Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle (ePrint 2022/001, ACNS 2022)

Akiko Inoue, Tetsu Iwata, and Kazuhiko Minematsu

Fifth NIST Lightweight Cryptography Workshop 2022
May 9-11, 2022, virtual event

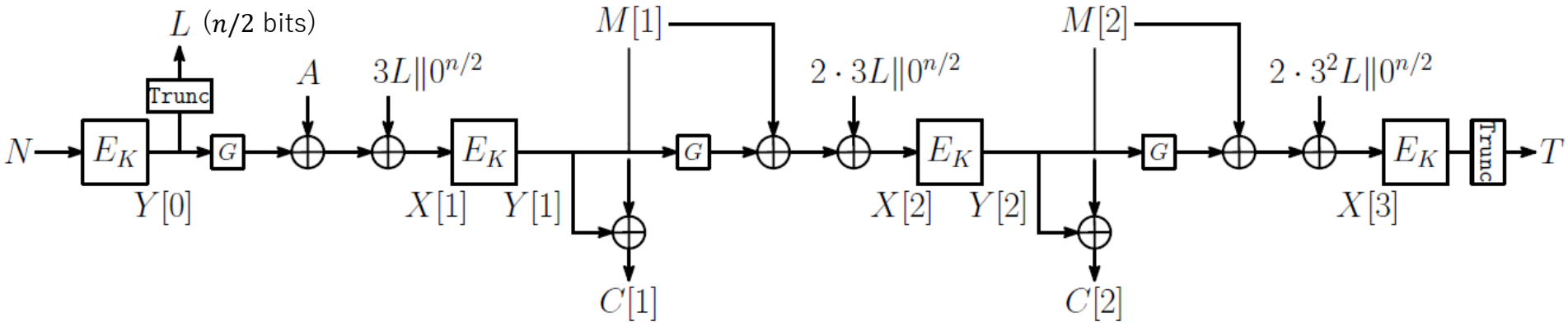
GIFT-COFB and Photon-Beetle

- Two of the finalists
- GIFT-COFB
  - block cipher-based design, GIFT-128 as a primitive
  - uses a combined-feedback mode
  - n/2-bit security in privacy and (n/2-log n)-bit security in authenticity (n = block len.)
- Photon-Beetle
  - permutation-based design, 256-bit permutation Photon as a primitive
  - Beetle mode, Sponge + ρ-function
  - 121-bit security when the rate is 128, and 128-bit security when the rate is 32
- We study the provable security claims of these schemes
  - A privacy attack against GIFT-COFB
  - Two authenticity attacks against Photon-Beetle
  - These attacks do not contradict the bit security claims

GIFT-COFB [BCI+21]

- GIFT-COFB
  - GIFT-128 as a primitive
  - rate 1: 1 block is processed with 1 primitive call
  - small state: 1.5n + key len. (n = block len.)
- E_K: GIFT-128, N: nonce, A: associated data (|A|=n), M: plaintext (|M|=2n), C: ciphertext (|C|=2n), T: Tag

$$G \cdot X := (X[2], X[1] \lll 1) \text{ for } X[1], X[2] \xleftarrow{n/2} X$$

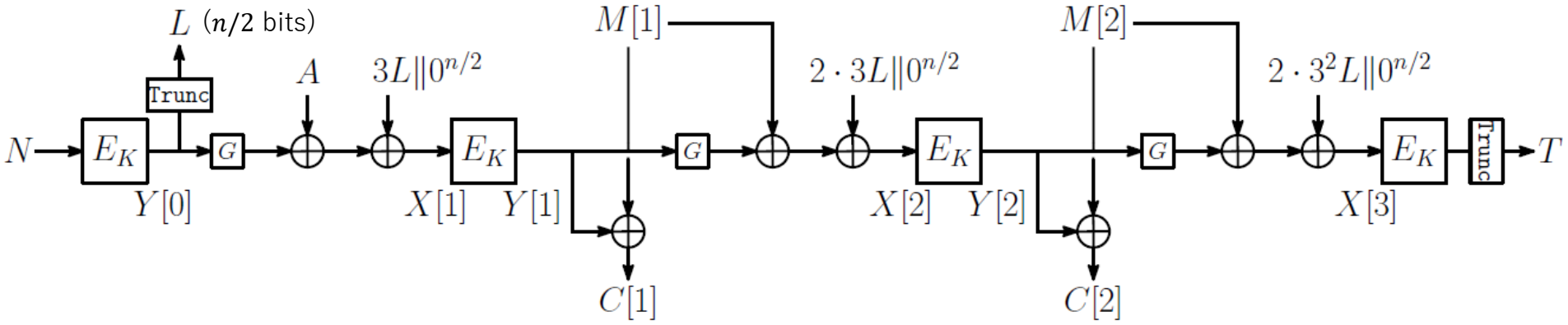


[BCI+21]: Banik, S., Chakrabort, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S., Todo, Y.: GIFT-COFB v.1.1. Submission to NIST LWC

Previous Attacks on COFB Mode

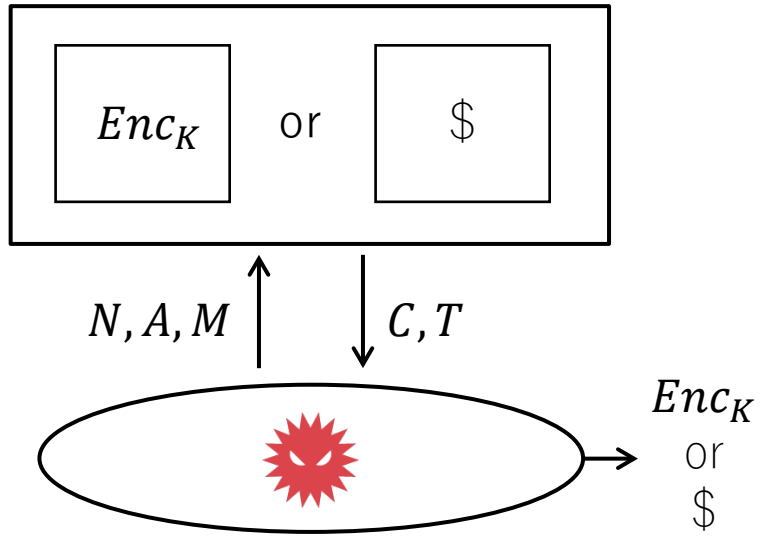
- [Kha20a@FSE20]: authenticity attack based on the fact that masks are zero when L = 0
- [Kha20b]: authenticity attack based on the collision of L
- [Kha21@FSE22]: authenticity attack by guessing the value of L
  - pointed out an error in [CIMN20@JoC20]
- [IM21]: authenticity attack based on a state collision

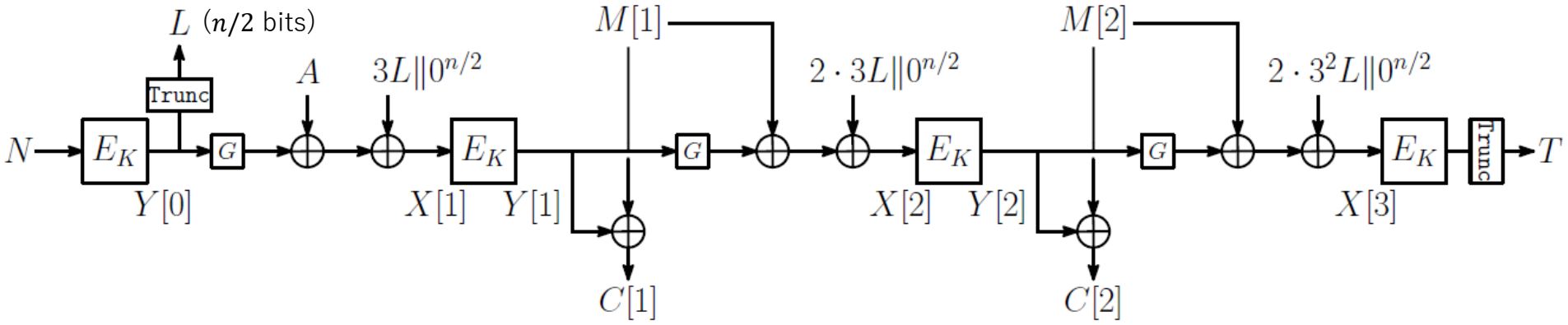
- These results do not contradict the claimed bound in [BCI+21]; show (almost) tightness



Privacy Attack

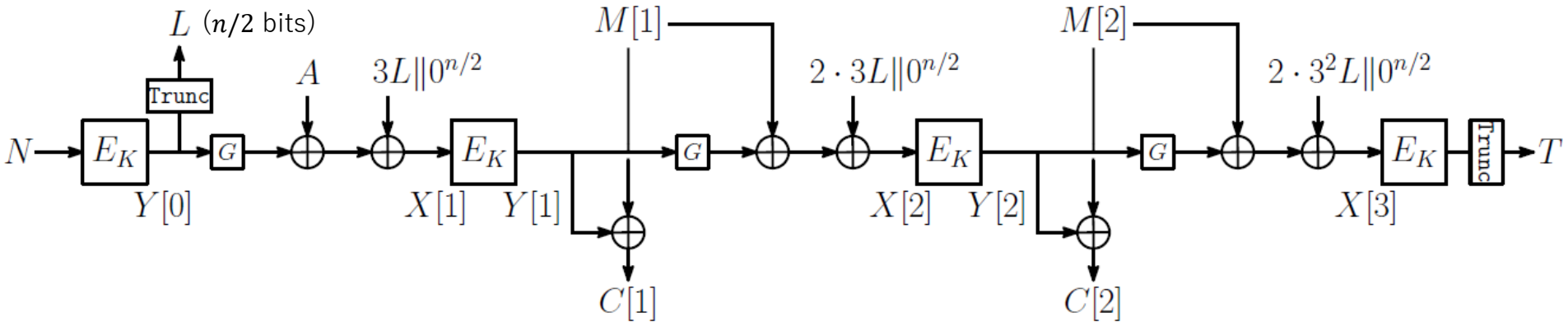
- The goal is to distinguish the encryption oracle Enc_K from $-oracle (random oracle)
- Nonce-respecting adversary





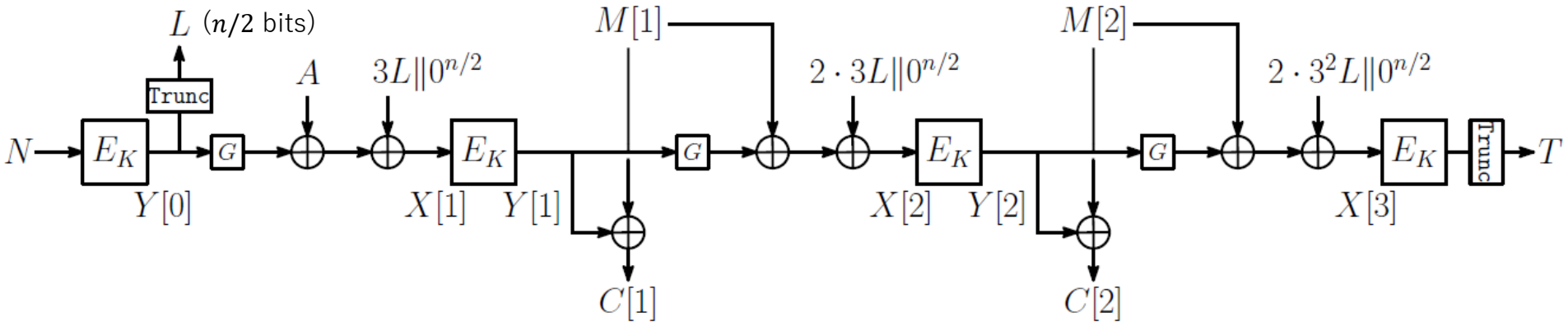
Privacy Attack: Idea

- If the adversary has one input-output pair of E_K, this immediately allows a privacy attack
  - Assume that the adversary has (X, Y) s.t. $E_K(X) = Y$
  - The adversary can use X as a nonce N in an encryption query, $L = \mathrm{msb}_{n/2}(Y)$ is known
  - The adversary can force $X[1] = X$
  - By repeating this, in the real world, the adversary obtains $C[1] = M[1] \oplus Y$ and $C[2] = M[2] \oplus Y$ with prob. 1
  - In the ideal world, $C[1]$ and $C[2]$ are random, the equalities hold with prob. $1/2^{2n}$



Privacy Attack: Procedure

- Make an encryption query (N, A, M) s.t. $|A| = n$ and $|M| = 2n$ to obtain (C, T)
- The adversary can compute $Y[1], Y[2], \mathrm{lsb}_{n/2}(X[2])$, only $\mathbf{msb}_{n/2}(X[2])$ is unknown
- Try all the $2^{n/2}$ possibilities of $\mathbf{msb}_{n/2}(X[2])$ and use $X[2]$ as a nonce to see if the attack in the previous slide works
  - Real world: works with prob. almost 1
  - Ideal world: works with prob. $1/2^{1.5n}$
  - Nonce-respecting condition is maintained (with a high probability)



Implication

- The success prob. is $q/2^{n/2}$ with q encryption queries
  - linear with respect to q, $q \approx 2^{n/2}$ for non-neg. prob.
- The claimed bound in [BCI+21]:

$$\mathbf{Adv}^{\mathrm{AE}}_{\mathrm{COFB}}((q,q_f),(\sigma,\sigma_f),t) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{GIFT}}(q',t') + \frac{\binom{q'}{2}}{2^n} + \frac{1}{2^{n/2}} + \frac{q_f(n+4)}{2^{n/2+1}} + \frac{3\sigma^2 + q_f + 2(q+\sigma+\sigma_f)\cdot\sigma_f}{2^n}$$

- about $q^2/2^n$ if $\sigma_f = q_f = 0$ and $\sigma \approx q$
  - $q^2/2^n < q/2^{n/2}$ when $0 < q < 2^{n/2}$

- The term $q/2^{n/2}$ is needed in the bound

Remarks/Updates from GIFT-COFB Team

- GIFT-COFB team (with Akiko Inoue) has reviewed the proof, confirmed that one bad event was missing in the proof, and confirmed that the proof can be fixed
- The bound can be fixed by adding a term $\sigma/2^{n/2}$:

$$\mathbf{Adv}^{\mathrm{AE}}_{\mathrm{COFB}}((q,q_f),(\sigma,\sigma_f),t) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{GIFT}}(q',t') + \frac{\binom{q'}{2}}{2^n} + \frac{\sigma+1}{2^{n/2}} + \frac{q_f(n+4)}{2^{n/2+1}} + \frac{3\sigma^2 + q_f + 2(q+\sigma+\sigma_f)\cdot\sigma_f}{2^n}$$

- The bit security remains unchanged and unaffected:

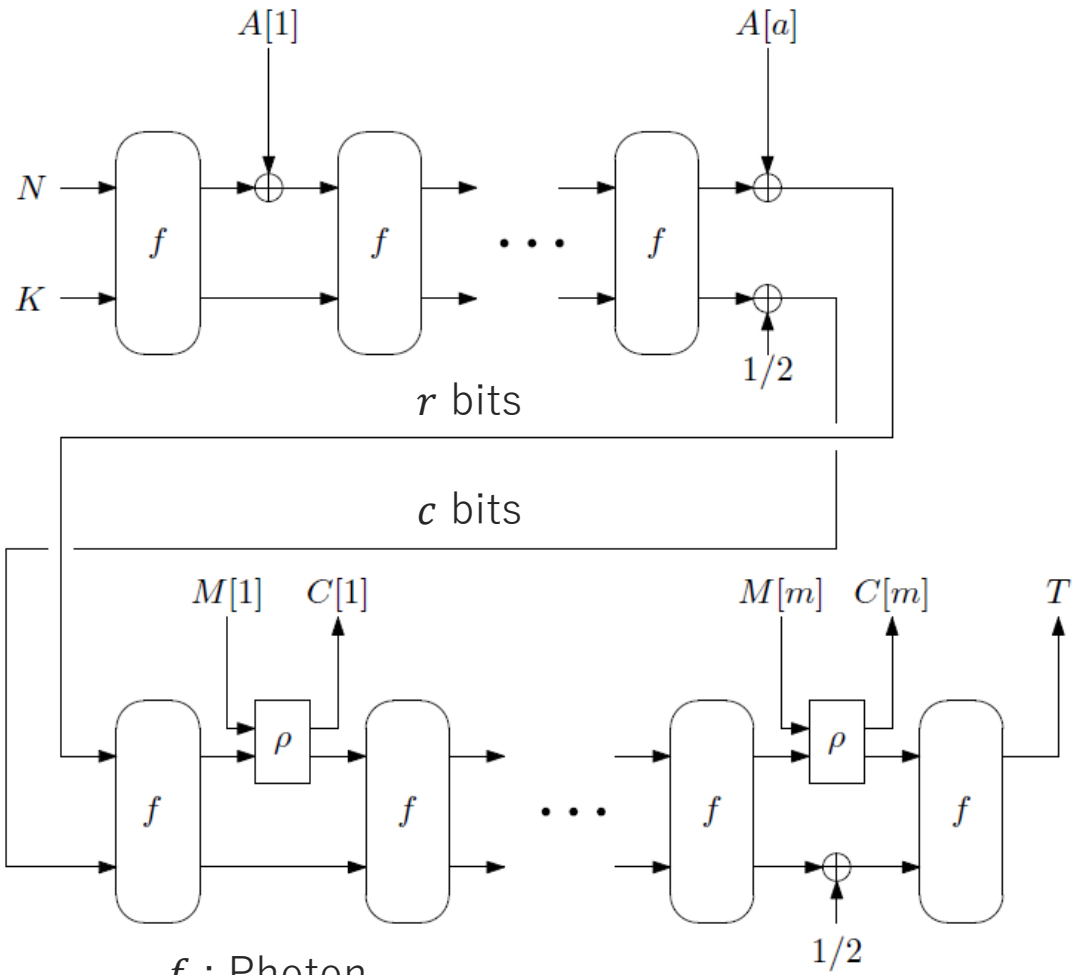
Construction	State Size(bits)	IND-CPA(bits)	INT-CTXT(bits)
GIFT-COFB	192 (excluding the key state)	64	58

- Akiko Inoue now joins the team
- Additional remark:
  - [HZZ19] claims biclique attacks on full-round GIFT
  - The attacks do not work, as detailed in the message sent to NIST ML on May 6, 2022

[HZZ19]: Han, G., Zhao, H., and Zhao, C.: Unbalanced Biclique Cryptanalysis of Full-Round GIFT. IEEE Access, 7:144425–144432, 2019.

Photon-Beetle [BCD+21]

- One of the finalists
- Beetle mode based on Photon
- $r + c = 256$
- Claimed bit security:
  - 121-bit security when $r = 128$
  - 128-bit security when $r = 32$
- Previous analyses on Photon-Beetle
  - [DM20]: key recovery with encryption queries
  - [CJN20]: Provable security result of Sponge-type AE, including Photon-Beetle
  - [Mège21]: Analysis on Photon-Beetle-Hash



[BCD+21]: Bao, Z., Chakraborti, A., Datta, N., Guo, J., Nandi, M., Peyrin, T., Yasuda, K.: PHOTON-Beetle Authenticated Encryption and Hash Family. Submission to NIST LWC

Security Bounds [BCD+21]

- Privacy: $O\left(\frac{\sigma^2}{2^{256}} + \frac{q_p}{2^{256-r}} + \frac{q \cdot q_p}{2^{256}} + \frac{r q_p}{2^{128}} + \frac{\sigma_e^r}{2^{128(r-1)}}\right)$
- Authenticity: $O\left(\frac{q_p(q+q')}{2^{256}} + \frac{r q_p}{2^{128}} + \frac{q_p^r}{2^{128(r-1)}} + \frac{r\sigma'}{2^{256-r}}\right)$
- Authenticity bound in detail:
  - $O\left(\frac{r\sigma'}{2^{256-r}}\right)$ when $q_p = 0$ (i.e., when # of permutation queries is zero)
  - claims that encryption queries have no effect on the authenticity security
    - The first attack invalidates this
  - claims $O\left(\frac{32\sigma'}{2^{224}}\right)$ security when $r = 32$
    - The second attack invalidates this

r: rate

q_p: # of permutation queries

q: # of encryption queries

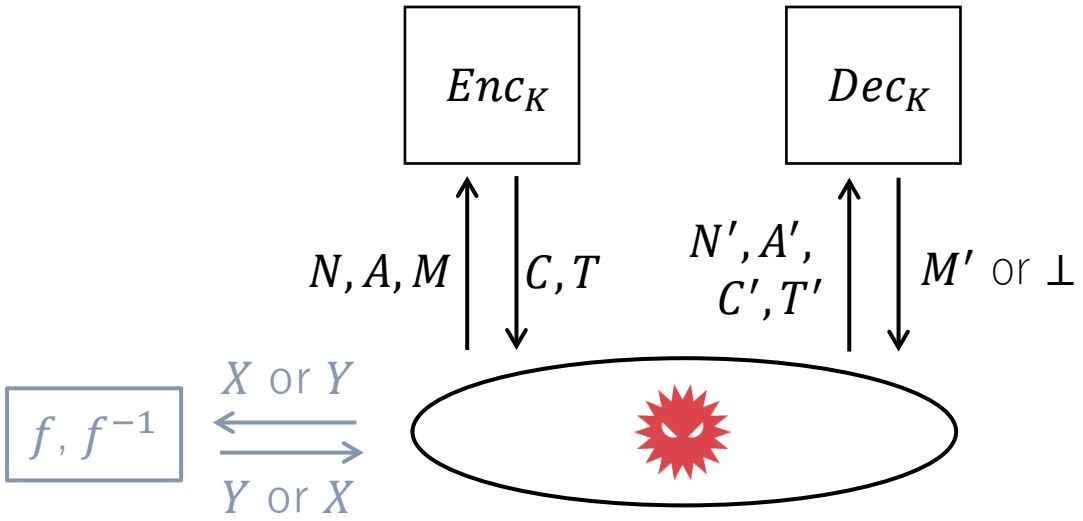
σ, σ_e: # of total blocks in encryption queries

q': # of decryption queries

σ': # of total blocks in decryption queries

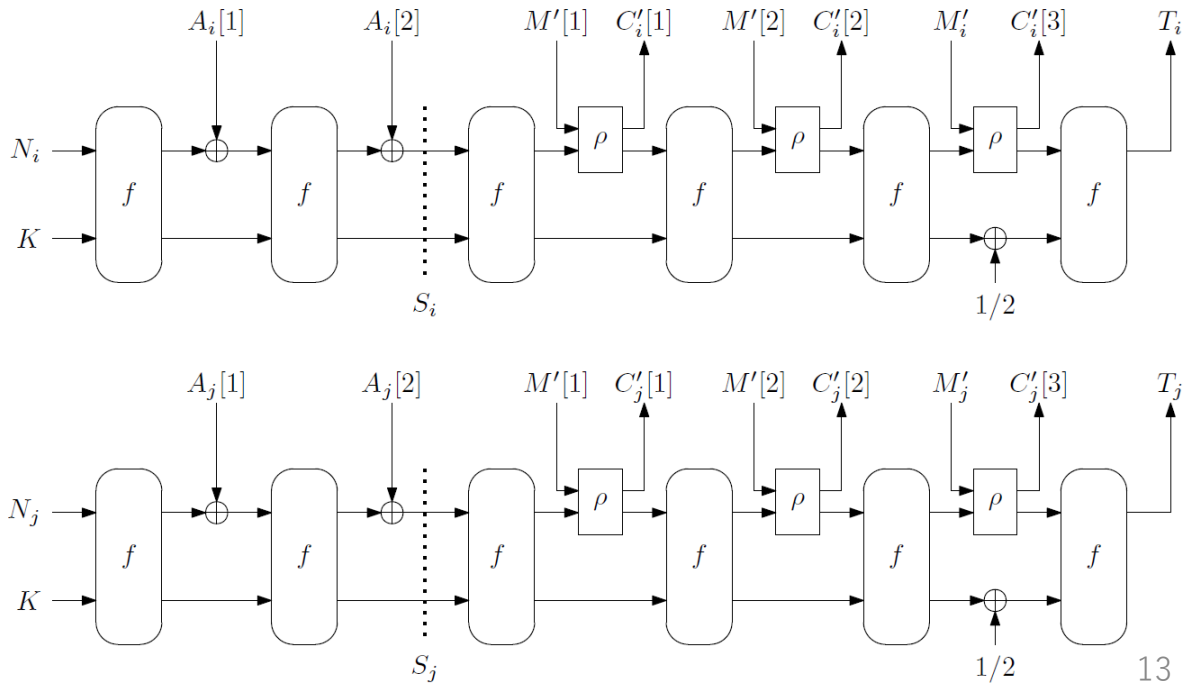
Authenticity Attack

- The adversary has encryption and decryption oracles
  - The adversary also has f and f^{-1} oracles
- The goal is to output a forgery, i.e., the adversary wins if the decryption oracle returns $M' \neq \perp$
- Nonce-respecting adversary with respect to encryption queries



The First Attack ($r = 128$)

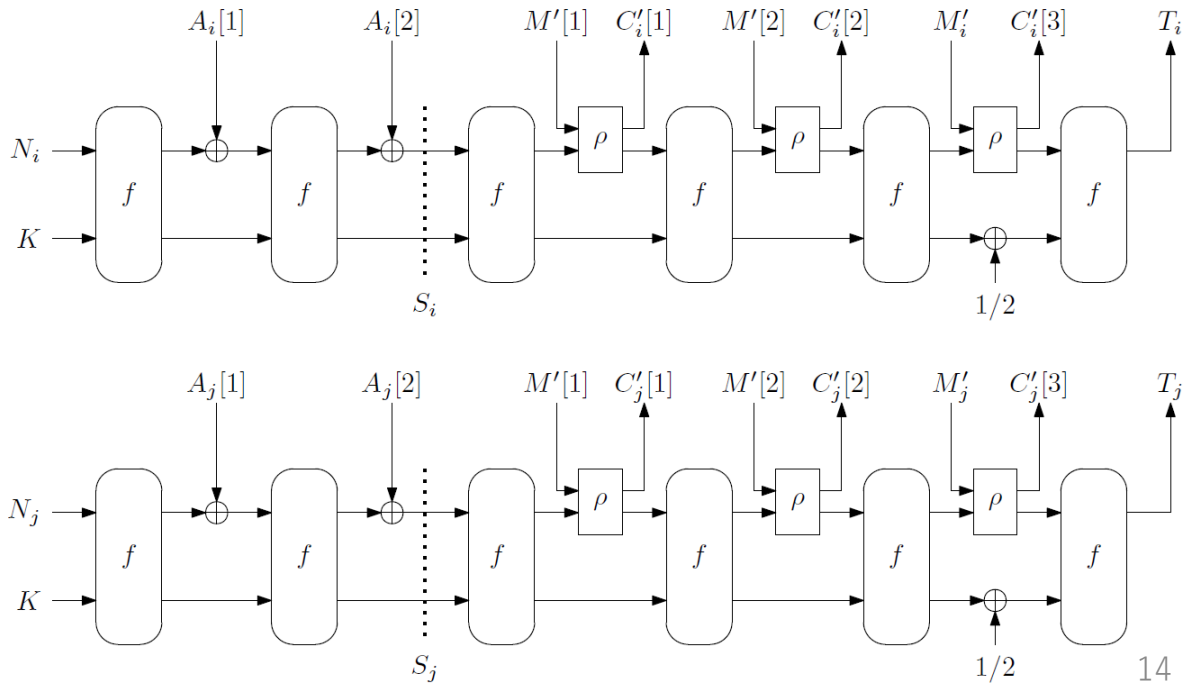
- Let $q = 2^{128}$, make q encryption queries $(N_1, A_1, M_1), \ldots, (N_q, A_q, M_q)$
  - $A_i = A_i[1]||A_i[2] \in \{0,1\}^{2n}$, $M_i = M'[1]||M'[2]||M'_i \in \{0,1\}^{3n}$
  - N_i's are distinct, A_i's are distinct, M'_i's are distinct, $M'[1]||M'[2]$ is fixed
- With a high prob. $S_i = S_j$ for some (i, j)
- This can be detected by seeing if $C'_i[1] = C'_j[1]$ and $C'_i[2] = C'_j[2]$ hold
- (N_i, A_i, C_j, T_j) is a valid forgery
  - (N_j, A_j, C_i, T_i) is also a valid forgery



The First Attack ($r = 128$)

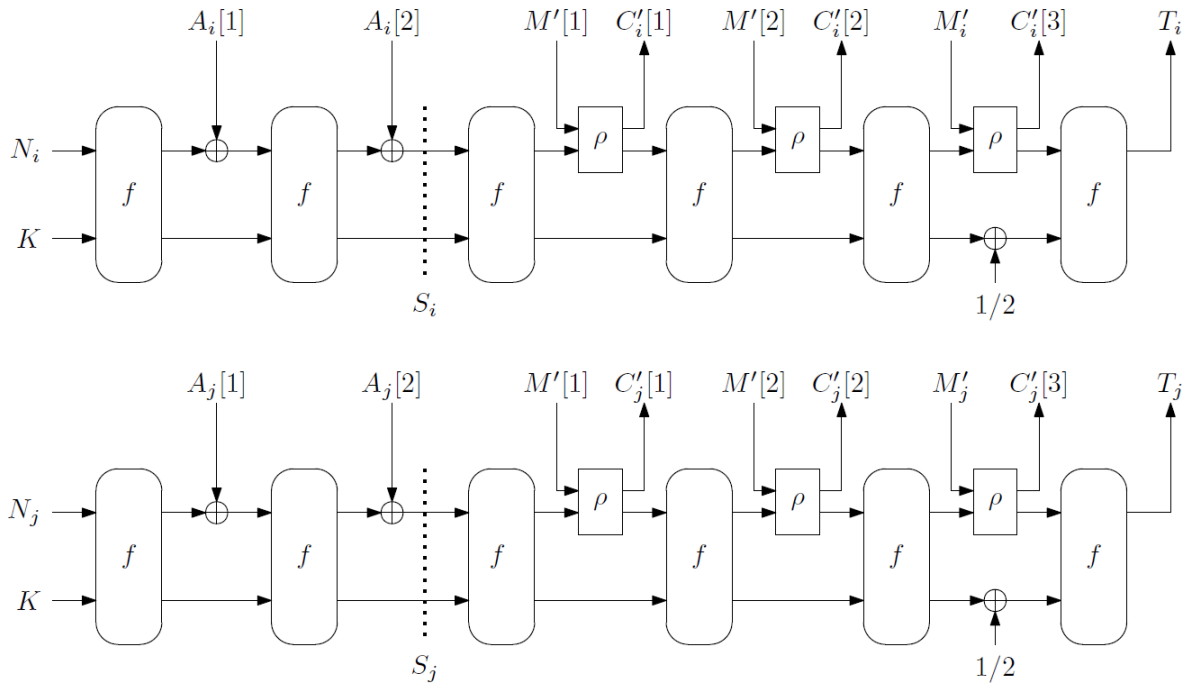
- $C_i'[1] = C_j'[1]$ and $C_i'[2] = C_j'[2]$ may hold without $S_i = S_j$
  - Sufficiently long plaintexts can be used to avoid this
- The same attack works for $r = 32$

- The attack uses 2^{128} encryption queries and one decryption query
  - The success prob. is high
  - The bound in [BCD+21] says the success prob. is $O\left(\frac{r\sigma'}{2^{256-r}}\right)$



The Second Attack ($r = 32$)

- The bound is $O\left(\frac{r\sigma'}{2^{256-r}}\right) = O\left(\frac{32\sigma'}{2^{224}}\right)$ when $r = 32$ and $q_p = 0$
- The tag length is only 128 bits
  - a simple tag guessing:
  - make $q' = 2^{128}$ decryption queries (N, A, C, T_i)
    - for fixed N, A, C and all the 2^{128} possibilities of T_i
  - The success prob. is high
- with q' decryption queries, $\frac{q'}{2^{128}} \gg O\left(\frac{32\sigma'}{2^{224}}\right)$



Implication and Discussion

- These attacks do not violate the bit security of Photon-Beetle
  - 121-bit security when $r = 128$ and 128-bit security when $r = 32$
  - The first attack: 2^{128} encryption queries plus 1 decryption query
  - The second attack: 2^{128} decryption queries
- Outline of the proof in [BCD+21, Sect. 4.2]:

> "Also, if an adversary can obtain a state collision among the input/output of a permutation query with the state of an encryption query or decryption query, it can use the fact to mount an forgery attack."

  - a state collision between encryption queries matters

> "The trivial solution for forging is to guess the key or the tag which can be bounded by $\frac{q+q'}{2^{128}}$."

  - This analysis is fine, but the actual claim of $O\left(\frac{32\sigma'}{2^{224}}\right)$ is much stronger
- A state collision between encryption queries is covered in the privacy bound

Conclusions

- We have investigated the provable security claims in the specification documents of GIFT-COFB and Photon-Beetle
  - A distinguishing attack on GIFT-COFB
  - Two authenticity attacks on Photon-Beetle
- Revised provable security bound of GIFT-COFB
- We remark that the attacks do not invalidate the claimed bit security levels of them

- Additional results
  - Analysis of the provable security treatment of Photon-Beetle in [CJN20]
  - related-key forgery attack on Photon-Beetle

References

- [Kha20a@FSE20]: Khairallah, M.: Weak keys in the rekeying paradigm: Application to COMET and mixFeed. IACR Trans. Symm. Cryptol. 2019(4), 272–289 (2019).
- [Kha20b]: Khairallah, M.: Observations on the tightness of the security bounds of GIFT-COFB and HyENA. Cryptology ePrint Archive, Report 2020/1463 (2020).
- [Kha21@FSE22]: Khairallah, M.: Security of COFB against Chosen Ciphertext Attacks. IACR Trans. Symm. Cryptol. 2022(1), 138–157 (2022).
- [CIMN20@JoC20]: Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M.: Blockcipher-based authenticated encryption: How small can we go? Journal of Cryptology 33(3), 703–741 (Jul 2020).
- [IM21]: Inoue, A., Minematsu, K.: GIFT-COFB is tightly birthday secure with encryption queries. Cryptology ePrint Archive, Report 2021/737 (2021).
- [DM20]: Dobraunig, C., Mennink, B.: Key recovery attack on PHOTON-Beetle. OFFICIAL COMMENT: PHOTON-Beetle (2020).
- [CJN20]: Chakraborty, B., Jha, A., Nandi, M.: On the security of sponge-type authenticated encryption modes. IACR Trans. Symm. Cryptol. 2020(2), 93–119 (2020).
- [Mège21]: Mège, A.: OFFICIAL COMMENT: PHOTON-Beetle (2021).