An Area Optimization and Power Efficient Method for HMAC-PHOTON Lightweight Cryptography

Duc Nhan Le, Seungbum Baek, Kang-Un Choi and Jong-Phil Hong, *Member, IEEE*

School of Electrical Engineering, Chungbuk National University, Republic of Korea

Motivations

➢ HMAC → the most popular method of MAC → provide authentication and integrity of information

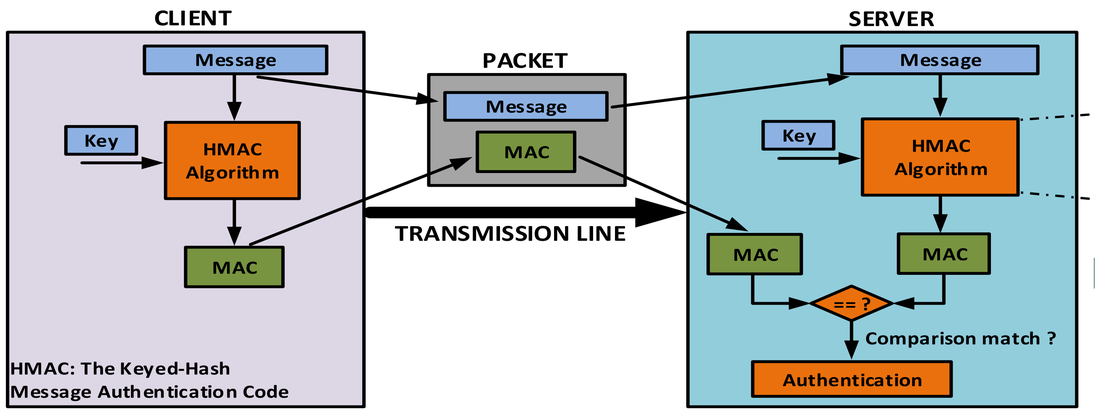


Figure 1: The HMAC in information authentication application

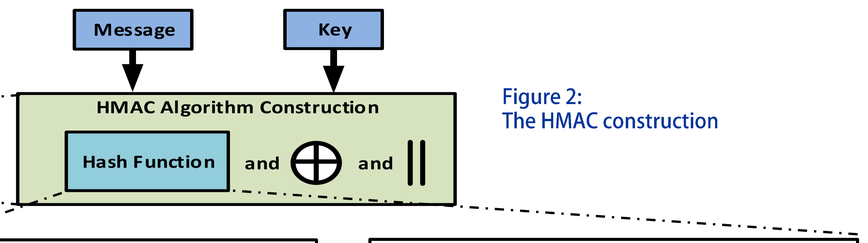


Figure 2: The HMAC construction

Conventional (SHA 2, SHA 3, …):
→ Large area occupation
→ High power consumption

Lightweight (PHOTON, SPONGENT, …):
→ Small area occupation
→ Low power consumption
→ Still meet the security requirements

Implement HMAC lightweight PHOTON-80
✓ 128-bit message
✓ 128-bit key
→ For typical application

However, Problem is …
HMAC-PHOTON utilizes either 2 or 3 hash function blocks → increase power and area

Proposed method:
Reducing to a single hash function block → save power and area

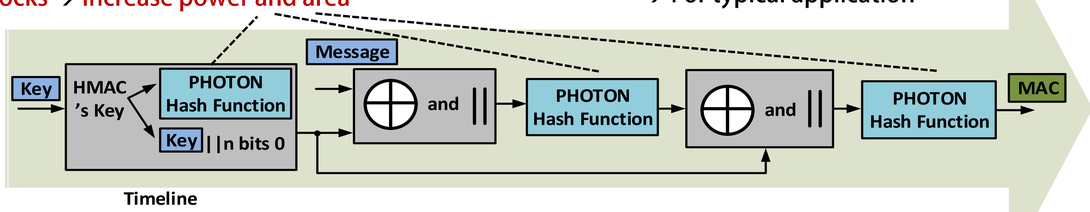


Figure 3: The HMAC-PHOTON conventional operation flow

Hardware Architecture

The proposal reduces to a single PHOTON hash function in architecture

The main block of proposed architecture:
✓ HMAC Controller: manage sequential operation

HMAC Controller is constructed from:
✓ Counter → enable PHOTON and select message, hash out
✓ Feedback from sequential block → message with the corresponding step

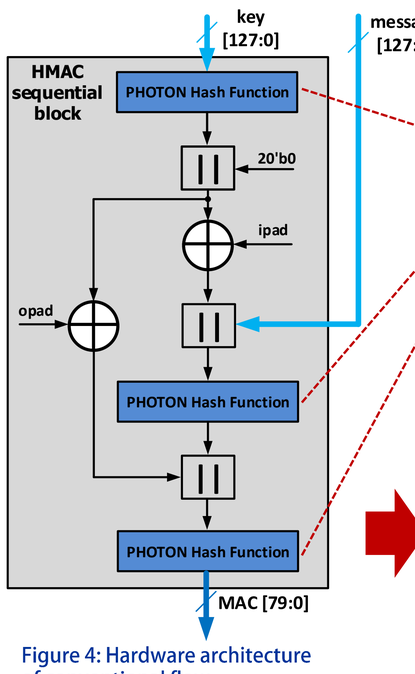


Figure 4: Hardware architecture of conventional flow

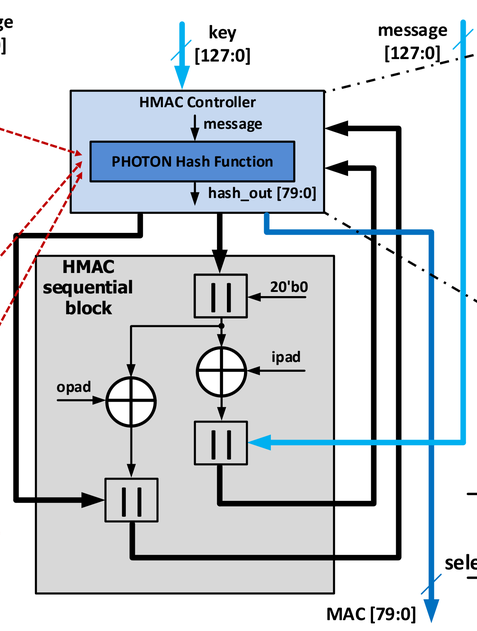


Figure 5: Hardware architecture of proposed flow

Concatenation operation

XOR operation

Ipad: inner pad (**8'h36**)

Opad: outer pad (**8'h5c**)

PHOTON hash function construction:

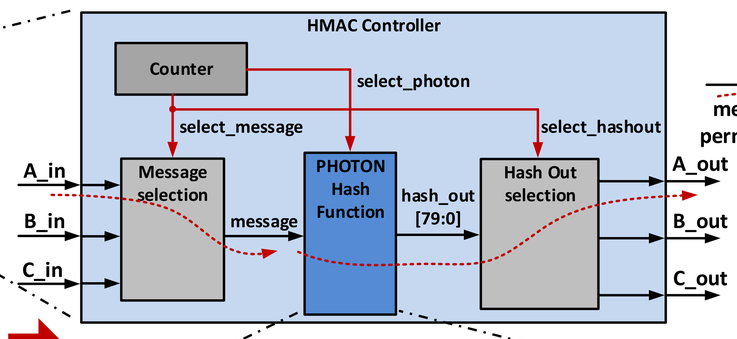
Padding with different bit-width of message

Absorbing process: absorb message dependent on bit-width of padded message

Squeezing process: squeeze to final hash out (5 rounds with PHOTON-80)

A PHOTON permutation includes:
✓ 12 rounds of PHOTON round

Figure 6: Hardware architecture of HMAC Controller block



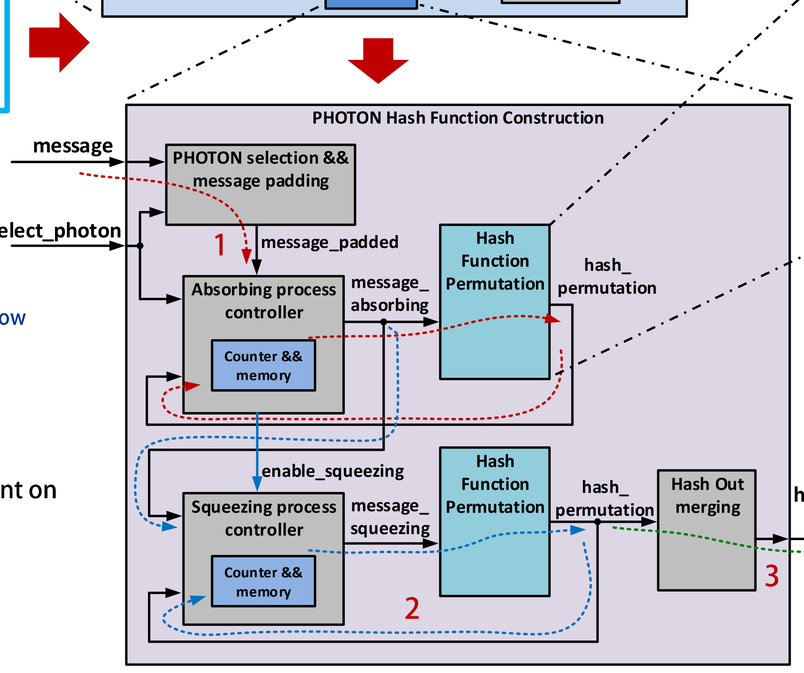


Figure 7: Hardware architecture of PHOTON hash function

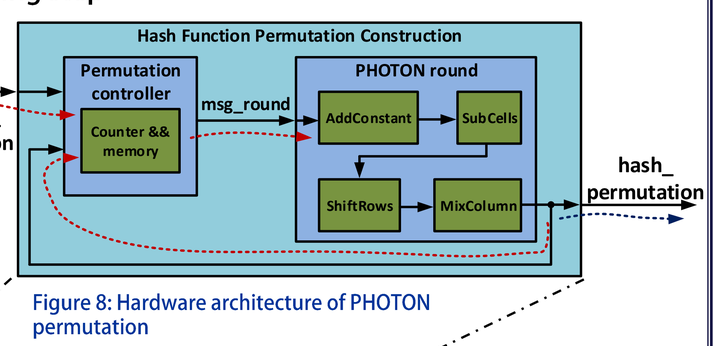


Figure 8: Hardware architecture of PHOTON permutation

✓ Area → Reduced by 41.57% compared to its of conventional way
✓ Power → Reduced by 26.62% compared to its of conventional way

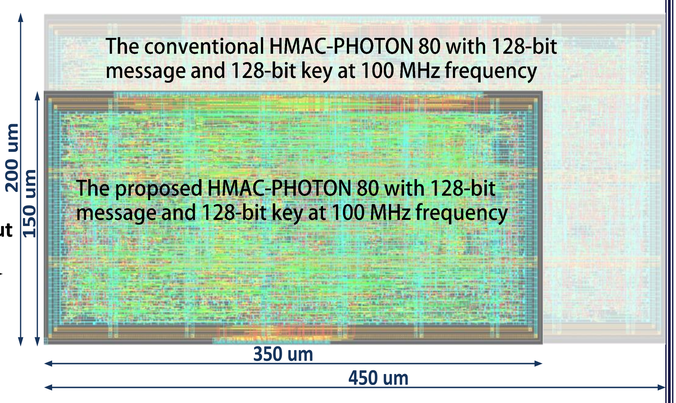


Figure 9: PnR results

Implementation Results

		HMAC-PHOTON 80 (this work)	HMAC-PHOTON 80 (conventional)	HMAC-SHA 256	HMAC-SHA 1 [1]
Parameter	Message (bits)	128	128	128	32
	Key size (bits)	128	128	128	32
	Hash size (bits)	80	80	256	160
Performance	Latency (clk)	880	880	320	20.2-25.3
	Frequency (MHz)	100	100	100	66
	Throughput[1] (Mbps)	14.5	14.5	40	83.4-104.3
	Area (GEs)	20698	35423	41681	29200
	Power (mW)	2.62	3.57	10.6	-
	Process	65 nm	65 nm	65 nm	250 nm
Security	Entropy (bits per byte)	3.296	3.296	4.873	-
	Avalanche effect (%)	50.40	50.40	49.53	-
	Collision resistance (bits)	40	40	128 [2]	< 80 [2]
	Preimage resistance (bits)	80	80	256 [2]	160 [2]
	Second preimage resistance (bits)	40	40	201-224 [2]	105-160 [2]

Table I: Performance and security comparison of HMAC-PHOTON 80 (proposed and conventional design), HMAC-SHA 256 and HMAC-SHA 1

➢ The security strength of HMAC (HMAC-PHOTON 80) based on:
✓ HMAC key → can be improved by physical unclonable function (PUF)
✓ The hash function strength → PHOTON-80 resistances (enough for IoT application) [3]
✓ The length of MAC output → 80 bits of HMAC-PHOTON 80 (typical application requires 64 bits) [3]
✓ Entropy and Avalanche effect → high and acceptable in randomness and computation complexity

[1]. $\text{Throughput} = \frac{\#\text{ bits of data input}}{\text{latency}} \text{ x frequency}$

[1] M-Y Wang *et al.*, "An HMAC Processor with Integrated SHA-1 and MD5 Algorithms", ASP-DAC 2004: Asia and South Pacific Design Automation Conference 2004.
[2] Information Technology Laboratory, National Institute of Standards and Technology, "Recommendation for Applications Using Approved Hash Algorithms", NIST Special Publication 800-107, August 2012.
[3] K. A. McKay *et al.*, National Institute of Standards and Technology, "Report on Lightweight Cryptography", NISTIR 8114, March 2017.

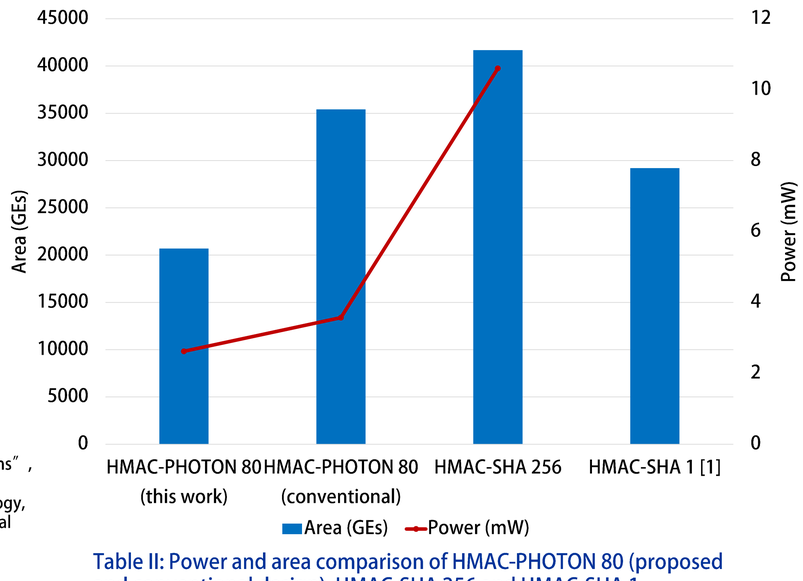


Table II: Power and area comparison of HMAC-PHOTON 80 (proposed and conventional design), HMAC-SHA 256 and HMAC-SHA 1

Acknowledgment

This research was supported by Korea Electric Power Corporation. (Grant number: R17XA05-70). This work was also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07042607).