Slide Attack on CLX-128

Alexandre Mège
AIRBUS DEFENCE AND SPACE
ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 ELANCOURT Cedex - France
alexandre.mege@airbus.com

***Abstract*—This paper presents a slide attack on the LWC candidate cipher CLX. This attack allows key recovery attack on the primary member CLX-128 cipher with 2^108.5 complexity.**

***Keywords*—LWC, CLX , slide,attack**

I. Introduction

The Cryptography (LWC) Standardization is an ongoing effort coordinated by NIST. Its aim is to standardize a new cryptographic protocol to secure resource constrained devices.

Round 1 of the LWC effort is ongoing, with Round 2 candidates selection expected before September 2019.

Two categories of cryptographic functions are covered by the LWC initiative, an authenticated encryption with associated data (AEAD) primitive and a hash primitive. The LWC minimal security requirement is 2^112 classical computations, and each key shall be able to process at least 2^50-1 Bytes before rekeying is required.

CLX is a round 1 candidate submission for LWC by Hongjun Wu and Tao Huang. The primitive cryptographic function is a permutation created from a Nonlinear Feedback Shift Register.

In the security analysis of CLX, the authors acknowledge that CLX is vulnerable to slide attacks, but that it should not affect its claimed security. This paper presents a slide attack on CLX with impact on CLX-128 claimed security.

II. CLX Round Function

A. Description

CLX is based on a Nonliner Feedback shift register (NFSR). A family of permutations is specified with different security levels. The primary submission is the CLX-128, with a 160 bits permutation.

The processing function for ciphering a block of text with CLX-128 is defined below and shown in *Fig. 1* and *Fig. 2*:

```
/* processing the full blocks of plaintext, each block 32bits*/
    for i from 0 to bmlen=32c:
        $s_{\{68…70\}} = s_{\{68…70\}} \oplus \text{FrameBits}_{\{0…2\}}$
        Update the state using $\mathbf{P_{160,1152}}$
        $S_{\{128…159\}} = s_{\{128…159\}} \oplus m_{\{32i…32i+31\}}$
        $c_{\{32i…32i+31\}} = s_{\{128+x…159+x\}}$
    end for

    $\mathbf{P_{160,1152}}$ => 1152 iterations of StateUpdate(S)
    StateUpdate(S) :
        feedback = $s_0 \oplus s_{35} \oplus (\sim (s_{93} \& s_{106})) \oplus s_{127}$
        for i from 0 to 158: $s_i = s_{i+1}$
        $s_{159}$ = feedback
    end
```

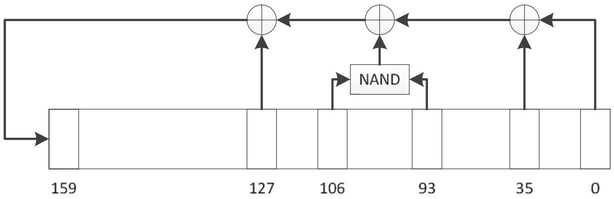

Fig. 1. CLX-128 nonlinear Feedback Shift Register

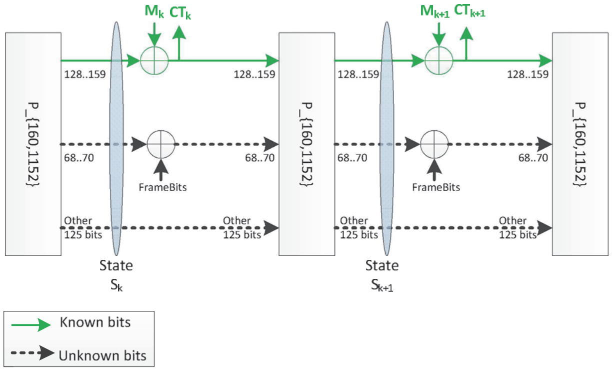

Fig. 2. Two consecutive rounds of CLX-128

B. FrameBits addition

The FrameBits are added at the beginning of every round, before the permutation to some bits of the state. Those FrameBits are meant to provide domain separation and slide protection to the round update.

The slide protection is efficient between two rounds, but it does not protect the inner permutation against slide attack.

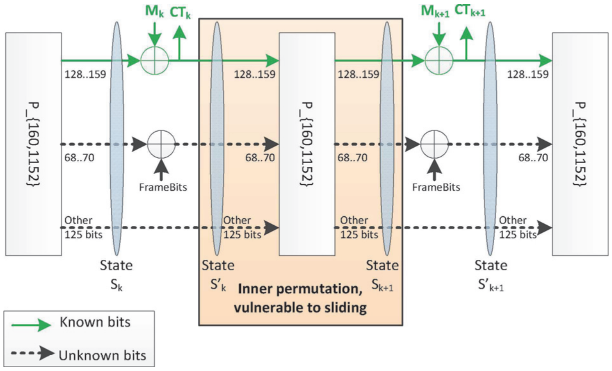

Fig. 3. Inner permutation vulnerable to sliding

C. Analysis of slide property of the permutation

The two following properties are verified by the CLX permutation $\mathbf{P}_{160,1152}$:

Property 1:

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

Property 2:

If the bits 128 to 159 of state S are known, then the bits 128-j to 159-j of $\mathbf{P}_{160,\ j}$ (S) (i.e. the State after j iterations of StateUpdate) are also known (and identical to the former bits) for j from 0 to 128

Combining those two properties leads to:

Property 3:

Knowing the bits 128 to 159 of S and the bits 128 to 159 of $\mathbf{P}_{160,1152}$**(S)**, then the following bits are also known:

- Bits 128-j to 159-j of $\mathbf{P}_{160,j}$ **(S)** are known and equals to bits 128 to 159 of S for j from 0 to 128.
- Bits 128-j to 159-j of $\mathbf{P}_{160,1152}$ **(** $\mathbf{P}_{160,j}$ **(S))** are known and equals to bits 128 to 159 $\mathbf{P}_{160,1152}$(S) for j from 0 to 128.

This property is shown in Fig. 4.

Property 3 allows from 2 consecutive ciphered blocks with known bits to get known bits for 128 additional states $\mathbf{S}_j$ = $\mathbf{P}_{160,j}$ **(S)**.

32 bits are known in $\mathbf{S}_j$ and 32 bits are known in $\mathbf{P}_{160,1152}$($\mathbf{S}_j$).

If the complete internal state of the cipher from one of those 128 states $\mathbf{S}_j$ is known, then the original state S can be recovered by inverting $\mathbf{P}_{160,j}$. Once **S** is known, the initial key can be recovered since CLX provides no key security if the internal state is known.

The additional states reached by the slide property are used in the following slide attack to get more states from the online cipher calls to find a collision with offline computed states.

III. SLIDE-ENHANCED ATTACK ON CLX-128

A. Principle

The slide enhanced attack uses slide property to get more internal states from the online cipher calls than would be accessible within the 2^50 ciphered bytes limit.

Starting from two consecutive rounds of the cipher, 32 bits of the internal state of each round are known. Additional states with known bits can be generated using $\mathbf{P}_{160,1}$ and $\mathbf{P}_{160,-1}$.

For a slide of $\mathbf{P}_{160,j}$ with j in -31 to 31, the number of known bits inside the 32+32 MSB of the two states is 64 - 2×| j |. The remaining 2×| j | bits are unknown.

Figure 5. shows this additional state generation.

B. Attack Implementation

The following attack on CLX-128 uses 2^48 Online calls, 2^108.5 offline cipher calls and 2^108.3 Hashtables lookup.

- **2^48 Online Calls**

Online cipher a message of length 2^50 bytes with known random data. From the resulting Ciphertext, extract the internal state bits 128…159 for each step k and store in **V(k)** for k=0 to (2^48) -1.

From the pair of 32 known state bits from two consecutive steps, extract the 32+32 MSB known state bits. Concatenate in a 64 bits vector and use this vector as key in a hashtable.

Use the slide property to generate more states using $\mathbf{P}_{160,j}$ with a slide window of size 2W+1 (=> j in -W to W).

For the unknown bits in the 32+32 MSB, generate all possible values and store the resulting 64 bit vectors as key in the hashtable.

The number of generated keys for each cipher call is:

$$KeysperCall = \sum_{-W}^{W}(2^{2*W}) \qquad \mathbf{(1)}$$

The number of correct keys per cipher call is:

$$CorrKeysperCall = \ 2*W+1 \qquad \mathbf{(2)}$$

For W =6, the values give

Ciphered Block calls	2^48
Slide Window	-6 to +6
Generated Keys per call	10921
Correct Keys per call	13
Total Keys	2^61.4
Total Correct Keys	2^51.7

- **2^108.5 Offline Calls and lookup table calls**

Generate a random state S and its transform $\mathbf{P}_{160,1152}$**(S).** Concatenate the 32+32 MSB of the two states and check for a collision with the vectors from the online calls in the hashtable.

A collision with a correct key will be found after around 2^(160-51.7) ≈2^108.3 cipher calls and lookup calls.

Of the 2^108.3 hashtable look-ups, around 2^105.7 calls will lead to collisions with correct or invalid keys.

The collisions with invalid keys are filtered by running an additional offline cipher call to validate the result.

The total number of cipher calls is 2^180.3+2^105.7 = 2^108.5 cipher calls.

C. Possible optimisations

The slide property can also be used to generate more 32+32 MSB bit pairs from the offline ciphers calls. This optimization can reduce the number of offline cipher calls, but the total number of operations is not changed, since the same number of look up calls are still required.

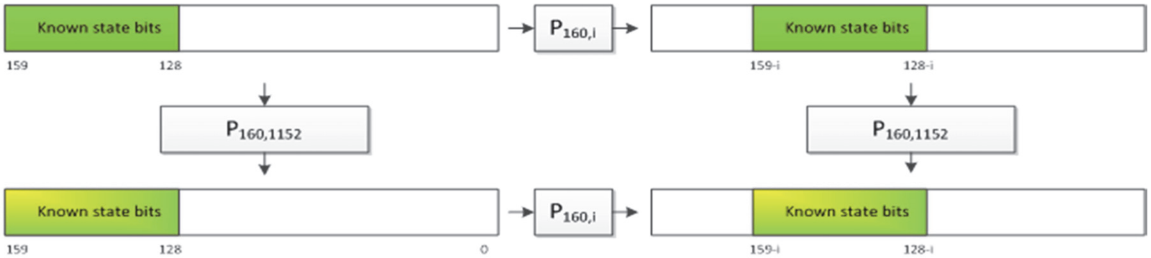

Fig. 4. Slide properties of CLX

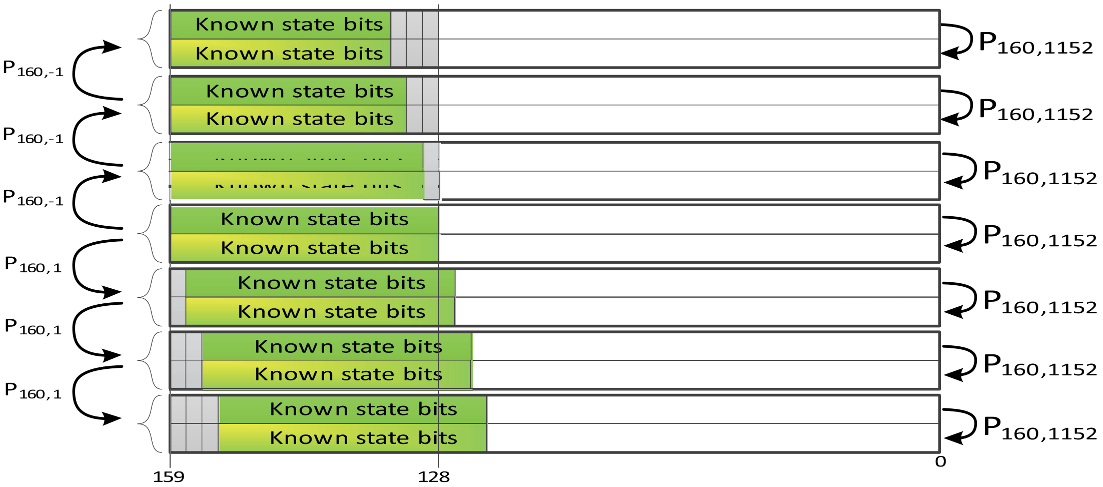

Fig. 5. Using the slide property to generate more pairs of consecutive states with known MSB bits.

D. *Extension to other members of the CLX family*

The attack described in previous chapter for CLX-128 can be extended to the other members of the CLX family, since the only assumptions for the attack are:

- knowledge of 32 bits of the state before and after the permutation during plaintext processing
- the permutation must be susceptible to sliding

The other members of the CLX family have a larger internal state with additional security margin against collisions and slide attacks. The slide attacks for those members require more computations than a brute force attack on the Key and it does not impact the security goal of those members.

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

IV. Demonstration with Reduced Version

To demonstrate the attack a reduced security version of CLX-128 is proposed, with following parameters:

- 40 bits state
- 8 bit rate
- 2^12 max ciphered Byte
- 2^28 bit security goal.

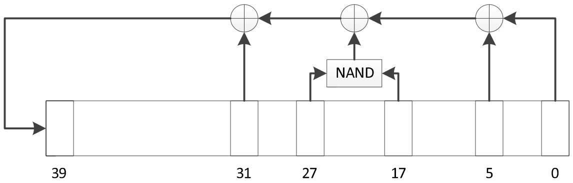

Fig. 6. CLX-32R NFSR

A. *CLX-32R definition*

The feedback function for CLX-32R is defined as
feedback = $s_0 \oplus s_5 \oplus (\sim (s_{17} \& s_{27})) \oplus s_{31}$

```
/* processing the full blocks of plaintext, each block 8bits*/
    for i from 0 to bmlen=8c:
        $s_{\{8...10\}} = s_{\{8...10\}} \oplus FrameBits_{\{0...2\}}$
        Update the state using $\mathbf{P_{40,288}}$
        $S_{\{32...39\}} = s_{\{32...39\}} \oplus m_{\{8i...8i+7\}}$
        $c_{\{8i...8i+7\}} = s_{\{32+x...39+x\}}$
    end for
```

```
$\mathbf{P_{40,288}}$ => 288 iterations of StateUpdate(S)
StateUpdate(S) :
    feedback = $s_0 \oplus s_5 \oplus (\sim (s_{17} \& s_{27})) \oplus s_{31}$
    for i from 0 to 38: $s_i = s_{i+1}$
    $s_{39}$ = feedback
end
```

B. Slide attack on CLX-32R

The attack uses 2^12 Online ciphered Bytes, with a slide window of -1 to 1.

This leads to the following values:

Ciphered Block calls	2^12
Slide Window	-1 to 1
Generated Keys per call	9
Correct Keys per call	3
Total Keys	2^13.6
Total Correct Keys	2^15.2
Mean number of *Offline calls before collision with correct Key with slide attack*	2^26.4
mean number of offline calls to Collision with valid key with standard collision attack	2^28
Total Complexity of slide attack on CLX-32R	2^27.1

C. Measured collision rate

Simulations with 2^12 online cipher calls and 2^33 offline cipher calls were performed and statistics of collision compared to expected values.

	Expected	Measured by simulation
mean number of offline calls to Collision with valid key with standard collision attack	2^28	**2^28.19**
mean number of offline calls to Collision with valid key with slide attack	2^26.4	**2^26.36**
mean number of offline calls to Collision with any key with standard collision attack	16	**16.00**
mean number of offline calls to Collision with any key with slide attack	1. 78	**1.78**

The measure collision rates are coherent with expected values.

V. FUTURE WORK

A. Extend code on CLX-32R to Key recovery

Current code on CLX-32R is limited to collision detection. The final part of the attack with the key recovery is not yet implemented.

B. Study Slide attack on cipher with similar structure

Tini JAMBU is another candidate for LWC from the same team as CLX. It shares many similarities with CLX.
First analysis show that it may be vulnerable to slide attacks.
However, due to the larger internal state (128 bit state + 128 bit key), those attacks are unlikely to impact the claimed security of those ciphers.

ACKNOWLEDGMENT

The author would like to thank the CLX designers Hongjun Wu and Tao Huang for their feedbacks and improvements suggestions on this article, including the impact of FrameBits and the suggestion to use a 40-bits reduced version of CLX for demonstration.

REFERENCES

[1] Hongjun Wu and Tao Huang, “CLX: A Family of Lightweight Authenticated Encryption Algorithms,” LWC round 1 candidate, 29 March 2019