FPGA-Based Lightweight Hardware Architecture of the PHOTON Hash Function for IoT Edge Devices

Journal:	*IEEE Access*
Manuscript ID	Access-2020-40888
Manuscript Type:	Regular Manuscript
Date Submitted by the Author:	17-Aug-2020
Complete List of Authors:	Al-Shatari, Mohammed; Universiti Teknologi PETRONAS, Electrical and Electronic Engineering Hussin, Fawnizu Azmadi B.; Universiti Teknologi PETRONAS, Electrical and Electronic Engineering Abd Aziz, Azrina; Universiti Teknologi PETRONAS, Electrical and Electronic Engineering Djaswadi, Gunawan Witjaksono; BRI Institute Tran, Xuan-Tu; VNU University of Engineering and Technology, Key Laboratory for Smart Integrated Systems
Keywords: Please choose keywords carefully as they help us find the most suitable Editor to review:	Field programmable gate arrays, Hardware, Information security, Cryptography, Encryption
Subject Category Please select at least two subject categories that best reflect the scope of your manuscript:	Circuits and systems, Computers and information processing
Additional Manuscript Keywords:	FPGA, Hardware Security, Lightweight Cryptography, PHOTON Hash Function, Sponge Construction

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

FPGA-Based Lightweight Hardware Architecture of the PHOTON Hash Function for IoT Edge Devices

Mohammed Al-Shatari[1], Student Member, IEEE, Fawnizu Azmadi Hussin[1], Senior Member, IEEE, Azrina Abd Aziz[1], Member, IEEE, Gunawan Witjaksono[2], Member, IEEE, Xuan-Tu Tran[3], Senior Member, IEEE

[1]Department of Electrical and Electronic Engineering, Universiti Teknologi Petronas, Seri Iskandar, Perak, Malaysia
[2]Department of Information Technology, BRI Institute of Technology & Business, Jakarta 12550, Indonesia
[3]SISLAB, VNU University of Engineering and Technology, Vietnam National University, Hanoi, Vietnam

Corresponding author: Mohammed Al-Shatari (e-mail: m.alshatari@gmail.com, mohammed_17005247@utp.edu.my).

This research was supported by the Yayasan UTP Fundamental Research Grant (YUTP-FRG) under grant scheme 015LC0-140

ABSTRACT PHOTON is an ultra-lightweight cryptographic hash function targeting low-resource devices. RFID and other resource-constrained devices' security raises major challenges to current cryptographic algorithms. The currently implemented hardware architectures of PHOTON hash function utilize high amount of resources and have low operating frequencies with low rate of throughputs. Performance of PHOTON architecture can be improved but at the cost of larger area utilization. Therefore, to improve the area-performance trade-offs of PHOTON hash function, an iterative architecture is implemented in this work. The concern is with the most lightweight version of PHOTON hash function with the hash size of 80 bits. It is implemented and verified on several Xilinx and Altera Field Programmable Gate Array (FPGA) devices using their synthesis and simulation tools. Low-cost and high-processing FPGA devices were both considered. The design is optimized for performance whereas the area utilization is also taken into consideration. The overall performance and logic utilization are benchmarked with the existing implementations. The results show an improvement rate of 10.26% to 51.04% in the speed performance and a reduction rate of 7.55% to 60.64% in area utilization compared to existing implementations of PHOTON hash functions.

INDEX TERMS FPGA, Hardware Security, Lightweight Cryptography, PHOTON Hash Function, Sponge Construction

I. INTRODUCTION

In our daily life, lightweight devices such as RFID cards are increasingly used in many applications either to grant access to private data or to be used in monitoring and control. These trending technologies have raised new challenges for cryptographers where private data could be leaked and modified through these low-processing devices resulting in high costs. Therefore, these devices should be secured with a high level of authentication to avoid such cases. Conventional and high-processing hash functions do not suit such constrained devices. As a result, several lightweight authentication schemes were proposed [1-4] and implemented in hardware and software on diverse platforms [5-10] with some applied cryptanalysis [11-13]. The internal structure of these hash function schemes is mainly focusing on the area-performance trade-offs with different size of message digest. They can be hardware-oriented or software-oriented, where some of them are compact in hardware and efficient in software too. The processing capabilities of the current lightweight hash functions are low due to the constraints of their applications resources. However, these devices need to process real-time data. Therefore, the area-performance trade-offs should be considered. PHOTON is a lightweight hash function proposed by J. Guo *et al.* [4]. It is compact in hardware and efficient in software. Its permutation is similar to LED block cipher [14] as they are both proposed by the same group, but with different sizes of data-path and state dimensions. LED has an AES-like permutation which can be designed in hardware with a very small area [15]. In the original paper of PHOTON hash function [4], the architecture was hardware-oriented and explored in Application Specific Integrated Circuit (ASIC) with the gate equivalent as the main parameter for area utilization. Lately, the design space exploration of PHOTON hash function was proposed by [5, 16, 17] on FPGA targeting different FPGA devices. The main limitation of the existing PHOTON architectures is the large utilization of logic area compared to the achieved frequency and throughput. In this work, PHOTON architecture is designed and implemented with the focus on high performance while considering the logic utilization too.

The contribution of this paper is in the implementation of efficient hardware architecture of PHOTON hash function achieving higher speed performance with smaller logic utilization than the existing designs. The algorithm of PHOTON hash function was designed in a way where all the permutation modules of a single round are executed in one clock cycle to achieve higher throughput. The linear feedback shift register (LFSR) used to generate the round constants is also utilized as a counter and a controller of the rounds. The intensive computation of the *MixColumns* module is reduced with the use of Look-Up Tables (LUTs) instead of Galois multiplication. The usage of LFSR and LUTs significantly reduces the utilization of logic resource.

II. PHOTON ALGORITHM

The algorithm of PHOTON hash function was designed with the main goal as lightweight and low-area utilization. The architecture of PHOTON algorithm is based on Sponge construction as shown in Figure 10, and introduced by Bertoni *et al*. [18]. It consists of two phases; the absorbing phase where the message m is fully absorbed and processed through the permutation function *f*, and the squeezing phase where the output hash *z* is squeezed and generated. The structure of the internal round permutation f is an AES-like with slight differences to allow low area implementation. PHOTON algorithm is described in their original paper [4]. They defined five variants of PHOTON hash function distinguished by the size of the hash output $(80 \leq n \leq 256)$ and the input and output bitrates *r* and r', respectively. Therefore, the function is indicated as PHOTON-$n/r/r'$. This also results in different security levels, performance and logic utilization. These different configurations of PHOTON are illustrated in Table I.

Bertoni *et al.* [18] also extended the Sponge construction to use different input and output rates for better security [19]. The internal state of PHOTON ($t=c+r$) is interpreted in a two-dimensional way, where *c* is the capacity and *r* is the rate. Therefore, the state size *t* depends on the capacity and rate to form the matrix dimensions ($d \times d$) with the cell size *s*. The parameter *d* determines the number of rows and columns in the two-dimensional matrix representation (d^2 cells) while the number of bits per cell is defined by the parameter *s*, where *s* $\in \{4, 8\}$, and thus $t = sd^2$. The input message *m* is permuted with the input rate *r* and concatenated with the capacity *c* to form the state *t* which is mapped to a matrix representation of dimension ($d \times d$) of the state *h* with *s* cell size as in (1).

$$h[i][j][k] = t[sdi + sj + k] \tag{1}$$

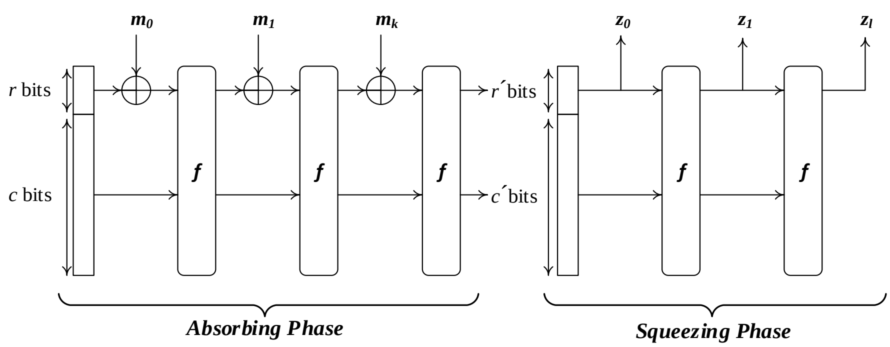

Figure 1. Sponge construction

TABLE I:
VARIANTS OF PHOTON HASH FUNCTION

PHOTON Variants	State Size *t* [bit]	Hash Digest *n* [bit]	Input Rate *r* [bit]	Output Rate r' [bit]	Capacity *c* [bit]	Cell Size *s* [bit]	Matrix Size *d* [cell]	Rounds N_r
PHOTON-80/20/16	100	80	20	16	80	4	5	12
PHOTON-128/16/16	144	128	16	16	128	4	6	12
PHOTON-160/36/36	196	160	36	36	160	4	7	12
PHOTON-224/32/32	256	224	32	32	224	4	8	12
PHOTON-256/32/32	288	256	32	32	256	8	6	12

The output is mapped to the size of the output rate r' to form the message digest n by concatenating the segments of output z.

The padding rule of PHOTON hash function is by appending the string 10* where the length of the message is a multiple of the rate r and defined as in (2).

$$pad\ (m) = m \mid\mid 1 \mid\mid 0^k \tag{2}$$

where, m is the message of an arbitrary length of {0,1} bit strings $m \in \mathbb{Z}_2^{\geq 0}$ and k = (|m|-1 mod r).

The state is initialized by a pre-defined initialization vector (IV) based on the variant of PHOTON as in (3).

$$IV = 0^{t-24} \mid\mid n/4 \mid\mid r \mid\mid r' \tag{3}$$

where t is the size of the internal state, n is the size of the output hash, r and r' are the input and output rates respectively.

The permutation and round function of PHOTON are very much like AES and composed of four modules; *AddConstants* (AC), *SubCells* (SC), *ShiftRows* (SR) and *MixColumns* (MC) as shown in Figure 2.

AddConstants (AC): There are two constants in this module; a four-bit round-dependent constant (RC) generated from a Linear Feedback Shift Register (LFSR), and a pre-defined d-dependent internal constant (IC_d). The *RC* is initialized to a specific value and updated every round by the LFSR whereas the IC_d is initialized based on the value of the dimension d. These two constants are both XORed with the first column of the $d \times d$ internal state. In this operation, only the first column is permuted while other columns are left unchanged. Overall, for N_r round number, the updated state is given as in (4).

$$h'[i,j] = h[i,j] \oplus RC_{N_r}(i) \oplus IC_d(i) \tag{4}$$

where, $h[i,j]$ is the current state, i represents the row number, j represents the column number, and N_r is the round number.

As the AC operation is dealing with the first column only, j is fixed to 0 as shown in (5).

$$h'[i,0] = h[i,0] \oplus RC_{N_r}(i) \oplus IC_d(i) \tag{5}$$

Therefore, the overall *AddConstants* function is as in (6).

$$\text{AC: } h'[i,j] = \begin{cases} h[i,0] \oplus RC_{N_r}(i) \oplus IC_d(i) & for\ \ j = 0 \\ h[i,j] & for\ \ 0 < j < d \end{cases} \tag{6}$$

<u>*SubCells (SC):*</u> The second operation of PHOTON is to perform cell substitution. PHOTON uses two different S-boxes based on the size of the cell s. For the variants where *s=4 bits*, PRESENT [20] S-Box $SB_{PRESENT}$ is used while AES [21] S-Box SB_{AES} is used for *s=8 bits* variant. Each cell of the state is replaced by a corresponding cell from the nonlinear S-Boxes. PRESENT S-Box is shown in Table II. The overall function of SubCells is given in (7).

$$\text{SC: } h'[i,j] = \begin{cases} SB_{PRESENT}(h[i,j]) & for\ \ s = 4 \\ SB_{AES}(h[i,j]) & for\ \ s = 8 \end{cases} \tag{7}$$

<u>*ShiftRows (SR):*</u> this function is almost identical to that of the AES transformation function. All the rows of the state matrix are rotated to the left by i cells (columns) where i is row index and starts counting from *0*. Within this module, the first row is not permuted, while other rows are updated accordingly. Therefore, the formal notation of SR function is as in (8).

$$\text{SR: } h'[i,j] = h[i,(i+j)\ mod\ d] \quad for\ \ 0 \leq i,j < d \tag{8}$$

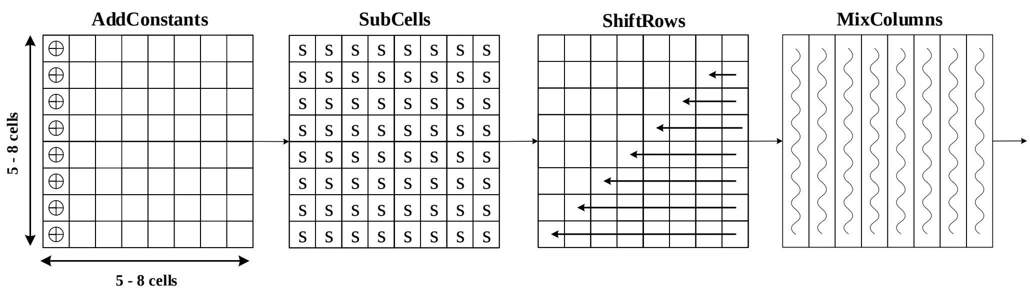

Figure 2. PHOTON Permutation

TABLE II
SUBSTITUTION BOX OF PRESENT CIPHER.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

MixColumns (MC): The MC is a finite field multiplication based on maximum distance separable (MDS) matrix. The columns of the internal state are independently multiplied with the pre-defined matrix based on the dimension size *d*. The design of *MC* for PHOTON has some shared similarities with AES but focusing on minimum area consumption. Matrix multiplication for the MC operation uses Galois Field with the irreducible polynomial x^4+x+1 for GF(2^4) when $s=4$ and the AES polynomial $x^8+x^4+x^3+x+1$ for GF(2^8) when $s=8$. MC for PHOTON is defined as in (9).

$$(h'[0,j],\dots,h'[d-1,j])^T = A_t^d \times (h[0,j],\dots,h[d-1,j])^T \quad (9)$$

where, *A* is the pre-defined *d*-dependent matrix, *t* is the size of the state. *A*, *d* and *t* are different for each PHOTON variant.

III. IMPLEMENTATION OF PHOTON ON FPGA

PHOTON architecture is designed in various flavors with different level of security with the focus on low-area utilization. It can be parallelized in a round-based mode for considerable throughput or it can also be designed in serialized nibble/byte-wise mode for low-area optimization. In this work, the architecture of the most lightweight variant of PHOTON hash function is presented. The design is based on PHOTON-80/20/16 variant with a hash size of 80-bit *n*, 20-bit input rate *r*, 16-bit output rate *r'*, 100-bit state size *t*, (5×5) state dimension d^2 and 4-bit cell size *s*. Verilog HDL is used to design the internal permutation and round functions of this architecture and implemented on several Altera and Xilinx FPGAs. Altera Quartus II and ModelSim are used as synthesis and simulation tools for Altera FPGAs whereas Xilinx ISE and ModelSim for Xilinx FPGAs. Figure 3 illustrates the block diagram of the proposed PHOTON-80/20/16 architecture. We have optimized the architecture for high throughput while considering the area utilization too.

We have considered only one 20-bit input message where we omitted the padding block for now. Therefore, only one message can be processed at a time. The initialization vector for PHOTON-80/20/16 is as in (10).

$$IV_{100} = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 4 & 1 & 4 & 1 & 0 \end{Bmatrix} \quad (10)$$

Therefore, the input capacity *c* and rate *r* are initialized with the *IV*, where *r* is the most left. For this variant of PHOTON, the width of $IV = t = c + r = 100$ bits. The rate *r* is XORed with the message and the result is concatenated with the capacity *c* and loaded into the *STR* register then input to the permutation block. PHOTON permutation processes the message in 12 rounds. In each round, these four functions are executed: *AddConstants*, *SubCells*, *ShiftRows* and *MixColumns*. After the last round, the 16-bit output *h* is generated

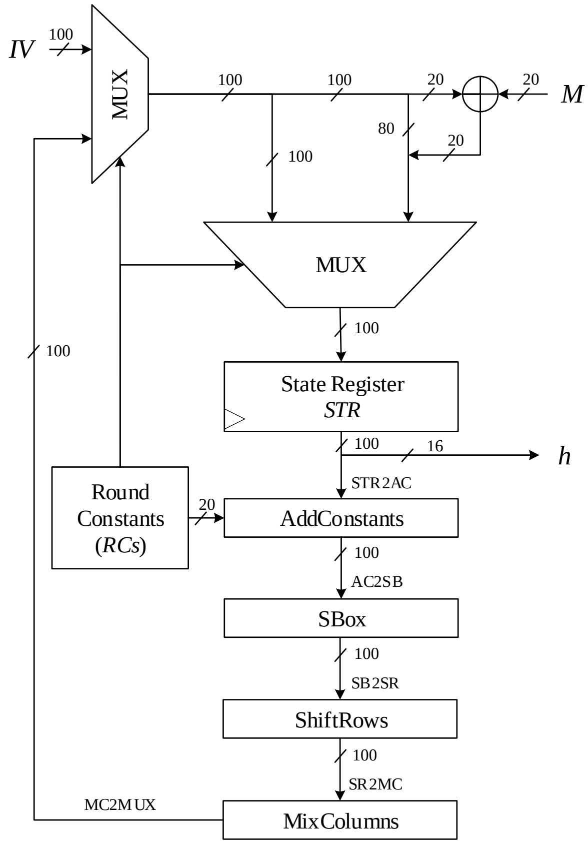

Figure 3. **Architecture of iterative round-based PHOTON-80/20/16**

In the *AddConstants* operation, the round constants are XORed with the internal constants and XORed with the first columns of the state and the result is passed to the *SubCells* module. The internal constants depend on the *d* size. For this PHOTON variant, $IC_d = [0,1,3,6,4]$ or using LFSR with feedback function $FB(X_r) = x_2\ NOR\ x_1$ for serial implementation. The round constants depend on the round number and the row position as shown in Table III.

TABLE III
ROUND CONSTANTS FOR PHOTON-80/20/16 (D = 5)

N_R / ROW	1	2	3	4	5	6	7	8	9	10	11	12
1	1	3	7	E	D	B	6	C	9	2	5	A
2	0	2	6	F	C	A	7	D	8	3	4	B
3	2	0	4	D	E	8	5	F	A	1	6	9
4	7	5	1	8	B	D	0	A	15	4	3	12
5	5	7	3	A	9	F	2	8	D	6	1	E

The *Round Constants* module is supplying the Internal Constants and round constants to the *AddConstants* module every round. Instead of using a round controller, the RC is utilized as a counter to control number of rounds and the output of both multiplexers to the state register, which reduces the logic resources.

The *SubCells* module depends on the size of the cell *s*. Since *s=4 bits* for PHOTON-80/20/16, the state is updated from the PRESENT substitution box given in Table II. Every cell in the state matrix is substituted by its corresponding value from PRESENT S-box and the result is input to the *ShiftRows* module.

The *ShiftRows* module distributes every single column over all columns by rotating the rows to the left by *i* nibble position for $(0 \leq i < d)$.

The *MixColumns* module is to enhance the diffusion property. It has the highest resource consumption among the PHOTON permutation blocks due to the matrix multiplication. The *MixColumns* finite multiplication can be designed in parallel by applying column-wise single multiplication with matrix *A* given in (11). It can also be serialized by multiplying matrix A^5 five times with the matrix columns independently. In this work, the design of *MixColumns* module is based on Look-up Tables (LUT) similar to the *SubCells* to mitigate the intensive computation of the matrix multiplication.

$$A_{100} = \begin{Bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 9 & 9 & 2 \end{Bmatrix}^5 = \begin{Bmatrix} 1 & 2 & 9 & 9 & 2 \\ 2 & 5 & 3 & 8 & D \\ D & B & A & C & 1 \\ 1 & F & 2 & 3 & E \\ E & E & 8 & 5 & C \end{Bmatrix} \quad (11)$$

The flow process of the proposed architecture of PHOTON-80/20/16 is illustrated in the ASM chart in Figure 4. It is a round-based architecture where the permutation module is applied in one cycle and the state register *STR* is loaded every round. Therefore, the twelve rounds of PHOTON will be achieved in 12 clock cycles. The round constants of the first row *Row0* are used as a round counter which controls the multiplexers and the loading of the state register *STR* and the output *Z*. When the RC of *Row0* is initialized to *0*, the *STR* register is loaded with the initialization vector IV where its first 20 bits are XORed with the input message *m*, and the LFSR is updated. When *Row0* is 10, it indicates the end of the twelve rounds. Therefore, the *STR* is updated directly from the *MixColumns* block, the output *z* is generated, and the RC is reinitialized. Otherwise, the *STR* is taking the output of the *MixColumns* and the LFSR is updated.

The architecture is implemented on various families of Altera and Xilinx FPGA devices including Arria and Cyclone from Altera and Spartan3, Virtex5, Artix7 and Kintex7 from Xilinx. Only 200 logic registers were utilized to implement PHOTON-80/20/16 where 100 bits are holding the state matrix, 20 bits are utilized by the round constants and also used as a counter and 80 bits holding the concatenating output. FPGA devices have different configuration of logic resources resulting in distinct performance and area utilization for each device. Old and low-processing FPGAs have smaller Look-Up Tables (LUT) while the latest and high-processing FPGA can have up to 6-input LUTs. The performance and logic-area utilization for Altera FPGA are illustrated in Table IV and Xilinx FPGA in Table V.

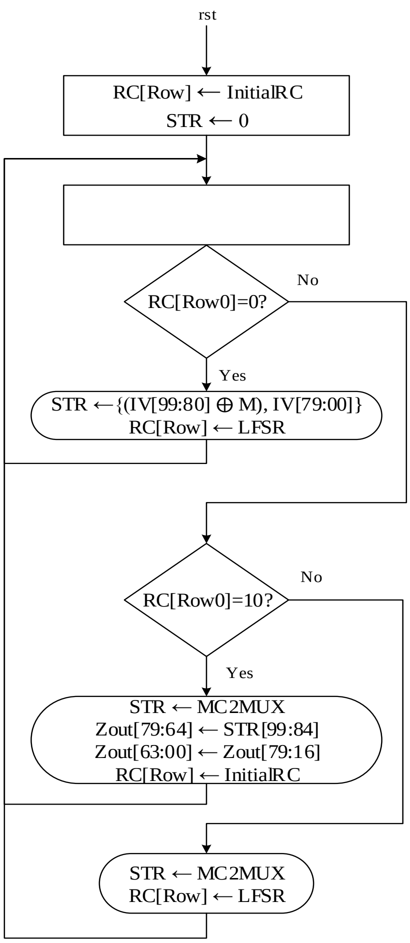

Figure 4. ASM chart of round-based PHOTON-80/20/16

V. RESULTS AND DISCUSSIONS

The architecture of PHOTON-80/20/16 variant is implemented on RTL using Verilog HDL. The design is verified on various FPGA devices from Xilinx and Altera using their respective synthesis and simulation tools. The whole permutation operation takes only one cycle to process 100 bits of data. The algorithm of PHOTON-80/20/16 takes 12 cycles/rounds to absorb one 20-bit input message and 48 cycles/rounds to squeeze the message and produce the 80-bit output digest.

Therefore, in this single-round architecture, the hash output is generated after 60 cycles as demonstrated in the simulation waveform in Figure 5. Twelve cycles/rounds are utilized by the absorbing phase of the sponge construction to process a single 20-bit input message, whereas the squeezing phase takes 48 cycles/rounds to produce the output of the 80-bit hash. Only 200 dedicated logic registers are used to process this variant of PHOTON hash where a 100-bit register is to update the state register, a 20-bit register holding the LFSR Round Constants and the counter and an 80-bit register is to hold the concatenated hash output. Several PHOTON hash function architectures of different design optimization goals were presented in [5, 16, 22] and implemented on Spartan3, Virtex5, Artix7 and Kintex7 FPGAs from Xilinx. The implementation of these existing designs utilizes large amount of logic resources compared to the achieved performance. The trade-off of our proposed architecture outperforms all the current existing works as illustrated in Table IV and Table V.

The architecture was implemented on several FPGA families from Altera and Xilinx. For Altera devices, there is no available work in the literature for PHOTON hash function. On these Altera families, our design utilizes around 500 logic elements (LEs) which are approximately 3% of the total FPGA logic resources. The proposed design achieves performance from 208.07 MHz to 380.66 MHz for operating frequency f_{max} and 346.78 Mbps to 634.43 Mbps for throughput. Table IV summarizes the results of PHOTON-80/20/16 implemented on Altera FPGAs

For Xilinx devices, PHOTON-80/20/16 was implemented on Spartan-3, Vertix-5, Artix-7 and Kintex-7. Performance results and logic utilization are improved compared to the available implementations in literature as shown in Table V with our results highlighted in bold. In this architecture, Xilinx FPGA devices utilize 126 to 265 slices and 363 to 510 Look-Up-Tables to implement this variant of PHOTON. They achieved a performance of 157.24 MHz to 376.43 MHz for operating frequency and 262.07 Mbps to 627.38 Mbps for throughput.

The efficiency is the ratio of the achieved throughput to the number of the utilized slices (Mbps/slices). This architecture achieves better trade-offs between performance and the utilization of logic area than other existing works. Therefore, the proposed architecture outperforms the existing works and achieves higher efficiency except for the case of [16] as they achieved higher efficiency at the cost of a very large area because their implementation of PHOTON was in double length sponge construction. For Spartan-3, an efficiency of 0.99 was achieved and it is much better than all the existing implementations except for the design proposed by [16] as they achieved slightly higher efficiency because their implementation is for high performance at the cost of 3x higher resources utilization. The implementation on Artix-7 and Kintex-7 achieves almost double the efficiency of the benchmarking architectures, with the same exception mentioned earlier. The detailed results of PHOTON-80/20/16 implementation on Xilinx FPGAs and their benchmarking existing results are shown in Table V.

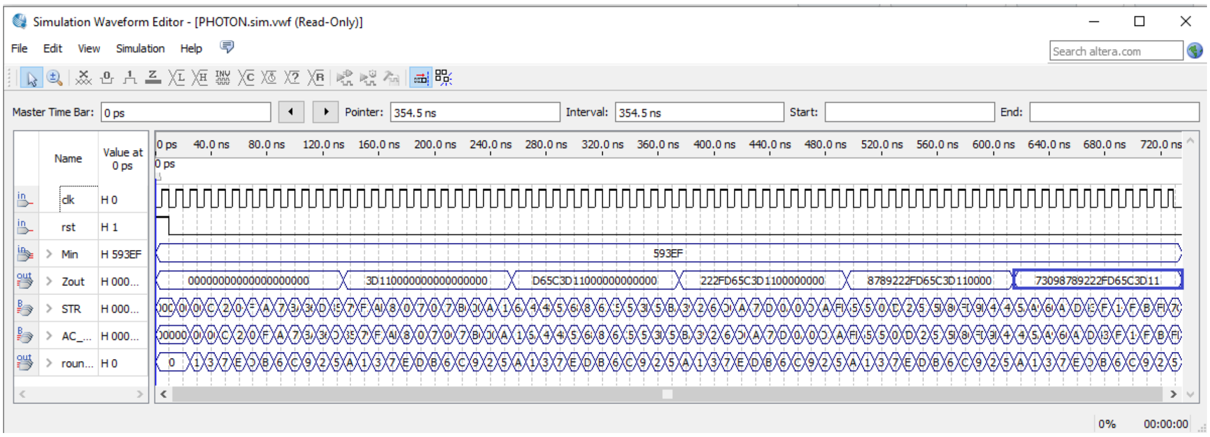

Figure 5. Simulation results of round-based PHOTON-80/20/16 with message (593EF)

TABLE IV
ROUND-BASED IMPLEMENTATION RESULTS OF PHOTON-80/20/16 HASH FUNCTION ON ALTERA FPGAS

Design	Data-path (bits)	No. of LEs	No. of FFs	No. of LUTs	No. of Clock Cycles	Max. Freq. (MHz)	T/put (Mbps)	Eff. (Mbps/LE)	FPGA Device
Our Paper Round-based	100	540	200	465	60	245.82	409.7	0.76	Cyclone II
	100	540	200	465	60	307.41	512.35	0.95	Cyclone III
	100	539	200	463	60	267.38	445.63	0.83	Cyclone III LS
	100	536	200	465	60	291.29	485.48	0.90	Cyclone IV E
	100	539	200	464	60	312.40	520.67	0.97	Cyclone IV GX
	100	238 (ALMs)	200	384	60	208.07	346.78	-	Cyclone V
	100	474 (ALMs)	200	385	60	380.66	634.43	-	Arria II GX

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

TABLE V
ROUND-BASED IMPLEMENTATION RESULTS OF PHOTON-80/20/16 HASH FUNCTION ON XILINX FPGAS

Design	Data-path (bits)	No. of slices	No. of FFs	No. of LUTs	No. of Clock Cycles	Max. Freq. (MHz)	T/put (Mbps)	Eff. (Mbps/slices)	FPGA Device
Our Paper Round-based	**100**	**265**	**200**	**510**	**60**	**157.24**	**262.07**	**0.99**	
Round-based [5]	100	285	127	565	12	78.53	130.88	0.46	
Serialized [5]	4	146	137	256	648	100.43	3.10	0.02	**Spartan-3 XC3S50-5**
SRL16 [5]	20	112	68	20.	360	118.19	6.57	0.06	
DLP-PHOTON [16]	100	615	-	-	-	308	1027	1.67	
Our Paper Round-based	**100**	**145**	**188**	**363**	**60**	**376.43**	**627.38**	**4.33**	
Round-base [5]	100	142	111	336	12	232.65	387.75	2.73	
Serialized [5]	4	67	134	167	648	329.51	10.17	0.15	**Artix-7 XC7A100T-3**
SRL16 [5]	20	58	89	144	360	329.95	18.33	0.32	
DLP-PHOTON [16]	100	402	-	-	-	903	3010	7.48	
Our Paper Round-based	**100**	**188**	**200**	**425**	**60**	**337.27**	**562.12**	**2.99**	
Serialized [5]	4	82	135	188	648	302.68	9.34	0.11	
SRL16 [5]	20	69	89	759	360	285.2	15.84	0.22	**Virtex-5 XC5VLX50-1**
Iterative [22]	20	302	415	508	12	172.7	287.83	0.95	
Folding [22]	20	251	414	515	24	205.7	171.42	0.68	
Unrolling [22]	20	1066	411	3065	1	25.43	508.6	0.48	
Our Paper Round-based	**100**	**126**	**188**	**366**	**60**	**358.42**	**597.37**	**4.7**	**Kintex-7 XC7K70T-1**

VI. CONCLUSION

An iterative architecture of PHOTON-80/20/16 lightweight hash function is implemented on several Altera and Xilinx FPGA devices. It is a round-based architecture where all the permutation operations are executed in one round. The absorbing phase of the sponge construction takes 12 rounds to process a single 20-bit input message. The squeezing phase takes 48 rounds to produce the output of the 80-bit hash. The proposed design achieves better area-performance trade-offs than the existing designs as the architecture of the *MixColumns* module is designed using look-up tables to avoid the intensive computations of the multipliers. The round constants are also utilized as rounds counter to reduce the logic resources. It consumes less logic resource and achieves higher performance resulting in a higher efficiency. For future work, it is recommended to serialize PHOTON architecture for smaller area utilization and authenticating the existing lightweight block ciphers which have similar internal architecture.

ACKNOWLEDGMENT

The authors would like to acknowledge the support from Universiti Teknologi PETRONAS for providing the Graduate Assistantship (GA) and Graduate Research Assistantship (GRA) as this research is supported by the Yayasan UTP Fundamental Research Grant (YUTP-FRG) under grant scheme 015LC0-140.

REFERENCES

[1] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede, "SPONGENT: A lightweight hash function," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2011: Springer, pp. 312-325.

[2] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak sponge function family main document," *Submission to NIST (Round 2),* vol. 3, no. 30, 2009.

[3] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A lightweight hash," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2010: Springer, pp. 1-15.

[4] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Annual Cryptology Conference*, 2011: Springer, pp. 222-239.

[5] N. N. Anandakumar, T. Peyrin, and A. Poschmann, "A very compact FPGA implementation of LED and PHOTON," in *International Conference on Cryptology in India*, 2014: Springer, pp. 304-321.
[6] B. Jungk, L. R. Lima, and M. Hiller, "A systematic study of lightweight hash functions on FPGAs," in *2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14)*, 2014: IEEE, pp. 1-6.
[7] F. Kahri, H. Mestiri, B. Bouallegue, and M. Machhout, "High speed FPGA implementation of cryptographic KECCAK hash function crypto-processor," *Journal of Circuits, Systems and Computers,* vol. 25, no. 04, p. 1650026, 2016.
[8] E. Aerabi, M. Bohlouli, M. H. A. Livany, M. Fazeli, A. Papadimitriou, and D. Hely, "Design Space Exploration for Ultra-Low-Energy and Secure IoT MCUs," *ACM Transactions on Embedded Computing Systems (TECS),* vol. 19, no. 3, pp. 1-34, 2020.
[9] R. Martino and A. Cilardo, "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey," *IEEE Access,* vol. 8, pp. 28415-28436, 2020.
[10] A. Alzahrani and F. Gebali, "Multi-Core Dataflow Design and Implementation of Secure Hash Algorithm-3," *IEEE Access,* vol. 6, pp. 6092-6102, 2018.
[11] K. Bussi, D. Dey, P. R. Mishra, and B. Dass, "MGR Hash Functions," *Cryptologia,* vol. 43, no. 5, pp. 372-390, 2019.
[12] C.-Y. Lu, Y.-W. Lin, S.-M. Jen, and J.-F. Yang, "Cryptanalysis on PHOTON hash function using cube attack," in *2012 International Conference on Information Security and Intelligent Control*, 2012: IEEE, pp. 278-281.
[13] C. Dobraunig and B. Mennink, "Key Recovery Attack on PHOTON-Beetle."
[14] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2011: Springer, pp. 326-341.
[15] M. Al-Shatari, F. A. Hussin, A. A. Aziz, G. Witjaksono, M. S. Rohmad, and X. T. Tran, "An Efficient Implementation of LED Block Cipher on FPGA," presented at the First International Conference of Intelligent Computing and Engineering (ICOICE), 2019.
[16] B. T. Hammad, Y. A. Abbas, N. Jamil, M. E. Rusli, and M. R. Zaba, "FPGA Implementation of DLP-PHOTON Hash Function," *International Journal of Future Generation Communication and Networking,* vol. 10, no. 12, pp. 71-78, 2017.
[17] B. Jungk, "FPGA-based evaluation of cryptographic algorithms," Goethe University Frankfurt am Main, 2016.
[18] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "On the indifferentiability of the sponge construction," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2008: Springer, pp. 181-197.
[19] N. Kishore and P. Raina, "Parallel cryptographic hashing: Developments in the last 25 years," *Cryptologia,* vol. 43, no. 6, pp. 504-535, 2019.
[20] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2007: Springer, pp. 450-466.
[21] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.
[22] N. N. Anandakumar, "SCA Resistance Analysis on FPGA Implementations of Sponge Based MAC-PHOTON," in *International Conference for Information Technology and Communications*, 2015: Springer, pp. 69-86.

MOHAMMED AL-SHATARI (Student Member, IEEE) received the bachelor's degree. in computer engineering and the master's degree in electronic and telecommunication from Universiti Teknologi Malaysia (UTM), Skudai, Johor Bahru, Malaysia, in 2013 and 2016 respectively. He is Ph.D. student and graduate assistant at the Department of Electrical and Electronic Engineering, at Universiti Teknologi PETRONAS (UTP), Seri Iskandar, Perak, Malaysia. His recent research interest is in hardware security and cryptography.

FAWNIZU AZMADI HUSSIN (M'02, SM'14) received the bachelor's degree in electrical engineering from the University of Minnesota, Twin Cities, Minneapolis, MN, USA, in 1999 under PETRONAS scholarship, the M.Eng.Sc. degree in systems and control from the University of New South Wales, Sydney, NSW, Australia, in 2001 under UTP scholarship, and the Ph.D. degree in core-based testing of system-on-a-chip (SoCs) from the Nara Institute of Science and Technology, Ikoma, Japan, in 2008, under the scholarship from the Japanese Government (Monbukagakusho). He is currently an Associate Professor of Electrical & Electronic Engineering at Universiti Teknologi Petronas. He was the Program Manager of Master by coursework program (2009-2013), the Deputy Head of Electrical & Electronic Engineering department (2013-2014) and the Director of Strategic Alliance Office (2014-2018) at UTP. He spent one year as a Visiting Professor at Intel Microelectronics (Malaysia)'s SOC DFx department in 2012-13. He is actively involved with the IEEE Malaysia Section as volunteers since 2009. He was the 2013 & 2014 Chair of the IEEE Circuits and Systems Society Malaysia Chapter and currently serving as the Chair of IEEE Malaysia Section (2019 & 2020).

AZRINA ABD AZIZ (M'07) received the bachelor's degree (Hons.) in electrical and electronic engineering from the University of Queensland, Australia, in 1997, the M.Sc. degree in system level integration from the Institute for System Level Integration, U.K., in 2003, and the Ph.D. degree in electrical and computer systems engineering from Monash University, Melbourne, Australia, in 2013. She is currently a Lecturer with the Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Malaysia, where she is also a member of the Centre for Intelligent Signal and Imaging Research Group. Her recent research interests focus on energy-efficient techniques for topology control in wireless sensor networks and wireless body area networks for biomedical applications and medical imaging. She is a member of the Board of Engineers Malaysia.

GUNAWAN WITJAKSONO BIN DJASWADI received the B.S. (magna cum laude) and M.S. degrees in electrical engineering from Michigan Technological University, Houghton, MI, USA, in 1992 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Wisconsin–Madison in 2002. From 1994 to 1996, he was with the National Aeronautics and Space Agency, Indonesia. In 2002, he joined Denselight Semiconductors Pte Ltd., Singapore, where he developed high-speed, long wavelength, and distributed feedback lasers. He was with Finisar Malaysia to develop uncooled and high-speed optical transceiver. He was with the Department of Electrical Engineering, University of Indonesia, from 2005 to 2007, before joining MIMOS when he held various key positions such as a Principal Researcher and the Director of Research and Sensor System Architect, until 2016. He is currently an Associate Professor with the Electrical and Electronics Department, Universiti Teknologi PETRONAS, where he is also an Indonesia-Chapter Professional Engineer.

XUAN-TU TRAN (Senior Member, IEEE) received the Ph.D. degree in micro nano electronics from Grenoble INP (at the CEA-LETI), France, in 2008. He is currently an Associate Professor with the VNU University of Engineering and Technology, Vietnam National University (VNU), Hanoi. He was an Invited Professor with the University Paris-Sud 11, France, in 2009, 2010, and 2015, the University of Electro-Communication, Tokyo, in 2019, Grenoble INP, in 2011 and 2020, and an Adjunct Professor with University of Technology Sydney, from 2017 to 2020. He is currently the Director of the VNU Key Laboratory for Smart Integrated Systems (SISLAB). His research interests include design and test of systems-on-chips, networks-on-chips, design-for-testability, asynchronous/synchronous VLSI design, low-power techniques, and hardware architectures for multimedia applications. He has published more than 80 journal articles and conference papers in these areas and given invited talks as well as courses at several universities. He is a Senior Member of the IEEE Circuits and Systems (CAS), IEEE Solid-State Circuits and Systems (SSCS), member of IEICE, and the Executive Board of the Radio Electronics Association of Vietnam (REV). He serves as the Chairman of IEICE Vietnam Section and the IEEE SSCS Vietnam Chapter

MOHAMMED AL-SHATARI (Student Member, IEEE) received the bachelor's degree. in computer engineering and the master's degree in electronic and telecommunication from Universiti Teknologi Malaysia (UTM), Skudai, Johor Bahru, Malaysia, in 2013 and 2016 respectively. He is Ph.D. student and graduate assistant at the Department of Electrical and Electronic Engineering, at Universiti Teknologi PETRONAS (UTP), Seri Iskandar, Perak, Malaysia. His recent research interest is in hardware security and cryptography.

FAWNIZU AZMADI HUSSIN (M'02, SM'14) received the bachelor's degree in electrical engineering from the University of Minnesota, Twin Cities, Minneapolis, MN, USA, in 1999 under PETRONAS scholarship, the M.Eng.Sc. degree in systems and control from the University of New South Wales, Sydney, NSW, Australia, in 2001 under UTP scholarship, and the Ph.D. degree in core-based testing of system-on-a-chip (SoCs) from the Nara Institute of Science and Technology, Ikoma, Japan, in 2008, under the scholarship from the Japanese Government (Monbukagakusho). He is currently an Associate Professor of Electrical & Electronic Engineering at Universiti Teknologi Petronas. He was the Program Manager of Master by coursework program (2009-2013), the Deputy Head of Electrical & Electronic Engineering department (2013-2014) and the Director of Strategic Alliance Office (2014-2018) at UTP. He spent one year as a Visiting Professor at Intel Microelectronics (Malaysia)'s SOC DFx department in 2012-13. He is actively involved with the IEEE Malaysia Section as volunteers since 2009. He was the 2013 & 2014 Chair of the IEEE Circuits and Systems Society Malaysia Chapter and currently serving as the Chair of IEEE Malaysia Section (2019 & 2020).

AZRINA ABD AZIZ (M'07) received the bachelor's degree (Hons.) in electrical and electronic engineering from the University of Queensland, Australia, in 1997, the M.Sc. degree in system level integration from the Institute for System Level Integration, U.K., in 2003, and the Ph.D. degree in electrical and computer systems engineering from Monash University, Melbourne, Australia, in 2013. She is currently a Lecturer with the Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Malaysia, where she is also a member of the Centre for Intelligent Signal and Imaging Research Group. Her recent research interests focus on energy-efficient techniques for topology control in wireless sensor networks and wireless body area networks for biomedical applications and medical imaging. She is a member of the Board of Engineers Malaysia.

GUNAWAN WITJAKSONO BIN DJASWADI received the B.S. (magna cum laude) and M.S. degrees in electrical engineering from Michigan Technological University, Houghton, MI, USA, in 1992 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Wisconsin–Madison in 2002. From 1994 to 1996, he was with the National Aeronautics and Space Agency, Indonesia. In 2002, he joined Denselight Semiconductors Pte Ltd., Singapore, where he developed high-speed, long wavelength, and distributed feedback lasers. He was with Finisar Malaysia to develop uncooled and high-speed optical transceiver. He was with the Department of Electrical Engineering, University of Indonesia, from 2005 to 2007, before joining MIMOS when he held various key positions such as a Principal Researcher and the Director of Research and Sensor System Architect, until 2016. He is currently an Associate Professor with the Electrical and Electronics Department, Universiti Teknologi PETRONAS, where he is also an Indonesia-Chapter Professional Engineer.

XUAN-TU TRAN (Senior Member, IEEE) received the Ph.D. degree in micro nano electronics from Grenoble INP (at the CEA-LETI), France, in 2008. He is currently an Associate Professor with the VNU University of Engineering and Technology, Vietnam National University (VNU), Hanoi. He was an Invited Professor with the University Paris-Sud 11, France, in 2009, 2010, and 2015, the University of Electro-Communication, Tokyo, in 2019, Grenoble INP, in 2011 and 2020, and an Adjunct Professor with University of Technology Sydney, from 2017 to 2020. He is currently the Director of the VNU Key Laboratory for Smart Integrated Systems (SISLAB). His research interests include design and test of systems-on-chips, networks-on-chips, design-for-testability, asynchronous/synchronous VLSI design, low-power techniques, and hardware architectures for multimedia applications. He has published more than 80 journal articles and conference papers in these areas and given invited talks as well as courses at several universities. He is a Senior Member of the IEEE Circuits and Systems (CAS), IEEE Solid-State Circuits and Systems (SSCS), member of IEICE, and the Executive Board of the Radio Electronics Association of Vietnam (REV). He serves as the Chairman of IEICE Vietnam Section and the IEEE SSCS Vietnam Chapter.