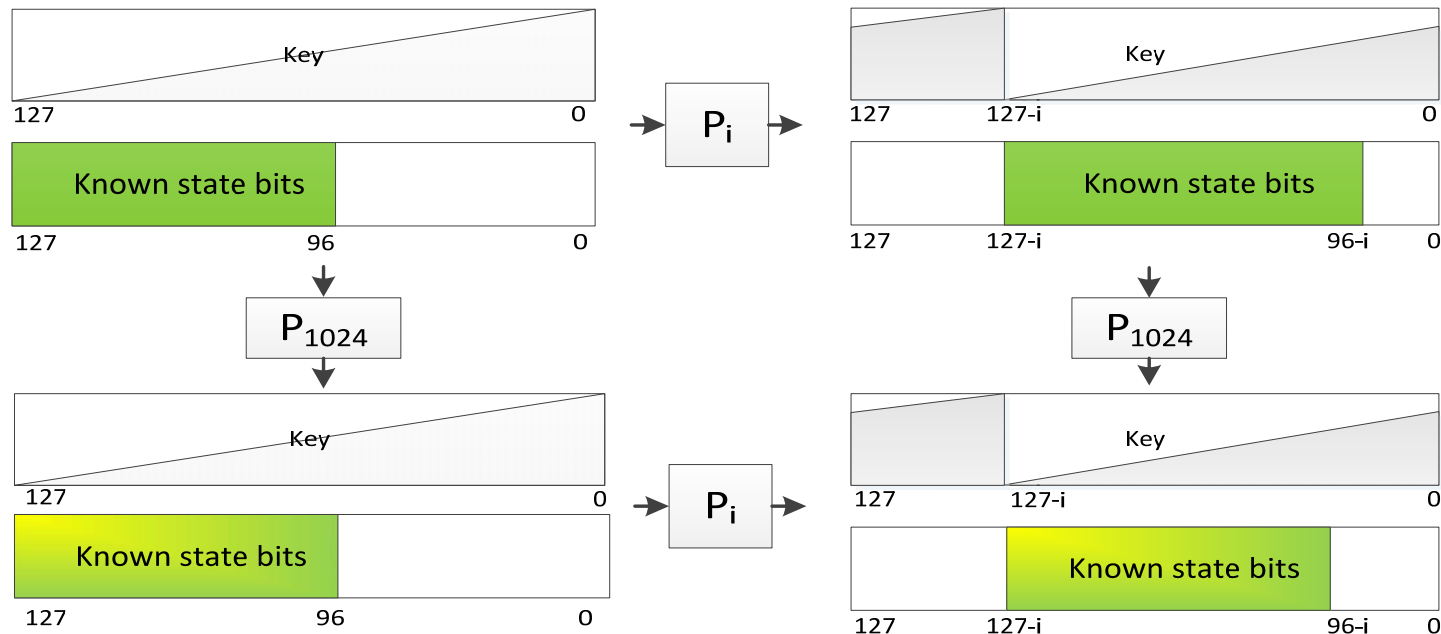
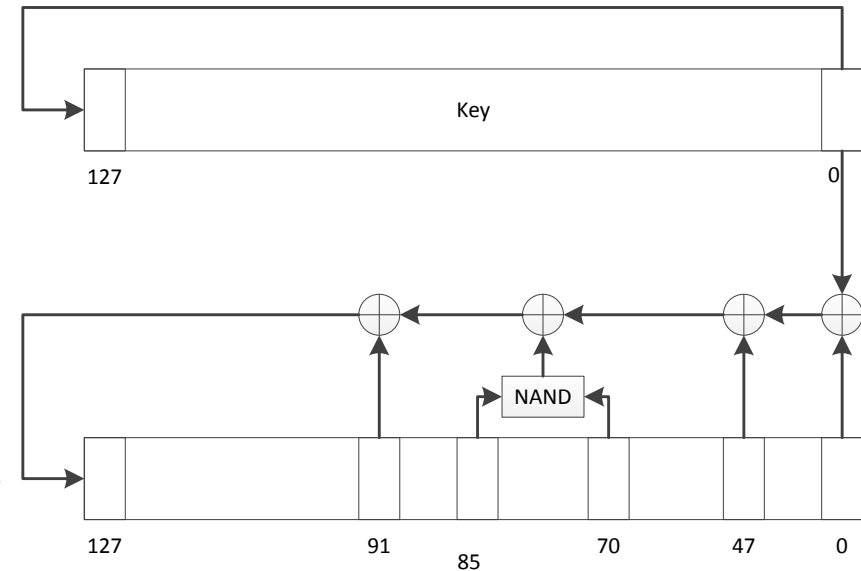
- All CLX family members possess the sliding property, and are thus vulnerable to the sliding attack
- This attack is faster than key brute force for CLX-128 variant. For other variants, brute force attacks on the key are faster.

Variant	Internal state size	Key Brute Force (log2)	Security Goal (log2)	This work (log2)
CLX-128	160	128	112	108.5
CLX-128Q	192	128	112	140.5
CLX-128H	192	128	112	140.5
CLX-192Q	256	192	168	204.5
CLX-192H	256	192	168	204.5
CLX-256Q	320	256	224	268,5
CLX-256H	320	256	224	268,5

Tab 1. : Attack complexity for this work and brute force

# Sliding property in Tiny-JAMBU

- Tiny-JAMBU algorithm uses a NLFSR as permutation, with the Key XORED in at each iteration.
- The inner permutation of Tiny-JAMBU has similar slide property as CLX, if we consider a slide of the complete internal state (NLFSR + Key)
- This slide property seems to have no impact on the security of Tiny-JAMBU in the single key model.





*Equipment Data Processing Expert*  
**Airbus Defence and Space,**  
Spacecraft equipments

**AIRBUS**