BILINGUAL PUBLISHING GROUP

Electrical Science & Engineering

https://journals.bilpubgroup.com/index.php/ese

ARTICLE

High-Throughput CBC Mode Crypto Circuit

***Kai-Chun Chang*[1], *You-Tun Teng*[1], *Wen-Long Chin*[2*]**

[1] *MediaTek Inc., Hsinchu City, Taiwan, 300, China*

[2] *Department of Engineering Science, National Cheng Kung University, Taiwan, 701, China*

ABSTRACT

The objective of this study is to investigate a high-throughput cipher-block chaining (CBC) mode crypto circuit, which can be embedded in commercial home gateways or switches/routers. Concurrently, the area efficiency of block ciphers can be improved as well. However, the CBC mode encounters the problem of data dependency. To solve this issue, a data scheduling mechanism of network packets is proposed to eliminate the data dependency of input data for CBC mode pipelined crypto engines. The proposed CBC mode architecture can be applied to advanced encryption standards (AES), triple data encryption standards (3DES), and other block ciphers. In addition, to increase the throughput, deeply pipelined AES-CBC and 3DES-CBC circuits with balanced paths are proposed. With the proposed scheduling and pipelined circuits, the authors can effectively encrypt the packet data of multiple network channels at the same time. Using the proposed architecture, throughputs of 137.8 and 44.75 Gbps using a copy of pipelined AES-CBC and 3DES-CBC circuits can be achieved in TSMC 45 nm and TSMC 130 nm processes, respectively.

Keywords: 3DES-CBC; AES-CBC; Area efficiency; ASIC; FPGA; Security; Throughput

1. Introduction

Security is imperative for many systems, such as the water-based automatic security marking platform [1], cognitive radios [2-5], smart grid [6], physical layer [7], and cloud and fog computing [8]. Moreover, in addition to high-performance packet switching [9,10], commercial home gateways [11] or switches/routers necessitate high-throughput crypto processors. Also, security is of paramount importance for many consumer electronics [12,13]. The private and public key crypto processor was proposed [12]. However, to the best of our knowledge, the high-throughput crypto

*CORRESPONDING AUTHOR:

Wen-Long Chin, Department of Engineering Science, National Cheng Kung University, Taiwan, 701, China; Email: wlchin@mail.ncku.edu.tw

ARTICLE INFO

Received: 10 April 2023 | Revised: 28 April 2023 | Accepted: 10 May 2023 | Published Online: 24 May 2023

DOI: https://doi.org/10.30564/ese.v5i1.5636

CITATION

Chang, K.C., Teng, Y.T., Chin, W.L., 2023. High-Throughput CBC Mode Crypto Circuit. Electrical Science & Engineering. 5(1): 21-31. DOI: https://doi.org/10.30564/ese.v5i1.5636

processor for feedback operation modes, such as the cipher-block chaining (CBC) mode, has never been studied.

In cryptography, a mode of operation describes how to repeatedly apply the single-block operation of a cipher to securely operate on data larger than a block. In the CBC mode, each block of plaintext is exclusively-ORed (XORed) with the previous ciphertext block before being encrypted, as presented in **Figure 1**, where $\oplus$ denotes the XOR logic operation, ENC denotes the block cipher, and an initialization vector must be used in the first block to make each message unique. The block cipher operates on a whole block and requires that the data be padded to a full block if it is smaller than the block size. Consequently, in the CBC mode, each ciphertext block relies on all plaintext blocks processed up to that point.

1.1 Advanced encryption standard

In 2001, National Institute of Standard and Technology (NIST) invited proposals for the new algorithm of the advanced encryption standard (AES) [14]. The Rijndael algorithm, designed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, was finally selected as the AES specification and became a FIPS standard.

Nowadays, the AES algorithm is the most popular symmetric block cipher, within which both the outbound and inbound respectively use the same main key for encryption and decryption. Additionally, the AES is an iterative algorithm and uses a round function repeatedly. The number of iterations is determined by the number of rounds. In encryption, each round is composed of four different processing steps: substitute bytes (SubBytes), shift rows (ShiftRows), mix columns (MixColumns), and add round key (AddRoundKey), while the last round does not contain the MixColumns step.

The decryption is a reverse process of encryption and the round keys are used in the reverse order. In decryption, each round is also composed of four different processing steps: inverse substitute bytes (InvSubBytes), inverse shift rows (InvShiftRows), inverse mix columns (InvMixColumns), and add round key (AddRoundKey), while the last round does not contain the InvMixColumns step.

Compared to the software solution [15], the hardware implementation [16-22] is more suitable for high-throughput data applications. Among hardware implementations, the non-linear SubBytes transformation realized using look-up tables (LUTs) [16,17] requires a large area compared to those using the composite field arithmetic (CFA) [18-22]. The study [18] proposed a pipelined and unfolded AES circuit using the $\mathrm{GF}(2^4)^2$, where GF(.) denotes the Galois field. The work [19] combined and optimized all building blocks in the devised S-box of SubBytes [18]. The work [20] proposed to use of a single-round circuit of AES repeatedly. The whole AES processing is performed in $\mathrm{GF}(2^4)^2$ and pipelining registers are inserted between iterative rounds [21]. The work [22] adopted the pre-computation technique and proposed a three-block design of the S-box. A 2-stage pipelined round circuit is finally obtained [22]. The works [21,22] unroll the whole AES circuit.

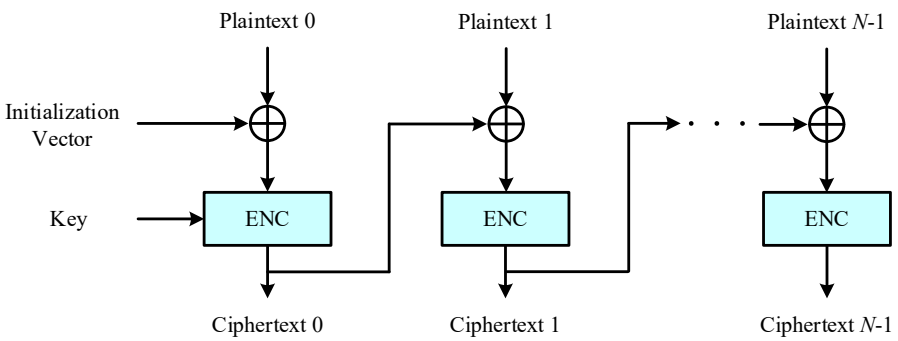

Figure 1. CBC operation mode of encryption.

1.2 Data encryption standard

The data encryption standard (DES) algorithm is also a symmetric key encryption algorithm, which was established as a data encryption standard by the NIST in 1976. However, with the advancement of technology, the key length of DES was too short to be easily cracked. Therefore, a triple data encryption algorithm (TDEA or 3DES) [23] was invented to solve this problem by increasing the key length. Nowadays, there are more and more specialized hardware circuits developed to handle the data encryption task [24]. The work [25] combined two sets of single-round DES circuits in parallel and used two different-phase clocks to control the circuit. The work [26] unrolled the DES circuit and inserted registers between each round of the DES circuit to implement a pipelined architecture. The works [27,28] decreased the critical path of single-round DES by removing the XOR logic gate. Furthermore, the work [27] combined multiple rounds of DES to reduce the number of cycles for encryption.

1.3 Motivation

With the development of communication technology, not only the high data throughput rate is an important issue, but data security is also highly noticed. The CBC mode is considered to be more secure than traditional electronic codebook (ECB) mode. Therefore, how to realize the CBC mode circuit with high throughput has become a critical issue.

On a network router/switch, packet data of multiple independent network channels are multiplexed into a port. To increase the clock rate of a crypto engine, a pipelined engine is typically designed for the ECB mode of operation. However, for the popular CBC mode, owing to the XOR operation of a plaintext block with the previous ciphertext block, pipelining will not increase the data throughput. Rather, throughput may be lowered due to pipelining because of unbalanced path delays and the overhead of register access time. Meanwhile, inserting pipelining registers will cause a waste of hardware resources.

To solve the impact of packet data dependency and enhance the throughput of the CBC mode encryption system, the novelty of this work is that we use an architecture for data scheduling to eliminate the data dependency. In addition, the pipelined architecture focuses on balancing the latency of crypto engines to achieve high throughput. More specifically, this study provides several contributions outlined below. 1) With the proposed architecture [17], we can easily schedule the input data of multiple network channels to remove the impact of data dependency and allocate hardware resources flexibly to each network channel. 2) The pipelined stages are fully utilized. Therefore, only a copy of the proposed circuit is required to encrypt the packet data of multiple network channels at the same time. 3) We propose new pipelined AES and 3DES circuits to achieve high throughput. 4) The proposed scheme is verified using both AES-CBC and 3DES-CBC.

The rest of this work is organized as follows. Section 2 illustrates the design consideration and proposed architecture for the CBC mode of operation. Section 3 describes the proposed crypto engines, including the AES-CBC and 3DES-CBC. Section 4 demonstrates the implementation result and comparison. Finally, Section 5 draws conclusions.

2. Design considerations

Many works in the literature focus on designing the ECB mode crypto engine, instead of the popular CBC mode. However, due to the CBC mode of operation, there exists data dependency in the data to be encrypted. Conventional data scheduling of CBC mode using a 3-stage pipelined engine is presented in **Figure 2**, where pt and ct denote the plaintext and ciphertext, respectively. At the first cycle, the first plaintext, pt0, is fed into the first pipelined stage to start encryption. Next cycle, pt0 will be shifted to the second pipeline stage, and concurrently, the second plaintext, pt1, will be fed into the first pipeline stage. However, due to the CBC mode, pt1 cannot start the encryption until pt1 has been completely encrypted at cycle 4. Therefore, pt1 will be held at the first pipeline stage for two cycles to wait for the first ciphertext. As displayed, the pipeline stages cannot be

fully utilized for the CBC mode of operation.

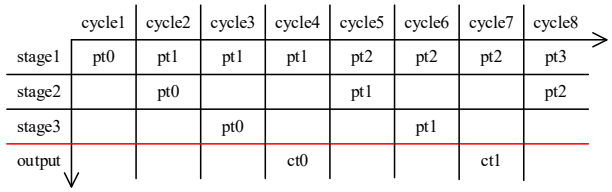

Figure 2. Conventional data scheduling of CBC mode using a 3-stage pipelined engine.

To improve the throughput of CBC encryption mode, the parallel architecture[29] was proposed in **Figure 3(A)**. In order to encrypt multiple network channels at the same time, multiple sets of pipelined circuits are used in parallel. The major difference of this work between the parallel architecture is that, to maintain the same throughput as the parallel architecture while reducing the required chip area, the multi-channel crypto engine using the folded architecture [17] was proposed in **Figure 3(B)**. This work implements the multi-channel crypto engines based on the AES and 3DES. The pseudocode of the proposed algorithm is presented in **Table 1**. The encryption algorithms of AES and DES can be found in the literature and are briefly introduced in Section 1, and hence, they are omitted here for clarity.

Objectives of this work

The objective of this study is to investigate a high-throughput CBC mode crypto circuit, which can be embedded in commercial home gateways or switches/routers. Concurrently, the area efficiency of block ciphers can be improved as well. However, the CBC mode encounters the problem of data dependency. To solve this issue, a data scheduling mechanism of network packets is proposed to eliminate the data dependency of input data for CBC mode pipelined crypto engines. The pros and cons of the proposed method are summarized in **Table 2**.

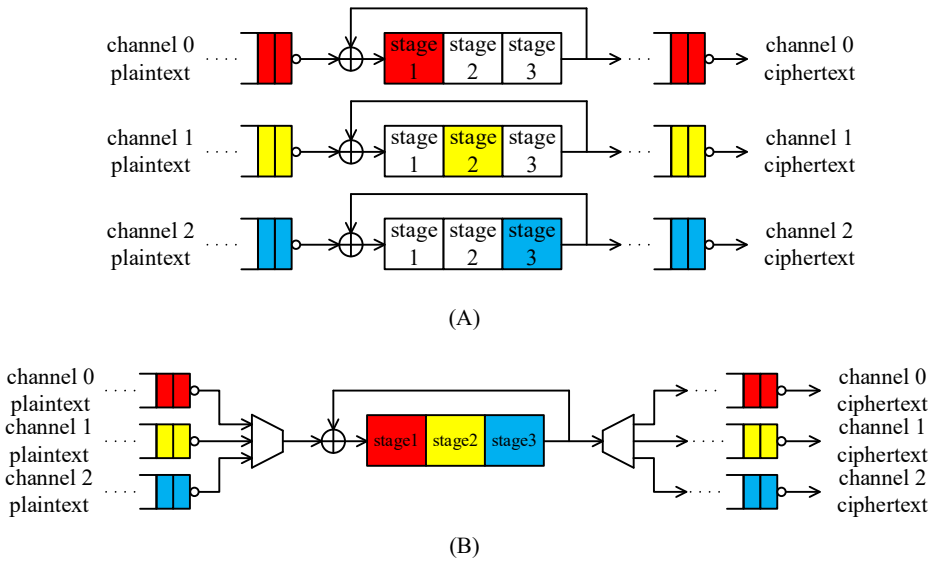

Figure 3. Pipelined architectures of CBC mode: (A) parallel, (B) folded

Table 1. Pseudocode of the proposed algorithm

Input: plaintext of each channel
1 for each channel;
2 encrypt plaintext;
3 end
Output: ciphertext

Table 2. Pros and Cons of the proposed method.

	Pros	**Cons**
Proposed Method	High throughput and area efficiency	Round-robin data scheduling is needed

3. Crypto engines

3.1 Pipelined AES-CBC engine

To increase the clock rate, an intuitive solution is to use a pipelined architecture. However, making path delays balanced is the key point of pipelined circuits. Considering the path delays of combinational circuits, we propose to implement the 7-stage pipelined single-round circuit of AES in **Figure 4**, where the detailed design of S-box (for SubBytes) sub-block can be found[19] and it is omitted here. The AddRoundKey is simply the XOR operation shown in **Figure 4**. The ShiftRows and InvShiftRows are rewiring their inputs and do not cost any logic gates.

Figure 5 displays the detailed architecture of the integrated Mixcolumns and InvMixcolumns for the encryption and decryption, respectively, where *a*, *b*, *c*, *d* denote the inputs, a'_1, b'_1, c'_1, d'_1 denote the outputs of Mixcolumns, *W*, *X*, *Y*, *Z* denote the outputs of InvMixcolumns, $\oplus$ denotes the XOR operation, and xtime denotes the circuit that multiplies input by 2. Notably, the last round of AES needs not the Mixcolumns operation so it has 6-stage pipelining, which is omitted here. Notice that the dashed lines are locations where the registers are placed.

Next, as shown in **Figure 6**, every round of the AES circuit with a 128-bit key is unrolled to achieve the highest throughput so that one ciphertext can be obtained in every clock cycle.

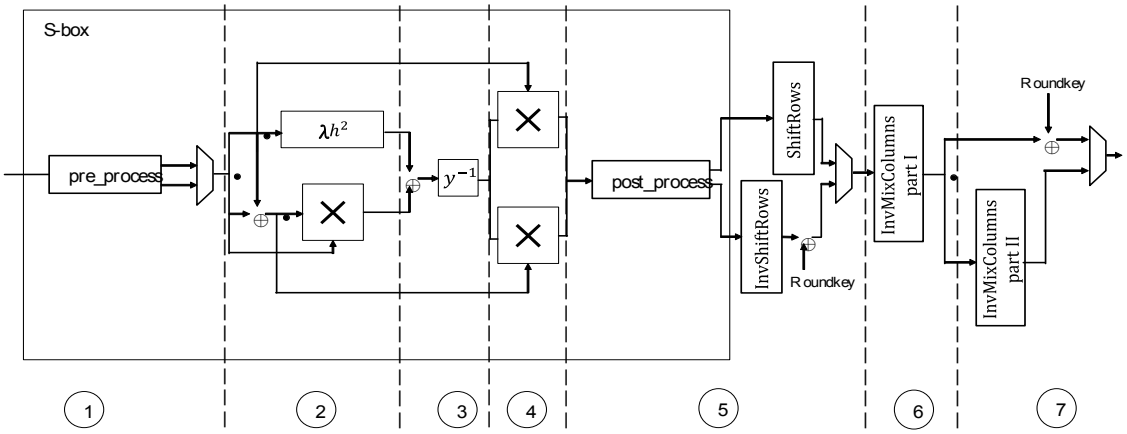

Figure 4. Pipelined architectures of single-round circuit of AES.

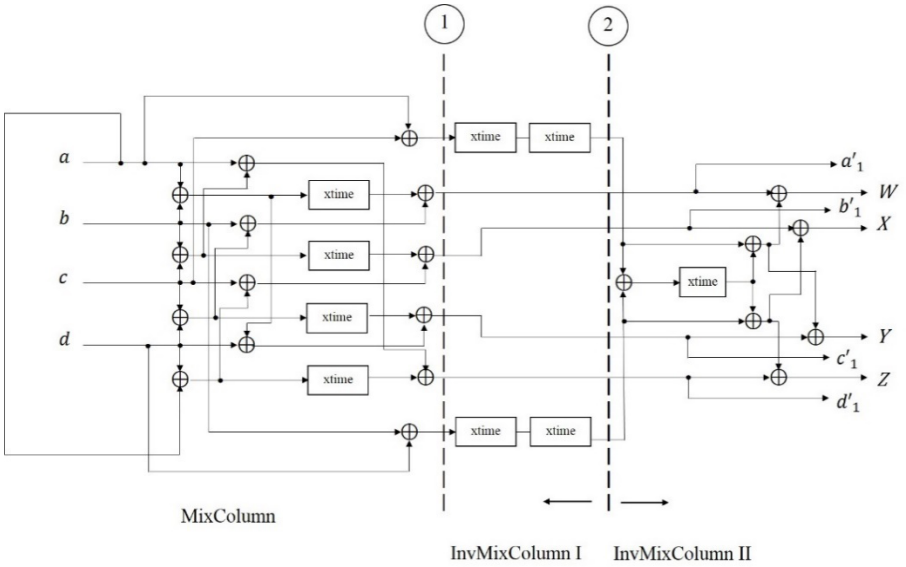

Figure 5. Detailed architecture of the integrated Mixcolumns and InvMixcolumns for the encryption and decryption, respectively.

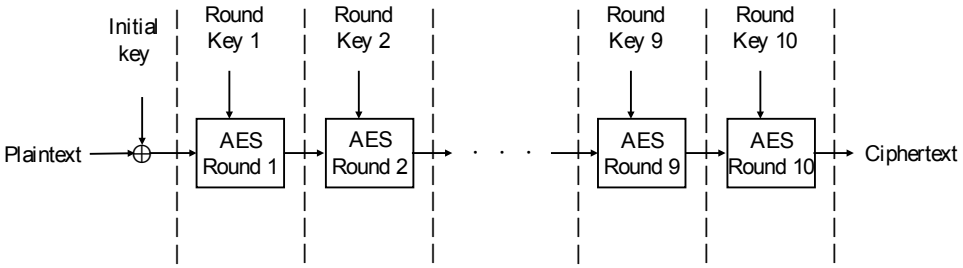

Figure 6. Overall combined encryption and decryption circuit of AES-128.

3.2 Pipelined 3DES-CBC engine

To balance the path delay of every pipelined stage, we start with the S-box because it has the longest delay in the 3DES-CBC circuit. The 64-to-1 multiplexer that composes the S-box is replaced with a tree structure composed of different-size multiplexers, and registers (marked by the dashed lines) are placed between the multiplexers, as shown in **Figure 7**.

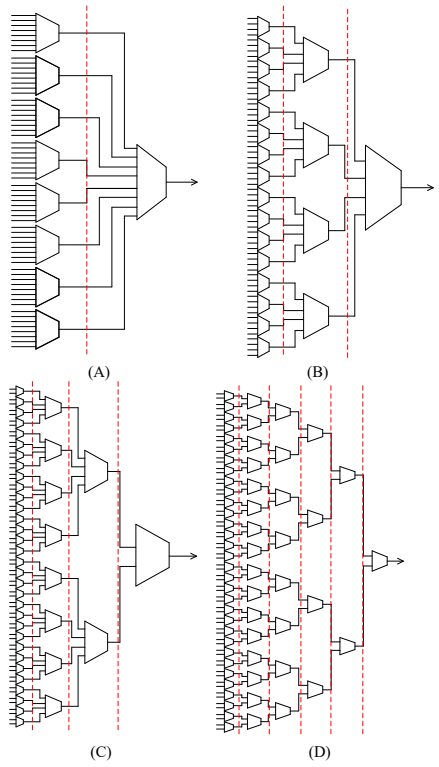

Figure 7. The architectures of S-box for 3DES with different pipeline stages, (A) 2-stage, (B) 3-stage, (C) 4-stage, and (D) 6-stage.

We investigate four kinds of S-box architectures: 2-stage pipeline with 8-to-1 multiplexers, 3-stage pipeline with 4-to-1 multiplexers, 4-stage pipeline with 2-to-1 multiplexers and 4-to-1 multiplexers, and 6-stage pipeline with 2-to-1 multiplexers. Applying them to the 3DES-CBC circuits, critical paths of the pipelined architectures are shown in **Table 3**. Furthermore, in order to facilitate the evaluation of the critical path for different pipelined architecture, the XOR logic gates and multiplexers of each critical path are replaced with equivalent NAND gates.

Table 3. The critical paths of each pipelined architecture and their NAND gate equivalents.

Pipelined Architecture	Critical Path	Equivalent NAND
2-Stage Pipeline	1 XOR, 1 8-to-1 MUX	12 NANDs
3-Stage Pipeline	1 XOR, 1 4-to-1 MUX	9 NANDs
4-Stage Pipeline	1 4-to-1 MUX	6 NANDs
8-Stage Pipeline	1 2-to-1 MUX	3 NANDs

According to the critical path target, the 3DES-CBC can be designed. First, the single-round circuit of the i-th round of the 3DES-CBC is shown in **Figure 8**, where the 2-stage pipelined S-box is assumed, L_i and R_i denote the left and right 32-bit halves of the i-th round, and the blocks E and P denote the expansion and permutation functions, respectively. Notably, expansion and permutation functions are just rewiring of their inputs and do not cost any logic gates except buffers if required. The red dashed lines are the positions where the registers are placed. S-box part 1 and S-box part 2 respectively represent the two parts of the 2-stage S-box shown in **Figure 7(A)**. Second, in addition to pipelining a single-round circuit, we unroll and pipeline 16 rounds of a DES and it is reused for 48 rounds of operation of 3DES-CBC, as shown in **Figure 9**, where "pipelined 3DES round" represents the pipelined single-round circuit.

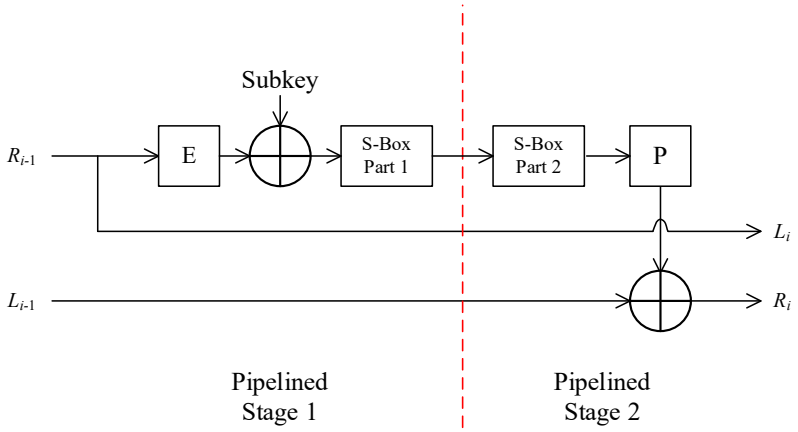

Figure 8. Single-round circuit of the i-th round of 3DES-CBC.

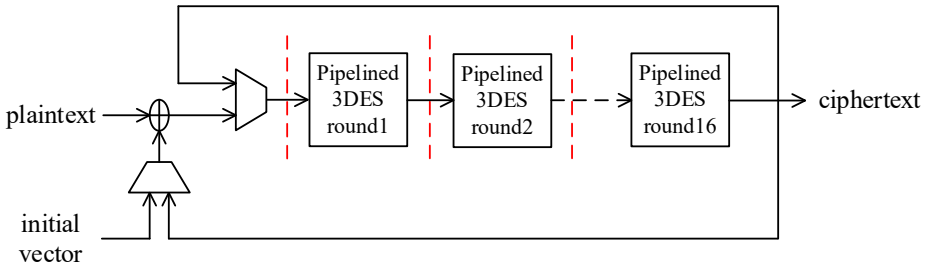

Figure 9. The architecture of Pipelined 3DES-CBC.

4. Implementation result and comparison

For comparison purpose, the ASIC implementation of AES-CBC is based on the TSMC 45 nm standard cell library and the synthesis tool of Synopsys Design Compiler. The implementation results of various crypto engines are displayed in **Table 4**. As presented, the proposed AES-CBC achieves the highest throughput and area efficiency. However, owing to the deep pipelining, the area of the proposed design is also the largest.

For comparison purpose, the ASIC implementation of 3DES-CBC is based on the TSMC 130 nm and 65 nm standard cell libraries and the synthesis tool of Synopsys Design Compiler. The implementation results of various crypto engines are displayed in **Table 5**. The authors [27] combined the multiple iterative rounds in one clock cycle. Besides, a set of XOR gates was removed from the critical path to reduce the critical path delay. The highest throughput [27] is "16 rounds in 1 cycle" and can reach 1.94 Gbps. The work [28] removed two XOR gates from the critical path and reused the single-round hardware, and can reach a throughput of 1.69 Gbps. As presented in **Table 5**, the proposed 8-stage pipelined architecture has the highest throughput of 44.75 Gbps, while the proposed 2-stage pipelined architecture has the high-

Table 4. Comparison among different AES-CBC ASIC designs.

	Tech.	Architecture	Freq. (Mhz)	Throughput (Gbps)	Area	Efficiency
[20]	NanGate 45nm	AES-128, Enc/ Dec	694.4	0.889/0.808	17368 GE	51.18/46.52 Kbps/GE
[21]	High-metal gate CMOS 45nm	AES-128, Enc/ Dec	2100	2.65	0.15 mm^2	17.67 Kbps/μm^2
Our Work	TSMC 45nm	AES-128, Enc/ Dec	1075	137.8	75832 μm^2/ 111517 GE	1817 Kbps/μm^2 1235 Kbps/GE

est area efficiency of 85.37 Kbps/μm^2. Moreover, the throughput of the proposed design implemented using of 130 nm standard cell library still outperforms the works [27,28] in literature implemented using of 65 nm standard cell library, which validates the efficiency of the proposed architecture.

We compare state-of-the-art works [30,31] to show the robustness of the implemented AES-CBC design through FPGA implementation in **Table 6**. As displayed, under the same throughput, the proposed design can achieve the best area efficiency. This justifies the advantages of the proposed architecture.

Table 5. Comparison among different 3DES-CBC ASIC designs.

	Tech.	Architecture	Freq. (Mhz)	Throughput (Gbps)	Area (μm^2)	Efficiency (Kbps/μm^2)
[27]	SMIC 130nm	CBC, 4 rounds in 1	275.6	1.47	N/A	N/A
[27]	SMIC 130nm	CBC, 16 rounds in 1	90.93	1.94	N/A	N/A
[27]	SMIC 65nm	CBC, 16 rounds in 1	156.09	3.33	164599	20.23
[28]	SMIC 130nm	CBC	N/A	1.69	38688.8	43.68
[28]	SMIC 65nm	CBC	2130	2.84	12852	220.9
Our Work	TSMC 130nm	CBC, 2-stage pipelined	574.052	36.74	430338	85.37
Our Work	TSMC 130nm	CBC, 3-stage pipelined	638.978	40.89	536974	76.14
Our Work	TSMC 130nm	CBC, 4-stage pipelined	671.59	42.98	625685	68.69
Our Work	TSMC 130nm	CBC, 8-stage pipelined	699.3	44.75	1048556	42.68

Table 6. Comparison among different AES-CBC FPGA designs.

	Arch.	Devices	Slices	Freq. (Mhz)	Throughput (Gbps)	Efficiency (Mbps/Slice)
[30]	AES-128, Enc	Virtex-6 xc6vlx240t	4830	617.6	79	16.36
Our Work	AES-128, Enc	Virtex-6 xc6vlx240t	3140	631.2	80.8	25.37
[31]	AES-128, Enc/Dec	Virtex-5 xc5vfx70t	9756	460	60	6.15
Our Work	AES-128, Enc/Dec	Virtex-5 xc5vfx70t	5277	473.2	60.6	11.47

5. Conclusions and future works

In this paper, we presented a folded architecture for encrypting the packet data of different network channels at the same time. The resources of the pipelined crypto engine can be fully utilized without any waste. Only one copy of pipelined circuit is required to maintain the same throughput of the parallel architecture. There typically exists a tradeoff between throughput and the area of digital circuits. In addition to enhancing the throughput, adopting the proposed technique can also enhance the area efficiency (throughput/area).

Future works can implement the layout of the proposed design. Another research direction can realize the buffer space required to store the plaintexts of each channel.

Nomenclature

AddRoundKey	add round key
AES	advanced encryption standard
CBC	cipher-block chaining
CFA	composite field arithmetic
ECB	electronic codebook
InvMixColumns	inverse mix columns
InvShiftRows	inverse shift rows
InvSubBytes	inverse substitute bytes
LUTs	look-up tables
MixColumns	mix columns
NIST	National Institute of Standard and Technology
ShiftRows	shift rows
SubBytes	substitute bytes
TDEA or 3DES	triple data encryption standard
XOR	exclusively-OR

Author Contributions

Kai-Chun Chang: Design and implementation of 3DES.

You-Tun Teng: Design and implementation of AES.

Wen-Long Chin: Supervision.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

This research received no external funding.

References

[1] Li, A., Gong, C., Huang, X., et al., 2022. Overview of key technologies for water-based automatic security marking platform. Electrical Science & Engineering. 4(1), 30-40.

[2] Chin, W.L., Tseng, C.L., Tsai, C.S., et al. (editors), 2012. Channel-based detection of primary user emulation attacks in cognitive radios. 2012 IEEE 75th Vehicular Technology Conference (VTC Spring); 2012 May 6-9; Yokohama. New York: IEEE.

[3] Le, T.N., Chin, W.L., Kao, W.C., 2015. Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks. IEEE Communications Letters. 19(5), 799-802.

[4] Chin, W.L., 2019. On the noise uncertainty for the energy detection of OFDM signals. IEEE Transactions on Vehicular Technology. 68(8), 7593-7602.

[5] Chin, W.L., Kao, C.W., Chen, H.H., et al., 2013. Iterative synchronization-assisted detection of OFDM signals in cognitive radio systems. IEEE Transactions on Vehicular Technology. 63(4), 1633-1644.

[6] Chin, W.L., Lin, Y.H., Chen, H.H., 2016. A framework of machine-to-machine authentication in smart grid: A two-layer approach. IEEE Communications Magazine. 54(12), 102-107.

[7] Chin, W.L., Le, T.N., Tseng, C.L., 2015. Authentication scheme for mobile OFDM based on security information technology of physical layer over time-variant and multipath fading channels. Information Sciences. 321, 238-249. DOI: https://doi.org/10.1016/j.ins.2015.01.040

[8] Yoosuf, M.S., Muralidharan, C., Shitharth, S., et al., 2022. FogDedupe: A Fog-Centric deduplication approach using multi-key homomorphic encryption technique. Journal of Sensors. 6759875. DOI: https://doi.org/10.1155/2022/6759875

[9] Jin, Z., Jia, W.K., 2022. P^3FA: Unified unicast/multicast forwarding algorithm for high-performance router/switch. IEEE Transactions on Consumer Electronics. 68(4), 327-335.

[10] Chin, W.L., Chen, S.G., 2009. IEEE 1588 clock synchronization using dual slave clocks in a slave. IEEE Communications Letters. 13(6), 456-458.

[11] Cho, E.A., Moon, C.J., Baik, D.K., 2008. Home gateway operating model using reference monitor for enhanced user comfort and privacy. IEEE Transactions on Consumer Electronics. 54(2), 494-500.

[12] Kim, H.W., Lee, S., 2004. Design and implementation of a private and public key crypto processor and its application to a security system. IEEE Transactions on Consumer Electronics. 50(1), 214-224.

[13] Kim, D.S., Lee, S.Y., Kim, B.S., et al., 2008. On the design of an embedded biometric smart card reader. IEEE Transactions on Consumer Electronics. 54(2), 573-577.

[14] National Institute of Standards and Technology, 2001. Specification for the advanced encryption standard (AES), FIPS PUB197 [Interenet]. Available from: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[15] Singha, T.B., Palathinkal, R.P., Ahamed, S.R. (editors), 2020. Implementation of AES using

composite field arithmetic for IoT applications. 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP); 2020 Feb 27-Mar 1; Guwahati. New York: IEEE. p. 115-121.

[16] Janveja, M., Paul, B., Trivedi, G., et al. (editors), 2020. Design of efficient AES architecture for secure ECG signal transmission for low-power IoT applications. 2020 30th International Conference Radioelektronika (RADIOELEKTRONIKA); 2020 Apr 15-16; Bratislava. New York: IEEE. p. 1-6.

[17] Chin, W.L., Ko, H.A., Chen, N.W., et al., 2023. Securing NFV/SDN IoT using Vnfs over a compute-intensive hardware resource in NFVI. IEEE Network. 1-8.
DOI: https://doi.org/10.1109/MNET.135.2200558

[18] Zhang, X., Parhi, K.K., 2004. High-speed VLSI architectures for the AES algorithm. IEEE Transactions on very Large Scale Integration (VLSI) Systems. 12(9), 957-967.

[19] Teng, Y.T., Chin, W.L., Chang, D.K., et al., 2021. VLSI architecture of S-Box with high area efficiency based on composite field arithmetic. IEEE Access. 10, 2721-2728.

[20] Manjith, B.C. (editor), 2019. Improving overall parallelism in AES accelerator using BRAM and multiple input blocks. 2019 Innovations in Power and Advanced Computing Technologies (i-PACT); 2019 Mar 22-23; Vellore. New York: IEEE.

[21] Ueno, R., Morioka, S., Miura, N., et al., 2019. High throughput/gate AES hardware architectures based on datapath compression. IEEE Transactions on Computers. 69(4), 534-548.

[22] Mathew, S.K., Sheikh, F., Kounavis, M., et al., 2011. 53 Gbps native GF $(2^4)^2$ composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors. IEEE Journal of Solid-State Circuits. 46(4), 767-776.

[23] American National Standards Institute, Inc., 1998. Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 [Internet]. Available from: https://standards.globalspec.com/std/546836/X9.52

[24] Khan, Z., Benaissa, M., 2015. Throughput/area-efficient ECC processor using montgomery point multiplication on FPGA. IEEE Transactions on Circuits and Systems II: Express Briefs. 60(11), 1078-1082.

[25] Lim, Y.W. (editor), 2000. Efficient 8-cycle DES implementation. Proceedings of Second IEEE Asia Pacific Conference on ASICs; 2000 Aug 30-31; Cheju. New York: IEEE. p. 175-178.

[26] Zeebaree, S.R., 2020. DES encryption and decryption algorithm implementation based on FPGA. Indonesian Journal of Electrical Engineering and Computer Science. 18(2), 774-781.

[27] Fu, T., Li, S. (editors), 2017. A 3DES ASIC implementation with feedback path in the CBC mode. 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC); 2017 Oct 18-20; Hsinchu. New York: IEEE. p. 1-2.

[28] He, Y., Li, S. (editors), 2017. A 3DES implementation especially for CBC feedback loop mode. 2017 IEEE International Symposium on Circuits and Systems (ISCAS); 2017 Sep 28; Baltimore. New York: IEEE. p. 1-4.

[29] Wee, C.M., Sutton, P.R., Bergmann, N.W., et al. (editors), 2006. VPN acceleration using reconfigurable system-on-chip technology. 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines; 2006 Dec 11; Napa, CA. New York: IEEE. p. 281-282.

[30] Oukili, S., Bri, S. (editors), 2017. High speed efficient advanced encryption standard implementation. 2017 International Symposium on Networks Computers and Communications (ISNCC); 2017 May 16-18; Marrakech. New York: IEEE. p. 1-4.

[31] Kouzehzar, H., Moghadam, M.N., Torkzadeh, P. (editors), 2018. A high data rate pipelined architecture of AES encryption/decryption in storage area networks. Iranian Conference on Electrical Engineering (ICEE); 2018 May 8-10; Mashhad. New York: IEEE. p. 23-28.

Appendix A

Synthesis Constraints

create_clock -period 1.565 [get_ports clk]

set_ideal_network -no_propagate [get_clocks clk]

set_ideal_network [get_ports rst]

set_dont_touch_network [get_ports {clk rst}]

set_clock_latency 0.5 [get_clocks clk]

set_input_delay 0.1 -clock clk [remove_from_collection [all_inputs]/

[get_ports {clk rst}]]

set_output_delay 0.1 -clock clk [all_outputs]

set_fix_multiple_port_nets -all -buffer_constants

set_load 0.05 [all_outputs]

set_drive 0 [get_ports rst]

set_driving_cell -lib_cell INVXL -no_design_rule [remove_from_collection/ [all_inputs] [get_ports {clk rst}]]

set_max_area 0

set_max_fanout 4 TDESCBC_intra_pipelined

set_operating_conditions -min_library fast -min fast -max_library slow/ -max slow

set_wire_load_model -name tsmc13_wl10 -library slow

set_wire_load_mode top

remove_unconnected_ports -blast_buses [get_cells -hierarchical *]

Appendix B

FPGA Implementation Setup in ISE 14.7

Family: Virtex4

Device: XC4VLX25

Package: FF676

Speed: -10

Compile Option: default