Small IoT Security

Small Keccak Cryptography
Advancing Security into Small Things

IETF 100
Singapore

Robert Moskowitz
HTT Consulting

Small Keccak Cryptography

- What is Keccak?
  - New approach to symmetric cryptography
    - ‘Sponge function’
      - Total break from traditional ARX (Addition, Rotation, and XOR)
    - Learn more at https://keccak.team
  - Maximum strength Keccak (b = 1600) selected for SHA-3
    - FIPS 202 and SP 800-185
    - Optimized for 32 and 64 bit, multi-core CPUs and large messages
  - Basis for Ketje in CAESAR crypto competition

Keccak Sponge Function

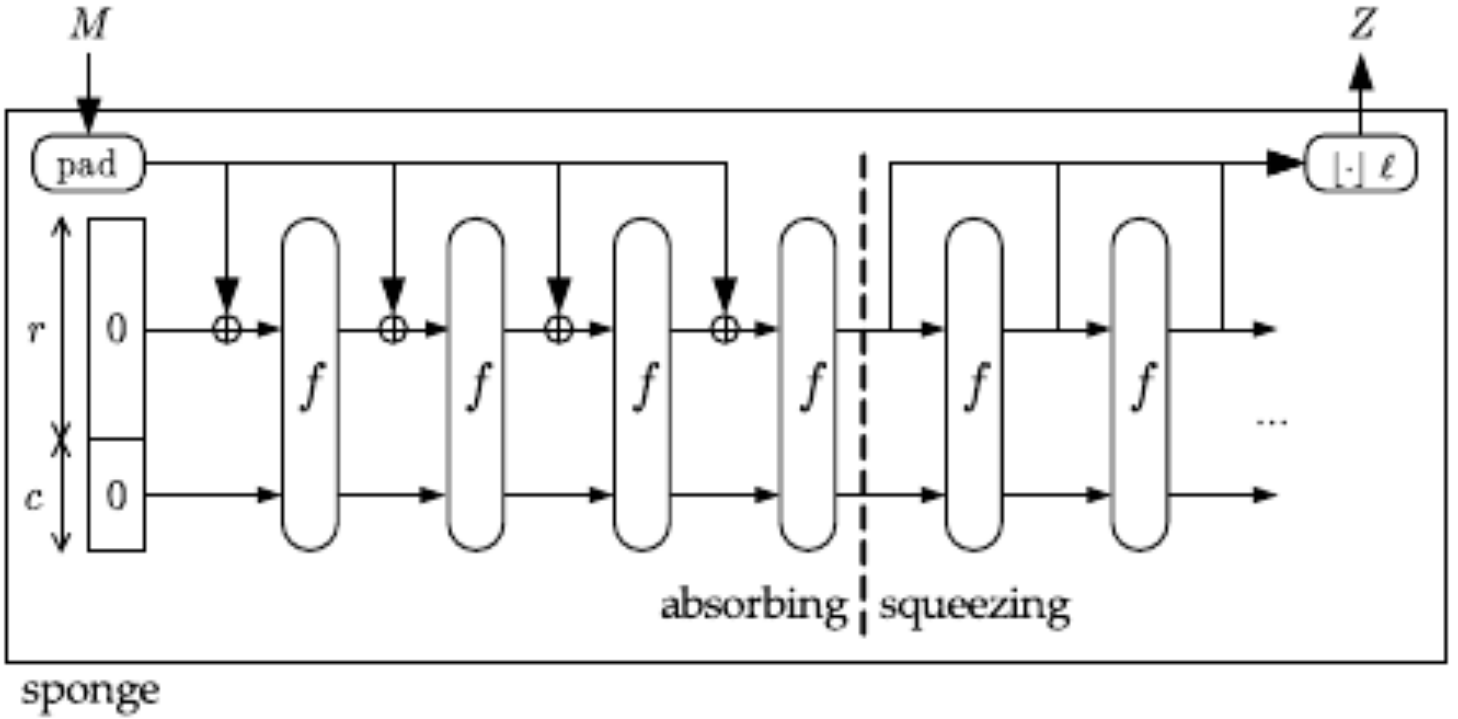

Figure 2.1: The sponge construction $Z = \text{SPONGE}[f, \text{pad}, r](M, \ell)$

https://keccak.team/files/CSF-0.1.pdf

Small Keccak Cryptograpy

- Keccak provides a complete symmetric cryptography solution
  - Cryptographic Hash
  - Keyed Hash
  - PRF – Pseudo Random Function
  - Data encryption with Additional Authenticated Data (AEAD cipher) – Ketje
- Single primitive to implement
  - Replacing AES, HMAC, SHA-2, etc.

Small Keccak Cryptography

- Keccak is highly parameterized and comes in all ‘sizes’
  - B (‘width’) = (25, 50, 100, 200, 400, 800, 1600)
    - 25 and 50 called ‘toy’ for learning about Keccak
  - Keccak defines a bitrate, r, rather than block size
  - r = b – c
    - Where capacity, c, determines the proven strength against generic attacks
    - For a strength of n bits, c = 2n
  - Thus b = 400 can deliver 128 bits of proven strength with c = 256 and r = 144

Small Keccak Cryptography

- Keccak strength also a function of rounds
  - 24 rounds defined
  - Attacks against 6 rounds published
  - ‘Easy’ to increase rounds if higher round attacks develop
    - Rounds just another Keccak parameter
      - Can even reduce rounds for performance where ‘little risk’, though not advised

Small Keccak Cryptography

- Keccak b = 400 well tuned for Truly constrained IoT
  - r = 144 well suited for small messages
  - 128 bit strength more than adequate
  - SHAKE128 based on b = 400 out-performs SHA-2 with smaller code size
    - Factor of 10 observed
  - KMAC out-performs HMAC with smaller code size
  - Ketje SR out-performs AES-CCM
    - 4 byte block, 8 byte tag

Keccak Duplex Construction
Used by Ketje

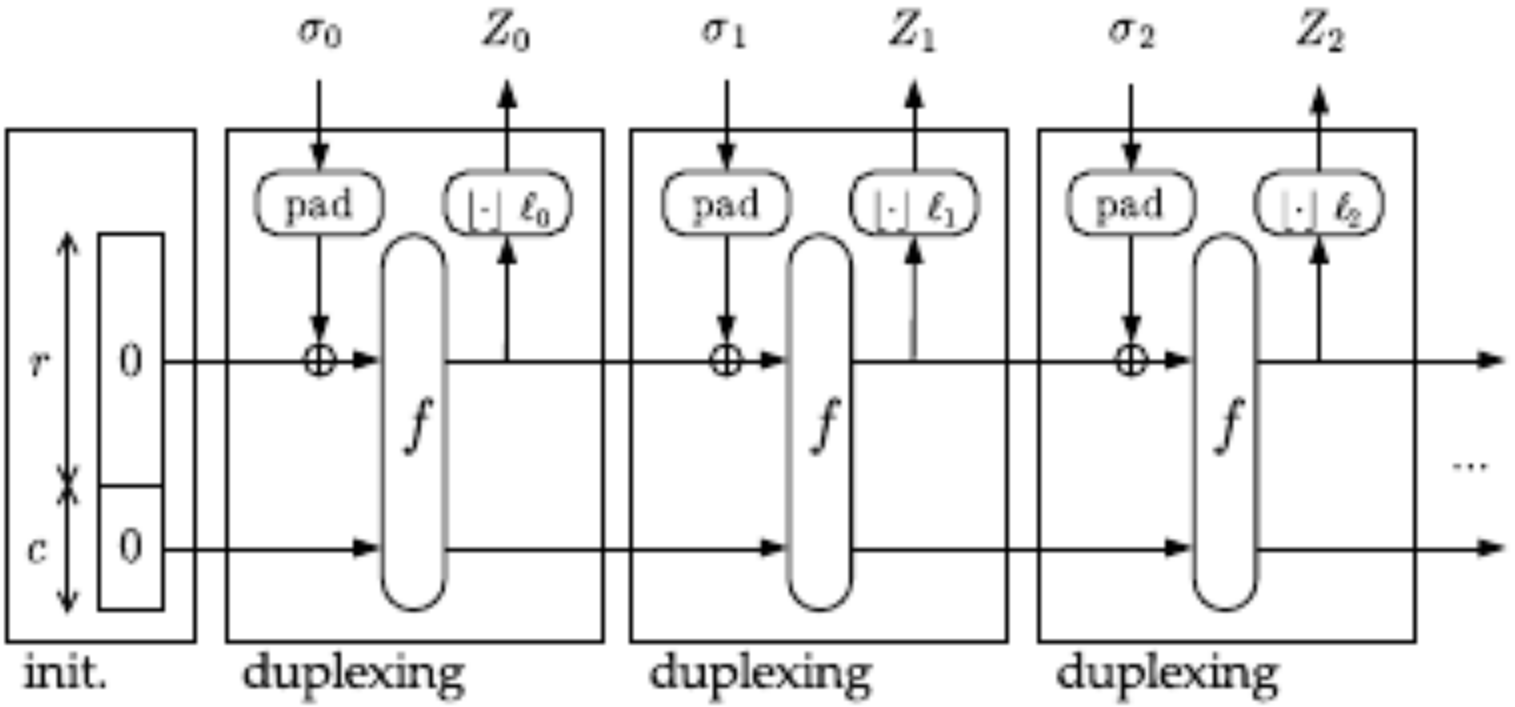

Figure 2.2: The duplex construction

Small Keccak Cryptography

- Status of work
  - Skeleton draft published
    - Draft-moskowitz-small-crypto
  - Work progressing on extracting performance and security text from existing Keccak documents for ID
  - Open code exists on keccak.team site
- Next steps
  - Add Keccak b =400 to protocols (CCI, IPsec, HIP, TLS) – that is write Drafts
  - Develop PoC IoT devices

Discussions