Security Analysis of Beetle and SpoC

Bishwajit Chakraborty, Ashwin Jha and Mridul Nandi

Indian Statistical Institute,Kolkata

6th Nov 2019

Introduction

- NIST's SHA-3 competition had several sponge-based candidates.
- **JH** and **Keccak** were among the five finalists. **Keccak** became the eventual winner.
- **Sponge** based AE: The **duplex** mode.
- More than dozen Submissions in CEASAR Competition.
- **Ascon**, a winner in lightweight applications (resource constrained use-case)

Sponge in lightweight cryptography

- **HASH Functions:** Quark, PHOTON, SPONGENT, sLiSCP etc.
- **AE Schemes:** ASCON , Beetle (sponge-like), SpoC (sponge-like)
- Majority of the NIST submissions are inspired by the **Sponge** paradigm.

Existing Security Bounds of **Sponge** based AE

NOTATION:

- b-bit permutation: split into a c-bit inner state, called the capacity, and an r-bit outer state, called the rate.
- The security of Sponge based AE modes can be represented and understood in terms of two parameters:
  - data complexity D.
  - time complexity T.

Existing Security Bounds of **Sponge** based AE

- The dominating term (in integrity analysis) present in all of the existing analysis of **duplex** authenticated encryption is

$$DT/2^c.$$

- In D decryption attempts we fix rate part of inputs to 0^r and we make T primitive queries with 0^r in top.
- A collision in capacity leads to degeneracy in the next block output of the decryption call.

The Beetle Mode of AEAD

Introducing a combined feedback based absorption/squeezing (similar to the feedback paradigm of CoFB).

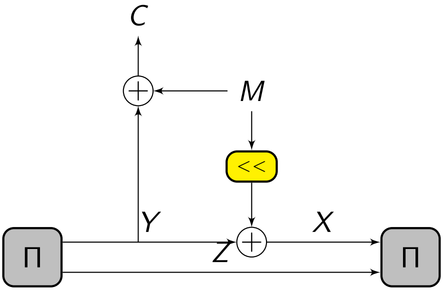


Figure: Beetle Feedback function

Existing Security of The Beetle Mode

- Got rid of the term $DT/2^c$. However,

  1. integrity security up to $DT \ll 2^b$,

$$T \ll \min\{2^{c-\log_2 r},\ 2^r,\ 2^{b/2}\}.$$

- This means that for $c = r = b/2$, the beetle mode achieves close to $(c - \log_2 r)$-bit security.
- Beetle-based schemes requires close to 120-bit capacity and 120-bit rate to achieve NIST LwC requirements.
- Secondary version of PHOTON-Beetle submission has $r = 32$.

The SpoC Mode of AEAD

- Here $b = 192/256, r = 64/128, \kappa = 128$ depending on the two different variations.

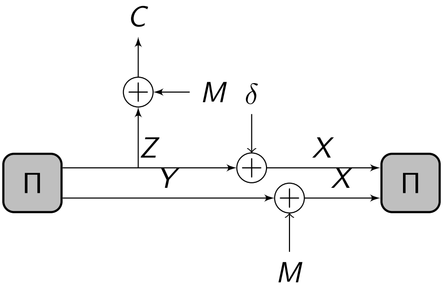


Figure: SpoC Feedback function

Sponge-based AE in Light of NIST LwC Requirement

- In NIST's LwC call for submissions, it is mentioned that the primary AE version should have
  - Data complexity $2^{50} - 1$ bytes
  - Time complexity 2^{112}.
- In order to satisfy these requirements, a traditional **duplex**-based scheme must have a capacity size of at least 160-bit.
- All sponge based submission to NIST LwC standardization process uses 192-bit capacity, except CLX

Multichain Structure

Multi-Chain Structure I

- $\mathcal{L} = ((u_1, v_1), \ldots, (u_t, v_t))$, $u_1, \ldots u_t \in \{0,1\}^b$ are distinct and $v_1, \ldots, v_t \in \{0,1\}^b$ are distinct.
- domain$(\mathcal{L}) = \{u_1, \ldots, u_t\}$ and range$(\mathcal{L}) = \{v_1, \ldots, v_t\}$.
- $L : \{0,1\}^b \to \{0,1\}^b$ (Linear)
- Graph $(V :=$ range$(\mathcal{L}), E)$, where $E = \{v_i \xrightarrow{x} v_j | L(v_i) \oplus x = u_j\}$

- Single Chain: Given $x = (x_1, \ldots, x_k)$ a label walk

$$\mathcal{W} : w_0 \xrightarrow{x_1} w_1 \xrightarrow{x_2} w_2 \cdots \xrightarrow{x_k} w_k.$$

- Simply write $\mathcal{W} = w_0 \xrightarrow{x} w_k$

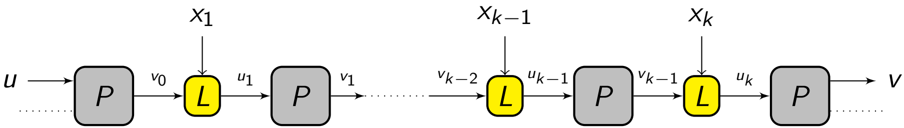


Figure: An element of a k-length multi-chain.

- W_k is the maximum number of chains with (i) same labels and (ii) same top part of the starting and last node.

Multi-Chain Structure III

- $\mathcal{A}$ interacts t times with $\Pi^{\pm}$, obtains $\mathcal{L} = ((u_1, v_1), \ldots, (u_t, v_t))$.
- The following term is appeared in the security analysis:

$$\mu_{k,\mathscr{A}} := \mathsf{Ex}\,[\mathsf{W}_k].$$

$$\mu_{k,t} = \max_{\mathscr{A}} \mu_{k,\mathscr{A}}$$

- $\mathcal{M} \in (\{0,1\}^r)^+$ where r is the rate of Transform-then-Permute.
- Key size $\kappa < b$. Nonce size $b - \kappa$. Tag Size $\tau < b$.

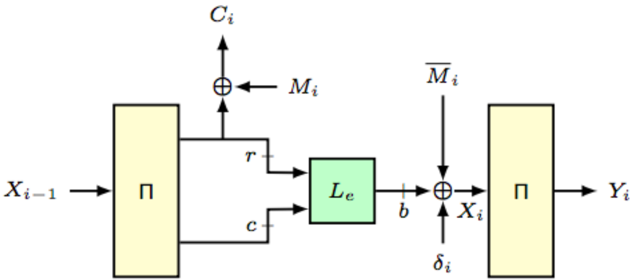


Figure: For decryption we replace L_e by L_d and $\overline{M}_i$ by $\overline{C}_i$.

Security of Transform-then-Permute

Encompasses Beetle, SpoC and many other sponge like constructions.

Theorem

Let, $\mathcal{D}$ denote the set of query indices for decryption queries. Given $\sigma := \sigma_e + \sigma_d \leq q_p$. For any $(q_p, q_e, q_d, \sigma_e, \sigma_d)$-adversary $\mathscr{A}$,

$$\mathbf{Adv}^{\mathrm{aead}}_{\mathrm{TtP}}(\mathscr{A}) \leq \frac{q_p}{2^\kappa} + \frac{2q_d}{2^\tau} + \frac{5\sigma q_p}{2^b} + \frac{rq_p}{2^c} + \sum_{i \in \mathcal{D}} \frac{\mu_{m_i^*, q_p}}{2^c}.$$

Proof Sketch : BAD events I

Bad events due to encryption and primitive transcript (mainly collisions):

B1: Primitive input and Key collision

B2: Primitive and encryption query block output collision

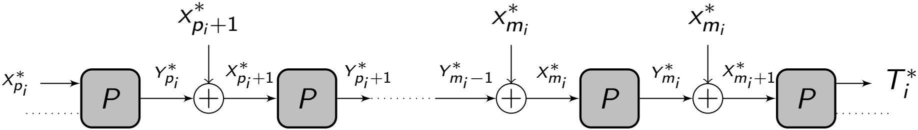
B3: Primitive and encryption query block input collision

B4: Output collision between encryption query blocks

B5: Input collision between encryption query blocks

B6: Bad events due to decryption transcript: Successful forgery.

Proof Sketch : BAD events II



$$v_0^1 \xrightarrow{(x^*_{p_i+1}, \ldots, x^*_{m_i})} v_k^1$$

$$v_0^2 \xrightarrow{(x^*_{p_i+1}, \ldots, x^*_{m_i})} v_k^2$$

- - - - - - - - - - - - - -

$$v_0^j \xrightarrow{(x^*_{p_i+1}, \ldots, x^*_{m_i})} v_k^j$$

- - - - - - - - - - - - - -

Figure: Multi-chains contributing to B6.

Transform-then-Permute with Invertible Feedback

- If L_d is invertible then: If $v_i \xrightarrow{x} v_k$ and $v_j \xrightarrow{x} v_k$ then $v_i = v_j$.
- $\mathrm{W}^{\mathrm{fwd},a} := |\{i : \mathrm{dir}_i = +, \lceil v_i \rceil_\tau = a\}|$; $\mathrm{W}^{\mathrm{fwd}} := \max_a \mathrm{W}^{\mathrm{fwd},a}$
- $\mathrm{W}^{\mathrm{bck},a} := |\{i : \mathrm{dir}_i = -, \lceil v_i \rceil_r = a\}|$; $\mathrm{W}^{\mathrm{bck}} := \max_a \mathrm{W}^{\mathrm{bck},a}$
- $\mathrm{W}^{\mathrm{mitm},a} := |\{(i,j) : \mathrm{dir}_i = +,\ \mathrm{dir}_j = -,\ v_i \oplus u_j = a\}|$; $\mathrm{W}^{\mathrm{mitm}} := \max_a \mathrm{W}^{\mathrm{mitm},a}$

Lemma

For any transcript, we have

$$\mathrm{W}_k \leq \mathrm{W}^{\mathrm{fwd}} + \mathrm{W}^{\mathrm{bck}} + k \cdot \mathrm{W}^{\mathrm{mitm}}.$$

Transform-then-Permute with Invertible Feedback

Theorem

If the feedback function L_d is invertible, then we have

$$\begin{aligned}\mu_{t,k} &\leq \mathsf{Ex}\left[\mathsf{W}^{\mathsf{fwd}}\right] + \mathsf{Ex}\left[\mathsf{W}^{\mathsf{bck}}\right] + k \cdot \mathsf{Ex}\left[\mathsf{W}^{\mathsf{mitm}}\right] \\ &\leq \mathsf{mcoll}(t, 2^{\tau}) + \mathsf{mcoll}(t, 2^{r}) + k \cdot \mathsf{mcoll}'(t^2, 2^{b})\end{aligned}$$

Improved Security Bound for Beetle

- $L_d(x, y) \mapsto (x_2 \oplus x_1, x_1, y)$, where $(x_1, x_2, y) \in \{0,1\}^{r/2} \times \{0,1\}^{r/2} \times \{0,1\}^c$
- Clearly the L_d function is invertible.

Corollary

For $r, \tau, b \geq 16$ and any $(q_p, q_e, q_d, \sigma_e, \sigma_d)$-adversary $\mathscr{A}$, we have

$$\mathbf{Adv}^{\text{aead}}_{\text{Beetle}}(\mathscr{A}) \leq \frac{q_p}{2^\kappa} + \frac{2q_d}{2^\tau} + \frac{5\sigma q_p}{2^b} + \frac{rq_p}{2^c} + \frac{2\tau q_p q_d}{2^b} + \frac{2bq_p^2\sigma_d}{2^{b+c}}.$$

Security Bound for SpoC

- L_d is defined as $L(x, y) \mapsto (x, x\|0^c \oplus y)$, where $(x, y) \in \{0,1\}^r \times \{0,1\}^c$.
- Clearly the L_d function is invertible.

Corollary

For $r, \tau, b \geq 16$ and any $(q_p, q_e, q_d, \sigma_e, \sigma_d)$-adversary $\mathscr{A}$, we have

$$\mathbf{Adv}^{\mathrm{aead}}_{\mathrm{SpoC}}(\mathscr{A}) \leq \frac{q_p}{2^\kappa} + \frac{2q_d}{2^\tau} + \frac{5\sigma q_p}{2^b} + \frac{rq_p}{2^c} + \frac{2\tau q_p q_d}{2^b} + \frac{2bq_p^2\sigma_d}{2^{b+c}}.$$

Conclusion

1. Get rid of restriction on rate (required in the previous analysis of Beetle).
2. Security analysis of SpoC.
3. Unified sponge-like constructions.
4. Understanding tight (integrity) security of sponge is still open.

Thank You!