# Provably Secure Online Authenticated Encryption and Bidirectional Online Channels

Arghya Bhattacharjee, Ritam Bhaumik, Daniel Collins, Mridul Nandi

SAC 2024, Montréal, Québec

# Outline

- Online Authenticated Encryption (OAE)
- Building Block: Tweakable Online Cipher (TOC)
- Generic OAE Construction from TOC
- Bidirectional Online Channels (BOCH)
- Generic BOCH Construction from OAE

# Online Authenticated Encryption (OAE)

# Authenticated Encryption

- Length-expanding encryption mode (variable expansion):
  - enc(k, $\tau$, m) -> c, dec(k, c) -> m
- Combines privacy and integrity in a single ciphertext
- Privacy is measured by pseudorandomness of the output
- Integrity is measured by difficulty of forging
- Usually accepts additional inputs called Associated Data (a)
  - enc(k, $\tau$, a, m) -> c, dec(k, a, c) -> m
- Associated Data doesn't need privacy, but is authenticated

# Online Authenticated Encryption

- Standard Authenticated Encryption often uses a nonce (enc(k, $\tau$, n, m) -> c)
  - Nonce misuse can compromise standard security
  - Nonce misuse-resistant designs are usually slow
- A proposed alternative is Online Authenticated Encryption (OAE)
  - Online property: One-pass encryption *and* decryption
- Pseudorandomness defined w.r.t. ideal *online* permutations/injections
  - Indistinguishable up to common input prefixes
- Different notions of OAE have been proposed

# Tweakable Online Encryption

- Online Ciphers: Encryption and Decryption can be performed online
- Tweakable Online Cipher: Accepts a tweak t as an additional input
  - enc(k, t, m) -> c
- Ideal Behaviour: An independent online cipher for each distinct tweak
- Online-but-last: The last block is not ‘online’ to avoid length-extension attacks

# Our Notion of OAE

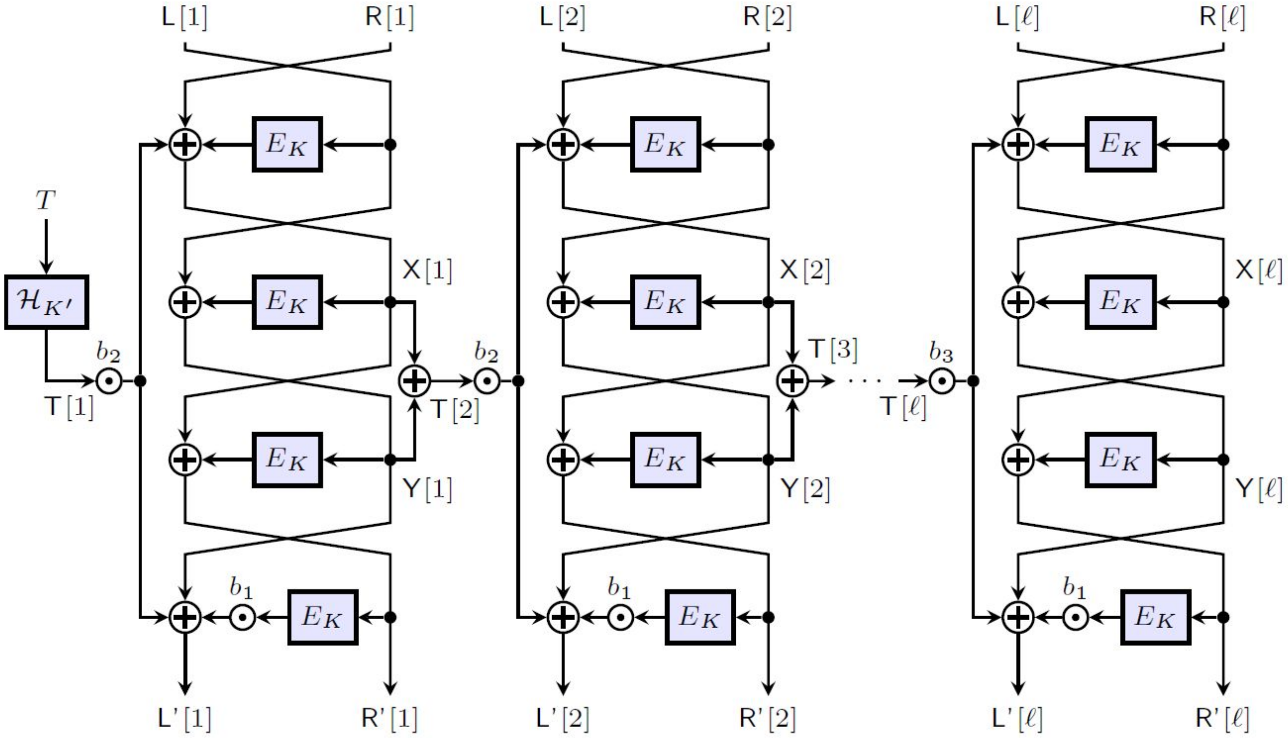
- We keep the length-expansion $\tau$ as a parameter
- Privacy and Integrity games
- Privacy game is played against an ideal tweakable online injective function
- Oracles $\text{Enc}_b$, $\text{Dec}_b$ and $\text{Ver}_b$
  - $\text{Dec}_b$: Release of unverified plaintext (RUP)
- In the Integrity game, a target-expansion $\tau^*$ is fixed for the forging attempt
- Only a successful forgery with expansion $\tau^*$ wins the Integrity game

# Building Block: Tweakable Online Cipher (TOC)

# Tweakable Online Encryption: T-OleF

- Our TOC proposal: t-OleF
- Tweakable variant of the online cipher OleF (Bhaumik & Nandi, ToSC 2016(2))
- Built from a block cipher E and an almost-XOR universal (AXU) hash function H

# t-OleF


L[1]
R[1]
L[2]
R[2]
L[ℓ]
R[ℓ]
T
$\mathcal{H}_{K'}$
$E_K$
$b_2$
$b_2$
$b_3$
$b_1$
T[1]
T[2]
T[3]
T[ℓ]
X[1]
X[2]
X[ℓ]
Y[1]
Y[2]
Y[ℓ]
L'[1]
R'[1]
L'[2]
R'[2]
L'[ℓ]
R'[ℓ]

# Security of t-OleF

- Strong Pseudorandom Tweakable Online Permutation (SPRTOP) security game
  - Strong: Adversary can make evaluation *and* inverse queries
  - Online: Indistinguishable up to common prefixes
- Advantage bound: $7\sigma^2/2^n + 3q^2\epsilon$ + PRF advantage of E
  - $\sigma$: Total number of blocks queried
  - q: Total number of queries (can have q << $\sigma$)
  - $\epsilon$: Universality parameter of H

# Generic OAE Construction from TOC

# Generic OAE Construction

- Encode-then-Encipher based on a Tweakable Online Cipher
- Associated Data is treated as Tweak
- Uses an injective suffix pad $\phi$ to generate a $\tau$-bit expansion on the message
- Expanded message is encrypted using TOC
- For verification, decrypt and check if in range of $\phi$
- Allows flexible choice of $\tau$

# Security of Generic Construction

- Privacy-bound ≤ SPRTOP-security of the underlying TOC
- Integrity-bound ≤ SPRTOP-security of the underlying TOC $+q'/2^{\tau^*}$
  - $q'$: Number of forging attempts
  - $\tau^*$: Target expansion
- Note that the latter bound is only useful for reasonable values of $\tau^*$, say 128.

# OIÆF

- Instantiation of the generic construction with t-OIeF[E, H] as the TOC
- Injective Suffix Pad: 10* = 10000…
- Privacy-bound ≤ $7\sigma^2/2^n + 3q^2\epsilon$ + PRF advantage of E
- Integrity-bound ≤ $7\sigma^2/2^n + 3q^2\epsilon$ + PRF advantage of E + $q'/2^{\tau^*}$
  - $\epsilon$: Universality parameter of H

# Bidirectional Online Channels (BOCH)

# Secure Channels

- We use authenticated encryption to build secure channels in practice
- Naive idea: use two (unidirectional) modes to construct bidirectional channels, and everything is fine
  - Marson and Poettering (ToSC 2017(1)): this is not always true!
- Different settings require different formalisms for channels…

# Bidirectional Online Channels (BOCH)

- Init(L; r) -> ($st_A$, $st_B$)
- Send(m, $\tau$, a, st) -> (c, i, st)
- Receive(c, $\tau$, a, st) -> (i, m)
- Features:
  - Variable expansion, Associated Data as in online AE
  - Stateful (indices), but supports state resets
  - Encryption in batches of L blocks (larger L => less expansion)

# BOCH Correctness

- Online: send(., ., ., st) is a tweakable online injection
- Good-case sequentiality:
  - Indices output when ciphertexts delivered in-order are consistent
- Correctness: For a consistent sequence of send/receive calls:
  - Consider (c, i, $st_P$) <- send(m, $\tau$, a, $st_P$) and (m', i', $st_Q$) <- receive(c, $\tau$, a, $st_Q$) for P != Q
  - Then (i, m) = (i', m')

# BOCH Security

- Monolithic real-or-random security notion
- Adversary can make Send, Receive, Leak and Reset queries for parties A and B
- Leak: captures release of unverified plaintext (RUP) (left-or-right game less natural)
- Reset: reverts a party's state to its original value
- Security:
  - No state reset or out-of-order delivery: Full security
  - Otherwise: At least online security (L-blocks of tweakable online injections)

# Generic BOCH Construction from OAE

# Construction

- Init(L; r) -> ($st_A$, $st_B$): Sample an OAE key, store L
- Send(m, $\tau$, a, st):
  - Uses OAE to encrypt in L block batches
  - OE tweak/OAE associated data: send counter, encryption index, associated data, previous ciphertext, party identifier
    - Previous ciphertext: ‘binds’ L-blocks together
    - Party identifier: can use the same key
- Receive(c, $\tau$, a, st) -> (i, m): Analogous
- Security: follows from OAE privacy and integrity

# Conclusion

# Conclusion

- Explored online authenticated encryption
- Generic construction of OAE
  - Different constructions?
  - Beyond birthday bound security?
- New bidirectional channels primitive
  - Extensions and variants are possible

Paper: https://eprint.iacr.org/2024/1346

# Merci et bon voyage !

# t-OleF: handling incomplete blocks