AES S-Box Hardware With Efficiency Improvement Based on Linear Mapping Optimization

Ayano Nakashima, Rei Ueno, *Member, IEEE*, and Naofumi Homma, *Senior Member, IEEE*

***Abstract*—This brief presents a new Advanced Encryption Standard (AES) S-Box hardware design based on linear mappings optimized by combining multiplicative and exponential offsets. Generally, the performance of S-Box with composite field representations depends on the structure of linear mappings (i.e., transformation matrices) between the polynomial field and composite field before and after the S-Box. So far, multiplicative and exponential offsets have been applied only to Boyar-Peralta type S-Box variants for optimizing the transformation matrix. In this brief, we apply the offset methods to another S-Box based on the redundant Galois field arithmetic and evaluate the performance by logic synthesis. Specifically, we design and evaluate two new types of S-Box hardware: one for encryption only (ENC) and the other for both encryption and decryption (ENC/DEC). The evaluation result confirms that the proposed ENC and ENC/DEC S-Boxes achieve a performance up to 8.7% and 28.8% higher, respectively, than the highest-performing conventional ones in terms of the area timing (AT) product.**

***Index Terms*—AES, S-Box, hardware, linear mapping optimization, ASIC.**

I. Introduction

Advanced Encryption Standard (AES) is the most widely used for common key cryptography, and dedicated circuits are indispensable to implement AES efficiently for both transaction servers and embedded devices. Among the AES subfunctions, SubBytes is a major factor in determining the circuit area and delay of the AES datapath. In addition, the SubBytes design has many variations in contrast to other subfunctions (i.e., ShiftRows, MixColumns, and AddRoundKey). Many studies have presented efficient implementations of the S-Box constituting SubBytes since 2001 [1]. There are two hardware implementation methods for AES S-Boxes: one is based on direct mapping, and the other is based on the composite field arithmetic. The former method is to implement the input-output relationship directly as a table, which reduces latency at the expense of hardware resources. On the other hand, the latter method utilizes the Itoh–Tsujii algorithm [2] for the $GF(2^8)$ inversion circuit to make the S-Box more efficient. The composite field S-Box provides lower power and higher area-timing (AT) efficiency than direct mapping.

The present study focuses on the composite field S-Box. Its performance strongly depends on the composite field and the basis representation used. $GF((2^2)^2)^2)$ and $GF((2^4)^2)$ are commonly used as the composite field, and a polynomial basis (PB) or normal basis (NB) is selected as the basis representation. Several S-Boxes that combine the composite field and its representations have been reported [1], [3]–[6]. Jeon *et al.* showed that an S-box with the composite field $GF((2^4)^2)$ yields better performance than conventional S-boxes with $GF((2^2)^2)^2)$ [6]. Recently, more efficient $GF((2^4)^2)$-type S-Boxes with redundant basis representations were reported in [7], [8]. The S-box reported by Ueno *et al.* [8] achieved the highest efficiency so far among those using $GF((2^4)^2)$. Furthermore, Boyar and Peralta [9] presented structural optimization and logical minimization for a $GF(((2^2)^2)^2)$-type S-Box, which showed a relatively small area. More recently, on the basis of the $GF(((2^2)^2)^2)$ inversion circuit, Maximov and Ekdahl [10] reported three S-Box composite field structures that have the lowest latency, smallest area, and highest AT efficiency, respectively.

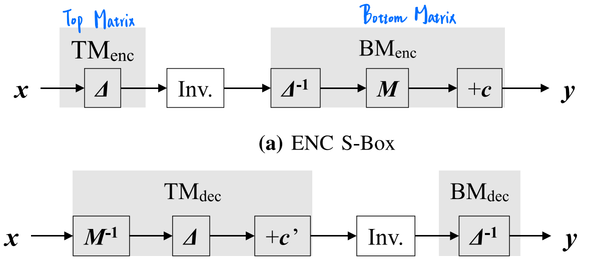
A further improved S-Box design includes the transformation circuits (i.e., the isomorphic mapping from/to the composite field and the affine transformation) before/after the inversion circuit. The above transformations are computed in the XOR matrices, and thus, the matrix representations of the transformations determine the total S-Box circuit performance. In general, a smaller hamming weight of the entire matrix leads to a smaller area. Similarly, a smaller maximum hamming weight of the rows (maxHW) leads to a lower delay. Accordingly, Mathew *et al.* and Gueron *et al.* focused on the composite field structure (i.e., irreducible polynomial coefficients and basis elements) to expand the matrix representation [11], [12]. Ueno *et al.* and Maximov and Ekdahl then extended the matrix representation using a multiplicative offset [8] and a multiplicative-and-exponential one [10], respectively. In the report by Maximov and Ekdahl [10], a $GF(((2^2)^2)^2)$-type S-Box variant [9] with this expansion technique showed better performance than any other S-Boxes reported so far. However, it is still unknown whether the performance of $GF((2^4)^2)$-type S-Boxes, such as that in [8], is improved by the above state-of-the art expansion technique.

In this brief, we present the design and evaluation of $GF((2^4)^2)$-type S-Boxes that consist of an inversion circuit with redundant basis representations [8] and the best matrices given from the expanded search space. The expanded search space is eight times larger than the original one reported by Ueno *et al.* [8] owing to the combination of multiplicative and

Manuscript received 24 February 2022; revised 17 June 2022; accepted 20 June 2022. Date of publication 23 June 2022; date of current version 26 September 2022. This brief was recommended by Associate Editor N. Wu. *(Corresponding author: Naofumi Homma.)*

The authors are with the Research Institute of Electrical Communication, Tohoku University, Sendai 980-9577, Miyagi, Japan (e-mail: nakashima.ayano.p3@dc.tohoku.ac.jp; rei.ueno.a8@tohoku.ac.jp; naofumi.homma.c8@tohoku.ac.jp).

Digital Object Identifier 10.1109/TCSII.2022.3185632



(a) ENC S-Box

(b) DEC S-Box

Fig. 1. Block diagrams of composite-field S-Boxes for (a) encryption and (b) decryption.

exponential expansions. We design two S-Boxes for encryption only (ENC) and both encryption and decryption (ENC/DEC). For each S-Box, we search for both a smaller hamming weight of the entire matrix and a smaller maximum hamming weight of the rows, and we synthesize a $GF((2^4)^2)$-type inversion circuit with the candidate matrices in an exhaustive manner. From the synthesis result, we demonstrate that the newly obtained S-Boxes improve the AT products by up to 23.2% and 20.1% for ENC and ENC/DEC, respectively, compared to the highest-performing conventional $GF((2^4)^2)$-type S-Box. Furthermore, the proposed implementations are up to 8.7% and 28.8% more area-timing efficient compared to the highest-performing conventional $GF(((2^2)^2)^2)$-type ones.

II. Related Works

A. *Composite-Field S-Box*

Fig. 1 shows the block diagrams of the composite-field S-Box for ENC and DEC, respectively. In S-Box for ENC, ①first, the isomorphic mapping $\boldsymbol{\Delta}$ converts the PB $GF(2^8)$ (i.e., AES field) representation to the composite field representation. ②Second, the inversion circuit computes the inverse element on the composite field $GF((2^4)^2)$. ③Third, the inverse isomorphic mapping $\boldsymbol{\Delta}^{-1}$ converts the representation to the AES field representation. ④Finally, the S-Box outputs the result of affine transformation $\boldsymbol{M}(\boldsymbol{x}^{-1})+\boldsymbol{c}$, where $\boldsymbol{M}$ and $\boldsymbol{c}$ are a multiplication matrix and constant coefficient, respectively.

The isomorphic and inverse isomorphic mappings are computed by XOR matrices. Here, we can pre-compute the latter linear operation matrix (BM: bottom matrix in Fig. 1) for the ENC S-Box by multiplying the inverse isomorphic mapping with the affine transformation. Similarly, we can pre-compute the former linear operation matrix (TM: top matrix in Fig. 1) for the DEC S-box by multiplying the inverse affine transformation and the isomorphic mapping. We denote by TM_{enc} and BM_{enc} the top and bottom matrices of the ENC S-Box, respectively, and by TM_{dec} and BM_{dec} the top and bottom matrices of the DEC S-Box.

Fig. 2 shows the NB-based $GF((2^4)^2)$ inversion circuit. Let $\boldsymbol{a} = \boldsymbol{h}\alpha^{16} + \boldsymbol{l}\alpha$ be the 8-bit input element, where α represents the indeterminate of $GF((2^4)^2)$ and h and l are the elements of $GF(2^4)$ (or $GF((2^2)^2)$) given by the upper and lower four bits of a, respectively. Furthermore, let $\alpha^2 + \mu\alpha + \nu$ be the quadratic irreducible polynomial that defines the operations on $GF((2^4)^2)$, where ν and μ are the constant coefficients on $GF(2^4)$. The inverse element $\boldsymbol{a}^{-1}$ on the composite field is computed as $\boldsymbol{a}^{16} \cdot (\boldsymbol{a}^{17})^{-1}$ for the Ito-Tsujii algorithm. The inversion circuit in Fig. 2 calculates for the following three stages: ①the 16th and 17th powers of a (i.e., $\boldsymbol{a}^{16}$ and a^{17}, respectively), ②the $GF(2^4)$ inversion given by $(\boldsymbol{a}^{17})^{-1}$, and ③the final multiplication given by $\boldsymbol{a}^{16} \cdot \boldsymbol{a}^{17^{-1}}$. In the first stage, the 16th power is given only by wiring, specifically swapping $\boldsymbol{h}$ and $\boldsymbol{l}$ because of the Frobenius endomorphism of $GF(2^4)$. The 17th power is given by multiplying the 16th power above by the input itself. In the second stage, the inverse of the 17th power is given by direct mapping or recursively using $GF((2^2)^2)$. In the third stage, the final multiplication to output $\boldsymbol{a}^{-1}$ is performed with two $GF(2^4)$ multipliers.

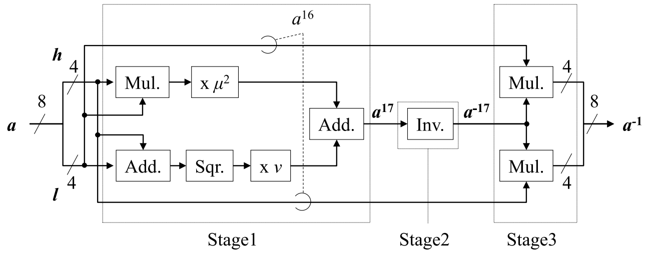


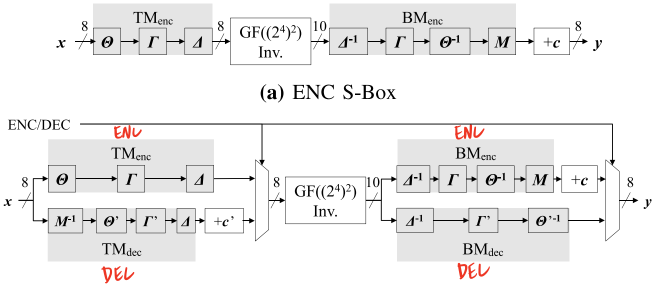
Fig. 2. Inversion circuit based on $GF((2^4)^2)$.

The performance of the composite-field inversion circuit depends heavily on the composite field and its basis representation. Canright [4] reported the structure of a small-area NB-based $GF(((2^2)^2)^2)$ S-Box. Ueno *et al.* [7], [8] utilized the three basis representations of NB, polynomial ring representation (PRR), and redundantly represented basis (RBB) for stages 1, 2, and 3, respectively, and demonstrated the fastest, most efficient, and smallest-area $GF((2^4)^2)$-type S-Box. Here, PRR and RRB are redundant representations, specifically providing each element on $GF(2^4)$ by 5 bits; the inversion-circuit output is of 10 bits, and the BM is a 10 × 8 matrix. Boyar and Peralta [9] reported that more compact circuits can be designed by the integration of first-stage TM/BM and third-stage TM/BM with the outer matrices, such as the isomorphic mapping and affine transformation matrices, for a $GF(((2^2)^2)^2)$-type S-Box. More recently, Maximov and Ekdahl [10] extended the design method to provide the logic minimization of integrated TM and BM consisting of 8 × 18 and 18 × 8 matrices, respectively. In particular, the TM/BM and composite field were selected such that the reconstructed TM/BM is as sparse as possible for the logical minimization.

B. *Optimization of Transformation Matrices*

TM and BM are determined by the basis of the composite field and isomorphic mappings. The total hamming weight of TM/BM determines the circuit area, and the maxHW (i.e., maximum depth in terms of 2-input XOR gates) determines the circuit delay. In general, as the number of possible matrix representations (i.e., search space) increases, the possibility of finding better matrices for circuit implementation increases.

For expanding the search space, Ueno *et al.* [8] used the multiplicative offset method, where the inversion circuit computes $a^{-1} = \gamma(a\gamma)^{-1}$ with the constant coefficient γ on $GF(2^8)$ given as an XOR matrix. Consequently, the search spaces of TM and BM are 255 times larger than their conventional counterparts. Note that there is no actual overhead of



(a) ENC S-Box

(b) ENC/DEC S-Box

Fig. 3. Proposed S-Boxes for (a) ENC and (b) ENC/DEC.

the multiplicative offset, because the XOR matrix representing the γ multiplication can be merged into TM/BM.

The exponential offset method, in addition to the above multiplicative offset, was used in [10], where the inversion circuit computes $a^{-1} = ((a^{2^\theta})^{-1})^{2^{8-\theta}}$ with the θ-th power of two on $GF(2^8)$ using an XOR matrix. The inversion circuit first raises the input to the power of 2^θ and, finally, raises the output to the power of $2^{8-\theta}$. The corresponding XOR matrices can also be merged into TM and BM as well as the multiplicative offsets. Here, θ can be an integer from 0 to 7, and thus, the combination of multiplicative and exponential offsets expands the search space of TM and BM 2040 (= 255 × 8) times. Maximov and Ekdahl [10] reported three S-Box configurations with different optimization goals (i.e., low delay, small area, and high AT efficiency) using the two offsets methods and logical minimization. However, the applicability of the above method to a $GF((2^4)^2)$-type S-Box design has not yet been discussed in the literature.

III. Proposed S-Box Design

A. Overview

Fig. 3 shows two block diagrams of the proposed S-Boxes: (a) an S-Box for encryption (ENC S-Box) and (b) an S-Box for both encryption and decryption (ENC/DEC S-Box). The ENC (DEC) S-Box selects TM$_{\text{enc}}$ (TM$_{\text{dec}}$) and BM$_{\text{enc}}$ (BM$_{\text{dec}}$) for encryption (decryption) by a multiplexer. The proposed S-Boxes utilize both exponential and multiplicative offsets for a $GF((2^4)^2)$ inversion circuit based on the redundant Galois arithmetic reported by Ueno *et al.* [7].

In the ENC S-Box, TM$_{\text{enc}}$ is given by merging linear mappings $\boldsymbol{\Theta}$ and $\boldsymbol{\Gamma}$ (i.e., the exponential and multiplicative offsets) and an isomorphic mapping $\boldsymbol{\Delta}$. Likewise, BM$_{\text{enc}}$ integrates the inverse of the above three mappings with the affine transformation multiplication. That is, BM is given by merging the following mappings: the inverse isomorphism $\boldsymbol{\Delta}^{-1}$, multiplicative offset $\boldsymbol{\Gamma}$, inverse exponential offset $\boldsymbol{\Theta}^{-1}$, and affine multiplication $\boldsymbol{M}$. Thus, the ENC S-Box consists of TM$_{\text{enc}}$, the inversion circuit on $(GF(2^4)^2)$, BM$_{\text{enc}}$, and $\boldsymbol{c}$ added at the affine transformation.

TABLE I
Best Possible Parameters of the S-Box for ENC

θ	0	0	0	1	1	1	1	1	2	2	2
γ	1	16	32	39	67	79	156	234	20	91	112
θ	2	2	2	2	3	4	4	4	5	5	5
γ	165	202	222	255	150	1	77	145	42	45	66
θ	5	5	6	6	6	6	6	6	6	7	
γ	78	86	24	110	169	193	199	231	254	155	

The TM$_{\text{enc}}$ and BM$_{\text{enc}}$ for encryption in the ENC/DEC S-Box are the same as those in the ENC S-Box. For decryption, TM$_{\text{dec}}$ is given by merging the following linear mappings: the inverse affine transform $\boldsymbol{M}^{-1}$, exponential offset $\boldsymbol{\Theta}'$, multiplicative offset $\boldsymbol{\Gamma}'$, and an isomorphic mapping $\boldsymbol{\Delta}$. Note that the values of exponential and multiplicative offsets (i.e., $\boldsymbol{\Theta}'$ and $\boldsymbol{\Gamma}'$) are not necessarily the same as those used for encryption (i.e., $\boldsymbol{\Theta}$ and $\boldsymbol{\Gamma}$). In addition, it is necessary to add the constant $\boldsymbol{c}^{-1}$ of the inverse affine transformation to the above mapping. Here, let x be the input to TM$_{\text{dec}}$. From the linearity of the above mapping, TM$_{\text{dec}}$ is given as follows:

$$\begin{aligned}&\boldsymbol{\Delta}(\boldsymbol{\Gamma}'(\boldsymbol{\Theta}'(\underline{\boldsymbol{M}^{\overset{\textcircled{1}}{-1}}(\boldsymbol{x}) + \boldsymbol{c}^{\overset{\textcircled{2}}{-1}}}))\\ &\quad =^{\textcircled{1}}\boldsymbol{\Delta}(\boldsymbol{\Gamma}'(\boldsymbol{\Theta}'(\boldsymbol{M}^{-1}(\boldsymbol{x})))) +^{\textcircled{2}}\boldsymbol{\Delta}(\boldsymbol{\Gamma}'(\boldsymbol{\Theta}'(\boldsymbol{c}^{-1})))\\ &\quad = \mathrm{TM}_{\text{dec}}(\boldsymbol{x}) + \boldsymbol{c}'\end{aligned}$$

Hence, $\boldsymbol{\Delta}(\boldsymbol{\Gamma}'(\boldsymbol{\Theta}'(\boldsymbol{c}^{-1})))$ is calculated in advance. BM$_{\text{dec}}$ is given by merging $\boldsymbol{\Delta}^{-1}$, $\boldsymbol{\Gamma}'$, and $\boldsymbol{\Theta}'^{-1}$. In summary, TM$_{\text{enc}}$, BM$_{\text{enc}}$, TM$_{\text{dec}}$, and BM$_{\text{dec}}$ in the proposed S-Box are given as follows:

$$\mathrm{TM}_{\text{enc}} = \boldsymbol{\Delta} \circ \boldsymbol{\Gamma} \circ \boldsymbol{\Theta},\quad \mathrm{BM}_{\text{enc}} = \boldsymbol{M} \circ \boldsymbol{\Theta}^{-1} \circ \boldsymbol{\Gamma} \circ \boldsymbol{\Delta}^{-1},$$
$$\mathrm{TM}_{\text{dec}} = \boldsymbol{\Delta} \circ \boldsymbol{\Gamma}' \circ \boldsymbol{\Theta}' \circ \boldsymbol{M}^{-1},\quad \mathrm{BM}_{\text{dec}} = \boldsymbol{\Theta}'^{-1} \circ \boldsymbol{\Gamma}' \circ \boldsymbol{\Delta}^{-1},$$

where $\circ$ denotes the merge operation multiplying XOR matrices. Note that each of TM$_{\text{enc}}$, BM$_{\text{enc}}$, TM$_{\text{dec}}$, and BM$_{\text{dec}}$ is finally given as a single integrated linear mapping matrix.

The proposed S-Box utilizes a $GF((2^4)^2)$ inversion based on the redundant Galois arithmetic in addition to the above mapping matrices. Here, the quadratic irreducible polynomial on $GF(2^4)$ is the same as in [7] because the $GF((2^4)^2)$ inversion circuit achieves the highest performance reported so far; therefore, $\boldsymbol{\Delta}$ and $\boldsymbol{\Delta}^{-1}$ correspond to the coefficients. Moreover, $\boldsymbol{\Delta}^{-1}$ is given as a 10 × 8 matrix owing to the redundant Galois arithmetic. For the same reason, the TM and BM in the proposed S-Box are given as 8 × 8 and 10 × 8 matrices, respectively.

B. Search for Possible Matrices

This section presents the search for TM and BM for the proposed S-Box. Pairs of TM$_{\text{enc}}$ and BM$_{\text{enc}}$ (TM$_{\text{dec}}$ and BM$_{\text{dec}}$) can be selected from a pool of 2,040 owing to the multiplicative and exponential offsets. Here, the maximum depth with the two-input XOR gate is considered an indicator of possible pairs as in [8]. In particular, we search for the pairs of TM and BM such that maxHW is less than or equal to 4. This is because the matrices are computed with a delay of $\lceil \log n \rceil T_{\text{XOR}}$, where T_{XOR} is the delay of a two-input XOR gate and maxHW is n. For example, the matrix depth (delay) for $n \leq 4$ is reduced by one step compared to that for $n \geq 5$.

We searched all the 2040 pairs of TMs and BMs from the viewpoint of maxHW. Consequently, we found 32 best possible pairs, where the maxHWs of TM$_{\text{enc}}$ and BM$_{\text{enc}}$ were 4 and 6, respectively. Table I lists the 32 offset parameters of the matrices, where γ and θ are the values of multiplicative and exponential offsets, respectively. Table II shows the 12 offset parameters of the matrices where the maxHWs of TM$_{\text{dec}}$ and BM$_{\text{dec}}$ are 4 and 6, respectively. This indicates that the logical depths of TM and BM are at least $2T_{XOR}$ and $3T_{XOR}$,

TABLE II
BEST POSSIBLE PARAMETERS OF THE S-BOX FOR DEC

θ'	0	0	2	2	2	3	4	4	6	6	6	7
γ'	92	149	14	51	64	72	92	196	29	82	131	245

respectively. The resulting minimum maxHWs are the same as those from 255 candidates derived only the multiplicative offset alone in the conventional method [8]. Note, however, that the number of prospective pairs for encryption and decryption increased from 3 to 32 and from 2 to 12, respectively. This leads to an increase in the possibility of increasing performance by logic optimization under the condition of the maximum depth of the two-input XOR gate.

From the viewpoint of arithmetic circuit design, such an optimization is closely related to the data representation, which is directly related to the circuit performance. The proposed method expands the design space of redundant GF representation, and thus it can exploit more optimal parameter than the conventional method. Moreover, in contrast to the conventional method [8], we consider not only maxHWs of the matrices but also how they can be implemented using common XOR gates in standard cell libraries; that is, we examine the factoring of XOR gates to reduce circuit area and improve the efficiency with a latency preserved. The advantage of the proposed method is validated through the implementation and synthesis results in Section IV.

IV. PERFORMANCE EVALUATION

We synthesized the proposed S-Boxes to evaluate the performance. We used Synopsys Design Compiler (Q-2019) with the Nangate 45nm Open Cell Library for the logic synthesis, where both hierarchy destruction (i.e., ungroup) and enhanced delay optimization (i.e., -map_effort high) were set to the synthesis options. Here, the evaluation was performed under the condition of an area constraint excluding the registers. For comparison, under the same condition, we also evaluated the other two S-Boxes in Ueno *et al.* [8] and Maximov and Ekdahl [10], which are the most efficient $GF((2^4)^2)$-type and $GF(((2^2)^2)^2)$-type S-Boxes thus far, respectively. We synthesized all the S-Boxes with the possible pairs having the offset values in Tables I and II. During the synthesis, we employed an area optimization with various timing constraints. The timing constraint is finally determined for each S-Box such that its performance is maximized in terms of AT product without timing violation. Thus, the synthesis maximizes the performance of each S-Box through both area and speed optimizations.

Table III lists the synthesis results of ENC and ENC/DEC S-Boxes. Here, Area denotes the combinational circuit area in terms of two-input NAND gate equivalents (GEs), Delay denotes the combinational circuit delay on the critical path, CPD stands for critical path delay and denotes the number of logic gate stages, and AT denotes the area-time product. There are two or three variations for each design. The proposed S-Box and the conventional $GF((2^4)^2)$-type S-Box have two variants, namely, small area and fast, as reported in [8]. The conventional $GF(((2^2)^2)^2)$-type S-Box has three variants, namely, tradeoff, bonus, and fast, as reported in [10].

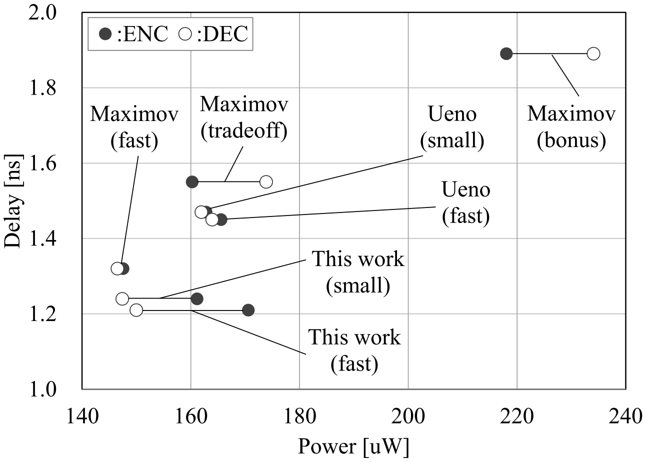


Fig. 4. Power-delay plots for ENC/DEC S-Boxes.

Table III indicates that the proposed ENC S-Box achieved AT products smaller by 23.2% and 21.3% compared with the small-area and fast variants of [8], respectively. The selected offset values of $\mathrm{TM}_{\mathrm{enc}}$ and $\mathrm{BM}_{\mathrm{enc}}$ were $\gamma = 231$ and $\theta = 6$ in both implementations. In addition, the proposed ENC/DEC S-Box achieved AT products smaller by 15.4% and 20.1% compared with the small-area and fast variants of [8], respectively. For the small-area implementation, the selected offset values of $\mathrm{TM}_{\mathrm{enc}}$, $\mathrm{BM}_{\mathrm{enc}}$, $\mathrm{TM}_{\mathrm{dec}}$, and $\mathrm{BM}_{\mathrm{dec}}$ were $\gamma = 79$, $\theta = 1$, $\gamma = 196$, and $\theta = 4$, respectively. In contrast, for the fast implementation, the selected offset values of $\mathrm{TM}_{\mathrm{enc}}$, $\mathrm{BM}_{\mathrm{enc}}$, $\mathrm{TM}_{\mathrm{dec}}$, and $\mathrm{BM}_{\mathrm{dec}}$ were $\gamma = 231$, $\theta = 6$, $\gamma' = 196$, and $\theta' = 4$, respectively. The proposed S-Boxes were also better than the highest-performing conventional S-Boxes reported in [10]. The proposed ENC S-Box achieved AT products smaller by 3.1% and 0.9% compared with the small-area (tradeoff) and efficient (bonus) variants of [10], respectively. Moreover, focusing on the fast variant, the proposed ENC S-Box achieves 8.9% higher area-timing efficiency than Maximov–EKdahl S-Box [10]. Similarly, the proposed ENC/DEC S-Box achieved AT products smaller by 14.5%, 28.8%, and 23.0% compared with the tradeoff, bonus, and fast variants of [10], respectively.

In addition, Fig. 4 shows the power and delay of encryption and decryption for each ENC/DEC S-Box presented in Table III. Here, the power value was also estimated at 100 MHz based on switching activities from the logic synthesis. Note that the power consumption is almost proportional to clock frequency as static power consumption is far smaller than dynamic one, and the advantages of proposed method over conventional method is independent of clock frequency. Moreover, Table III also reports the evaluation result of energy consumption per bit, which is a common evaluation metric related to power consumption invariant to clock frequency. From the figure and table, we can confirm that the power/energy consumption of the proposed ENC/DEC S-Box is smaller than those of [8] and [10], especially during decryption.

In addition to the logic synthesis, we compare the theoretical XOR gate counts of the proposed and conventional S-Boxes in Table IV, where the numbers of XOR gates for

TABLE III
SYNTHESIS RESULT OF S-BOXES

S-Box	Variant	ENC S-Box					ENC/DEC S-Box						Energy [f J/bit]	
		θ, γ	Area [GE]	Delay [ns]	CPD [Stage]	AT [GE · ns]	ENC θ, γ	DEC θ', γ'	Area [GE]	Delay [ns]	CPD [Stage]	AT [GE · ns]	ENC	DEC
Ueno et al. [8]	small area	0, 6	229.33	1.49	22	341.70	0, 6	0, 149	311.66	1.47	21	458.14	203	201
	fast		234.33	1.45	18	339.77			333.66	1.45	20	483.81	206	203
Maximov and Ekdahl [10]	tradeoff	*	205.00	1.32	18	270.60	*	*	292.66	1.55	22	453.62	200	220
	bonus		210.00	1.26	18	264.60			287.99	1.89	27	544.30	273	293
	fast		248.33	1.18	15	293.03			380.33	1.32	19	502.03	185	184
This work	small area	6, 231	222.33	1.18	18	262.34	1, 79	4, 196	312.66	1.24	18	387.70	201	185
	fast		228.66	1.17	15	267.53	6, 231		319.66	1.21	17	386.79	214	186

TABLE IV
GATE COUNTS OF LINEAR OPERATIONS

S-Box	Variant	ENC S-Box		ENC/DEC S-Box	
		$\mathrm{TM}_{\mathrm{enc}}$	$\mathrm{BM}_{\mathrm{enc}}$	$\mathrm{TM}_{\mathrm{enc}}$ $+\mathrm{TM}_{\mathrm{dec}}$	$\mathrm{BM}_{\mathrm{enc}}$ $+\mathrm{BM}_{\mathrm{dec}}$
Ueno et al. [8]	small area	15	21	25	38
	fast				
This work	small area	15	18	21	34
	fast			25	31

TM and BM are counted when the XOR trees are configured for achieving the minimum delay. For a fair comparison, we compare only the two $GF((2^4)^2)$-type S-Boxes because the $GF(((2^2)^2)^2)$-type S-Box has a different integration of linear operations. For the ENC S-Boxes, the $\mathrm{TM}_{\mathrm{enc}}$ gate count of this brief was the same as that of [8], and the $\mathrm{BM}_{\mathrm{enc}}$ gate count of this brief was smaller than that of [8]. For the ENC/DEC S-Boxes, the total TM gate count of this brief was equal to or less than that of [8], and the total BM gate count of this brief was smaller than that of [8]. Thus, the proposed linear operations require fewer gates than the conventional ones, which results in better performance after logic synthesis. Even compared with the highest-performing conventional $GF(((2^2)^2)^2)$-type S-Box, the proposed S-Box shows better performance under the experimental condition. This suggests that the proposed S-Box design clearly provides a class of the highest-performing circuit structures.

In general, the resulting performance could slightly depend on the technology and synthesis condition. In the present study, we considered only maxHW as a performance indicator. Even for a TM and BM with the same maxHW, the ease of factoring and the maximum/average fanout of gates in logic synthesis change with the matrix representations. However, the proposed method provides 32 types of ENC S-Boxes and 12 types of DEC S-Boxes, and there is a high possibility that the best circuit structure for other experimental conditions can also be obtained from them.

V. CONCLUSION

This brief presented the design and evaluation of new AES S-Boxes that combine the redundant Galois-field arithmetic with linear mapping optimization. The search space of the linear mappings could be expanded by eight times by the multiplicative and exponential offset techniques. Consequently, we found more than six times the number of candidates with the same (best) logical depth as before. We synthesized all the candidates of linear mappings and confirmed that the proposed S-Box decreased the AT product by more than 20% against the corresponding conventional S-Box. The proposed S-Box even performed better than the most efficient conventional S-Box reported thus far. Possible avenues for future work include a detailed evaluation of the power/energy of the designed S-Boxes, the development of a systematic selection method for optimal parameters, and a design of side-channel-resistant AES hardware that makes the best use of the proposed S-Boxes.

REFERENCES

[1] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A compact Rijndael hardware architecture with S-box optimization,” in *Advances in Cryptology (ASIACRYPT)* (Lecture Notes in Computer Science), C. Boyd, Ed. Berlin, Germany: Springer, 2001, pp. 239–254.

[2] T. Itoh and S. Tsujii, “A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases,” *Inf. Comput.*, vol. 78, no. 3, pp. 171–177, Sep. 1988.

[3] A. Rudra, P. K. Dubey, C. S. Jutla, V. Kumar, J. R. Rao, and P. Rohatgi, “Efficient Rijndael encryption implementation with composite field arithmetic,” in *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), Ç. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Germany: Springer, 2001, pp. 171–184.

[4] D. Canright, “A very compact S-box for AES,” in *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), J. R. Rao and B. Sunar, Eds. Berlin, Germany: Springer, 2005, pp. 441–455.

[5] K. Nekado, Y. Nogami, and K. Iokibe, “Very short critical path implementation of AES with direct logic gates,” in *Advances in Information and Computer Security* (Lecture Notes in Computer Science), G. Hanaoka and T. Yamauchi, Eds. Berlin, Germany: Springer, 2012, pp. 51–68.

[6] Y.-S. Jeon, Y.-J. Kim, and D.-H. Lee, “A compact memory-free architecture for the AES algorithm using resource sharing methods,” *J. Circuits Syst. Comput.*, vol. 19, pp. 1109–1130, Aug. 2010.

[7] R. Ueno, N. Homma, Y. Sugawara, Y. Nogami, and T. Aoki, “Highly efficient $GF(2^8)$ inversion circuit based on redundant GF arithmetic and its application to AES design,” in *Cryptographic Hardware and Embedded Systems (CHES)* (Lecture Notes in Computer Science), T. Güneysu and H. Handschuh, Eds. Berlin, Germany: Springer, 2015, pp. 63–80.

[8] R. Ueno, N. Homma, Y. Nogami, and T. Aoki, “Highly efficient $GF(2^8)$ inversion circuit based on hybrid GF representations,” *J. Cryptograph. Eng.*, vol. 9, no. 2, pp. 101–113, Jun. 2019.

[9] J. Boyar and R. Peralta, “A small depth-16 circuit for the AES S-box,” in *Information Security and Privacy Research* (IFIP Advances in Information and Communication Technology), D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Berlin, Germany: Springer, 2012, pp. 287–298.

[10] A. Maximov and P. Ekdahl, “New circuit minimization techniques for smaller and faster AES SBoxes,” *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2019, pp. 91–125, Aug. 2019. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8346

[11] S. Mathew *et al.*, “53Gbps native $G(2^4)^2$ composite-field AES-encrypt/decrypt accelerator for content-protection in 45nm high-performance microprocessors,” in *Proc. Symp. VLSI Circuits*, 2010, pp. 169–170.

[12] S. Gueron and S. Mathew, “Hardware implementation of AES using area-optimal polynomials for composite-field representation $GF(2^4)^2$ of $GF(2^8)$,” in *Proc. IEEE 23rd Symp. Comput. Arithmetic (ARITH)*, Jul. 2016, pp. 112–117.