$\mathbb{F}_{(2^4)^2}$ 上の複雑混合基底による基底変換を用いた AES の SubBytes 変換

根角 健太† 野上 保之† 森岡 恵理†

†岡山大学大学院自然科学研究科（工学部通信ネットワーク工学科）
700–8530 岡山県岡山市北区津島中 3–1–1
{nekado,nogami,morioka}@trans.cne.okayama-u.ac.jp

あらまし AES 暗号の SubBytes 変換では，線形解読法の対策として非線形処理である有限体 $\mathbb{F}_{2^8}$ 上の逆元計算を組み込んでいる．この逆元計算を回路実装する場合，逆元計算の処理時間を短くし，かつ使用する論理ゲートを少数で済ませるためには，$\mathbb{F}_{2^8}$ 上の逆元計算の替わりに，それと同型な逐次拡大体上の逆元計算を適用することが望ましい．SubBytes 変換に対して逐次拡大体上の逆元計算を組み込む場合，逐次拡大体上の逆元計算だけではなく，$\mathbb{F}_{2^8}$ から逐次拡大体への基底変換およびその逆変換が必要になる．そこで，本稿では $\mathbb{F}_{(2^4)^2}$ 上の複雑混合基底を提案し，その基底を用いることで基底変換および逆変換回路の処理時間をより短くできることを示す．

SubBytes Transform for AES Adopting Basis Conversion with More Miscellaneously Mixed Basis in $\mathbb{F}_{(2^4)^2}$

Kenta Nekado† Yasuyuki Nogami† Eri Morioka‡

†Graduate School of Natural Science and Technology
(Communication Network Engineering), Okayama University
3–1–1 Tsushima–naka, Kita–ward, Okayama–city, Okayama, 700–8530, JAPAN
{nekado,nogami,morioka}@trans.cne.okayama-u.ac.jp

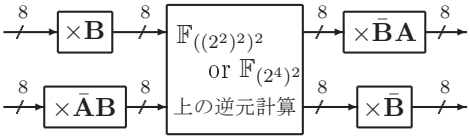
Abstract A lot of improvements and optimizations for the hardware implementation of SubBytes of AES, in detail *inversion* in $\mathbb{F}_{2^8}$ have been reported. Instead of the AES original $\mathbb{F}_{2^8}$, it is known that not only its isomorphic tower field $\mathbb{F}_{((2^2)^2)^2}$ but also $\mathbb{F}_{(2^4)^2}$ has more efficient inversions. In the case of using $\mathbb{F}_{(2^4)^2}$, SubBytes transform consists of the inversion in $\mathbb{F}_{(2^4)^2}$ and the basis conversion between $\mathbb{F}_{2^8}$ and $\mathbb{F}_{(2^4)^2}$. Therefore, not only the inversion but also the basis conversion must be carried out efficiently. This paper, in order to provide efficient basis conversion, proposes *More Miscellaneously Mixed Bases* (MMMB).

1 序論

AES [1] の SubBytes 変換を回路実装する際，8 次拡大された 2 元体（ガロア体）$\mathbb{F}_{2^8}$ 上の逆元計算の替りに，それと同型な逐次拡大体（合成体）上の逆元計算を採用した方が処理時間が短く，かつ論理ゲート総数の少ない SubBytes 変換回路を実装できる [2, 3, 4, 5, 6]．このように逐次拡大体を利用するためには，基底変換と呼ばれる処理が必要であり，図 1 のように SubBytes 変換回路に組み込まなければならない．ただし，図 1 の $\mathbf{A}$, $\mathbf{B}$, $\bar{\mathbf{A}}$ および $\bar{\mathbf{B}}$ はそれぞれアフィン変換行列，基底変換行列，それらの逆行列 $\mathbf{A}^{-1}$, $\mathbf{B}^{-1}$ を意味する．より高速な SubBytes 変換を実装するためには，$\mathbb{F}_{2^8}$ と同型な逐次拡大体上の逆元計算だけではなく，図 1 に示す $\times\mathbf{B}$, $\times\bar{\mathbf{B}}\mathbf{A}$, $\times\bar{\mathbf{A}}\mathbf{B}$, $\times\bar{\mathbf{B}}$ も高速に計算できる必要がある．こ

れらの行列計算は，$\mathbf{B}$，$\bar{\mathbf{B}}\mathbf{A}$，$\bar{\mathbf{A}}\mathbf{B}$，$\bar{\mathbf{B}}$ それぞれの種類を数多く準備できれば，計算効率の高い行列を選択可能になるため，高速化できる．行列の選択肢を増やす手法として，野上らは混合基底（Mixed Bases: MB）[4] を提案している．一方で，$\mathbb{F}_{2^8}$ と同型な $\mathbb{F}_{(2^4)^2}$ 上の逆元計算を高速化できる手法として，著者らは冗長表現基底（Redundantly Represesnted Basis: RRB）[6] を提案している．この RRB を採用した場合，計算効率が高い行列の条件が厳しくなるため，MB では役不足となる．そこで，本稿ではさらに多くの行列を準備できるように，MB を改良した複雑混合基底（More Miscellaneously Mixed Bases: MMMB）を提案する．

(a) SubBytes 変換時



(b) InvSubBytes 変換時

図 1: SubBytes および InvSubBytes 変換回路

2 基底変換

本節では，著者らが [6] で示している $\mathbb{F}_{2^4}$ 上の逆元計算実装を紹介しながら，基底変換の計算効率について考える．

2.1 基底変換処理を含む SubBytes 変換

$\mathbb{F}_{2^8}$ 上の既約多項式 $f(t)=t^8+t^4+t^3+t+1$ の根を α とするとき，AES の SubBytes 変換では本来，多項式基底 $\{1,\alpha,\alpha^2,\ldots,\alpha^6,\alpha^7\}$ を用いて $\mathbb{F}_{2^8}$ 上の元を表現する．ここで，$\tilde{C}$ を $\mathbb{F}_{2^8}$ 上の元（8–bit ベクトル）とする．これを多項式基底で表現すると，次式のようになる．

$$\begin{aligned}\tilde{C} &= \tilde{c}_0+\tilde{c}_1\alpha+\tilde{c}_2\alpha^2+\cdots+\tilde{c}_6\alpha^6+\tilde{c}_7\alpha^7\\ &= [\,\tilde{c}_0\ \ \tilde{c}_1\ \ \tilde{c}_2\ \ \cdots\ \ \tilde{c}_6\ \ \tilde{c}_7\,]. \end{aligned}\tag{1}$$

この $\tilde{C}$ に対して基底変換処理を含む SubBytes 変換を実行すると，次式のように計算される．

$$\tilde{L} = \Big(\big(\tilde{C}\mathbf{B}\big)^{-1}\Big)\bar{\mathbf{B}}\mathbf{A}+J,\tag{2a}$$

$$J = [\,1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\,].\tag{2b}$$

また，式 (2) の $\tilde{L}$ に対して基底変換処理を含む InvSubBytes 変換を実行すると，次式のように計算される．

$$\tilde{C} = \Big(\big(\tilde{L}\bar{\mathbf{A}}\mathbf{B}+K\mathbf{B}\big)^{-1}\Big)\bar{\mathbf{B}},\tag{3a}$$

$$K = [\,1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\,].\tag{3b}$$

ただし，式 (2) , (3) における $\bar{\mathbf{B}}\mathbf{A}$, $\bar{\mathbf{A}}\mathbf{B}$ および $K\mathbf{B}$ は事前計算される．ここで，$C=\tilde{C}\mathbf{B}$, $L=\tilde{L}\bar{\mathbf{A}}\mathbf{B}+K\mathbf{B}$ とする．これらは $\mathbb{F}_{2^8}$ と同型な逐次拡大体上の元であり，その逆元 C^{-1}, L^{-1} は効率良く計算される．

2.2 基底変換の計算効率

著者らは [6] にて，$\mathbb{F}_{2^8}$ と同型，かつ逆元計算が高速な逐次拡大体 $\mathbb{F}_{(2^4)^2}$ の構成例として，$\mathbb{F}_{2^4}$ を type–I Optimal Normal Basis (ONB) $\{\beta,\beta^2,\beta^{2^2},\beta^{2^3}\}$ で構成し，それを多項式基底 $\{1,\gamma\}$ で 2 次逐次拡大した $\mathbb{F}_{(2^4)^2}$ を紹介している．ただし，β および γ は，それぞれ $\mathbb{F}_2$ 上の 4 次既約多項式 $g(t)=t^4+t^3+t^2+t+1$ および $\mathbb{F}_{2^4}$ 上の 2 次既約多項式 $h(t)=t^2+Qt+R$ $(Q,R\in\mathbb{F}_{2^4})$ における根である．以降では基底変換の一例として，$\mathbb{F}_{2^8}$ からこの $\mathbb{F}_{(2^4)^2}$ への基底変換を考える．$\mathbb{F}_{2^8}$ に関しては，$f(t)$ の根 α に対する共役元，すなわち $f(t)$ における他の根として $\alpha^2,\alpha^{2^2},\ldots,\alpha^{2^6},\alpha^{2^7}$ が存在する．よって，$\mathbb{F}_{2^8}$ 上の元を表現する多項式基底は $\{1,\alpha^{2^j},(\alpha^{2^j})^2,\ldots,(\alpha^{2^j})^6,(\alpha^{2^j})^7\}$ $(0\le j\le 7)$ というように 8 種類存在し，$\mathbb{F}_{2^8}$ と同型な拡大体上の基底を用いて区別できる．基底元 $(\alpha^{2^j})^k$ が式 (4) で与えられれば，$\mathbb{F}_{2^8}$ から $\mathbb{F}_{(2^4)^2}$ への基底変換行列 $\mathbf{B}_j$ は式 (5) のように求まる．

$$\begin{aligned}(\alpha^{2^j})^k=&\{w_{j,k,0}\beta+w_{j,k,1}\beta^2+w_{j,k,2}\beta^{2^2}+w_{j,k,3}\beta^{2^3}\}\\ &+\{w_{j,k,4}\beta+w_{j,k,5}\beta^2+w_{j,k,6}\beta^{2^2}+w_{j,k,7}\beta^{2^3}\}\gamma,\\ &(0\le j\le 7,\ 0\le k\le 7,\ w_{j,k,l}\in\mathbb{F}_2).\end{aligned}\tag{4}$$

$$\mathbf{B}_j=\begin{bmatrix} w_{j,0,0} & w_{j,0,1} & w_{j,0,2} & & w_{j,0,6} & w_{j,0,7}\\ w_{j,1,0} & w_{j,1,1} & w_{j,1,2} & \cdots & w_{j,1,6} & w_{j,1,7}\\ w_{j,2,0} & w_{j,2,1} & w_{j,2,2} & & w_{j,2,6} & w_{j,2,7}\\ \vdots & & & \ddots & \vdots & \\ w_{j,6,0} & w_{j,6,1} & w_{j,6,2} & & w_{j,6,6} & w_{j,6,7}\\ w_{j,7,0} & w_{j,7,1} & w_{j,7,2} & \cdots & w_{j,7,6} & w_{j,7,7}\end{bmatrix}.\tag{5}$$

よって，式 (5) に示すように，基底変換行列は 8 種類準備でき，その中から最適な行列を選べる．

ここで，基底変換の計算効率を示すため，次

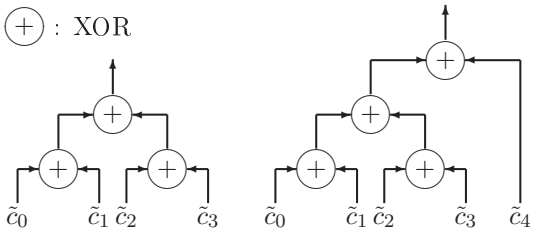
式の行列を例に考える．

$$\mathbf{B} = \left[\begin{array}{c:c:c:c:c:c:c:c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]. \quad (6)$$

このとき，$\times\mathbf{B}$ は次式のように求まる．

$$C = \tilde{C}\mathbf{B} = \left[\begin{array}{l} \tilde{c}_0 \\ \tilde{c}_0+\tilde{c}_1 \\ (\tilde{c}_0+\tilde{c}_1)+\tilde{c}_2 \\ (\tilde{c}_0+\tilde{c}_1)+(\tilde{c}_2+\tilde{c}_3) \\ \{(\tilde{c}_0+\tilde{c}_1)+(\tilde{c}_2+\tilde{c}_3)\}+\tilde{c}_4 \\ \{(\tilde{c}_0+\tilde{c}_1)+(\tilde{c}_2+\tilde{c}_3)\}+(\tilde{c}_4+\tilde{c}_5) \\ \{(\tilde{c}_0+\tilde{c}_1)+(\tilde{c}_2+\tilde{c}_3)\}+\{(\tilde{c}_4+\tilde{c}_5)+\tilde{c}_6\} \\ \{(\tilde{c}_0+\tilde{c}_1)+(\tilde{c}_2+\tilde{c}_3)\}+\{(\tilde{c}_4+\tilde{c}_5)+\{\tilde{c}_6+\tilde{c}_7)\} \end{array}\right]^{\mathcal{T}}. \quad (7)$$

式(7)の計算式を回路化すると図 2 の通りになる．



(a) 行列 4 行目　　(b) 行列 5 行目

図 2: 式 (7) の計算回路図（一部）

ここで，式 (5) の $\mathbf{B}_j$ における列ベクトルを次式のように表し，

$$W_{j,k} = [\, w_{j,0,k}\ w_{j,1,k}\ w_{j,2,k}\ \cdots\ w_{j,6,k}\ w_{j,7,k}\,]^{\mathcal{T}}, \quad (8)$$

ベクトル W に含まれる 1 の数，すなわち W のハミング重みを $\mathrm{Hw}(W)$ と記す．また，以降では XOR ゲートのクリティカルパスの遅延時間を T_{XOR} と表記する．式 (7) から分かるように，$\mathrm{Hw}(W_k) \leq 4$ のとき，ベクトルの積 $\tilde{C}W_k$ は図 2(a) に示すように $2T_{\mathrm{XOR}}$ 以下で計算できる．一方で，$\mathrm{Hw}(W_{j,k}) \geq 5$ のとき，図 2(b) に示すように $3T_{\mathrm{XOR}}$ で計算できる．したがって，すべての $W_{j,k}$ $(0 \leq k \leq 7)$ が $\mathrm{Hw}(W_{j,k}) \leq 4$ を満たす場合，$\times\mathbf{B}_j$ におけるクリティカルパスの遅延時間は $2T_{\mathrm{XOR}}$ 以下で済む．それ以外の場合は $3T_{\mathrm{XOR}}$ となる．8 行 8 列の非零行列の中で，すべての列ベクトルにおけるハミング重みが 4 以下になる行列は次式に示す確率で存在する．

$$P_1 = ({}_8\mathrm{C}_0+{}_8\mathrm{C}_1+{}_8\mathrm{C}_2+{}_8\mathrm{C}_3+{}_8\mathrm{C}_4)^8/(2^{8\times 8}-1) \approx 2.70\%. \quad (9)$$

上述の内容は，$\times\mathbf{B}$ だけではなく $\times\bar{\mathbf{B}}\mathbf{A}$，$\times\bar{\mathbf{A}}\mathbf{B}$，および $\times\bar{\mathbf{B}}$ に対しても該当する．AES の SubBytes 変換で実行される $\times\mathbf{B}$ と $\times\bar{\mathbf{B}}\mathbf{A}$ の両方を $2T_{\mathrm{XOR}}$ で計算するためには，$\mathbf{B}, \bar{\mathbf{B}}\mathbf{A}$ ともに列ベクトルすべてのハミング重みが 4 以下でなければならない．このような $\mathbf{B}$ と $\bar{\mathbf{B}}\mathbf{A}$ の組は $P_1 \times P_1 = 7.29\%_{00}$ の確率で存在する．一方で，InvSubBytes 変換で実行される $\times\bar{\mathbf{A}}\mathbf{B}$ と $\times\bar{\mathbf{B}}$ に対しても同様のことが言える．

3 冗長表現基底

著者らは [6] にて，$\mathbb{F}_{(2^4)^2}$ 上の逆元計算を高速化できる冗長表現基底（Represented Redundantly Basis: RRB）を提案している．これは，第 2.2 節で紹介した $\mathbb{F}_{2^4}$ 上の type–I ONB $\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\}$ に対し，$\{1\}$ を加えた集合である．以下では，RRB の性質について示す．

$\mathbb{F}_{2^4}$ 上の type–I ONB における基底元 β は，$\mathbb{F}_2$ 上の 4 次既約多項式 $g(t) = t^4+t^3+t^2+t+1$ の根であるため，次式に示す性質が導かれる．

$$g_3(\beta) = \beta^4+\beta^3+\beta^2+\beta+1 = 0,$$
$$\Leftrightarrow\ g_3(\beta) = \beta+\beta^2+\beta^{2^2}+\beta^{2^3}+1 = 0, \quad (10a)$$
$$\because\ (\beta+1)g_3(\beta)+1 = \beta^5 = 1. \quad (10b)$$

式 (10b) より，type–I ONB $\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\}$ は次式のように式変形できる．

$$\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\} = \{\beta, \beta^2, \beta^3, \beta^4\}. \quad (11)$$

一方で，β の共役元，すなわち $g(t)$ における他の根として β^2，β^{2^2}，β^{2^3} が存在する．これらの共役元から，式 (10b) より次式に示す 4 種類の多項式基底が考えられる．

$$\{1, \beta, \beta^2, \beta^3\} = \{1, \beta,\ \beta^2, \beta^3\}, \quad (12a)$$
$$\{1, \beta^2, (\beta^2)^2, (\beta^2)^3\} = \{1, \beta,\ \beta^2, \beta^4\}, \quad (12b)$$
$$\{1, \beta^{2^2}, (\beta^{2^2})^2, (\beta^{2^2})^3\} = \{1, \beta^2, \beta^3, \beta^4\}, \quad (12c)$$
$$\{1, \beta^{2^3}, (\beta^{2^3})^2, (\beta^{2^3})^3\} = \{1, \beta,\ \beta^3, \beta^4\}. \quad (12d)$$

式 (11)，(12) より，集合 $\{1, \beta, \beta^2, \beta^3, \beta^4\}$ から

元を 1 つ取り除いた集合は基底を成すと言える．一方で，RRB $\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}, 1\} = \{1, \beta, \beta^2, \beta^3, \beta^4\}$ は，元を 1 つも取り除いていない集合である．したがって，式 (10a) より RRB は簡単に式 (11)，(12) に示す基底へ変換できる．

$\mathbb{F}_{2^4}$ 上の RRB に加えて，第 2.2 節で紹介した $\mathbb{F}_{2^4}$ を 2 次逐次拡大するための多項式基底 $\{1, \gamma\}$ を採用した場合，$\mathbb{F}_{2^4}$ 上の逆元計算回路は図 3(a) の通りになる．一方で，多項式基底 $\{1, \gamma\}$ の替りに正規基底 $\{\gamma, \gamma^{16}\}$ を採用した場合，図 4(a) の通りになる．どちらの回路でも，入力 $D, E \in \mathbb{F}_{2^4}$ は式 (11)，(12) で示されている基底ならば，どの基底を用いて表現しても良い．このとき，$\mathbb{F}_{(2^4)^2}$ 上の逆元計算直前に行われる $\times\mathbf{B}$ および $\times\bar{\mathbf{A}}\mathbf{B}$ の計算効率を第 2.2 節で述べたように考えて構わない．一方で，図 3(a), 4(a) に示す逆元計算回路の出力 $Y, Z \in \mathbb{F}_{2^4}$ は RRB で表現されている．よって，$\mathbb{F}_{(2^4)^2}$ 上の逆元計算直後に行われる $\times\bar{\mathbf{B}}\mathbf{A}$ および $\times\bar{\mathbf{B}}$ の計算効率を改めて考え直さなければならない．本節では，その効率について考える．

3.1 冗長表現基底の影響

手始めに，第 2.2 節と同様に，$\mathbb{F}_{2^4}$ を type–I Optimal Normal Basis (ONB) $\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\}$ で構成し，それを多項式基底 $\{1, \gamma\}$ で 2 次逐次拡大した $\mathbb{F}_{(2^4)^2}$ を考える．基底元 β^{2^k} および $\beta^{2^k}\gamma$ とアフィン変換行列 $\mathbf{A}$ との積 $\beta^{2^k}\mathbf{A}$ および $\beta^{2^k}\gamma\mathbf{A}$ が式 (13) で与えられるとき，$\bar{\mathbf{B}}\mathbf{A}$ は式 (14) のように求まる．

$$\beta^{2^k}\mathbf{A} = u_{j,k,0} + u_{j,k,1}\alpha^{2^j} + u_{j,k,2}(\alpha^{2^j})^2 + \cdots + u_{j,k,6}(\alpha^{2^j})^6 + u_{j,k,7}(\alpha^{2^j})^7, \quad (13a)$$

$$\beta^{2^k}\gamma\mathbf{A} = v_{j,k,0} + v_{j,k,1}\alpha^{2^j} + v_{j,k,2}(\alpha^{2^j})^2 + \cdots + v_{j,k,6}(\alpha^{2^j})^6 + v_{j,k,7}(\alpha^{2^j})^7, \quad (13b)$$

$$(0 \le l \le 7,\ 0 \le k \le 4,\ u_{j,k,l},\ v_{j,k,l} \in \mathbb{F}_2). \quad (13c)$$

$$\bar{\mathbf{B}}_j\mathbf{A} = \begin{bmatrix} u_{j,0,0} & u_{j,0,1} & u_{j,0,2} & \cdots & u_{j,0,6} & u_{j,0,7} \\ \vdots & & \ddots & & \vdots & \\ u_{j,3,0} & u_{j,3,1} & u_{j,3,2} & \cdots & u_{j,3,6} & u_{j,3,7} \\ \hdashline v_{j,0,0} & v_{j,0,1} & v_{j,0,2} & \cdots & v_{j,0,6} & v_{j,0,7} \\ \vdots & & \ddots & & \vdots & \\ v_{3,0} & v_{j,3,1} & v_{j,3,2} & \cdots & v_{j,3,6} & v_{j,3,7} \end{bmatrix}. \quad (14)$$

ここで，$\times\bar{\mathbf{B}}\mathbf{A}$ の計算効率を示すため，次式の行列を考える．

$$\bar{\mathbf{B}}\mathbf{A} = \left[\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]. \quad (15)$$

図 3(a) に示されている回路の入力を $\mathbb{F}_{(2^4)^2}$ 上の非零元 $C = D + E\gamma$ $(D, E \in \mathbb{F}_2)$，出力をその逆元 $X = C^{-1} = Y + Z\gamma$ $(Y, Z \in \mathbb{F}_2)$ とする．図 3(a) のように Y と Z が RRB で表現されている場合，式 (10a) より次式のように簡単に正規基底表現へ変換できる．

$$\begin{aligned} Y &= \check{y}_0\beta + \check{y}_1\beta^2 + \check{y}_2\beta^{2^2} + \check{y}_3\beta^{2^3} + \check{y}_4 \\ &= (\check{y}_0+\check{y}_4)\beta + (\check{y}_1+\check{y}_4)\beta^2 \\ &\quad + (\check{y}_2+\check{y}_4)\beta^{2^2} + (\check{y}_3+\check{y}_4)\beta^{2^3}, \end{aligned} \quad (16a)$$

$$\begin{aligned} Z &= \check{z}_0\beta + \check{z}_1\beta^2 + \check{z}_2\beta^{2^2} + \check{z}_3\beta^{2^3} + \check{z}_4 \\ &= (\check{z}_0+\check{z}_4)\beta + (\check{z}_1+\check{z}_4)\beta^2 \\ &\quad + (\check{z}_2+\check{z}_4)\beta^{2^2} + (\check{z}_3+\check{z}_4)\beta^{2^3}. \end{aligned} \quad (16b)$$

このとき，$\times\bar{\mathbf{B}}\mathbf{A}$ は次式のように求まる．

$$X\bar{\mathbf{B}}\mathbf{A} = \begin{bmatrix} \check{y}_0+\check{y}_4 \\ \check{y}_0+\check{y}_1 \\ (\check{y}_0+\check{y}_4)+(\check{z}_0+\check{z}_4) \\ (\check{y}_0+\check{y}_1)+(\check{y}_2+\check{y}_4) \\ (\check{y}_0+\check{y}_1)+(\check{z}_0+\check{z}_4) \\ (\check{y}_0+\check{y}_1)+(\check{y}_2+\check{y}_3) \\ \{(\check{y}_0+\check{y}_1)+(\check{y}_2+\check{y}_4)\}+(\check{z}_0+\check{z}_4) \\ (\check{y}_0+\check{y}_1)+(\check{z}_0+\check{z}_1) \end{bmatrix}^{\mathcal{T}}. \quad (17)$$

ここで，$\bar{\mathbf{B}}\mathbf{A}$ の列を 2 つのベクトルを用いて，次式のように表す．

$$U_{j,k} = [u_{j,k,0}\ u_{j,k,1}\ u_{j,k,2}\ u_{j,k,3}]^{\mathcal{T}}, \quad (18a)$$

$$V_{j,k} = [v_{j,k,0}\ v_{j,k,1}\ v_{j,k,2}\ v_{j,k,3}]^{\mathcal{T}}. \quad (18b)$$

式 (17) から分かるように，列ベクトル U_k，V_k が，$\mathrm{Hw}(U_i) : \mathrm{Hw}(V_i) \neq 3:1$ かつ $1:3$，および $\mathrm{Hw}(U_i) + \mathrm{Hw}(V_i) \le 4$ を満たす場合，$\times\bar{\mathbf{B}}\mathbf{A}$ におけるクリティカルパスの遅延時間は $2T_{\mathrm{XOR}}$ 以下で済む．それ以外の場合は $3T_{\mathrm{XOR}}$ となる．$\bar{\mathbf{B}}\mathbf{A}$ の列ベクトルすべてにおいて，$\mathrm{Hw}(U_i) : \mathrm{Hw}(V_i) \neq 3:1$ かつ $1:3$，および $\mathrm{Hw}(U_i) + \mathrm{Hw}(V_i) \le 4$ を満たす確率は次式のように求まる．

$$P_2 = ({}_8\mathrm{C}_0{+}{}_8\mathrm{C}_1{+}{}_8\mathrm{C}_2{+}{}_8\mathrm{C}_3{+}{}_4\mathrm{C}_4{\cdot}{}_4\mathrm{C}_0{+}{}_4\mathrm{C}_2{\cdot}{}_4\mathrm{C}_2 + {}_4\mathrm{C}_0 \cdot {}_4\mathrm{C}_4)^8/(2^{8\times 8}-1) \approx 0.47\%. \quad (19)$$

上述の内容は，$\times\bar{\mathbf{B}}\mathbf{A}$ だけではなく $\times\bar{\mathbf{B}}$ に対しても該当する．したがって，RRB を採用した場合，AES の SubBytes 変換で実行される $\times\mathbf{B}$ と $\times\bar{\mathbf{B}}\mathbf{A}$ の両方を $2T_{\mathrm{XOR}}$ で計算できる $\mathbf{B}$ と $\bar{\mathbf{B}}\mathbf{A}$ の組は，$P_1 \times P_2 = 1.27\%_{00}$ の確率で存在する．一方で，InvSubBytes 変換で実行される $\times\bar{\mathbf{A}}\mathbf{B}$ と $\times\bar{\mathbf{B}}$ に対しても同様のことが言える．

4 複雑混合基底

野上ら [4] によって $\mathbf{B}$ と $\bar{\mathbf{B}}\mathbf{A}$，および $\bar{\mathbf{B}}$ と $\bar{\mathbf{A}}\mathbf{B}$ の組を増加させるための手法が提案されている．[4] には，入出力が別の基底で表現されている $\mathbb{F}_{((2^2)^2)^2}$ 上の逆元計算回路が示されている．この別々の基底は混合基底（Mixed Bases: MB）[4] と呼ばれている．逆元計算回路の入出力に別の基底を用いるため，行列の組を増やすことができる．[4] では，$\mathbb{F}_{(2^2)^2}$ の 2 次逐次拡大体 $\mathbb{F}_{((2^2)^2)^2}$ 上の MB が提案されているが，同様に $\mathbb{F}_{2^4}$ の 2 次逐次拡大体 $\mathbb{F}_{(2^4)^2}$ 上の MB を考えることができる．以降では，MB を用いた $\mathbb{F}_{(2^4)^2}$ 上の逆元計算を考える．

γ を $\mathbb{F}_{2^4}$ 上の 2 次既約多項式 $h(t) = t^2+Qt+R$ $(Q, R \in \mathbb{F}_{2^4})$ における根とする．$\mathbb{F}_{(2^4)^2}$ 上の非零元 C, $X = C^{-1}$ を次式のようにそれぞれ多項式基底 $\{1, \gamma\}$，正規基底 $\{\gamma, \gamma^{16}\}$ で表すとき，

$$C = D + E\gamma \qquad (D, E \in \mathbb{F}_{2^4}), \qquad (20a)$$

$$X = Y\gamma + Z\gamma^{16} \qquad (Y, Z \in \mathbb{F}_{2^4}). \qquad (20b)$$

伊東–辻井アルゴリズム（Itoh–Tsujii inversion Algorithm: ITA）[7] より，逆元 $X = C^{-1} = (CC^{16})^{-1}C^{16}$ は次式のように求まる（図 3(b)）．ただし，Q^{-1} は事前計算される．

$$X = \{D^2+DEQ+E^2R\}^{-1} \times \{DQ^{-1}\gamma+(DQ^{-1}+E)\gamma^{16}\}. \quad (21)$$

また，$\mathbb{F}_{(2^4)^2}$ 上の非零元 C, $X = C^{-1}$ を次式のようにそれぞれ正規基底 $\{\gamma, \gamma^{16}\}$，多項式基底 $\{1, \gamma\}$ で表すとき，

$$C = D\gamma + E\gamma^{16} \qquad (D, E \in \mathbb{F}_{2^4}), \qquad (22a)$$

$$X = Y + Z\gamma^{16} \qquad (X, Y \in \mathbb{F}_{2^4}). \qquad (22b)$$

ITA より，逆元 $X = C^{-1} = (CC^{16})^{-1}C^{16}$ は次式のように求まる（図 4(b)）．

$$X = \{DEQ+(D+E)^2R\}^{-1} \times \{DQ+(D+E)\gamma\}. \quad (23)$$

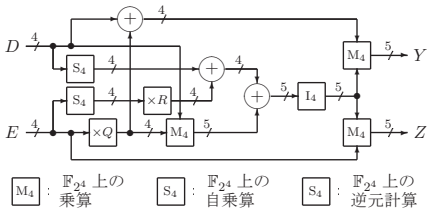
図 3(a), 4(a) に示す回路と図 3(b), 4(b) に示す回路におけるクリティカルパスの遅延時間は変わらない．ただし，図 3(b) の回路では，新たに $\mathbb{F}_{2^4}$ 上の Q^{-1} 倍算回路を必要としており，使用する論理ゲート数が増加する．

一方で，第 3 節で述べたように，図 3, 4 に示す回路の入力 $D, E \in \mathbb{F}_{2^4}$ は式 (11)，(12) に示す基底であれば，どれで表現しても構わない．また，同回路の出力 $Y, Z \in \mathbb{F}_{2^4}$ は RRB で表現される．第 3.1 節では，この RRB を式 (11) に示す正規基底に変換して $\bar{\mathbf{B}}\mathbf{A}$（$\bar{\mathbf{B}}$）を考えたが，正規基底ではなく式 (12) に示す多項式基底に変換しても構わない．よって，入力 D, E と出力 Y, Z を表現するために別の基底を採用できることになる．このとき，$8\times4\times5\times5 = 800$ 種類の $\mathbf{B}$ と $\bar{\mathbf{B}}\mathbf{A}$，および $\bar{\mathbf{A}}\mathbf{B}$ と $\bar{\mathbf{B}}$ の組それぞれを準備できる．しかし，効率の良い行列の組は $1.27\%_{00}$ しか存在しないため，これでは不十分である．そこで，さらに D と E の表現に別の基底を用い，Y と Z を表現する RRB もそれぞれ別の基底に変換することを考える．このように，入出力に対してだけではなく，2 つの入力，2 つの出力に対しても別々の基底を採用することで，行列の組をより増やすことができる．この別々の基底を複雑混合基底（More Miscellaneously Mixed Bases: MMMB）と呼ぶ．$8\times4\times5\times5\times5\times5 = 20,000$ 種類の $\mathbf{B}$ と $\bar{\mathbf{B}}\mathbf{A}$，および $\bar{\mathbf{A}}\mathbf{B}$ と $\bar{\mathbf{B}}$ の組それぞれを準備できる．

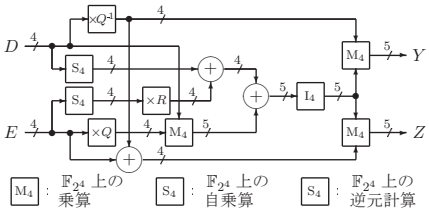
RRB と MMMB を利用すれば，SubBytes および InvSubBytes 内部の計算を図 1 に示す処理時間で行える．ただし，T_{AND} は AND ゲートにおけるクリティカルパスの遅延時間を意味する．

5 結論

本稿では，$\mathbb{F}_{(2^4)^2}$ 上の MMMB を提案し，$\mathbb{F}_{2^4}$ 上の RRB を採用した場合でも，MMB を用いれば $\times\mathbf{B}$，$\times\bar{\mathbf{B}}\mathbf{A}$，$\times\bar{\mathbf{B}}$ を $2T_{\mathrm{XOR}}$ で提供できることを示した．しかし，$\times\bar{\mathbf{A}}\mathbf{B}$ に関しては $3T_{\mathrm{XOR}}$ を必要とするため，これを $2T_{\mathrm{XOR}}$ まで削減するための手法を考えなければならない．

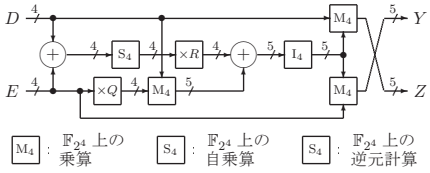


(a) MMMB 非採用時

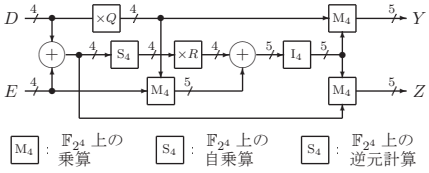


(b) MMMB 採用時（式 (21)）

図 3: 多項式底を採用した $\mathbb{F}_{(2^4)^2}$ 上の逆元計算回路



(a) MMMB 非採用時



(b) MMMB 採用時（式 (23)）

図 4: 正規基底を採用した $\mathbb{F}_{(2^4)^2}$ 上の逆元計算回路

表 1: クリティカルパスの遅延時間まとめ

実装		遅延時間
Morioka et al. [2]	$\times\mathbf{B}$	$3T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}\mathbf{A}$	$3T_{\mathrm{XOR}}$
	逆元計算 †	$4T_{\mathrm{AND}}+17T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}$	$\mathbf{2}T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{A}}\mathbf{B}$	$3T_{\mathrm{XOR}}$
Canright et al. [3]	$\times\mathbf{B}$	$3T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}\mathbf{A}$	$3T_{\mathrm{XOR}}$
	逆元計算 †	$4T_{\mathrm{AND}}+15T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}$	$3T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{A}}\mathbf{B}$	$3T_{\mathrm{XOR}}$
Nogami et al. [4]	$\times\mathbf{B}$	$\mathbf{2}T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}\mathbf{A}$	$\mathbf{2}T_{\mathrm{XOR}}$
	逆元計算 †	$4T_{\mathrm{AND}}+14T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}$	$\mathbf{3}T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{A}}\mathbf{B}$	$\mathbf{3}T_{\mathrm{XOR}}$
Jeon et al. [5]	$\times\mathbf{B}$	$3T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}\mathbf{A}$	$3T_{\mathrm{XOR}}$
	逆元計算 ‡	$4T_{\mathrm{AND}}+10T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}$	$2T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{A}}\mathbf{B}$	$3T_{\mathrm{XOR}}$
RRB と MMMB を適用	$\times\mathbf{B}$	$\mathbf{2}T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}\mathbf{A}$	$\mathbf{2}T_{\mathrm{XOR}}$
	逆元計算 ‡	$4T_{\mathrm{AND}}+\mathbf{7}T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{B}}$	$3T_{\mathrm{XOR}}$
	$\times\bar{\mathbf{A}}\mathbf{B}$	$\mathbf{2}T_{\mathrm{XOR}}$

† $\mathbb{F}_{((2^2)^2)^2}$ 上　‡ $\mathbb{F}_{(2^4)^2}$ 上

参考文献

[1] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” FIPS publication 197, “http://csrc.nist.gov/encryption/aes/”, 2001.

[2] S. Morioka and A. Satoh, “An Optimized S–box Circuit Architecture for Low Power AES Design,” Workshop on Cryptographic Hardware and Embedded Systems (CHES2002), LNCS 2523, pp. 172–186, Springer–Verlag, 2003.

[3] D. Canright, “A Very Compact S-Box for AES,” Workshop on Cryptographic Hardware and Embedded Systems (CHES2005), LNCS 3659, pp. 441–455, Springer–Verlag, 2005.

[4] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, and Y. Morikawa, “Mixed Bases for Efficient Inversion in $\mathbb{F}_{((2^2)^2)^2}$and Conversion Matrices of SubBytes of AES,” Workshop on Cryptographic Hardware and Embedded Systems (CHES2010), LNCS 6225, pp. 234–247, Springer–Verlag, 2010.

[5] Y. Jeon, Y. Kim, and D. Lee, “A Compact Memory-free Architecture for the AES Algorithm Using Resource Sharing Methods,” Journal of Circuits, Systems, and Computers, Vol. 19, No. 5, pp. 1109–1130, 2010.

[6] 根角健太, 野上保之, 森岡恵理, “$\mathbb{F}_{(2^4)^2}$ 上の複雑混合基底による基底変換を用いた AES の SubBytes 変換,” コンピュータセキュリティシンポジウム 2011 (CSS2011), 2011.

[7] T. Itoh and S. Tsujii, “A Fast Algorithm for Computing Multiplicative Inverse in GF(2^m) Using Normal Basis," Inf. Comput., Vol. 78, pp. 171–177, 1988.