Introduction to the Accordion Mode and Derived Functions

Alyssa Thompson

June 20, 2024

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

A New NIST Mode of Operation

NIST intends to standardize an *accordion*, or tweakable VIL-SPRP, mode of operation.

This talk: terminology and definitions

- accordion mode
- security goals
- derived functions

More details: "Proposal of Requirements for an Accordion Mode" [2]

Historical Background

The term *accordion mode* may be new, but the work is not ...

- EME [4] and AEZ [6] both use an encrypt-mix-encrypt approach to construct a tweakable SPRP
- HCTR2 [3] and TCT [5] both use a hash-encrypt-hash approach to construct a tweakable SPRP
- Bellare and Rogaway [1] achieved authenticated encryption using the encode-then-encipher approach on an SPRP
- Many other examples exist, these are just a few

Parameters of the Accordion Mode

n	block size of the underlying block cipher
k	length of the secret key
s_{min}	minimum allowed tweak size
s_{max}	maximum allowed tweak size
s	bit-size of a given tweak
g	granularity of allowed message sizes
a	integer: ag is the minimum allowed message size
b	integer: bg is the maximum allowed message size
ℓ	bit-size of a given message
	$\ell \in \{ag, (a+1)g, \ldots, bg\}$

Accordion Mode Notation

$K \in \{0,1\}^k$	secret key
$T \in \{0,1\}^s$	tweak
$M \in \{0,1\}^\ell$	message
$C \in \{0,1\}^\ell$	ciphertext

encryption: $\mathtt{A.enc}(K, T, M) = C$

decryption: $\mathtt{A.dec}(K, T, C) = M$

Accordion Mode Definition

enciphering mode

- length preserving (VIL)
- message space $\mathcal{M} = \bigcup_{\ell \in L} \{0,1\}^{\ell}$
- *enc* : $\mathcal{K} \times \mathcal{M} \to \mathcal{M}$

Accordion Mode Definition

enciphering mode

- length preserving (VIL)
- message space $\mathcal{M} = \bigcup_{\ell \in L} \{0,1\}^{\ell}$
- *enc* : $\mathcal{K} \times \mathcal{M} \to \mathcal{M}$

tweakable enciphering mode

- length preserving (VIL)
- tweak space $\mathcal{T}$ (tweakable)
- *enc* : $\mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$

Accordion Mode Definition

enciphering mode

- length preserving (VIL)
- message space $\mathcal{M} = \bigcup_{\ell \in L} \{0,1\}^\ell$
- *enc* : $\mathcal{K} \times \mathcal{M} \to \mathcal{M}$

tweakable enciphering mode

- length preserving (VIL)
- tweak space $\mathcal{T}$ (tweakable)
- *enc* : $\mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$

accordion mode

- length preserving (VIL)
- tweak space $\mathcal{T}$ (tweakable)
- adaptive CCA model (SPRP)
- *enc* : $\mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$

Security Goal of the Accordion Mode

Challenger $K \xleftarrow{\$} \{0,1\}^k$ and $b \xleftarrow{\$} \{0,1\}$

$\leq q$ times

Distinguisher $\mathscr{D}$ query: encrypt(T, x) or decrypt(T, x)

Challenger, $b = 0$

answer

encrypt: $y \leftarrow \mathtt{A.enc}(K, T, x)$

or

decrypt: $y \leftarrow \mathtt{A.dec}(K, T, x)$

Challenger, $b = 1$

select and remember $\Pi_{T,|x|}$

answer encrypt: $y \leftarrow \Pi_{T,|x|}(x)$

or

decrypt: $y \leftarrow \Pi^{-1}_{T,|x|}(x)$

Distinguisher $\mathscr{D}$ receive: y

Distinguisher $\mathscr{D}$ guess: $b = 0$ or $b = 1$

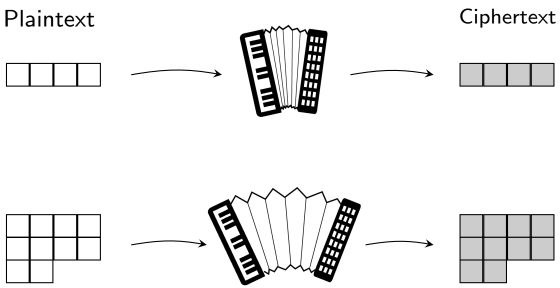
*Advantage of a (q, σ, t)-distinguisher should be negligible.

Accordion Mode Properties

- The accordion “shrinks” or “expands” to match the size of the input

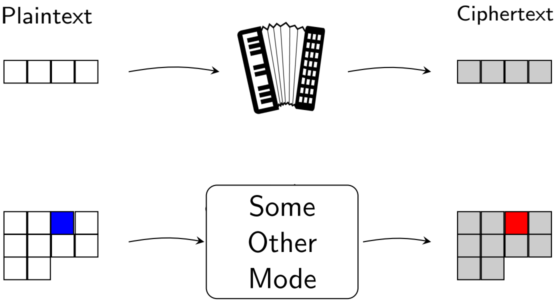
Accordion Mode Properties

- The accordion "shrinks" or "expands" to match the size of the input



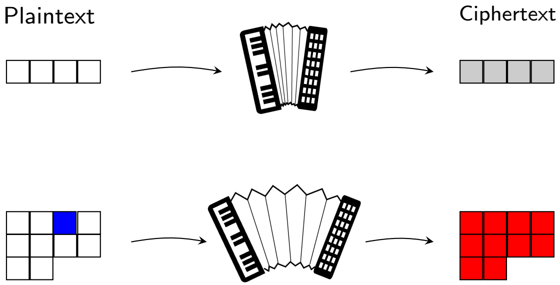
Accordion Mode Properties

- The accordion "shrinks" or "expands" to match the size of the input



Accordion Mode Properties

- The accordion “shrinks” or “expands” to match the size of the input



- Any change to the inputs has a randomizing effect on the outputs

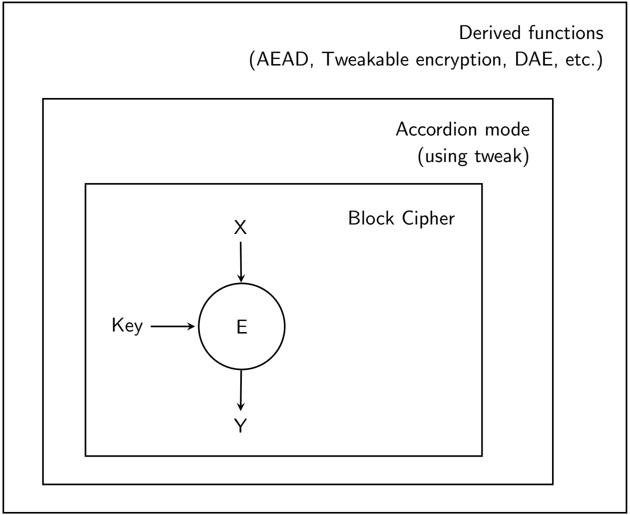
Why an accordion?

An accordion ...

- can achieve better security properties and additional features compared to current NIST standards
  - robust, length preserving
  - nonce misuse resistance, short tags, key commitment
- operates on an underlying block cipher
  - simplifies security analysis
  - can take advantage of AES instructions
- has a solid base of existing research and development
  - exact match does not necessarily exist (yet)

Derived Functions

- called by an application
- encodes the inputs to the accordion mode
- no crypto



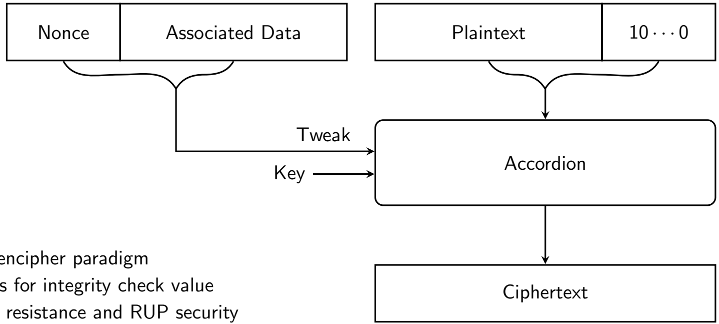
Derived Functions

Authenticated Encryption with Associated Data

Applications:	anywhere AEAD is used today ex - TLS, IPsec, SSH
Inputs:	nonce N, associated data AD
Parameters:	$\tau =$ number of authentication bits
Security Goal:	$\leq 2^{-\tau}$ probability of forging

Derived Functions

Authenticated Encryption with Associated Data



- encode-then-encipher paradigm
- τ or more bits for integrity check value
- nonce-misuse resistance and RUP security
- variable length, relatively long tweaks

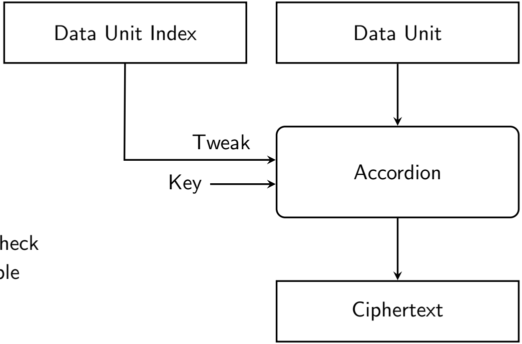
Derived Functions

Tweakable Encryption

Applications:	storage encryption
Inputs:	tweak T
Parameters:	same as accordion
Characteristics:	supports no ciphertext expansion
	$\Longrightarrow$ small granularity useful

Derived Functions

Tweakable Encryption



- no authentication/integrity check
- key-dependent input is possible
- tweak will change often

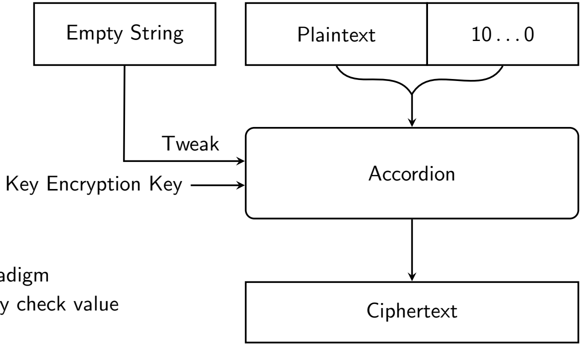
Derived Functions

Deterministic Authenticated Encryption

Applications:	key wrapping
Inputs:	fixed (or empty) tweak
Parameters:	$\tau =$ number of authentication bits
Security Goal:	$\leq 2^{-\tau}$ probability of forging

Derived Functions

Deterministic Authenticated Encryption



- encode-then-encipher paradigm
- τ or more bits for integrity check value
- support for empty tweak

Feedback Wanted

- Accordion mode - any general comments?
- Do the three derived functions cover the needed applications?
- Comments on the constructions for the derived functions. Others ideas to consider?
- Other comments on this content?

Proposed requirements, additional features and more to come.

References

[1] Mihir Bellare and Phillip Rogaway. "Encode-Then-Encipher Encryption: How to Exploit Nonces or Redundancy in Plaintexts for Efficient Cryptography". In: *Advances in Cryptology — ASIACRYPT 2000*. Ed. by Tatsuaki Okamoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 317–330. ISBN: 978-3-540-44448-0.

[2] Yu Long Chen et al. *Proposal of Requirements for an Accordion Mode: Discussion Draft for the NIST Accordion Mode Workshop 2024*. National Institute of Standards and Technology, Workshop Discussion Draft. 2024. URL: https://csrc.nist.gov/files/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd/docs/proposal-of-requirements-for-an-accordion-mode-discussion-draft.pdf.

[3] Paul Crowley, Nathan Huckleberry, and Eric Biggers. *Length-preserving encryption with HCTR2*. Cryptology ePrint Archive, Paper 2021/1441. 2021. URL: https://eprint.iacr.org/2021/1441.

[4] Shai Halevi and Phillip Rogaway. "A Parallelizable Enciphering Mode". In: *Topics in Cryptology – CT-RSA 2004*. Ed. by Tatsuaki Okamoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 292–304. ISBN: 978-3-540-24660-2.

[5] Thomas Shrimpton and R. Seth Terashima. "A Modular Framework for Building Variable-Input-Length Tweakable Ciphers". In: *Advances in Cryptology - ASIACRYPT 2013*. Ed. by Kazue Sako and Palash Sarkar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 405–423. ISBN: 978-3-642-42033-7.

[6] Phillip Rogaway Viet Tung Hoang Ted Krovetz. *AEZ v5: Authenticated Encryption by Enciphering*. 2017. URL: https://www.cs.ucdavis.edu/~rogaway/aez/aez.pdf.