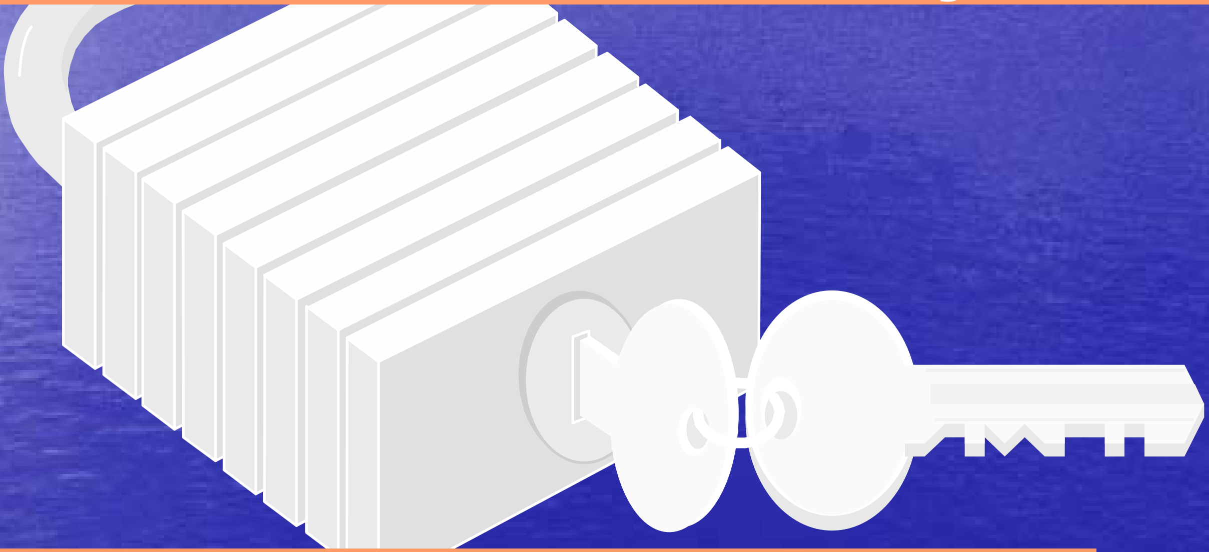
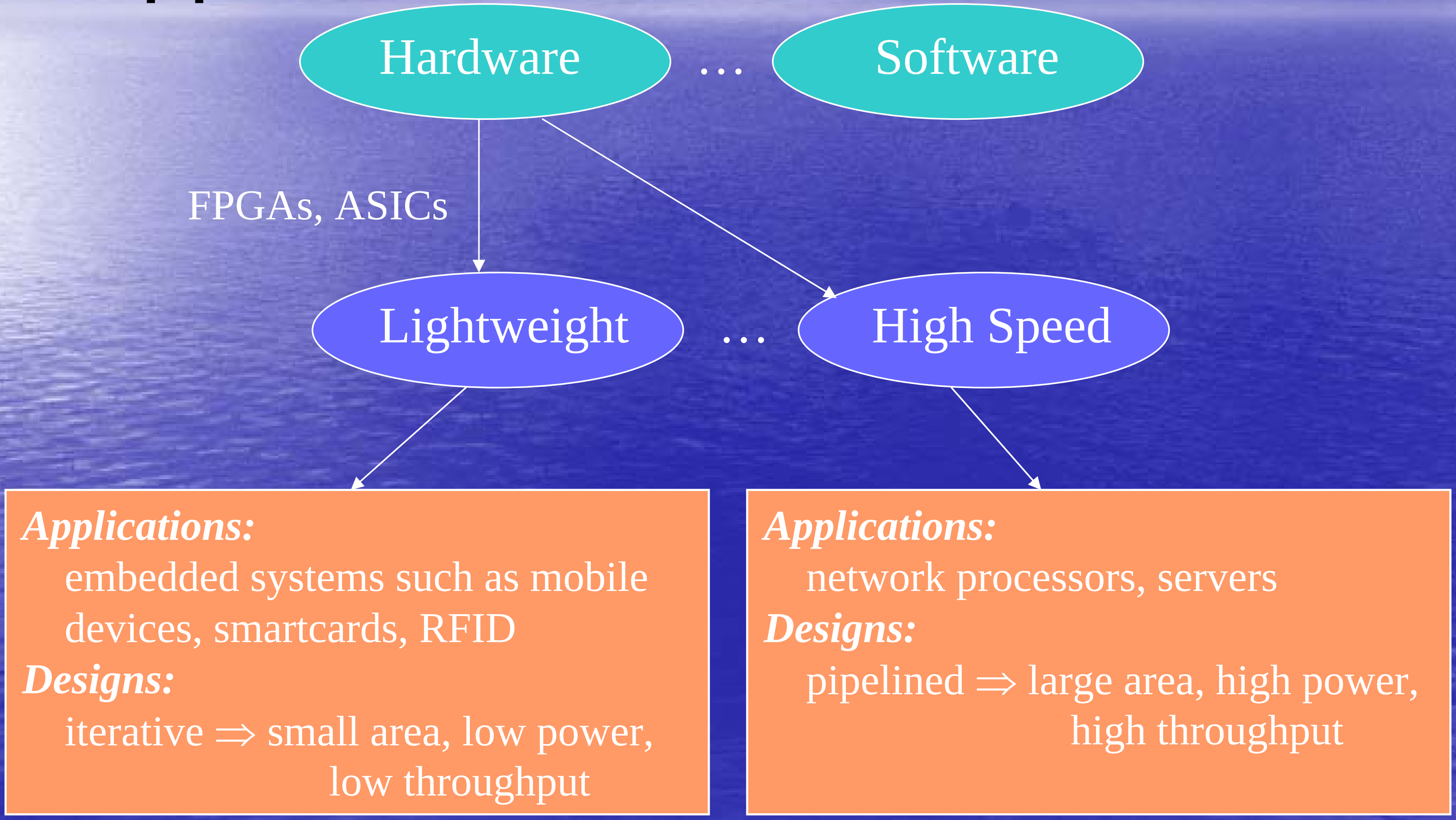
Cryptographic Hardware and Communications Security Research at Memorial University



Prinicipal Researcher:

Dr. Howard Heys
Electrical and Computer Engineering

Cryptography: Implementations and Applications



Hardware … Software

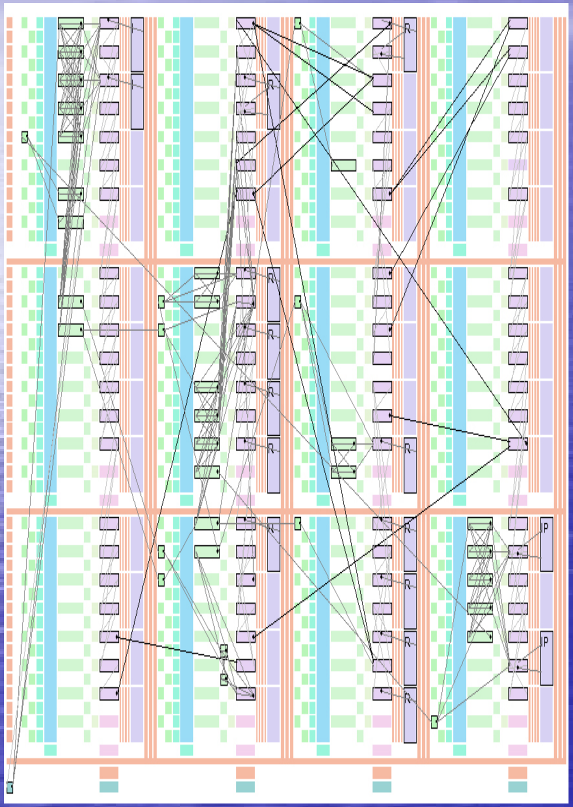
FPGAs, ASICs

Lightweight … High Speed

Applications:
embedded systems such as mobile devices, smartcards, RFID
Designs:
iterative ⇒ small area, low power, low throughput

Applications:
network processors, servers
Designs:
pipelined ⇒ large area, high power, high throughput

Lightweight Cryptography

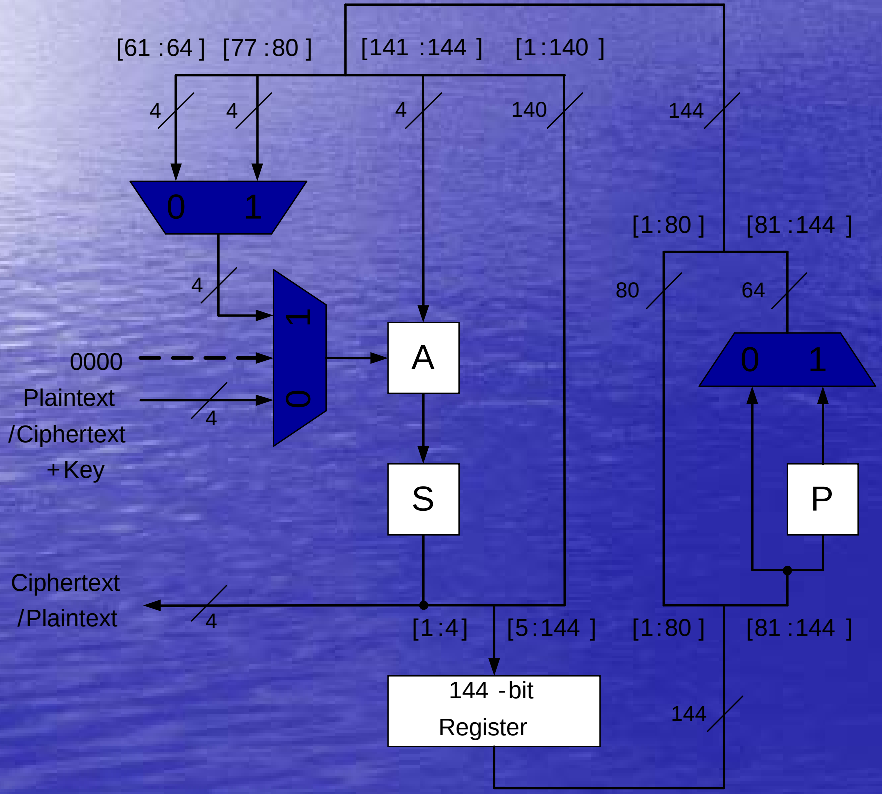


- *Compact and Low Power/Energy Hardware implementations*

→ application to small embedded devices such as smartcards and RFID tags

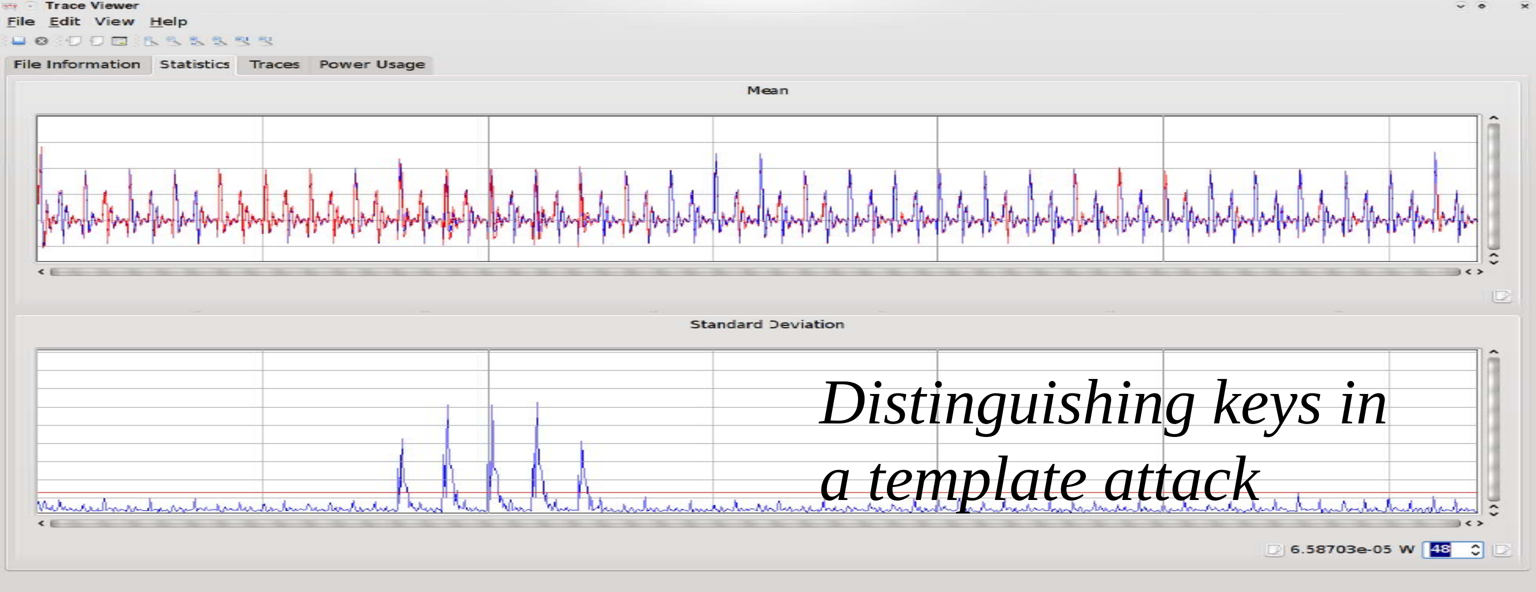
Actel
SCAB Mk1
Side Channel Analysis Board
Faculty of Engineering and Applied Science
Memorial University of Newfoundland

PUFFIN: A Novel Lightweight Block Cipher



- compact block cipher with 64-bit block and 80-bit key
- strong security properties
- only ~1000 gates to implement in 0.18 µm CMOS technology

Side Channel Analysis

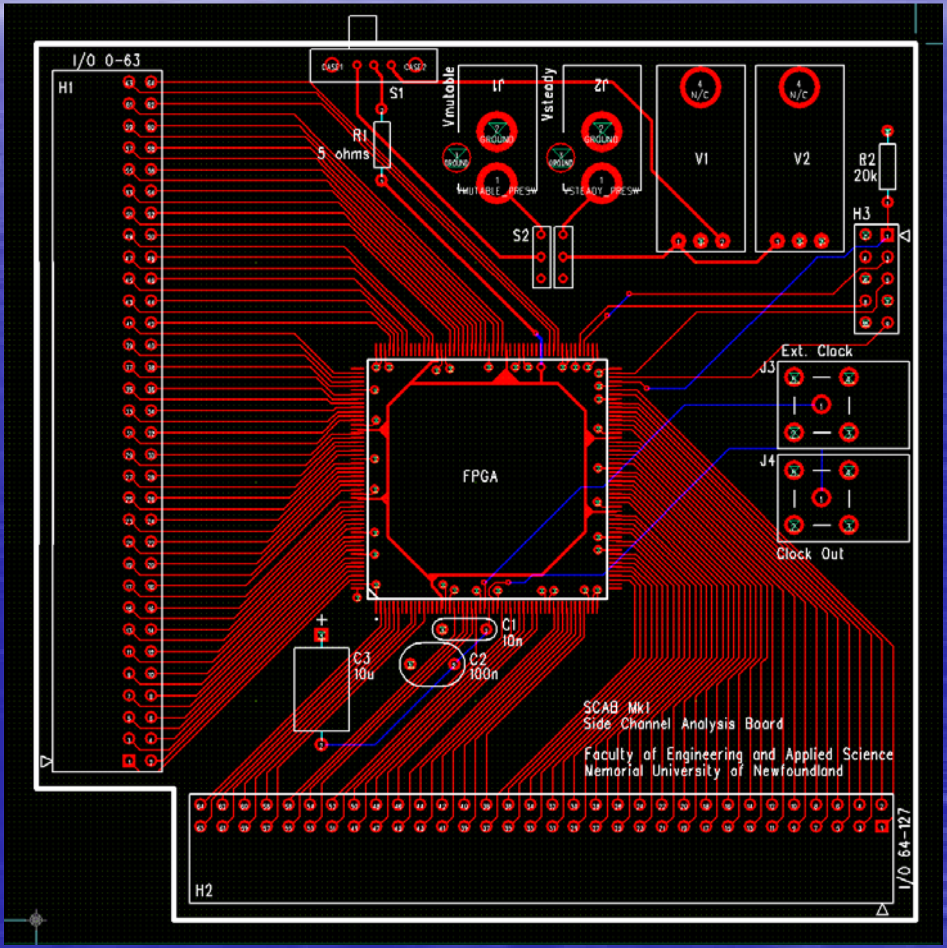


Distinguishing keys in a template attack

- implementation characteristics can be measured and related to data being processed to attack ciphers:
  → power analysis, timing analysis, fault attacks, template attacks

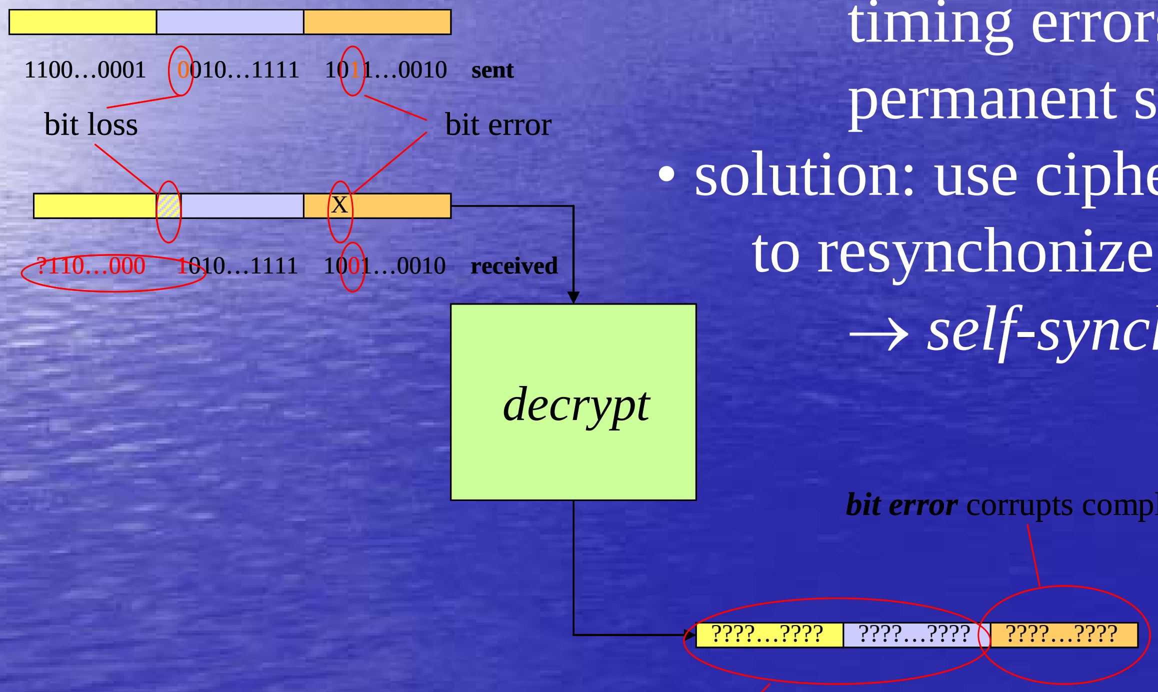
Side Channel Analysis Board

- testbed to study SCA applied to FPGA implementations
- initially applied to template attacks on stream ciphers
- can also be used to study power, timing, and fault attacks



Self-Synchronizing Ciphers

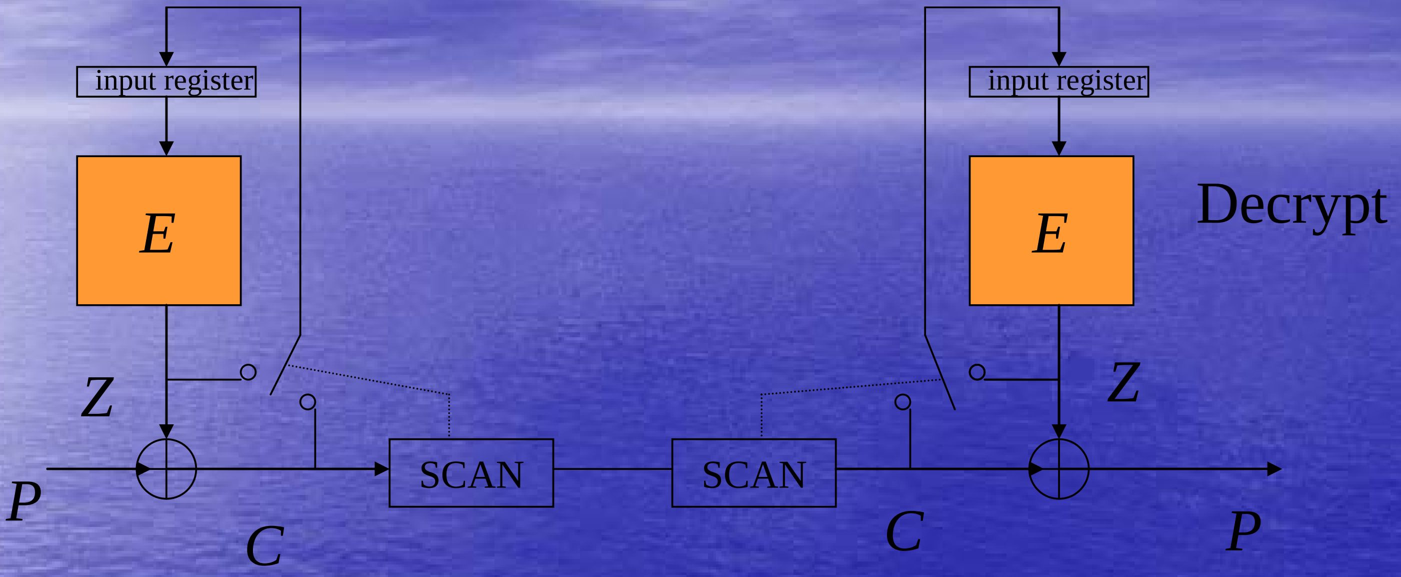
- encryption at physical layer:
  → loss or insertion of data due to timing errors can result in permanent synchronization loss
- solution: use ciphertext data at receiver to resynchonize
  → *self-synchronization*



bit error corrupts complete block

bit loss corrupts all subsequent blocks

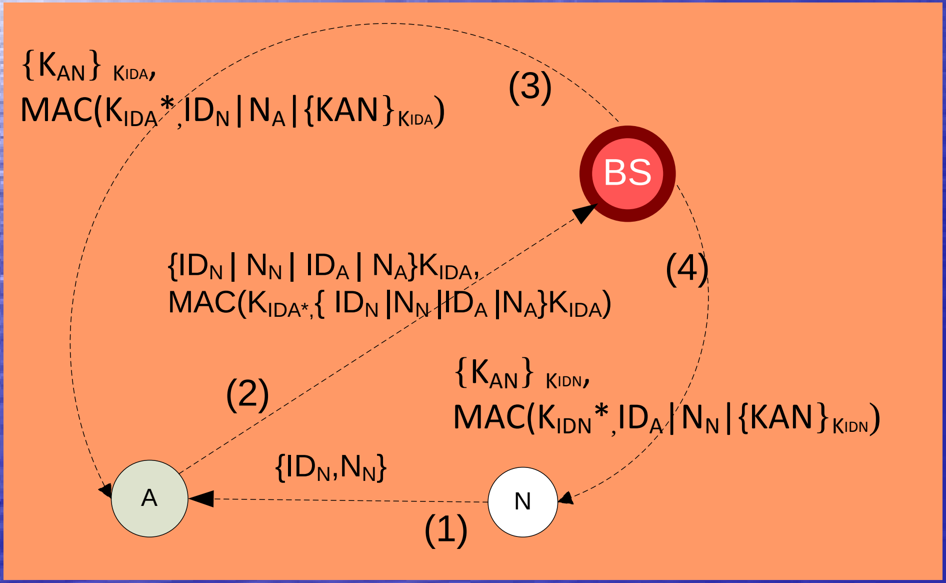
Statistical Cipher Feedback (SCFB)



- self-synchronizing hybrid of counter or output feedback (OFB) and cipher feedback (CFB) modes
  → in normal operation, configured as counter/OFB mode with *B* bit feedback
  → when *n* bit sync pattern detected in ciphertext, next *B* bits used as initialization vector to block operation

Wireless Sensor Network Security Protocols

- WSN useful for applications such as biomedical and environmental monitoring
- sensor nodes in network have limited battery life

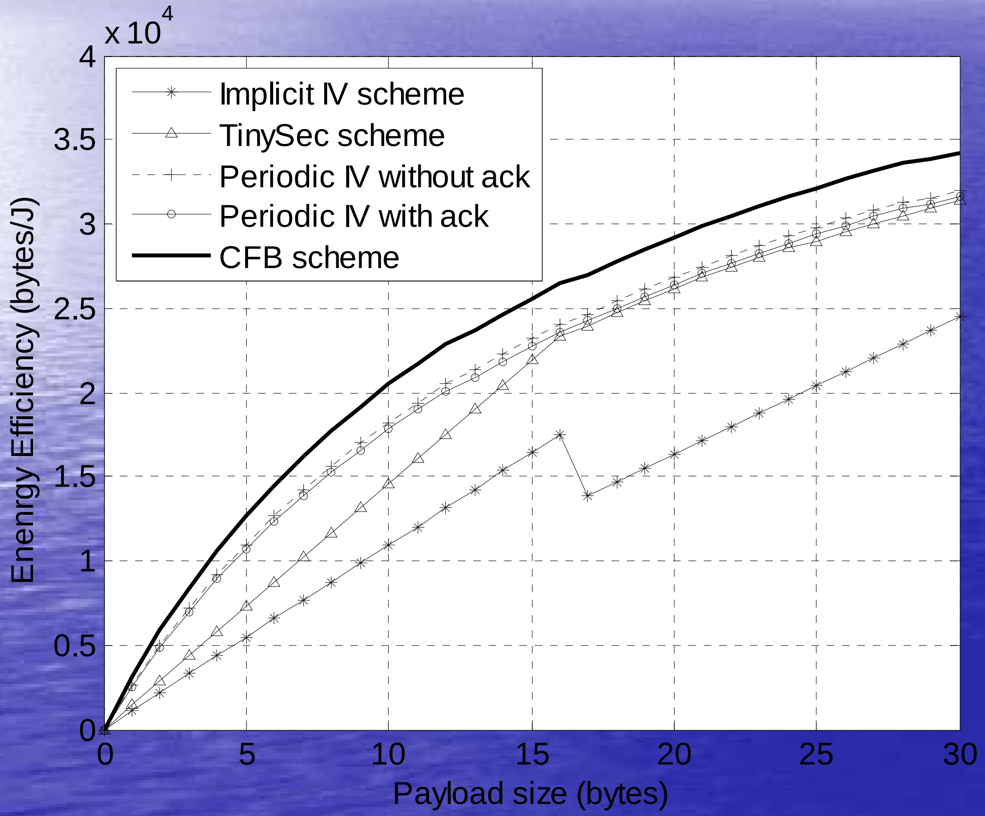

$\{K_{AN}\}_{K_{IDA}}$,
$MAC(K_{IDA}{*}, ID_N | N_A | \{KAN\}_{K_{IDA}})$
(3)
BS
$\{ID_N | N_N | ID_A | N_A\}K_{IDA}$,
$MAC(K_{IDA*}, \{ ID_N | N_N | ID_A | N_A\}K_{IDA})$
(4)
$\{K_{AN}\}_{K_{IDN}}$,
$MAC(K_{IDN}{*}, ID_A | N_N | \{KAN\}_{K_{IDN}})$
(2)
$\{ID_N, N_N\}$
A
N
(1)

Key Exchange in WSN

- cryptographic protocols and algorithms must minimize energy use in sensor nodes

⇒ efficient ciphers and protocols that minimize transmission energy are required

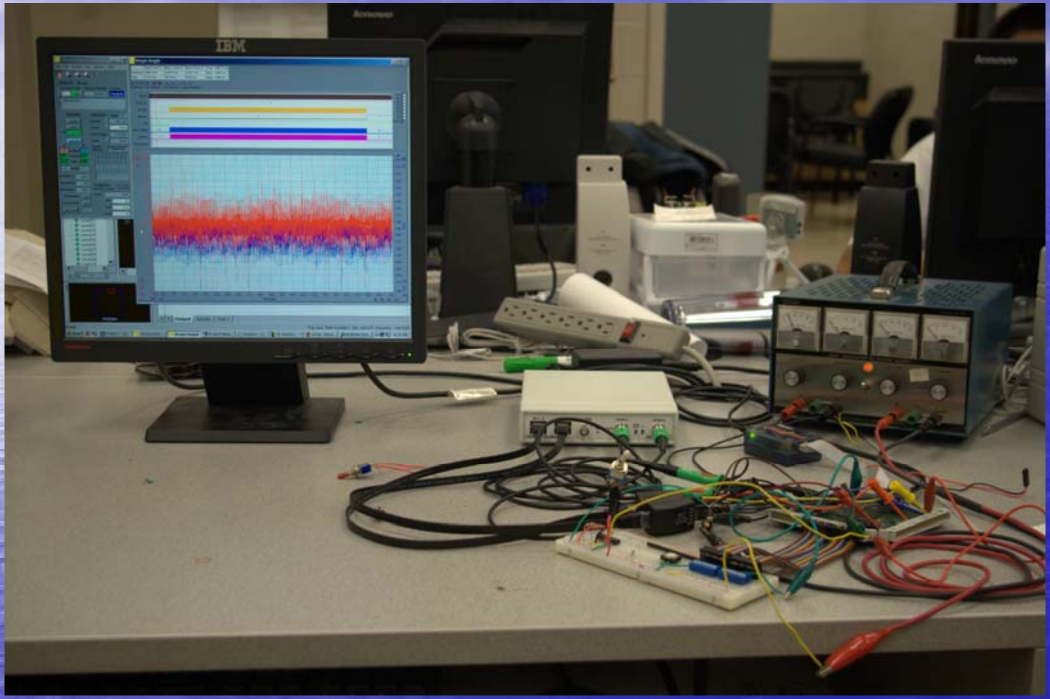
WSN Cipher Feedback



- block ciphers with ciphertext feedback
  - → minimizes transmission energy cost
  - → allows for error recover from lost packets

⇒ battery life maximized

Future Work



- lightweight embedded applications increasingly important, particularly for wireless applications

- new modes needed for high speed systems susceptible to sync loss

- cryptographic system design and hardware implementation critical to successful realization of embedded applications and high speed communication systems

Sample Publications

(1) H.M. Heys and L. Zhang, “Pipelined Statistical Cipherfeedback: A New Mode for High Speed Self-Synchronizing Stream Encryption”, to appear in IEEE Transactions on Computers, 2010.

(2) C. Wang and H.M. Heys, “Using a Pipelined S-box in Compact AES Hardware Implementations”, IEEE NEWCAS Conference, Montreal, Canada, 2010.

(3) H. Cheng, H.M. Heys, and C. Wang, "PUFFIN: A Novel Compact Block Cipher Targeted to Embedded Digital Systems", Euromicro DSD 2008, Parma, Italy, 2008.

(4) N. Yu and H.M. Heys, "A Hybrid Approach to Concurrent Error Detection for a Compact ASIC Implementation of AES", CSS 2007, Banff, Alberta, 2007.

(5) L. Zhang and H.M. Heys, "Hardware Design and Analysis of Statistical Cipher Feedback Mode Using Serial Transfer", IEEE CCECE 2007, Vancouver, BC, 2007.

(6) L. Xiao and H.M. Heys, "Software Performance Characterization of Block Cipher Structures", IEE Proceedings - Communications, 2005.

(7) L. Xiao and H.M. Heys, "A Simple Power Analysis Attack Against the Key Schedule of Camellia", Information Processing Letters, Elsevier, 2005.

(8) M. Furlong and H.M. Heys, "A Timing Attack on the CIKS-1 Block Cipher", IEEE CCECE 2005, Saskatoon, Saskatchewan, 2005.