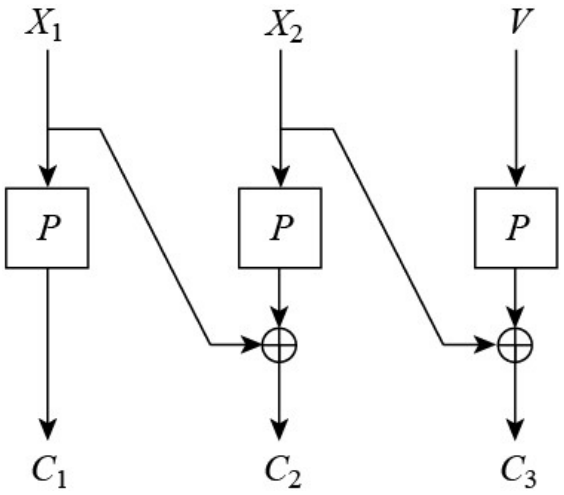
iFeed: the Input-Feed AE Modes

Liting Zhang
Joint work with Wenling Wu, Han Sui and Peng Wang
TCA @ ISCAS
ASK 2013 @ SDUW
2013.08.28

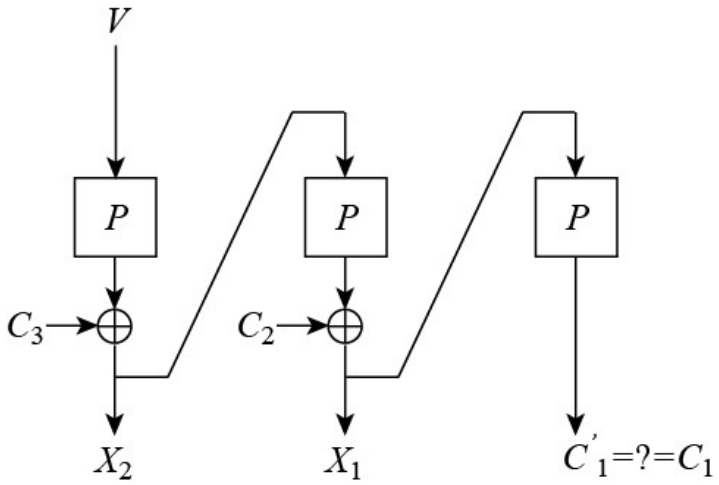
Outline

- Review of AEs
- Basic iFeed Construction
- iFeed AE Modes
- Wrap Up

Basic iFeed Construction



parallel encryption

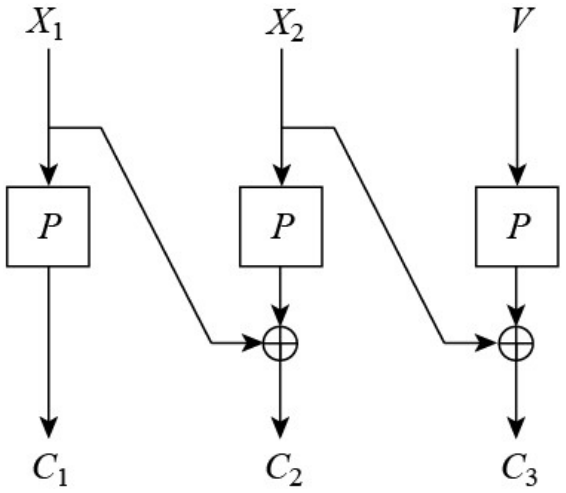


serial decryption

- V is an extra value
- Inputs to P should be pairwise distinct & SECRET

Basic iFeed Construction

- In encryption

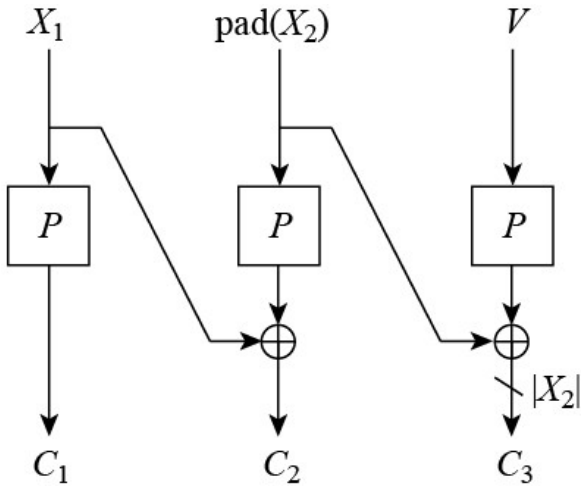


- Privacy for X_1 X_2
- Authenticity for X_1 X_2

Closely combine Privacy and Authenticity

Basic iFeed Construction

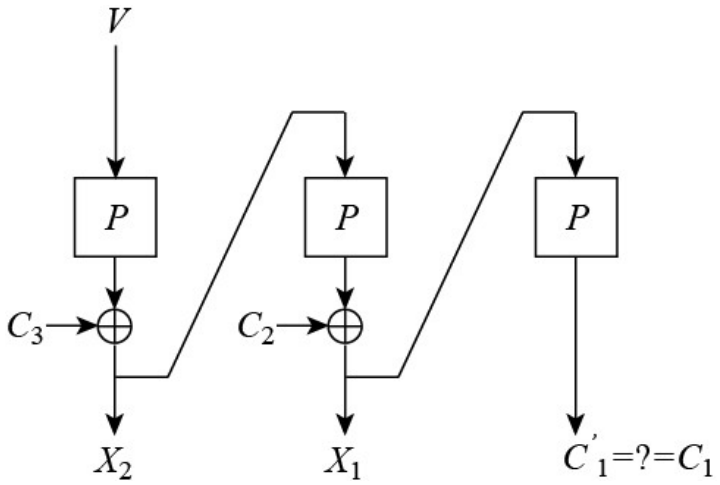
- In encryption



- For incomplete messages
  - pad the last plaintext block --- online
  - truncate the last ciphertext block

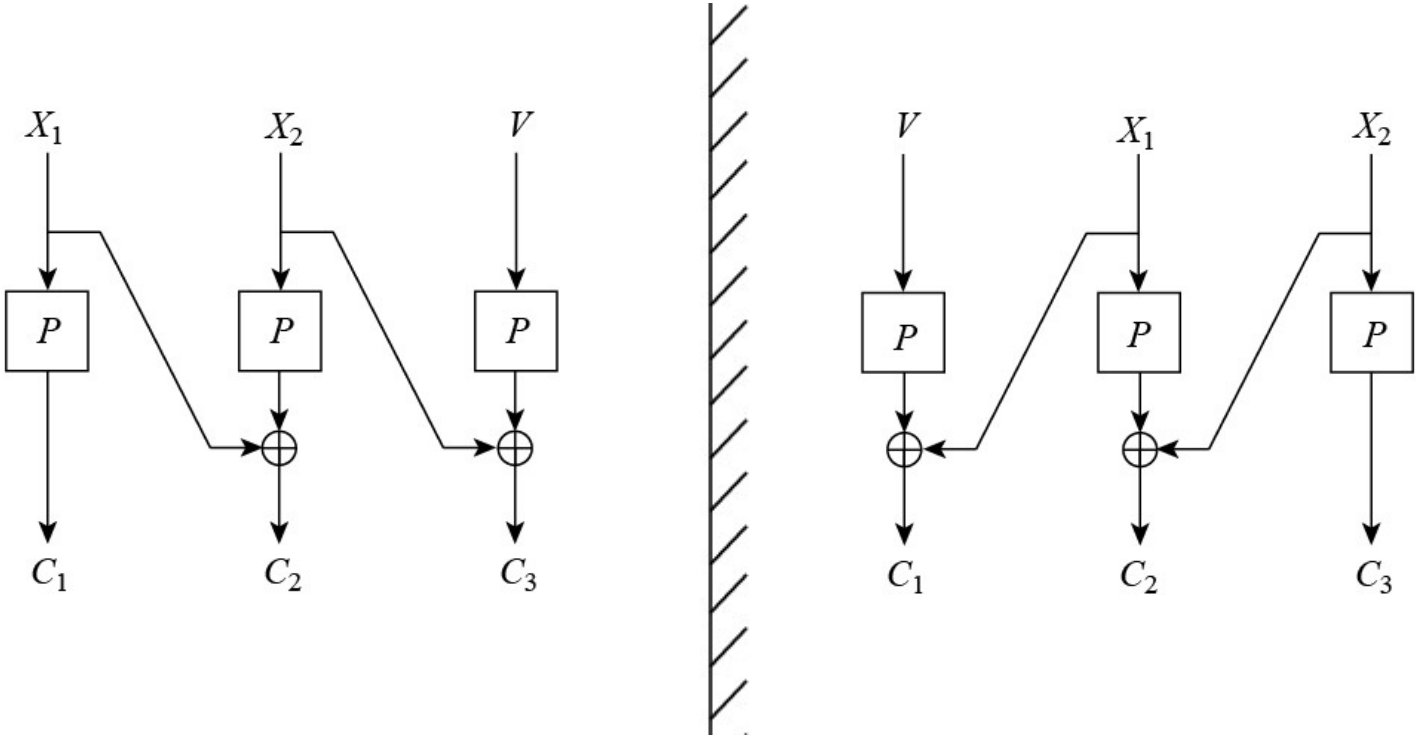
Basic iFeed Construction

- In decryption



- Offline --- start with the last block
- Authentication at last

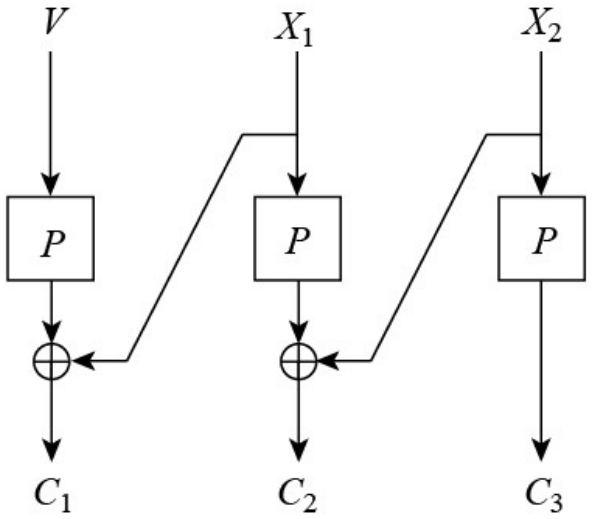
iFeed Basic in a Mirror

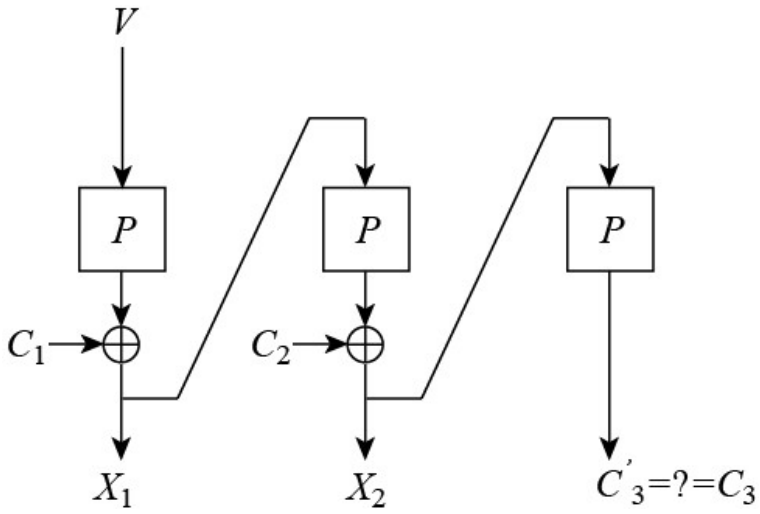


iFeed Basic

Mirrored iFeed Basic

Mirrored iFeed Basic



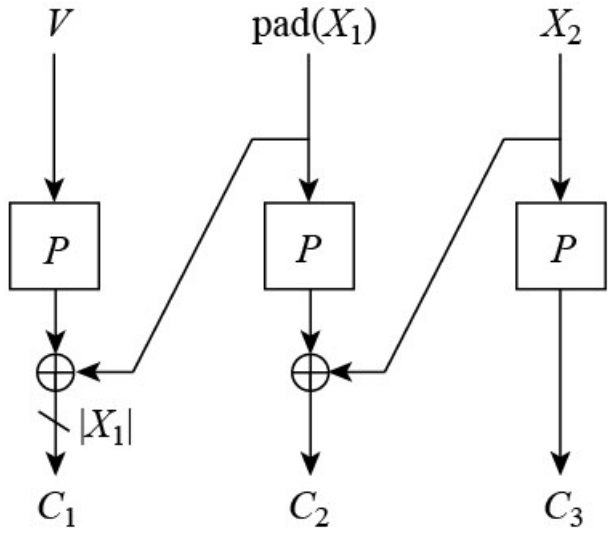


parallel encryption serial decryption

- Online decryption --- start with C_1

Mirrored iFeed Basic

- In encryption



- For incomplete messages
  - pad the first plaintext block → offline
  - truncate the first ciphertext block

Summary of iFeed Basic

- One-pass
- closely combine Priv and Auth
- inverse-free
  - PRP not SPRP on P
  - We can replace P with compression function CF or tweakable blockcipher TBC
- Parallel encryption, but serial decryption

Summary of iFeed Basic

	Online encryption	Online decryption
iFeed Basic	yes	no
Mirrored iFeed Basic	no	yes

- Online/offline encryption affects little
  - The sender knows the plaintext lengths --- usually has full messages in hand

Summary of iFeed Basic

	Online encryption	Online decryption
iFeed Basic	yes	no
Mirrored iFeed Basic	no	yes

- Online/offline decryption is
  - Important --- decrypting on-the-fly
  - Offline can be solved --- if the sender sends from the last ciphertext block

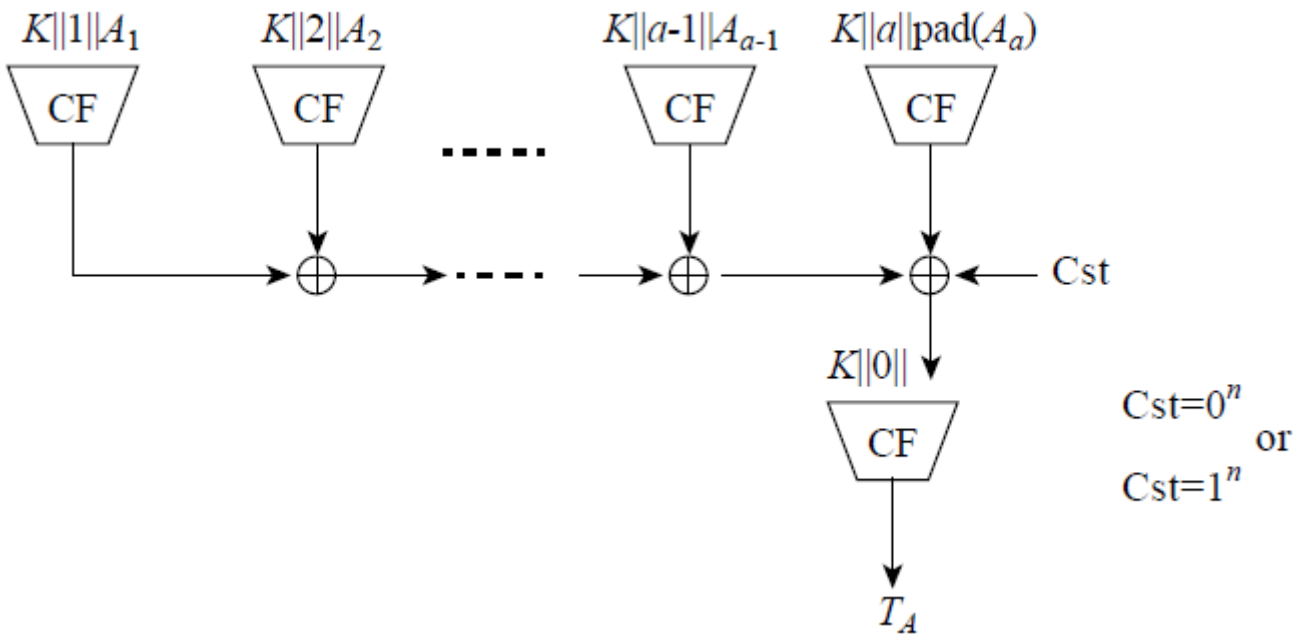
Outline

- Review of AEs
- Basic iFeed Construction
- iFeed AE Modes
- Wrap Up

Applying iFeed Basic

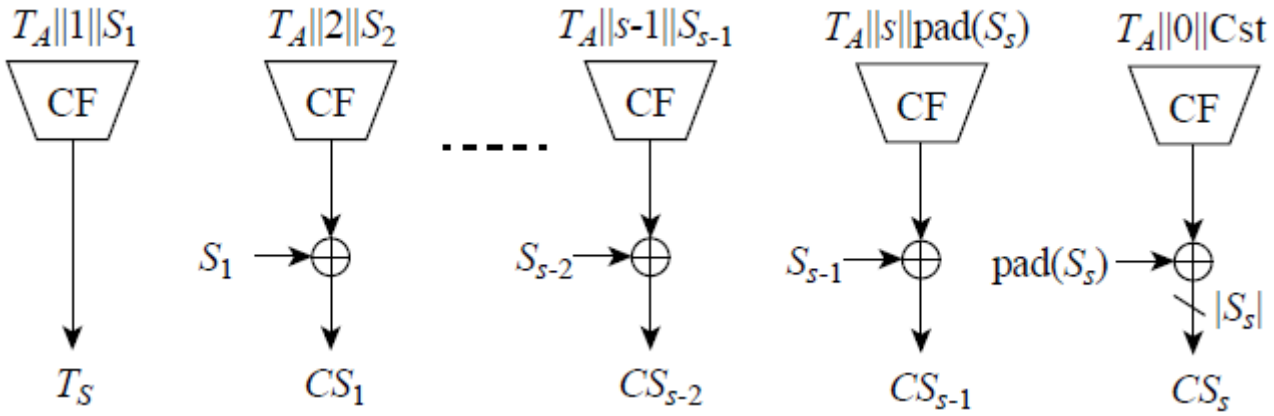
- Keep the inputs to P, CF and TBC pairwise distinct & SECRET
  - Generating secret masks XORed to the inputs to P
  - Carefully formatting the inputs to CF or TBC
- Process associated data
  - Introducing a MAC

The iFeed AE Mode



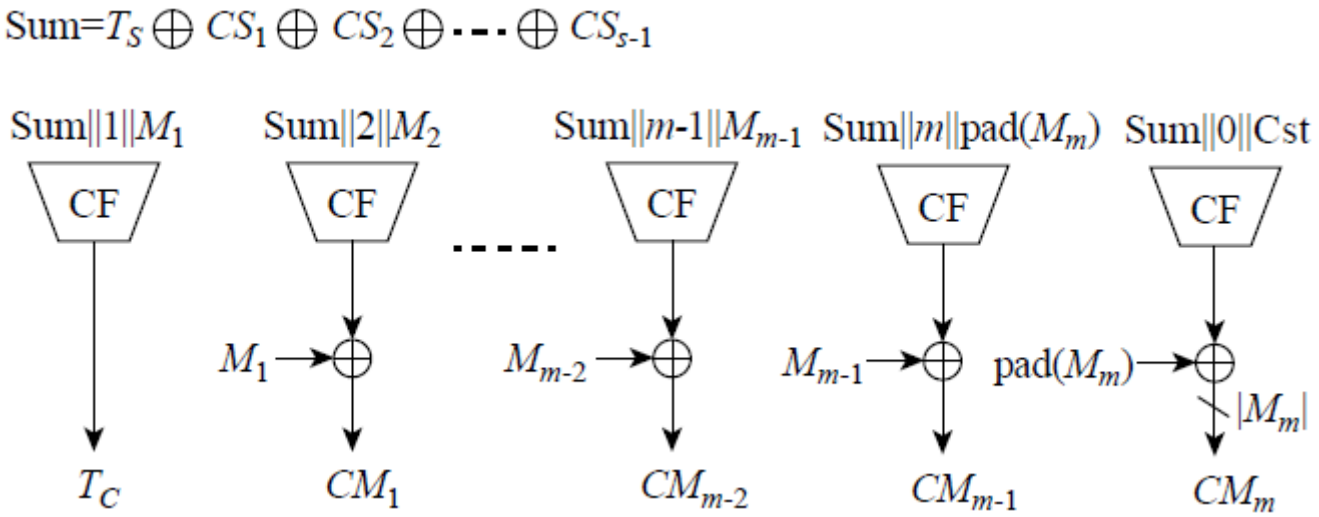
- A PMAC-like MAC processing A=AD||PMN
- CF is a compression function

The iFeed AE Mode



- Mirrored iFeed Basic to process SMN=S
- S can have any length here

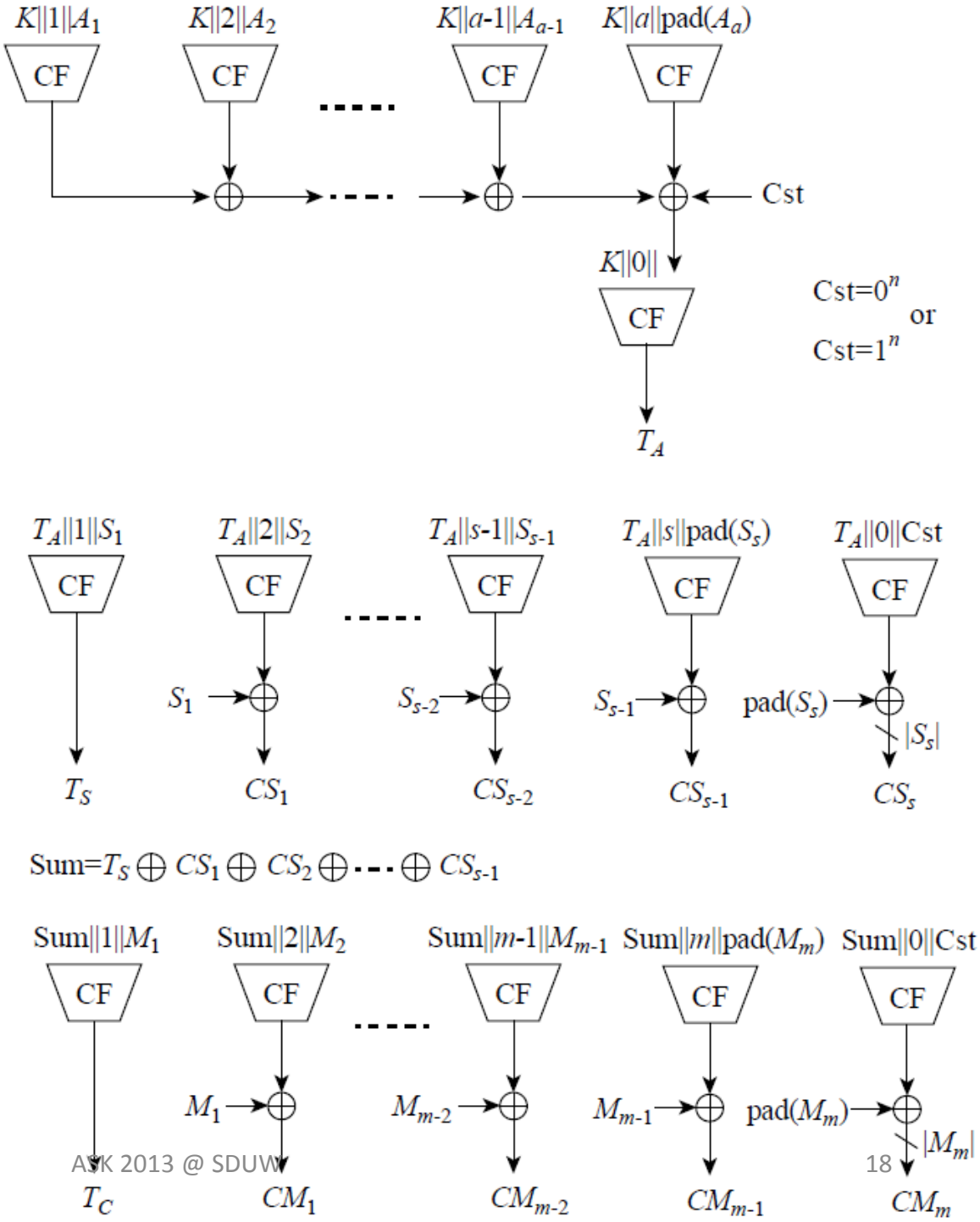
The iFeed AE Mode



- Mirrored iFeed Basic to process Message=M
- M can have any length

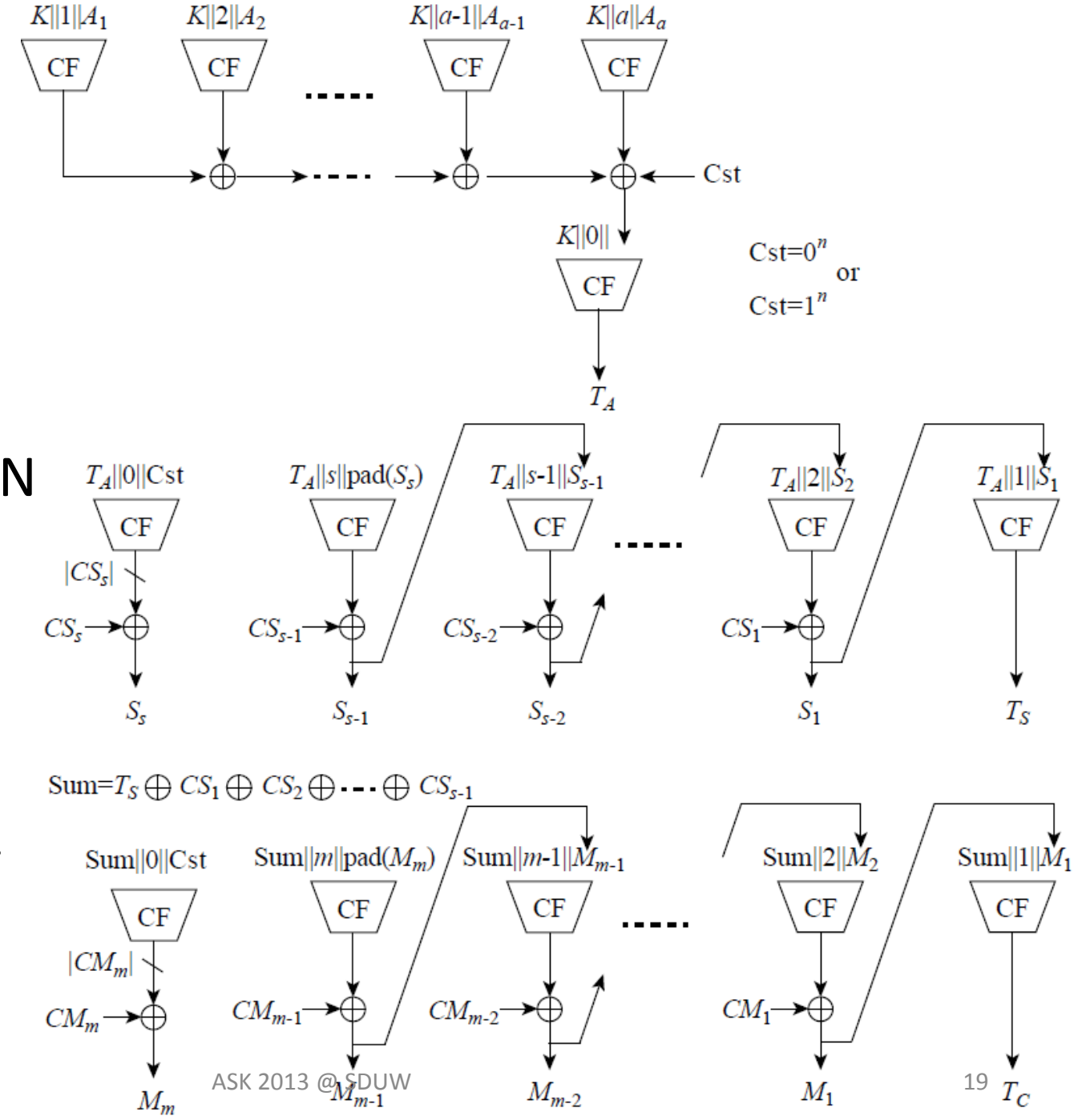
The iFeed AE Mode Encryption

- Input
  - Key K
  - A=AD||PMN
  - S=SMN
  - M=Message
- Output
  - CS, CM, T_C



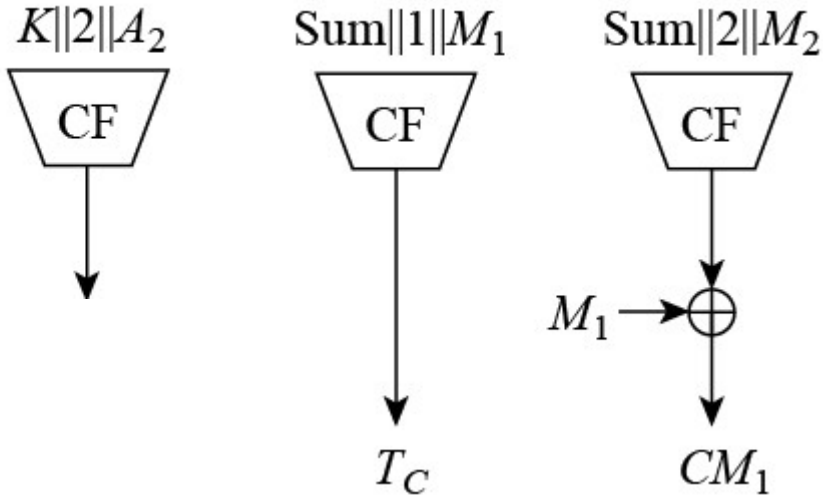
The iFeed AE Decryption

- Input
  - Key K
  - A=AD||PMN
  - CS, CM, T_C
- Output
  - (S, M) or ⊥



Compression Function CF

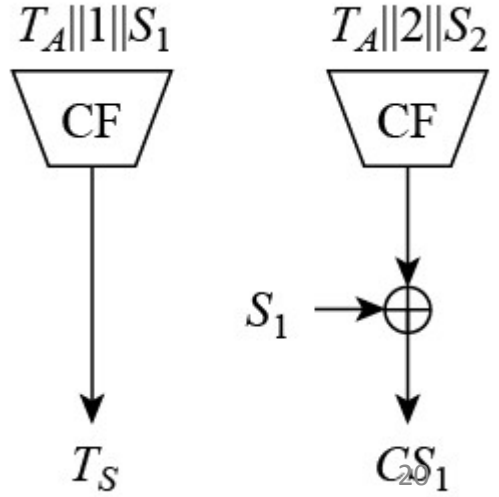
- |Sum| = k>=n bits
- |num| = a bits
- $|M_i|$ = n bits



- For each K, CF can process

At most MIN{2^a, $2^{n/2}$} blocks,

Including AD, PMN, SMN, and M



Standardized CFs

category	Hash function	Input length L_1+L_2	L_1 （message）	L_2	Output lengthL_H
ISO/IEC bc-based	Hash-function 1	2n	n	n	\leq n
	Hash-function 2	3n	n	2n	\leq 2n
	Hash-function 3	12n	4n	8n	2n
	Hash-function 4	12n	3n	9n	3n
ISO/IEC dedicated	RIPEMD-160	672	512	160	\leq 160
	RIPEMD-128	640	512	128	\leq 128
	SHA-1		512	160	\leq 160
	SHA-256		512	256	\leq 256
	SHA-224		512	256	224
	SHA-384		1024	512	384
	WHIRLPOOL		512	512	\leq 512
SM3			512	256	256

Summary of iFeed[CF]

- Depending on nonce (PMN, SMN)
- Provably secure with $O(L^2q^2/2^n)$
- In the ideal model
- avoiding generating many masks
- Supporting any-length AD, PMN, and SMN

- Parallel encryption, but serial decryption

Variants

- iFeed[BC] and iFeed[TBC]
  - Secure in the standard model
  - Needing to generate many masks, like OCB[1,2,3]
    - Gray code
    - Finite field multiplication
    - LFSR
- iFeed[CF, BC, TBC] with Mirrored iFeed Basic

Outline

- Review of AEs
- Basic iFeed Construction
- iFeed AE Modes
- Wrap Up

Wrap Up

- Too many criteria restrict the design of AE
  - Security - model, provable, tight bounds,
  - Efficiency - key size, rate, parallelizability, memory occupation, HW occupation, SW/HW speed, …
  - Usability - nonce (PMN, SMN), associated data, online, one-pass, inverse-free, patent, …
- Many AEs have been designed or being under design
- We introduce a new method to combine Privacy and Authenticity --- iFeed

Thanks

Q & A

Special thanks to Lei Wang for his insightful observations.