

A Case Against Currently Used Hash Functions in RFID Protocols

Workshop on RFID Security 2006 – RFIDSec06
July 13-14, 2006, Graz, Austria

Martin Feldhofer and Christian Rechberger

IAIK – Graz University of Technology
Martin.Feldhofer@iaik.tugraz.at
www.iaik.tugraz.at



Presentation outline

Cryptographic primitives in RFID systems

Hardware implementation of low-power SHA-256

Synthesis and power simulation results

Conclusions

Motivation

High-end security in RFID systems → standardized algorithms

Hash functions are conceptionally easy → mainly used by RFID protocol designers

Implementation costs?

**Comparison of popular hash functions with
AES block cipher in context of RFID tags**

Building blocks for RFID security

Authentication and/or anonymity is required

Commonly used cryptographic primitives

- Hash functions
- Block ciphers
- Universal hash functions
- PRNGs
- Public key algorithms
- Some “leightweight” solutions (HB, ...)

We focus on standardized cryptographic primitives

- MD4-family (SHA-256, SHA-1, MD5, MD4)
- AES-128

Survey on existing RFID security protocols

Proposal	Primitive	Authentication	Privacy
Molnar	PRF	No	Yes
Avoine	Hash	No	Yes
Choi	Hash	Yes	Yes
Henrici	Hash	Yes	Yes
Ohkubo	Hash	No	Yes
Dimitriou	Hash + PRNG	Yes	Yes
Lee	Hash + PRNG	Yes	Yes
Rhee	Hash + PRNG	Yes	Yes
Weis	Hash + PRNG	Yes	Yes
Feldhofer	AES + PRNG	Yes	Yes

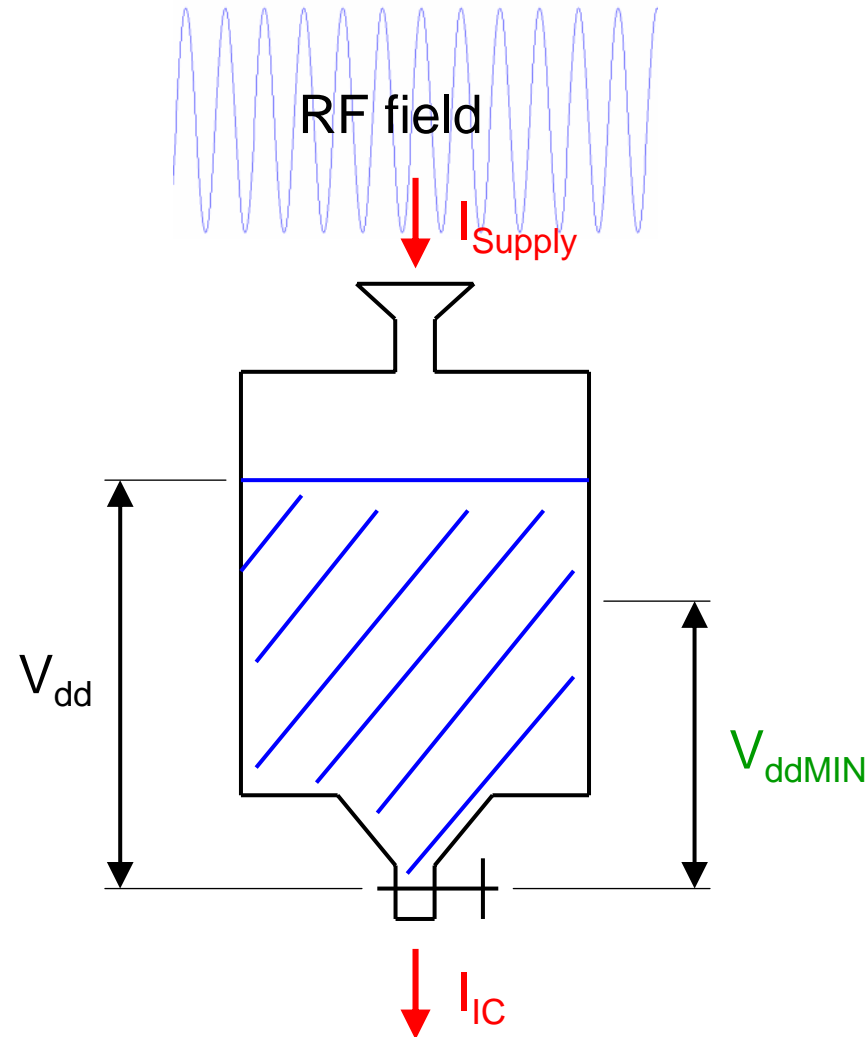
Design issues for RFID hardware

Not relevant for RFID tags

- Energy consumption per operation
- Power consumption per operation

Relevant for RFID tags

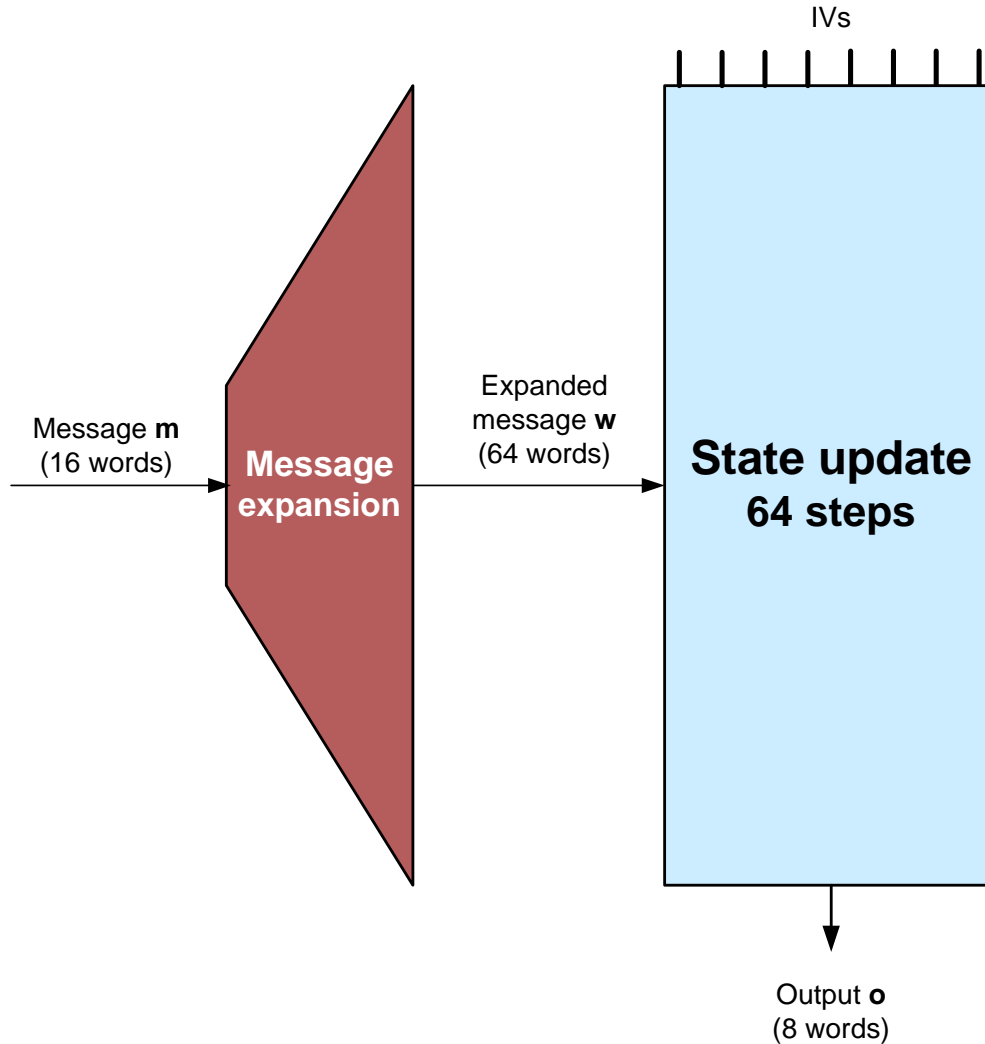
- Power consumption per cycle
- Mean current consumption must not exceed available energy in capacitor



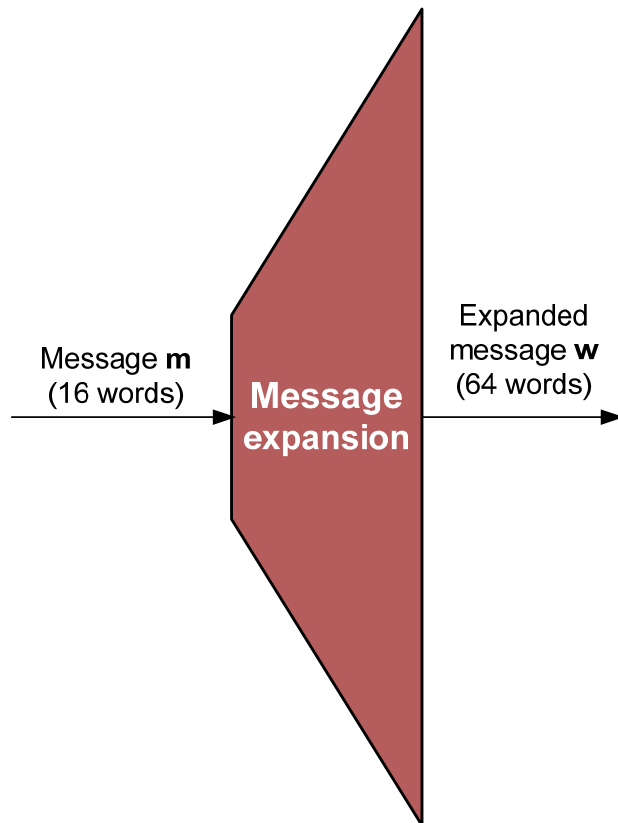
Implementation targets

	Target
Class of tags	Passive class 2 (HF 13.56 MHz)
Mean power consumption	< 15 μ A @ 1.5V
Hardware resources	< 1,000 - 10,000 GEs
Data rate of protocol	26 kbps
Clock frequency of crypto module	~100 kHz
Number of clock cycles (latency)	~50 for immediate answer (0.5ms) → use interleaved protocol instead
Available modules	No microcontroller or external memory available
Technology	Standard cells (no dedicated RAM)
Costs	~5-50 Cent per tag

Outline of SHA-256



Outline of SHA-256 – Message expansion

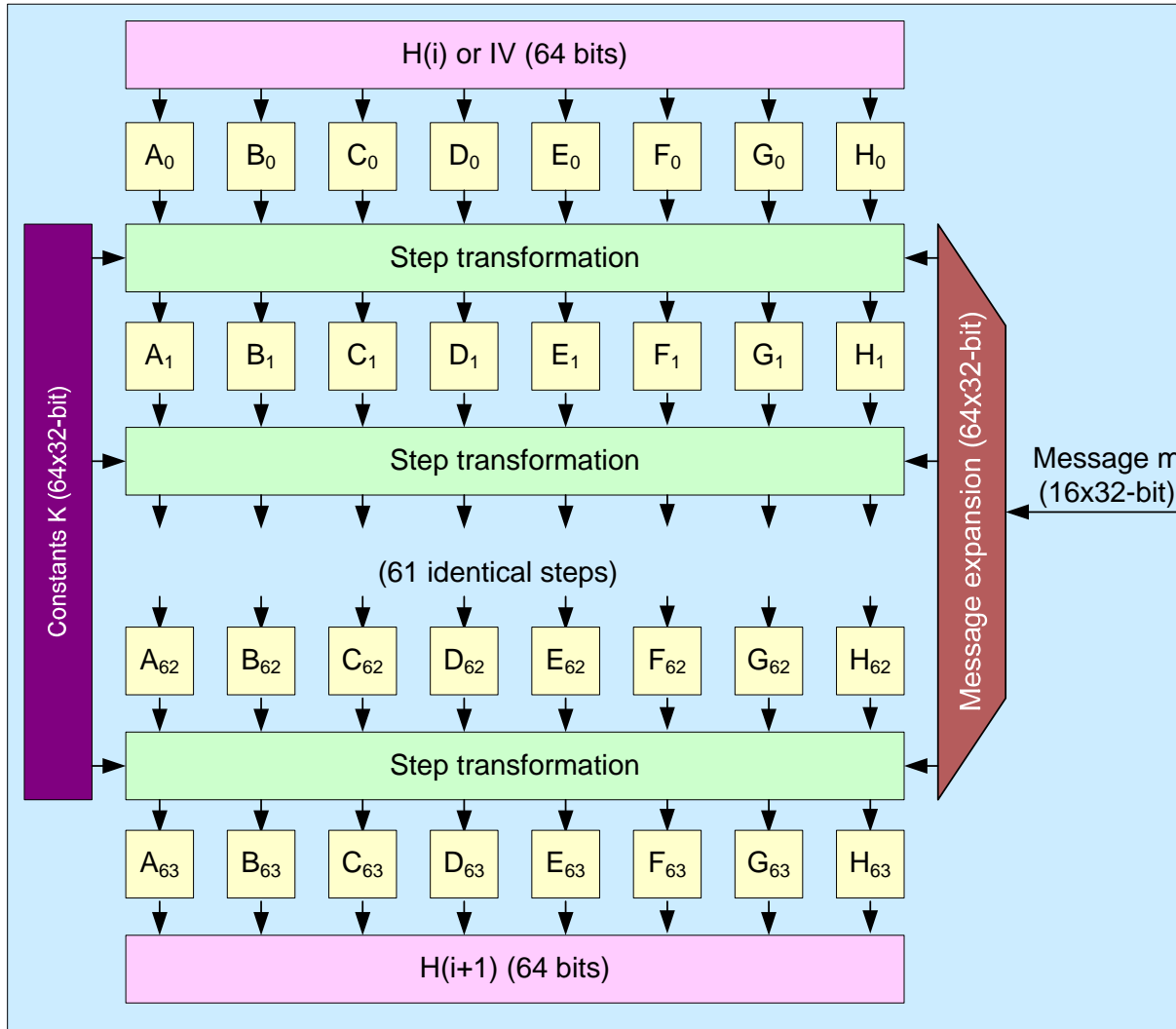


$$W_t = \begin{cases} M_t & \text{for } (0 \leq t \leq 15) \\ \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} & \text{for } (16 \leq t \leq 63) \end{cases}$$

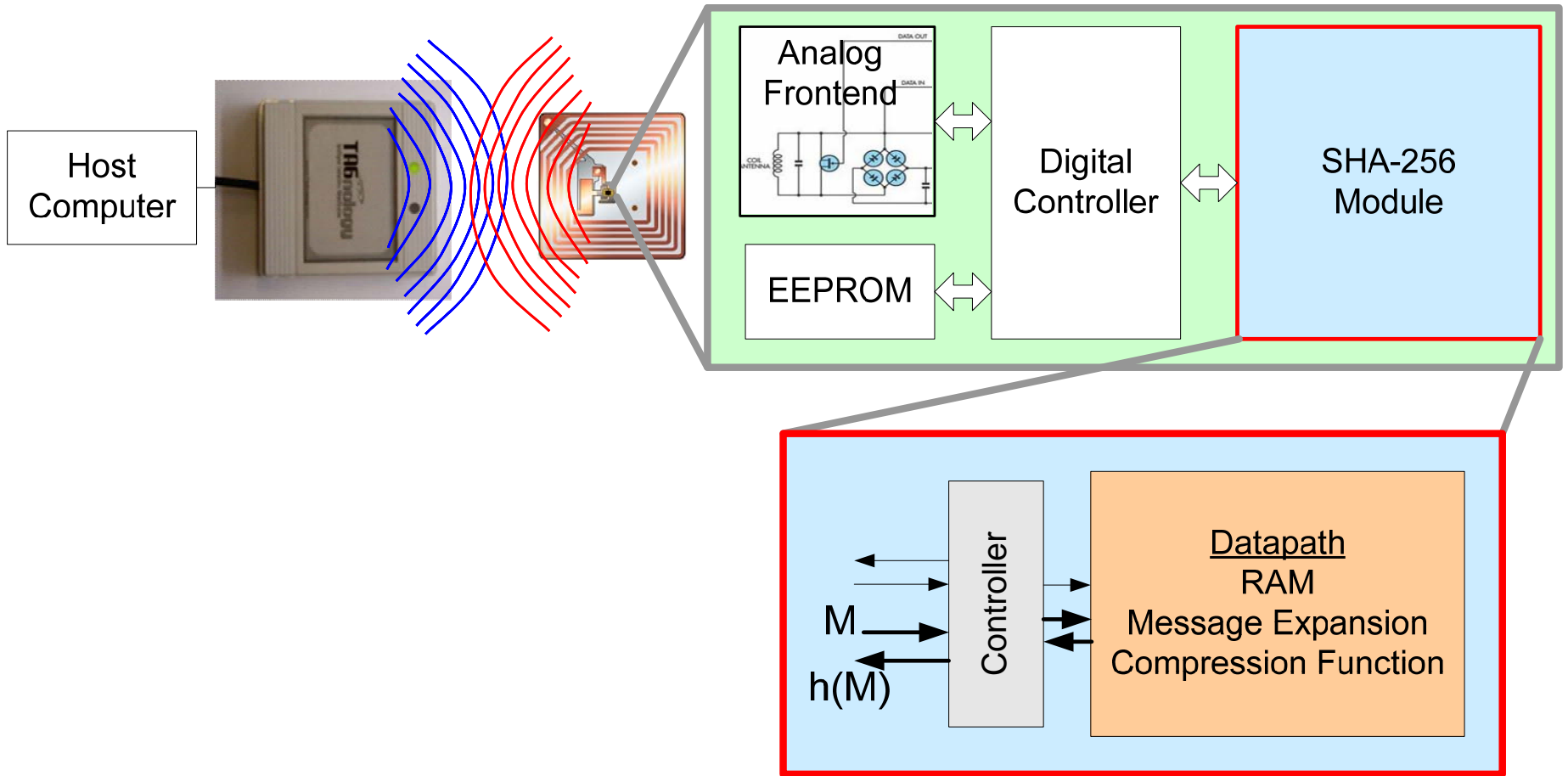
$$\sigma_0(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

$$\sigma_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

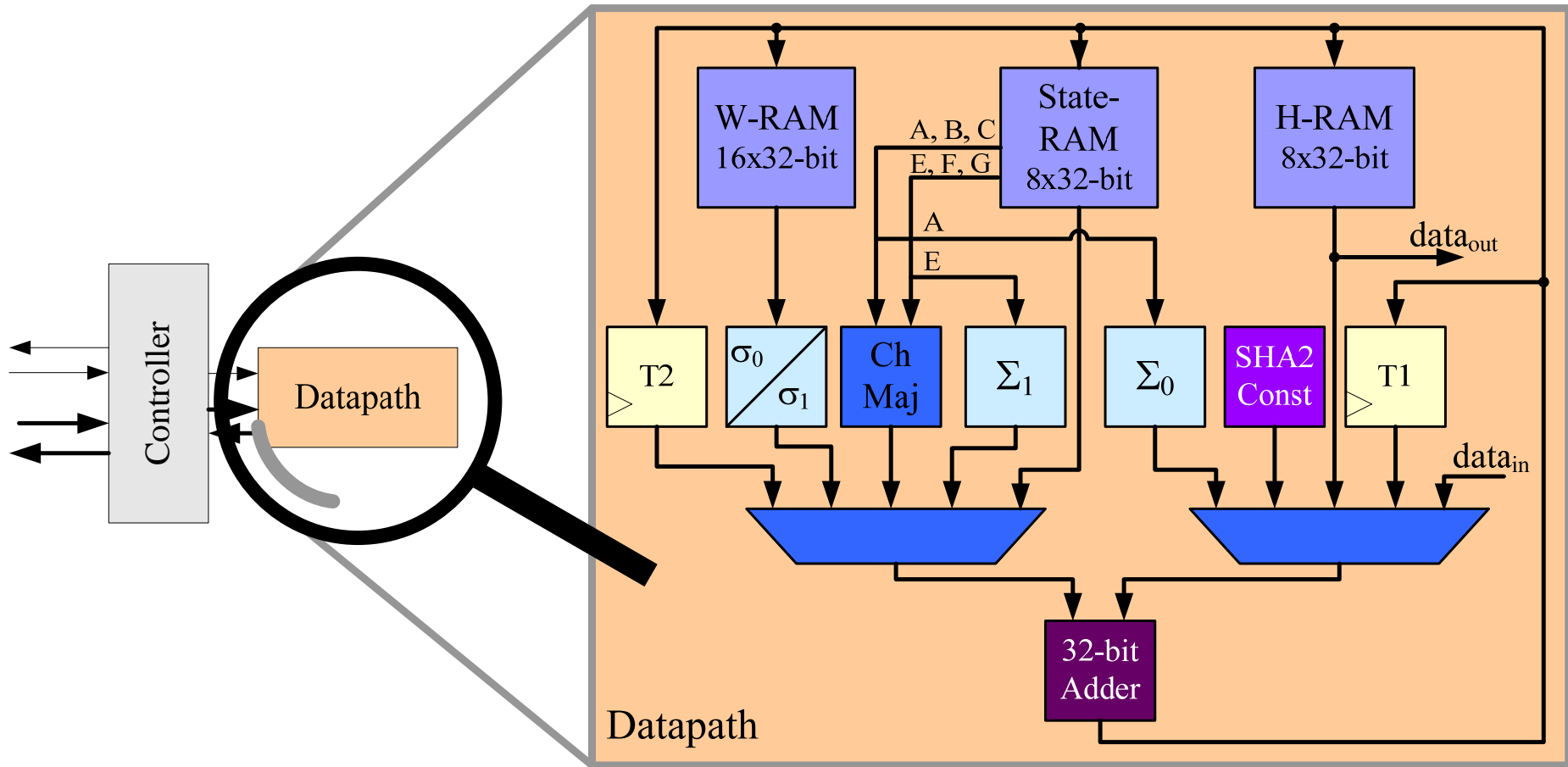
Outline of SHA-256 – State update



Secure RFID tag architecture

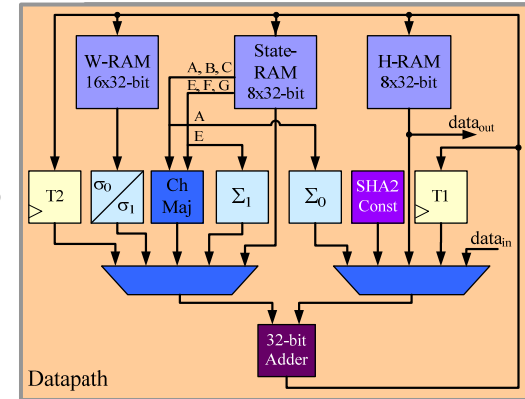
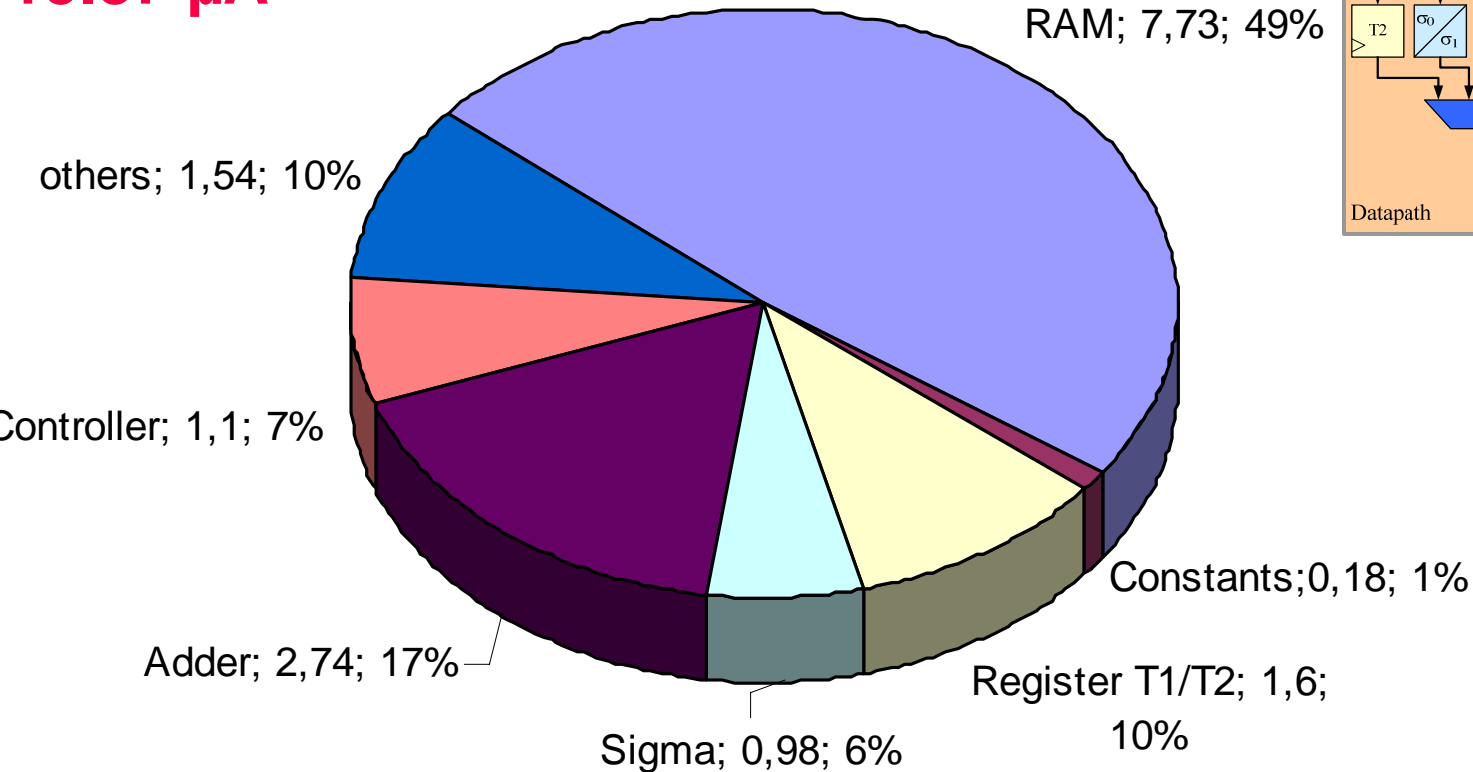


Architecture of low-power SHA-256



Power consumption [in μA @ 100kHz; 3.3V]

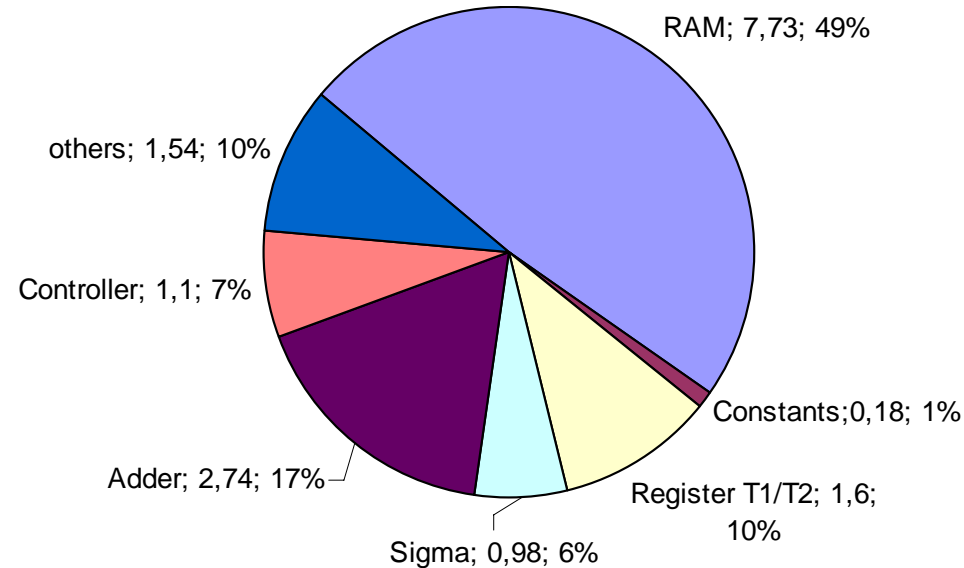
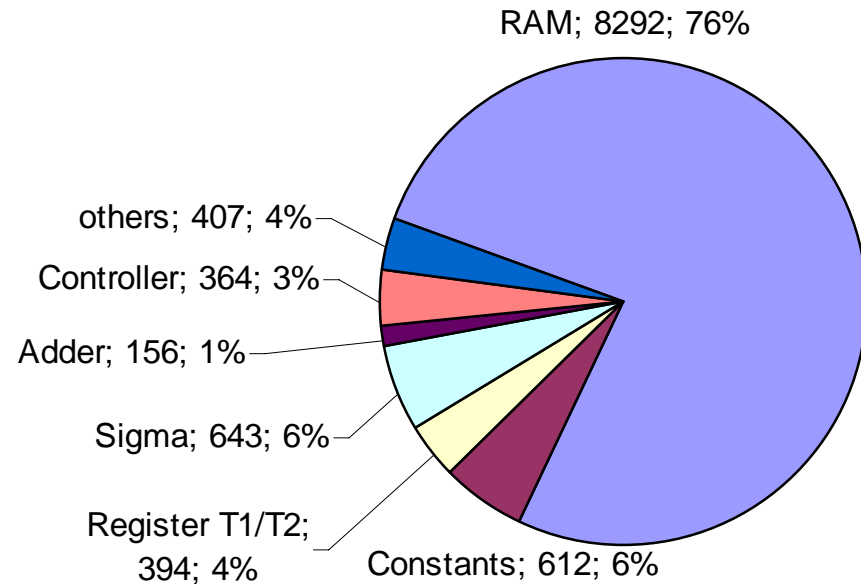
**Mean current consumption:
15.87 μA**



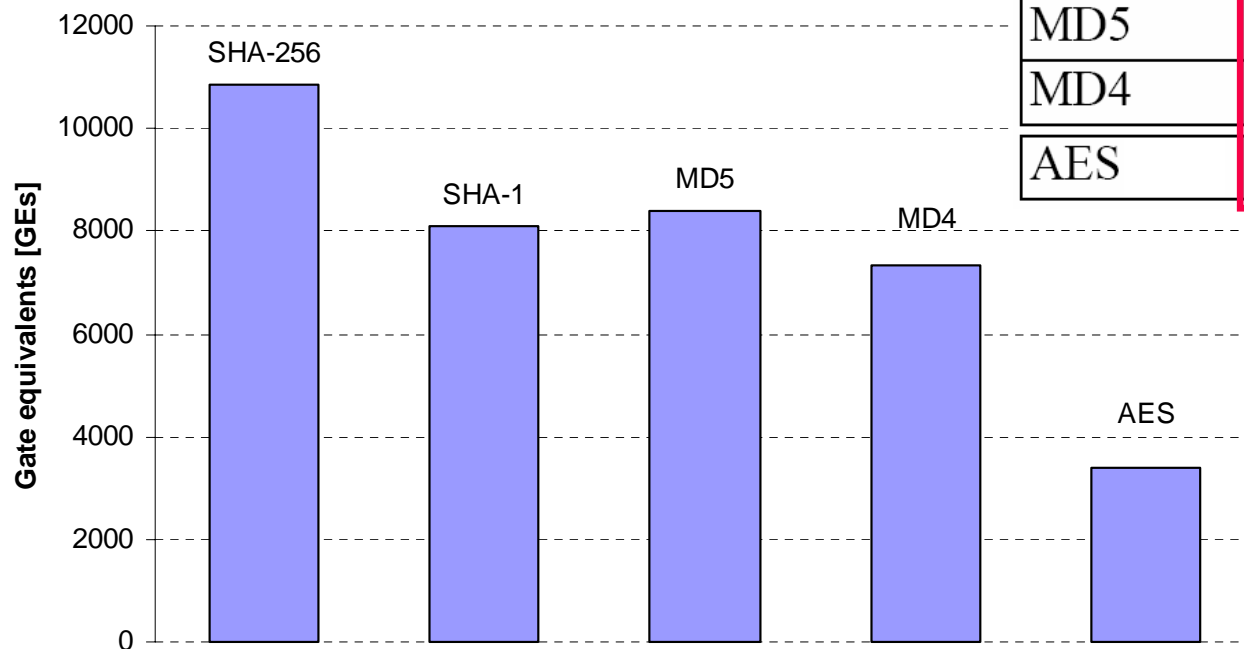
Comparison of chip area and power consumption

Area distribution

Power consumption distribution



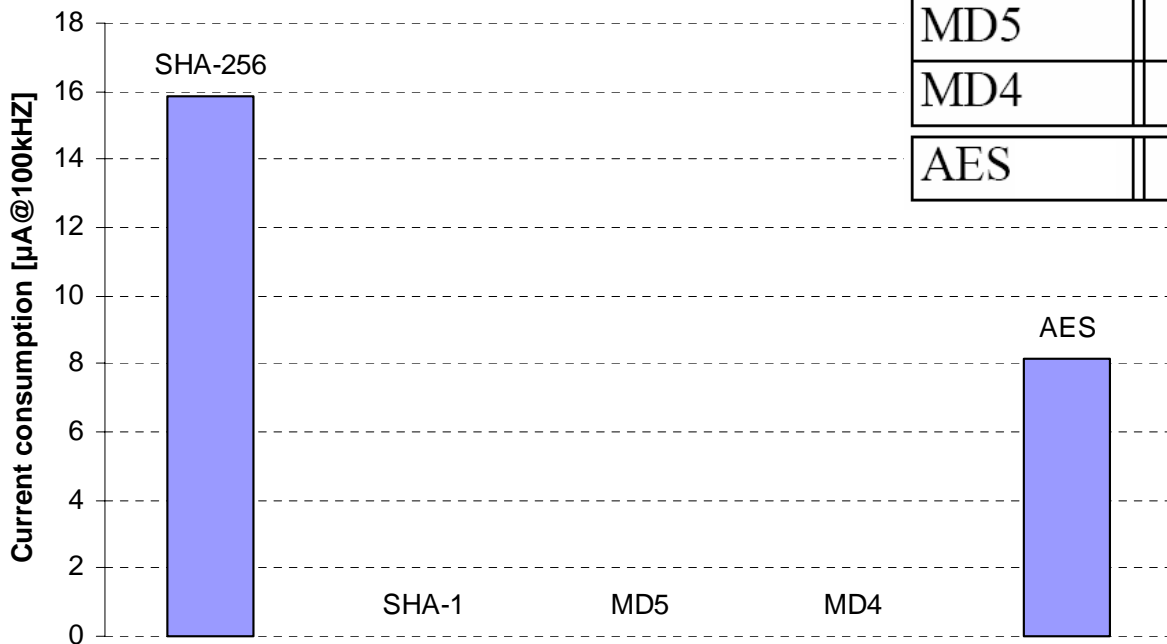
Comparison of SHA-256, SHA1, MD5, MD4 and AES – Chip area



Algorithm	Chip area GE	I_{mean} μA @100kHz	Clock cycles
SHA-256	10,868	15.87	1,128
SHA-1	8,120	–	1,274
MD5	8,400	–	612
MD4	7,350	–	456
AES	3,400	8.15	1,032

Comparison of SHA-256, SHA1, MD4, MD5 and AES – Mean current consumption

Algorithm	Chip area GE	I_{mean} μA @100kHz	Clock cycles
SHA-256	10,868	15.87	1,128
SHA-1	8,120	–	1,274
MD5	8,400	–	612
MD4	7,350	–	456
AES	3,400	8.15	1,032



3.3V !!!

Implications of this work

Two dominating factors decide on the suitability of a symmetric primitive for RFID tags

- The required number of registers (state variables, chaining variables and message words)
 - SHA-256 (1024 bits) vs. AES (256 bits)
- The underlying word size of the used primitive
 - How many flip flops have to be clocked at the same time
 - SHA-256 (32 bits) vs. AES (8 bits)

Input for future design of cryptographic primitives

Comparison with parallel work

Kaps et al. state that SHA-1 is more energy-efficient than AES

- Stated chip area: 4276 GEs
- This seems to contradict our conclusions

But:

1. Low energy consumption is not a main concern in RFID tag design
2. Necessary external memory for message expansion is not available on RFID tags (requires additional 3722 GEs)

Conclusions

We analyzed implementations of commonly used cryptographic primitives for RFID tags

Comparison of SHA-256 with AES-128 because of same level of security

- AES-128 requires less chip area
- AES-128 has less mean power consumption

Even older MD4-family hash functions (SHA-1, MD5, MD4) do not change conclusion