ABOUT A LIGHTWEIGHT BLOCK CIPHER, HIGH-SPEED ENCRYPTION ON VIRTEX6 CHIP GEARED TOWARDS WIRELESS SENSOR NETWORKS

Do Thi Bac*, Au The Linh

TNU - University of Information and Communication Technology

ARTICLE INFO	ABSTRACT
<p>Received: 04/8/2021</p> <p>Revised: 15/11/2021</p> <p>Published: 15/11/2021</p>	<p>The article of the study is the lightweight block cipher Crypt(BM)_64A and the performance evaluation model on FPGA (Field-programmable gate array) reconfigurable hardware. On that basis, the researcher executed the Crypt(BM)_64A block cipher on the Virtex6-XC6VLX75T/FF484 chip in the base cipher ring mode to evaluate its suitability for wireless applications through the cost of resources, throughput, etc. At the same time, the study also compared the efficiency of the Crypt(BM)_64A algorithm with the widely used encryption algorithms like the in the AES competition. Thereby the study will help system developers to have more grounds to choose the right encryption data security solution for each specific intensive application that the system is expecting to target. The results of research and the implementation of block cipher Crypt(BM)_64A on FPGA with Vertex6 series XC6VLX75T/FF484 confirmed that Crypt(BM)_64A is a complete lightweight block cipher algorithm which is suitable for applications for wireless sensor networks with high integration efficiency, low cost of the area, ensuring compactness, limited power dissipation through high- clock.</p>
<p>KEYWORDS</p> <p>Lightweight block cipher</p> <p>Field-programmable gate array</p> <p>Block cipher</p> <p>Wireless sensor network</p> <p>CSPN (controllable permutation network)</p>	

VỀ MỘT THUẬT TOÁN MÃ KHỐI HẠNG NHẹ, MÃ HÓA TỐC ĐỘ CAO TRÊN CHIP VIRTEX6 HƯỚNG TỚI ỨNG DỤNG CHO MẠNG CẢM BIẾN KHÔNG DÂY

Đỗ Thị Bắc*, Âu Thế Linh

Trường Đại học Công nghệ thông tin và Truyền thông – ĐHTT Thái Nguyên

THÔNG TIN BÀI BÁO	TÓM TẮT
<p>Ngày nhận bài: 04/8/2021</p> <p>Ngày hoàn thiện: 15/11/2021</p> <p>Ngày đăng: 15/11/2021</p>	<p>Bài báo nghiên cứu về thuật toán mã hóa khối hạng nhẹ Crypt(BM)-_64A và mô hình đánh giá hiệu quả trên phần cứng có khả năng tái cấu hình FPGA (Field-programmable gate array). Trên cơ sở đó tiến hành thực thi thuật toán mã hóa khối Crypt(BM)_64A trên chip Virtex6-XC6VLX75T/FF484 ở chế độ vòng mã hóa cơ sở để đánh giá tính phù hợp của nó cho các ứng dụng không dây thông qua các chi phí về tài nguyên, thông lượng,... Đồng thời, nghiên cứu cũng thực hiện so sánh hiệu quả thuật toán Crypt(BM)_64A với một số các thuật toán mã hóa đang được sử dụng rộng rãi như các thuật toán trong cuộc thi AES. Qua đó giúp các nhà phát triển hệ thống có thêm căn cứ trong việc lựa chọn giải pháp bảo mật dữ liệu bằng mã hóa phù hợp cho mỗi ứng dụng chuyên sâu cụ thể mà hệ thống dự kiến hướng tới. Kết quả nghiên cứu và thực thi thuật toán mã hóa khối Crypt(BM)_64A trên FPGA với dòng Vertex6 mã hiệu XC6VLX75T/FF484 có thể khẳng định, Crypt(BM)_64A là thuật toán mã hóa khối hạng nhẹ hoàn toàn phù hợp với các ứng dụng cho các mạng cảm biến không dây với hiệu quả tích hợp cao; chi phí về diện tích thấp, đảm bảo tính gọn nhẹ; tiêu hao năng lượng hạn chế thông qua xung nhịp cao.</p>
<p>TỪ KHÓA</p> <p>Mã hóa khối hạng nhẹ</p> <p>Công nghệ FPGA</p> <p>Mã khối</p> <p>Mạng cảm biến không dây</p> <p>CSPN (mạng hoán vị thay thế điều khiển được)</p>	

DOI: <https://doi.org/10.34238/tnu-jst.4843>

* Corresponding author. Email: dtbac@ictu.edu.vn

1. Giới thiệu

Với sự bùng nổ của cách mạng công nghệ số ngày nay, sự phát triển mạnh mẽ của dịch vụ số, đi kèm theo đó việc giữ thông tin, an toàn bảo mật dữ liệu của các hệ thống luôn luôn được chú trọng để nâng cao độ trên nhiều phương diện như độ an toàn, tính hiệu quả. Tuy nhiên, những năm gần đây tính hiệu quả được các nhà phát triển ứng dụng đánh giá và mong đợi. Bản chất là do các thuật toán bảo mật truyền thống dần dần không còn phù hợp trong các hệ thống nói chung và đặc biệt các ứng dụng chuyên biệt như mạng cảm biến không dây (WSN-Wireless Sensor Networks), điện thoại di động, các thiết bị cầm tay PDA,... Đặc trưng cơ bản của các thiết bị này là tính hạn chế về nguồn năng lượng, hạn chế về khả năng tính toán, hạn chế về diện tích bề mặt, yêu cầu có thể làm việc trong các môi trường khắc nghiệt khác nhau, trong các lĩnh vực khác nhau nhưng yêu cầu về tính an toàn bảo mật của chúng lại không giảm, đòi hỏi tốc độ truyền thông cao, đáp ứng chế độ thời gian thực, giá thành rẻ,... [1]. Vì vậy, việc xây dựng các thuật toán mã hóa chuyên biệt nhằm hướng đến ứng dụng riêng trong các mạng truyền thông không dây tốc độ cao và đạt hiệu năng cao trong thiết kế là yếu tố quan trọng, cấp thiết và phù hợp với sự phát triển của công nghệ ngày nay. Đây là vấn đề đã được các nhà khoa học về mật mã quan tâm, đại diện như các nghiên cứu [2]-[8] về thuật toán mật mã khối trên cơ sở mạng hoán vị thay thế được điều khiển (CSPN-Controlled Substitution Permutation Network) nhằm đáp ứng cho các yêu cầu về tốc độ đường truyền, thời gian thực, giá thành rẻ, hiệu năng sử dụng cao. Do vậy, giải pháp này đảm bảo được các yêu cầu đối với một mã hóa hạng nhẹ nhằm ứng dụng cho các hệ thống cảm biến như: phản hồi thời gian thực, chi phí thiết bị thấp, diện tích nhỏ, tiêu hao năng lượng ít, xong tốc độ xử lý cao.

Mặt khác, khi xây dựng một thuật toán mã khối hạng nhẹ, tốc độ cao cho một ứng dụng cụ thể, các tiêu chí thường được quan tâm như: tính an toàn, giá thành, năng lượng tiêu thụ, tốc độ mã hóa và giải mã, diện tích bộ nhớ, khả năng chống lại sự thám mã vi sai,... Do đó, để có nhiều sự lựa chọn thuật toán phù hợp với từng ứng dụng đó, trong bài báo này chúng tôi chứng minh tính phù hợp của thuật toán Crypt(BM)_64A [4] là mã khối hạng nhẹ, tốc độ cao phù hợp với các tiêu chí hướng tới là: Cài đặt trên FPGA cụ thể, ứng dụng trong các mạng cảm biến không dây đòi hỏi hiệu năng và tốc độ cao.

Bài báo được tổ chức như sau: Phần 1, giới thiệu tổng quan; Phần 2, trình bày thuật toán; Phần 3, trình bày về các thông số đánh giá khi thực hiện trên FPGA; Phần 4, triển khai thực hiện trên CHIP Virtex6-XC6VLX75T/FF484 và kết luận.

2. Mô hình thiết kế hình thức của thuật toán mã hóa Crypt(BM)_64A

Crypt(BM)_64A là thuật toán được phát triển bởi nhóm tác giả Đỗ Thị Bắc và Nguyễn Hiếu Minh [4]. Đây là thuật toán được thiết kế nhằm hướng tới sử dụng trong các mạng cảm biến không dây với nhiều ưu thế đã được công bố trước đó về độ an toàn và khả năng thay đổi khóa phiên thường xuyên.

Crypt(BM)_64A được thiết kế theo mô hình song song trong vòng mã hóa cơ sở và CSPN được thiết kế theo phương pháp đồng nhất. Crypt(BM)_64A có độ dài khối là 64 bit, với 10 vòng biến đổi và khóa có độ dài là 128 bit hoặc 192 bit hoặc 256 bit. Crypt(BM)_64A được xây dựng trên cơ sở phân tử nguyên thủy $Q_{2/1}$. Sơ đồ một vòng mã hóa cơ sở của Crypt(BM)_64A như hình 1a. Quá trình thiết kế CSPN sử dụng trong thuật toán được mô tả như sau: $Q_{2/1} \rightarrow Q_{4/4} \rightarrow Q_{16/32}$. Chi tiết thiết kế các phân tử trong thuật toán được mô tả trong hình 1.

Quá trình thực hiện của thuật toán được mô tả như sau:

Thuật toán Crypt(BM)_64A

1. 64 bit dữ liệu vào được chia thành 2 khối A và B, mỗi khối có kích thước 32 bit
2. For $j = 1$ to 9 do $\{(A, B) \leftarrow \text{Crypt}^{(e)}(A, B, Q_j, U_j); (A, B) \leftarrow (B, A)\}$
3. $\{(A, B) \leftarrow \text{Crypt}^{(e)}(A, B, Q_{10}, U_{10})\}$
4. $\{(A, B) \leftarrow (A \oplus Q_{11}, B \oplus U_{11})\}$

Trong hình 1 các hoán vị được mô tả như sau:

$I = (1) (2, 9) (3, 17) (4, 25) (5) (6, 13) (7, 21) (8, 29) (9, 2) (10) (11, 18) (12, 26) (13, 6) (14) (15, 22) (16, 30) (17, 3) (18, 11) (19) (20, 27) (21, 7) (22, 15) (23) (24, 31) (25, 4) (26, 12) (27, 20) (28) (29, 8) (30, 16) (31, 24) (32);$

$I_1 = (1, 9) (2, 13) (3, 10) (4, 14) (5, 11) (6, 15) (7, 12) (8, 16) (9, 1) (10, 3) (11, 5) (12, 7) (13, 2) (14, 4) (15, 6) (16, 8);$

$P = (1) (2, 5) (3, 9) (4, 13) (5, 2) (6) (7, 10) (8, 14) (9, 3) (10, 7) (11) (12, 15) (13, 4) (15, 12) (16);$

- Khối mở rộng E được xây dựng như sau: $E(X) = (X, X^{\ll 8})$.

Khóa vòng U_j/Q_j (mã hóa) hoặc Q'_j/U'_j (giải mã) của thuật toán Crypt(BM)_64A được lựa chọn từ các khóa con K_i và được liệt kê chi tiết trong bảng 1. Lịch biểu sử dụng khóa trong bảng 1 được xây dựng cho cả 3 cấp độ khóa 128 bit, 192 bit và 256 bit.

Hình 1. Sơ đồ thiết kế của thuật toán Crypt(BM)_64A
a) Vòng mã hóa cơ sở, b) $Q_{4/4}$ và $Q^{-1}_{4/4}$, c) $Q_{16/32}$ và $F^{-1}_{16/32}$.

Bảng 1. Lịch đồ khóa sử dụng trong Crypt(BM)_64A

Vòng	1	2	3	4	5	6	7	8	9	10	FT=11
Khóa 128 bit											
Q_j/U_j	K_1/K_3	K_2/K_3	K_3/K_2	K_4/K_1	K_4/K_2	K_1/K_3	K_4/K_3	K_1/K_2	K_2/K_4	K_4/K_1	K_1/K_3
Q'_j/U'_j	K_1/K_3	K_4/K_1	K_2/K_4	K_1/K_2	K_4/K_3	K_1/K_3	K_4/K_2	K_4/K_1	K_3/K_2	K_2/K_3	K_1/K_3
Khóa 192 bit											
Q_j/U_j	K_1/K_3	K_2/K_4	K_5/K_6	K_2/K_1	K_4/K_6	K_5/K_3	K_2/K_3	K_1/K_3	K_3/K_2	K_6/K_5	K_1/K_3
Q'_j/U'_j	K_1/K_3	K_6/K_5	K_3/K_2	K_1/K_3	K_2/K_3	K_5/K_3	K_4/K_6	K_2/K_1	K_5/K_6	K_2/K_4	K_1/K_3
Khóa 256 bit											
Q_j/U_j	K_1/K_3	K_2/K_4	K_5/K_8	K_7/K_6	K_4/K_2	K_2/K_8	K_6/K_5	K_1/K_3	K_3/K_7	K_7/K_4	K_1/K_3
Q'_j/U'_j	K_1/K_3	K_7/K_4	K_3/K_7	K_1/K_3	K_6/K_5	K_2/K_8	K_4/K_2	K_7/K_6	K_5/K_8	K_2/K_4	K_1/K_3

3. Mô hình thiết kế trên FPGA thuật toán mã hóa

Thông thường chi phí về tài nguyên (**Resource**) của mỗi thiết kế được xác định thông qua các chi phí theo một trong các thông số sau: số lượng slices; số lượng flip flop; số CLB (Configurable Logic Block); số lượng LUT (Look-Up Table); số lượng IOB (Input/Output Block); số lượng Block Select RAMs (BRAMs). Sự so sánh lý tưởng sẽ là so sánh về toàn bộ các nguồn tài nguyên trên và cùng được thiết kế trên các dòng thiết bị FPGA tương tự. Người ta cho rằng, thiết kế thuật toán có tốc độ mã/giải mã nhanh nhất là thiết kế mà có được kết quả tốc độ cao nhất (chỉ quan tâm đến lưu lượng thông tin) dù cho đó là loại thiết bị nào đã được dùng để triển khai thiết kế. Tuy nhiên, để đánh giá thiết kế thuật toán là hiệu quả (thiết kế được tối ưu hóa cho tài nguyên phần cứng) thì cần sử dụng kết quả so sánh giữa những thiết bị giống nhau để đưa ra thông số chi phí về tài nguyên bộ nhớ. Như vậy, cả tài nguyên và thông lượng đều giúp đánh giá hiệu quả của các thiết kế. Tuy nhiên, nhằm quyết định việc một thiết kế nào đó là hiệu quả hay không, cần xem xét thêm một số yếu tố khác như: Thông lượng/Tài nguyên, thông lượng/(tài

nguyên * tần số). Các thông số này cũng được nhóm phát triển sử dụng để công bố trong kết quả nghiên cứu dưới đây.

4. Thiết kế của thuật toán Crypt(BM)_64A trên FPGA CHIP Virtex6-XC6VLX75T/FF484

FPGA là một loại mạch tích hợp cỡ lớn, dùng cấu trúc mảng phần tử logic để người dùng có thể lập trình được. Trong công đoạn thiết kế để tối ưu hóa các mục tiêu, giảm chi phí, rút ngắn thời gian đưa sản phẩm vào sử dụng, các nhà thiết kế ứng dụng chọn giải pháp dùng FPGA, còn nếu so sánh với các dạng khác như PLA, PAL, CPLD thì FPGA ưu việt hơn bởi các yếu tố sau: tác vụ tái lập trình của FPGA thực hiện đơn giản hơn; khả năng lập trình linh động hơn; khác biệt quan trọng nhất là kiến trúc của FPGA cho phép nó có khả năng chứa khối lượng lớn cổng logic (logic gate), so với các vi mạch bán dẫn lập trình được trước đó. Thiết kế trên FPGA được thực hiện chủ yếu bằng các ngôn ngữ mô tả phần cứng HDL như VHDL, Verilog, AHDL. Các hãng sản xuất FPGA lớn như Xilinx, Altera thường cung cấp các gói phần mềm và thiết bị phụ trợ cho quá trình thiết kế. Nhiều hãng thứ ba cung cấp các gói phần mềm kiểu này như Synopsys, Synplify... Các gói phần mềm này có khả năng thực hiện tất cả các bước của toàn bộ quy trình thiết kế IC chuẩn với đầu vào là mã thiết kế trên HDL.

Hình 3. Giới thiệu Chip Virtex®-6

Để có các kết quả thảo luận cụ thể, nghiên cứu đã được triển khai thực hiện trên môi trường phần cứng và phần mềm cụ thể như sau: Hệ điều hành Windows 10 - 64 bit của máy tính DELL Vostro 3578 chip Core i5 – 8250U, ram 4G, ổ cứng 250G; Dòng chip FPGA được lựa chọn là Virtex-6 với số hiệu XC6VLX75T/FF484; Phần mềm mô phỏng phiên bản Xilinx 13.4; Ngôn ngữ lập trình VHDL. Đây các phần mềm và phần cứng thông dụng được sử dụng phổ biến hiện nay.

5. Giới thiệu về chip Virtex®-6 FPGA:

Virtex®-6 [9] là Kit được phát triển hướng đến sử dụng cho các ứng dụng đòi hỏi băng thông và hiệu suất cao. Nó được sử dụng trong nhiều phân khúc thị trường khác nhau tùy thuộc vào mục tiêu của nhà phát triển các ứng dụng trên đó. Bộ kết nối FPGA Virtex-6 cho phép thiết kế với các tiêu chuẩn nối tiếp phổ biến hoặc theo các tiêu chuẩn nối tiếp độc quyền thông qua giao diện SMA. Virtex®-6 (xem hình 3) được cấu thành từ các bộ phận: các khối logic cơ bản lập trình được (logic block); Hệ thống mạch liên kết lập trình được; Khối vào/ra (IO Pads); Phần tử thiết kế sẵn khác như DSP slice, RAM, ROM, nhân vi xử lý...

Thông số kỹ thuật của chip được mô tả trong bảng 2; trong đó, mỗi slide gồm 4 khối LUT và 8 khối flip-flops.

6. Giải pháp thực nghiệm

Nhóm nghiên cứu đã tiến hành thực nghiệm và lựa chọn chip Virtex6-XC6VLX75T/FF484 với chiến lược thiết kế IL-Iterative Looping (như đã mô tả trong hình 2a) cho thuật toán mã hóa Crypt(BM)_64A.

Thiết kế của thuật toán Crypt(BM)_64A trên FPGA theo chiến lược IL được mô tả trong 7 file và mỗi file có chức năng tương ứng được giải thích chi tiết trong bảng 3.

Bảng 2. Thông số kỹ thuật của các dòng thiết bị Virtex®-6.

Device	Logic Cells	Configurable Logic Blocks (CLBs)	DSP4 8E1 Slice	Block RAM Blocks			M MC Ms	Interface Blocks for PCI Express	Embedded MACs	Maximum Transceivers		Total I/O Banks	Max User I/O	
		Slices	Max Distributed RAM (Kb)	18 Kb	36 Kb	Max (Kb)				GT X	GT H			
XC6VLX75T	74,496	11,640	1,045	288	312	156	5,16	6	1	4	12	0	9	360
XC6VLX130T	128,000	20,000	1,740	480	528	264	9,504	10	2	4	20	0	15	600
XC6VLX195T	199,680	31,200	3,040	640	688	344	12,384	10	2	4	20	0	15	600
XC6VLX240T	241,152	37,680	3,650	768	832	416	14,976	12	2	4	24	0	18	720
XC6VLX365T	364,032	56,880	4,130	576	832	416	14,976	12	2	4	24	0	18	720
XC6VLX550T	549,888	85,920	6,200	864	1264	632	22,752	18	2	4	36	0	30	1200
XC6VLX760	758,784	118,560	8,280	864	1,440	720	25,344	18	0	0	0	0	30	1200
XC6VSX315T	314,880	49,200	5,090	1,344	1,408	704	25,344	12	2	4	24	0	18	720
XC6VSX475T	476,160	74,400	7,640	2,016	2,128	1,064	38,304	18	2	4	36	0	21	840
XC6VHX250T	251,904	39,360	3,040	576	1,008	504	18,114	12	4	4	48	0	8	320
XC6VHX255T	253,440	39,600	3,050	576	1,032	516	18,576	12	2	2	24	24	12	480
XC6VHX380T	382,464	59,760	4,570	864	1,536	768	27,648	18	4	4	48	24	18	720
XC6VHX565T	566,784	88,560	6,370	864	1,824	912	32,832	18	4	4	48	24	18	720

Bảng 3. Danh mục các file thiết kế trên FPGA và chức năng tương ứng

Tên file	Chức năng
1 alg_iterative.vhdl	Mô tả chế độ làm việc của thuật toán
2 alg_pack.vhd	Định nghĩa các phân tử điều khiển, các phép biến đổi sử dụng trong thuật toán và hàm biến đổi cho vòng mã hóa cơ sở
3 alg_top_iter.vhd	Mô tả công tín hiệu của các khối chức năng
4 controller_iter.vhdl	Mô tả khối điều khiển của chương trình
5 interface.vhdl	Mô tả tín hiệu đầu vào, tín hiệu ra, tín hiệu điều khiển, chuyển dữ liệu
6 reg64b.vhd	Mô tả việc chuyển đổi dữ liệu giữa 2 thanh ghi
7 key_schedule_iter.vhd	Mô tả lược đồ khóa của thuật toán

Trên cơ sở các modul thiết kế của từng khối chức năng, sơ đồ thiết kế tổng thể của thuật toán trên FPGA theo cấu trúc IL được biểu diễn trong hình 4.

7. Kết quả thực hiện

Nghiên cứu được triển khai thực thi trên CHIP Vertex6 mã hiệu **XC6VLX75T/FF484**, các kết quả chi tiết được minh họa trong hình 6; trong đó, vùng 1: mô tả các thông số trạng thái của thiết kế; vùng 2: thông tin về tài nguyên khi thực thi trên thiết bị đã chọn, bao gồm các thông số chi phí về tài nguyên như số các slide, số CLB, số Flip/flops,... đã sử dụng. Đồng thời, để có kết quả so sánh và đánh giá khách quan về tính phù hợp của thuật toán cho các ứng dụng không dây, nhóm nghiên cứu cũng đã tiến hành cài đặt thêm 2 thuật toán mã hóa đang được sử dụng phổ biến hiện nay là RC6 và Rijndael trên cùng dòng chip Vertex6 mã hiệu **XC6VLX75T/FF484**. Các số liệu được tổng hợp trong bảng 4.

Thông qua kết quả thực thi các thuật toán trên FPGA cho thấy, với chip Vertex6 mã hiệu XC6VLX75T/FF484 khi thực thi thuật toán Crypt(BM)_64A đạt được thông lượng cao nhất trong 3 thuật toán và cao hơn gần gấp 3 lần so với RC6, hơn 1,5 lần so với RIJNDEAL. Đồng thời, thông qua kết quả có được khi nghiên cứu cũng cho thấy chi phí về tài nguyên của thuật toán Crypt(BM)_64A là nhỏ hơn rất nhiều lần (xấp xỉ 43 lần) so với thuật toán RC6 và (gần 38 lần) so với RIJNDEA. Do đó, tính toán về hiệu quả tích hợp thông qua chi phí về thông lượng/tài nguyên là rất cao và gọn nhẹ hơn cả RIJNDEAL và RC6 rất nhiều lần (113 lần với RC6 và 57 lần với RIJNDEAL).

Hình 4. Sơ đồ thiết kế tổng thể của Crypt(BM)_64A trên FPGA (theo cấu trúc IL)

Hình 5. Giao diện kết quả thực hiện thuật toán trên Vertex6 mã hiệu XC6VLX75T/FF484

Bảng 4. Đánh giá hiệu quả tích hợp của một số thuật toán

Vertex6 mã hiệu XC6VLX75T/FF484						
Thuật toán	Khối	Chi phí tài nguyên (Slice)	Tần số (MHz)	Số vòng	Thông lượng (Mpbs)	Hiệu quả (thông lượng/tài nguyên)
Crypt(BM)_64A	64	255	225	10	1,440	0,00565
RC6	64	10978	85	10	544	0,00005
RIJNDEAL	64	9683	150	10	960	0,00010

8. Kết luận

Qua các kết quả nghiên cứu và thực thi thuật toán mã hóa khối Crypt(BM)_64A trên FPGA với dòng Vertex6 mã hiệu XC6VLX75T/FF484 có thể khẳng định, Crypt(BM)_64A là thuật toán mã hóa khối hoàn toàn phù hợp với các ứng dụng cho các mạng cảm biến không dây với hiệu quả tích hợp cao; chi phí về diện tích thấp, đảm bảo tính gọn nhẹ; tiêu hao năng lượng hạn chế thông qua xung nhịp cao. Tuy rằng việc lựa chọn thuật toán và đồng thiết bị cho mỗi ứng dụng cụ thể ngoài việc dựa vào các phân tích trên và phụ thuộc vào mô hình thiết kế trên FPGA thì việc lựa chọn mức độ an toàn và khả năng chống lại các cuộc tấn công cũng là một vấn đề cần xem xét song song. Đây sẽ là một chủ đề mà nhóm nghiên cứu sẽ tiếp tục có thảo luận trong các bài báo tiếp theo.

TÀI LIỆU THAM KHẢO/ REFERENCES

- [1] F. Hu, J. Ziobro, J. Tillett, and N. K. Sharma, "Secure wireless sensor networks: problems and solutions," *J. Syst., Cybern. Inf.*, vol. 11, no. 9, pp. 419-439, 2004.
- [2] H. M. Nguyen, N. D. Ho, and H. D. Luu, "Design and Estimate of a New Fast Block Cipher for Wireless Communications Devices," *The 2008 International Conference on Advanced Technologies for Communications (ATC'08) and REV'08*, Hanoi, 2008, pp. 409-412.
- [3] H. M. Nguyen, T. B. Do, and N. D. Ho, "New SDDO-Based Block Cipher for Wireless Sensor Network Security," *International Journal of Computer Science and Network Security*, vol. 10, no. 3, pp. 54-60, March 2010.
- [4] T. B. Do and H. M. Nguyen, "Crypt(BM)_64A - a new cipher oriented to Wireless Sensor Networks," *Proceedings of International Conference on Advanced Technologies for Communications (ATC) 2012*, 2012, pp. 294-299 (IEEE - IEEEExplore Digital Library).
- [5] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo, Cryptographic Hardware and Embedded Systems – CHES 2011," *Lecture Notes in Computer Science*, vol. 6917, pp. 342 - 357, 2011.
- [6] M. Knežević, V. Nikov, and P. Rombouts, *Low Latency Encryption - Is "Lightweight = Light + Wait"*, NXP Semiconductors, Leuven, Belgium 2015.
- [7] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT, A Lightweight Encryption Algorithm for Secure Internet of Things," (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 1, pp. 402-411, 2017.
- [8] H. M. Nguyen and T. B. Do, "Hybrid Model in the Block Cipher Applications for High-Speed Communications Networks," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 12, no. 4, July 2020, doi: 10.5121/ijcnc.2020.12404 55.
- [9] Xilinx Inc, "Development System Reference Guide," Jan 17, 2012. [Online]. Available: www.xilinx.com. [Accessed Jun. 25, 2021].