An Online Authenticated Encryption scheme with an Optimal Single-Keyed Inverse-Free Construction

DIAC 2016, Nagoya, Japan

Ritam Bhaumik and Mridul Nandi

Indian Statistical Institute, Kolkata

27 September 2016

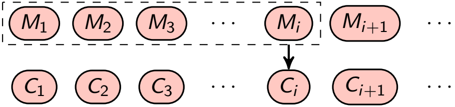
Online Encryption: Authenticated or Otherwise

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**

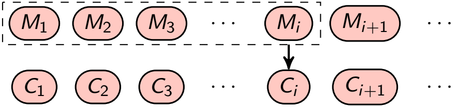
Online Encryption: Authenticated or Otherwise

- **What does Online mean?**



Online Encryption: Authenticated or Otherwise

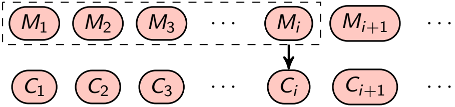
- **What does Online mean?**



  - *i*-th ciphertext block not affected by $(> i)$-th plaintext blocks

Online Encryption: Authenticated or Otherwise

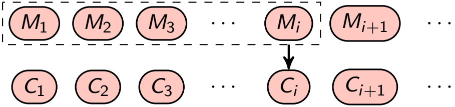
- **What does Online mean?**



  - i-th ciphertext block not affected by ($> i$)-th plaintext blocks
  - this is the classical definition; there can be variants

Online Encryption: Authenticated or Otherwise

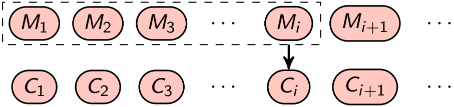
- **What does Online mean?**



  - i-th ciphertext block not affected by $(> i)$-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation

Online Encryption: Authenticated or Otherwise

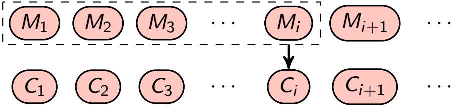
- **What does Online mean?**


M_1 M_2 M_3 $\cdots$ M_i M_{i+1} $\cdots$
C_1 C_2 C_3 $\cdots$ C_i C_{i+1} $\cdots$

  - i-th ciphertext block not affected by $(> i)$-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**

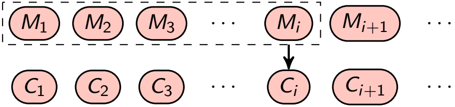


  - i-th ciphertext block not affected by ($> i$)-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

- **Online vs. Full**

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**

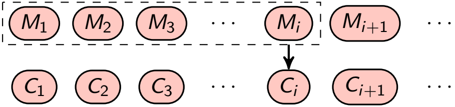


  - i-th ciphertext block not affected by $(> i)$-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

- **Online vs. Full**
  - full encryption only reveals whether two plaintexts are identical

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**

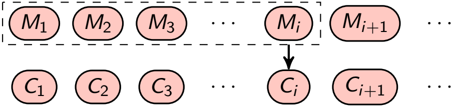


  - i-th ciphertext block not affected by ($> i$)-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

- **Online vs. Full**
  - full encryption only reveals whether two plaintexts are identical
  - online encryption leaks length of common prefix of plaintexts

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**

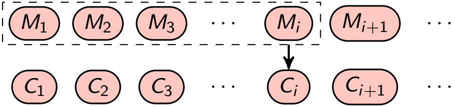


  - i-th ciphertext block not affected by $(> i)$-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

- **Online vs. Full**
  - full encryption only reveals whether two plaintexts are identical
  - online encryption leaks length of common prefix of plaintexts
  - *this is the only security degradation*

Online Encryption: Authenticated or Otherwise

- **What does Online mean?**



  - i-th ciphertext block not affected by $(> i)$-th plaintext blocks
  - this is the classical definition; there can be variants
  - central idea: one-pass computation
  - frequently low-memory as well

- **Online vs. Full**
  - full encryption only reveals whether two plaintexts are identical
  - online encryption leaks length of common prefix of plaintexts
  - *this is the only security degradation*
  - performance often outweighs this degradation

Variants of Online Encryption

Variants of Online Encryption

- **Online-but-last**

Variants of Online Encryption

- **Online-but-last**
    - last block violates online property

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks
  - diblock-online property replaces blocks with diblocks

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks
  - diblock-online property replaces blocks with diblocks
  - necessary for inverse-free constructions

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks
  - diblock-online property replaces blocks with diblocks
  - necessary for inverse-free constructions
- **Tweakable**

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks
  - diblock-online property replaces blocks with diblocks
  - necessary for inverse-free constructions
- **Tweakable**
  - takes an additional input as tweak

Variants of Online Encryption

- **Online-but-last**
  - last block violates online property
  - only reveals length of proper prefixes
  - at least *one full block of randomness* per query
- **Diblock-online**
  - a diblock is a chunk of two blocks
  - diblock-online property replaces blocks with diblocks
  - necessary for inverse-free constructions
- **Tweakable**
  - takes an additional input as tweak
  - each tweak produces a different online permutation

Online Authenticated Encryption Security Game

Online Authenticated Encryption Security Game

- Encryption Query:

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\boxed{\mathrm{Enc}(A, M)}$

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\text{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)
  - $\mathrm{Dec}(A, C) = \perp$ for invalid (A, C)

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)
  - $\mathrm{Dec}(A, C) = \perp$ for invalid (A, C)
  - Real oracle: $\mathrm{Dec}(A, C)$

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\text{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\text{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\text{Enc}(A, M) = C$)
  - $\text{Dec}(A, C) = \perp$ for invalid (A, C)
  - Real oracle: $\text{Dec}(A, C)$
  - Ideal oracle: $\perp$

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)
  - $\mathrm{Dec}(A, C) = \perp$ for invalid (A, C)
  - Real oracle: $\mathrm{Dec}(A, C)$
  - Ideal oracle: $\perp$
- Goals:

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)
  - $\mathrm{Dec}(A, C) = \perp$ for invalid (A, C)
  - Real oracle: $\mathrm{Dec}(A, C)$
  - Ideal oracle: $\perp$
- Goals:
  - *Privacy:* Indistinguishable from $\tilde{\$}$

Online Authenticated Encryption Security Game

- Encryption Query:
  - Real oracle: $\mathrm{Enc}(A, M)$
  - Ideal oracle: $\tilde{\$}(A, M)$
  - $\tilde{\$}$ is a random tweakable online permutation
- Decryption Query:
  - $\mathrm{Dec}(A, C) = M$ for valid (A, C) (i.e., when $\mathrm{Enc}(A, M) = C$)
  - $\mathrm{Dec}(A, C) = \perp$ for invalid (A, C)
  - Real oracle: $\mathrm{Dec}(A, C)$
  - Ideal oracle: $\perp$
- Goals:
  - *Privacy:* Indistinguishable from $\tilde{\$}$
  - *Integrity:* Unforgeable

Remarks

Remarks

- $\mathrm{Enc}(A, \cdot)$ should be injective for each A, for correctness

Remarks

- $\mathsf{Enc}(A, \cdot)$ should be injective for each A, for correctness
- $\mathsf{Enc}(A_1, \cdot)$ and $\mathsf{Enc}(A_2, \cdot)$ should be independent

Remarks

- $\mathrm{Enc}(A, \cdot)$ should be injective for each A, for correctness
- $\mathrm{Enc}(A_1, \cdot)$ and $\mathrm{Enc}(A_2, \cdot)$ should be independent
- $\mathrm{Enc}(A, \cdot)$ should *not* be surjective

Remarks

- $\mathsf{Enc}(A, \cdot)$ should be injective for each A, for correctness
- $\mathsf{Enc}(A_1, \cdot)$ and $\mathsf{Enc}(A_2, \cdot)$ should be independent
- $\mathsf{Enc}(A, \cdot)$ should *not* be surjective
- in fact, range of $\mathsf{Enc}(A, \cdot)$ should only be a small fraction of the co-domain

Remarks

- $\text{Enc}(A, \cdot)$ should be injective for each A, for correctness
- $\text{Enc}(A_1, \cdot)$ and $\text{Enc}(A_2, \cdot)$ should be independent
- $\text{Enc}(A, \cdot)$ should *not* be surjective
- in fact, range of $\text{Enc}(A, \cdot)$ should only be a small fraction of the co-domain
- typically, $\text{Enc}(A, \cdot)$ is a length-expanding function

Remarks

- $\mathsf{Enc}(A, \cdot)$ should be injective for each A, for correctness
- $\mathsf{Enc}(A_1, \cdot)$ and $\mathsf{Enc}(A_2, \cdot)$ should be independent
- $\mathsf{Enc}(A, \cdot)$ should *not* be surjective
- in fact, range of $\mathsf{Enc}(A, \cdot)$ should only be a small fraction of the co-domain
- typically, $\mathsf{Enc}(A, \cdot)$ is a length-expanding function
- integrity equivalent to number of expansion bits

Generic Construction

Generic Construction

- Toolkit:

Generic Construction

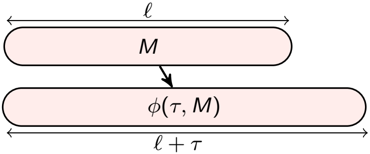
- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher

Generic Construction

- Toolkit:
    - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
    - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding

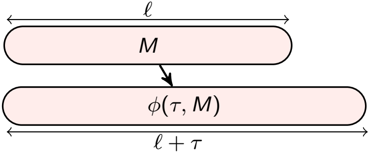
Generic Construction

- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
  - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding



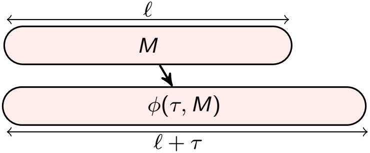
Generic Construction

- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
  - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding
  - e.g., $\phi(\tau, M) = M||0^\tau$



Generic Construction

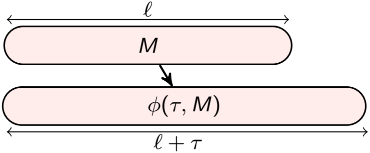
- Toolkit:
  - $P(\cdot,\cdot)$ is a variable input-length tweakable online cipher
  - $\phi(\tau,\cdot)$ is a suitable τ-expanding injective padding
  - e.g., $\phi(\tau, M) = M||0^{\tau}$



- Claim:

Generic Construction

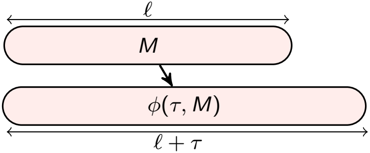
- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
  - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding
  - e.g., $\phi(\tau, M) = M||0^\tau$



- Claim:
  - $\boxed{\tilde{P}_\tau(\cdot,\cdot) = P(\cdot,\phi(\tau,\cdot))}$ is a τ-expanding OAE scheme

Generic Construction

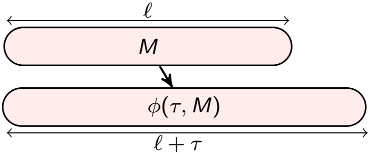
- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
  - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding
  - e.g., $\phi(\tau, M) = M||0^\tau$



- Claim:
  - $\boxed{\tilde{P}_\tau(\cdot,\cdot) = P(\cdot,\phi(\tau,\cdot))}$ is a τ-expanding OAE scheme
  - $\boxed{\tilde{P}(\cdot,\cdot,\cdot) = P(\cdot,\phi(\cdot,\cdot))}$ is a variable-stretch OAE scheme

Generic Construction

- Toolkit:
  - $\boxed{P(\cdot,\cdot)}$ is a variable input-length tweakable online cipher
  - $\boxed{\phi(\tau,\cdot)}$ is a suitable τ-expanding injective padding
  - e.g., $\phi(\tau, M) = M||0^\tau$



- Claim:
  - $\boxed{\tilde{P}_\tau(\cdot,\cdot) = P(\cdot, \phi(\tau,\cdot))}$ is a τ-expanding OAE scheme
  - $\boxed{\tilde{P}(\cdot,\cdot,\cdot) = P(\cdot, \phi(\cdot,\cdot))}$ is a variable-stretch OAE scheme
  - (τ, A, C) is valid when $\boxed{P^{-1}(A, C) \in \text{range of } \phi(\tau,\cdot)}$

Leakage Resilience

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:
  - Real oracle: $\boxed{P^{-1}(A, C)}$

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:
    - Real oracle: $\boxed{P^{-1}(A, C)}$
    - Ideal oracle: $\boxed{\tilde{\$}^{-1}_{\ell+\tau}(A, C)}$

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:
  - Real oracle: $P^{-1}(A, C)$
  - Ideal oracle: $\tilde{\$}^{-1}_{\ell+\tau}(A, C)$
- Leakage-resilience when P is online SPRP (CCA-secure):

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:
    - Real oracle: $P^{-1}(A, C)$
    - Ideal oracle: $\tilde{\$}^{-1}_{\ell+\tau}(A, C)$
- Leakage-resilience when P is online SPRP (CCA-secure):
    - When $P^{-1}(A, C) \notin$ range of $\phi(\tau, \cdot)$, no help in forging

Leakage Resilience

- Another property of recent interest (leakage-resilient/INT-RUP/Robust/Subtle)
- **Leakage model of generic construction**:
  - Real oracle: $P^{-1}(A, C)$
  - Ideal oracle: $\tilde{\$}^{-1}_{\ell+\tau}(A, C)$
- Leakage-resilience when P is online SPRP (CCA-secure):
  - When $P^{-1}(A, C) \notin$ range of $\phi(\tau, \cdot)$, no help in forging
  - By SPRP property, no help in distinguishing attack

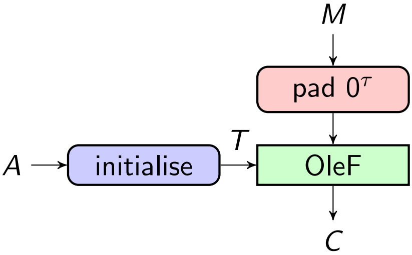
OIAF: An inverse-free OAE scheme

OIAF: An inverse-free OAE scheme

- **Deterministic Diblock-online Authenticated Encryption with Associated Data**

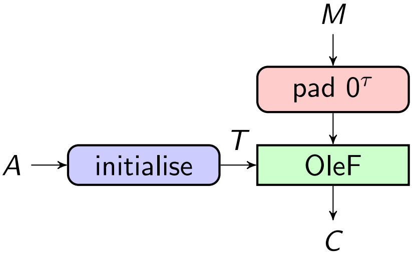
OIAF: An inverse-free OAE scheme

- **Deterministic Diblock-online Authenticated Encryption with Associated Data**



OIAF: An inverse-free OAE scheme

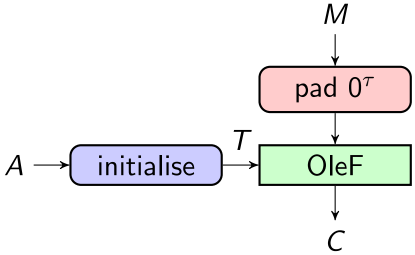
- **Deterministic Diblock-online Authenticated Encryption with Associated Data**



- OIeF is a tweakable (diblock) online cipher

OIAF: An inverse-free OAE scheme

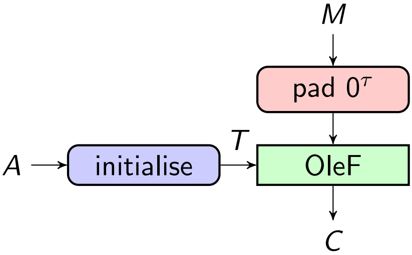
- **Deterministic Diblock-online Authenticated Encryption with Associated Data**



- OIeF is a tweakable (diblock) online cipher
- deterministic (uses no nonce)

OIAF: An inverse-free OAE scheme

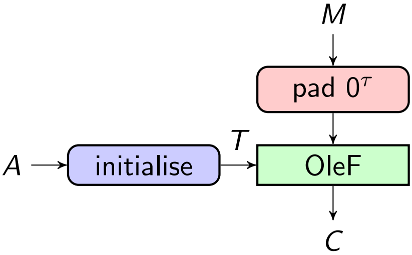
- **Deterministic Diblock-online Authenticated Encryption with Associated Data**



- OIeF is a tweakable (diblock) online cipher
- deterministic (uses no nonce)
- tweak T obtained from associated data A through a PMAC-like construction

OIAF: An inverse-free OAE scheme

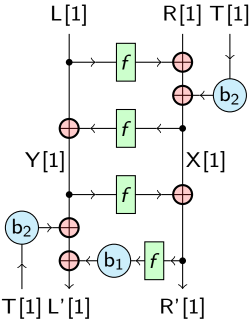
- **Deterministic Diblock-online Authenticated Encryption with Associated Data**



- OIeF is a tweakable (diblock) online cipher
- deterministic (uses no nonce)
- tweak T obtained from associated data A through a PMAC-like construction
- integrity upto $2n$ bits

OleF: A tweakable diblock-online cipher

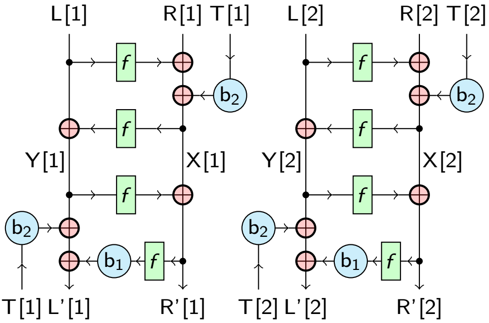
OleF: A tweakable diblock-online cipher



T[1] is the tweak

Figure: Tweakable OleF for ℓ Complete Diblocks

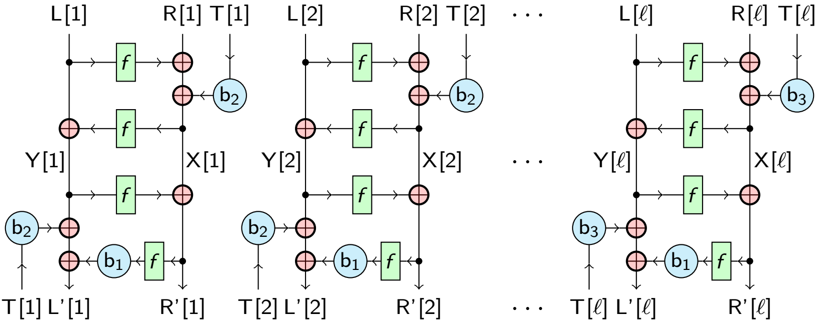
OleF: A tweakable diblock-online cipher



T[1] is the tweak $\qquad$ $T[2] = X[1] \oplus Y[1]$

Figure: Tweakable OleF for ℓ Complete Diblocks

OleF: A tweakable diblock-online cipher



T[1] is the tweak $\quad T[2] = X[1] \oplus Y[1] \quad T[\ell] = X[\ell-1] \oplus Y[\ell-1]$

Figure: Tweakable OleF for ℓ Complete Diblocks

Handling Variable Length Inputs

Handling Variable Length Inputs

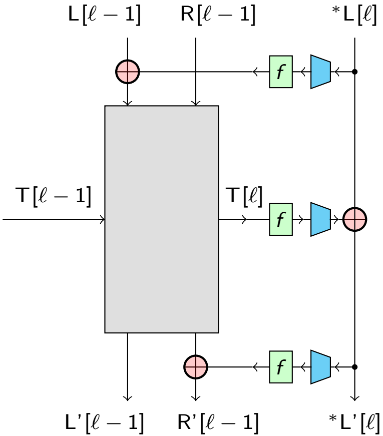


Figure: Tweakable OleF for Partial Diblocks, where $^{*}L[\ell]$ has less than n bits

Handling Variable Length Inputs

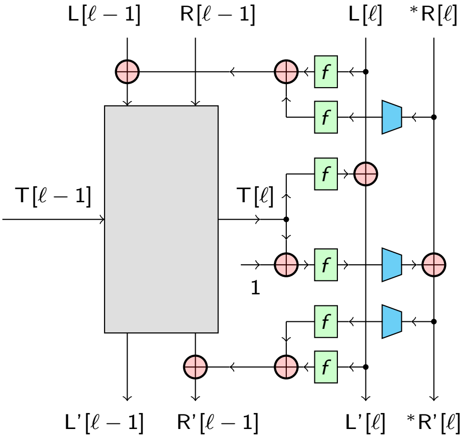


Figure: Tweakable OleF for Partial Diblocks, where $^*\mathsf{R}[\ell]$ has less than n bits

Getting Tweak from Associated Data

Getting Tweak from Associated Data

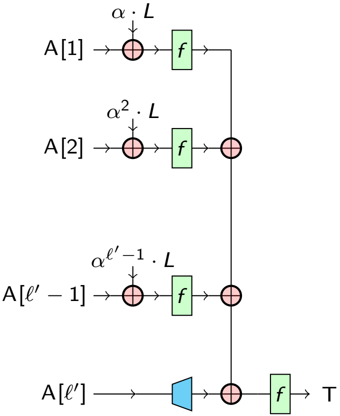
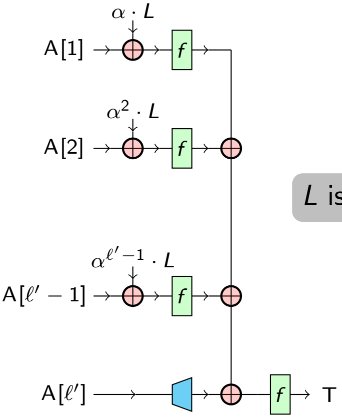


Figure: Obtaining tweak T from Associated Data

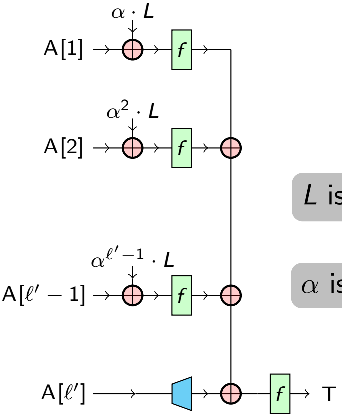
Getting Tweak from Associated Data



L is a masking key, e.g., $L = f(0)$

Figure: Obtaining tweak T from Associated Data

Getting Tweak from Associated Data



L is a masking key, e.g., $L = f(0)$

α is a primitive element

Figure: Obtaining tweak T from Associated Data

Summary of Advantages

Summary of Advantages

- an inverse-free design

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal
- leakage-resilient

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal
- leakage-resilient
- variable-stretch

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal
- leakage-resilient
- variable-stretch
- integrity upto $2n$ bits

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal
- leakage-resilient
- variable-stretch
- integrity upto $2n$ bits
- single-keyed construction

Summary of Advantages

- an inverse-free design
  - does not require E_K^{-1}
  - it is sufficient to have E_K a PRP
  - E_K^{-1} is at times slower
- 2 f-calls per block (for M), which is optimal
- leakage-resilient
- variable-stretch
- integrity upto $2n$ bits
- single-keyed construction
- provably secure

Thank you for your attention.

Judge a man by his questions rather than his answers. [Voltaire]