暗号VLSIプロセッサのための固有電力消費アーキテクチャ

松原裕之[†] 渡邊孝博[††] 中村維男[†]

現在の暗号 VLSI プロセッサは電力消費解析を行うことで，演算処理内容や暗号そのものを解読することが可能である．本論文では，暗号や演算処理内容にかかわらずつねに一定の電力消費パターンを発生させることで暗号解析を困難とする，暗号 VLSI プロセッサのための固有電力消費アーキテクチャを提案する．本アーキテクチャは二線式ダイナミック回路網で実現し，どのような入力信号系列が与えられても演算終了時までに一定回数のスイッチングを発生させ，消費電力および電力消費パターンを一定にすることを特徴とする．また，提案する固有電力消費アーキテクチャを用いて，0.6 μm 設計ルールの 64 ビット DES のデータパスを設計した．HSPICE によるシミュレーションの結果，従来の一線式 CMOS での実装と比較して電力消費解析が困難になることが明らかとなり，暗号プロセッサ用のアーキテクチャとして優れていることが分かった．

An Architecture for Secure Encryption VLSI Processors Using a Constant-characteristic Power Dissipation Concept

Hiroyuki Matsubara,[†] Takahiro Watanabe[††] and Tadao Nakamura[†]

As the power dissipation of present encryption VLSI processors fluctuates in operation, their processing contents and/or secret keys can easily be broken by power analysis methods. However, using a characteristic power dissipation concept, we propose an architecture for secure encryption processors whose power dissipation pattern is always constant-characteristic in spite of the behavior of the arithmetic contents. Our approach using dual-rail dynamic logic makes both the total power consumption and the number of switching times of a VLSI processor constant whatever series of input values may be input. We design a data-path of 64 bits DES by using our approach, and measure the current values and power dissipations using the HSPICE simulator in 0.6 μm CMOS technology. Experimental results show that in implementing the architecture based on the very difficult analysis of the power dissipation, our approach is more excellent than using conventional single-rail CMOS technologies. As a result, our concept is suitable for the implementation of encryption VLSI processors.

1. はじめに

コンピュータやインターネットの普及にともない，安全な利用を確保するために暗号技術が重要となっている．一方，システム LSI の設計・製造技術の発展から，暗号処理は VLSI プロセッサやそれを組み込んだ IC カードなどで身近に利用される機会が増している．しかし，現在の暗号 VLSI プロセッサは電力消費解析を行うことで，演算処理内容や暗号そのものを解読することが可能であり，安全上，きわめて大きな問題である[4]．

一方，ここ数年来，VLSI プロセッサをはじめとするシステム LSI 設計技術の研究開発では，集積度向上にともなう消費電力の正確な見積りや電力密度の管理の必要性に注目してきた[2),7)]．低電力かつ高性能という両立困難な仕様のシステム LSI を実現するために，様々な VLSI 設計技法やアーキテクチャが提案されている[1),3),6)]．しかし，システム LSI のアプリケーションによっては単純に電力削減するだけでは解決できないものもあり[13)]，それらに対して従来とは異なる体系的な電力評価に基づく設計技法の確立が望まれている．たとえば，電力消費の総和が低減されても部分的に電力密度が高まる場合や，電力消費の様子が可観測であるために，システム利用に不適切な場合があげられる．本論文で対象とする暗号 VLSI プロセッサはその典型的な例である．

† 東北大学大学院情報科学研究科情報基礎科学専攻
Department of Computer and Mathematical Sciences, Graduate School of Information Sciences, Tohoku University
†† 山口大学工学部知能情報システム工学科
Department of Computer Science and Systems Engineering, Faculty of Engineering, Yamaguchi University

暗号プロセッサを VLSI 化するにあたって，実装が容易であること，暗号が強度であることが重要である．さらに，暗号プロセッサの演算処理内容を解析することで暗号そのものを解読することが可能であるため，外部からの解析が困難なより安全な機構が望まれている．特徴的な暗号解析法として Differential Power Analysis（DPA）手法が知られている[4]．これは組込暗号 VLSI プロセッサが暗号処理を行うときに発生する電力消費量を解析し，そこから暗号を解析し埋め込まれている鍵を発見する手法である．最近の研究では DPA は演算アルゴリズムのみの改良では防ぐことが困難であることが判明している．そこで本論文では固有電力消費アーキテクチャを提唱し，原理的に DPA を困難にする回路技術と固有電力消費モデルについて言及する．また，一例として電力消費の面から安全な演算器を設計し，その評価を行う．

本論文の構成は，まず次章で従来の固定電力手法と提案手法の概要について示す．3 章では提案する固有電力消費アーキテクチャを示すとともに，固有電力消費を実現するための二線式ダイナミック回路網を用いた固有電力消費モデルについて述べる．4 章では 64 ビット DES の一部を実装したデータパスを設計し，入力データ系列による消費電力の測定とその電力消費パターンを定量的に評価する．最後にまとめと今後の研究の展望について述べる．

2. 従来手法と提案手法

本章では提案する固有電力消費の概要を従来手法と比較して説明する．**図 1** はある VLSI プロセッサの演算時に発生する電力消費波形を，1 演算サイクル単位で示したものである．電力消費波形は演算の種類，演算順序，データ，ハードウェア構成などに依存するため，すべてが同一でない限り異なる波形を示す．図 1 の例では，3 通りの異なる条件下では 3 通りの異なる波形をとることを示している．結果的に，電力消費波形より演算内容やハードウェア構成の類推や解析が可能となる．そこで，消費電力や電力消費波形から処理内容の推定を困難にする回路方式や設計手法を包含する設計思想（アーキテクチャ）が必要である．

2.1 従来の調整手法

従来手法は**図 2** で示すように演算の処理内容にかかわらず，つねに最大の電力消費を発生させる．演算データや演算アルゴリズムによらず消費電力を最大値に保持することで実際の演算処理内容を隠蔽する手法である．最大の電力消費発生手法の実現はソフトウェア，ハードウェアのいずれでも可能である．

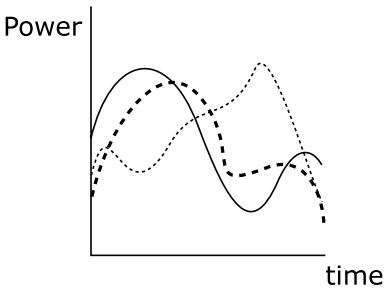

図 1 電力消費波形の例
Fig. 1 Power dissipation curves.

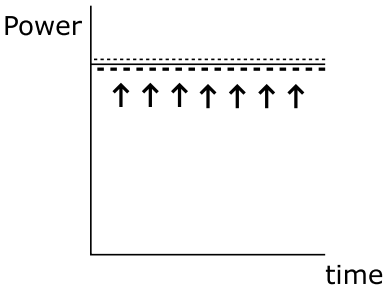

図 2 最大化
Fig. 2 Maximizing power dissipation.

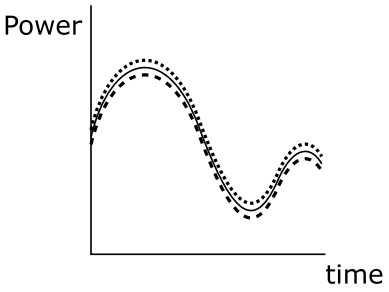

図 3 固有電力化
Fig. 3 Constant-characteristic power dissipation.

- ソフトウェア的な調整
  演算器の稼動状態を実行時にソフトウェア的に監視し，稼動率が低下しているときに無駄な演算を補うことで電力消費を一定にする．
- ハードウェア的な調整
  同一演算機能で消費電力のみ異なる演算器を複数用意し，組合せで電力消費を一定にする．

しかし，これらの手法は設計時の工夫や演算実行中の逐次監視が必要なために，非常に大きな負担となる．また，つねに最大電力に合わせた電力消費を発生させる必要があるため，低電力消費設計が原理的に困難である．

2.2 提案する固有電力消費手法

提案手法は**図 3** で示すように入力するデータ系列にかかわらず，つねに演算器固有の電力消費を実現する．演算手順が同一でありさえすれば，どのような演算処理を行ってもつねに演算器固有の電力消費パターンとなる．この結果，演算データそのものの解析が困難になる．また，従来手法と比べて低電力化が期待でき，ハードウェアの規模や対称性に実装上の制約がないという利点もある．以上により強度な暗号 VLSI プロセッサを実現できる．

3. 固有電力消費アーキテクチャ

前章で述べたように，固有電力消費の特徴を暗号 VLSI プロセッサに適用できる．しかし，CMOS で構成するゲートは入力信号の遷移パターンによって消費電力が大きく変動する．そこで，本章ではまず，入力信号の遷移パターンによらずつねに一定の電力消費を発生させる固有電力消費アーキテクチャの概要を示す．次に，従来の CMOS による電力消費モデルと提案する固有電力消費モデルを比較することで，固有電力消費を実現するための設計方法論を述べる．

3.1 固有電力消費アーキテクチャの概要

提案する固有電力消費アーキテクチャ（設計思想）は暗号プロセッサの設計思想に直接，対応する．そこで，固有電力消費アーキテクチャをコンセプト，回路方式，設計方法論の 3 点から概観する．

- **コンセプト**　電力消費波形を演算器固有化し個々の電力消費パターンの特徴を隠蔽することで電力消費解析を困難にするアイディアである．詳細は 2 章で述べたように，演算の種類・順序や入力データによらず，つねに同一の電力消費波形（パターン）を発生させる．
- **回路方式**　入力データによらず，つねに一定の電力消費パターンを発生させる論理回路（ハードウェア）として，本論文ではダイナミック二線式回路を採用する．3.3 節で述べる．
- **設計方法論**　ハードウェアの実装の容易さおよび設計の自由度を高めるために，電力消費パターンの調整が容易である必要がある．そのために 2 つの設計方針を用いる．(1) 入力データに依存せずつねに電力消費（充放電）を発生させる回路方式を用いて，一連の演算完了までに一定回数の充放電を行い，全体の消費電力を一定にする．(2) 1 回の基準となる充電または放電の電力消費を一定にする．詳細は 3.2，3.3 節で述べる．

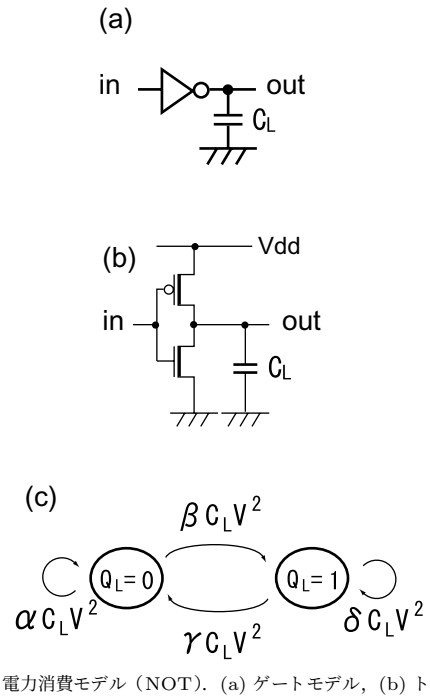

図 4　電力消費モデル（NOT）．(a) ゲートモデル，(b) トランジスタモデル，(c) Q_L の状態遷移モデル
Fig. 4　Power dissipation model (NOT). (a) gate model, (b) transistor model, (c) transition probability of output Q_L model.

3.2 CMOS の電力消費モデル

電力消費のモデルを用いて，入力データのパターンに依存せず，つねに固有電力消費を実現するための指針について述べる．

図 4 は電力消費の 3 つのモデルを，NOT ゲートを用いて示したものである．(a) は出力負荷としてキャパシタンス（C_L）を考慮したゲートレベルのモデルである．入力ノードとして IN，出力ノードとして OUT がある．(b) はトランジスタレベルのモデルである．CMOS では PMOS トランジスタと NMOS トランジスタで構成される．等価の出力負荷としてキャパシタンス（C_L）を考慮する．(c) は出力負荷の電荷（Q_L）の状態を状態遷移で記述したものである．Q_L は “0” または “1” の二値をとるため，状態遷移は次の 4 通りとなる：

(1)　Q_L が “0” に保持している状態の消費電力を $\alpha C_L V^2$ とする．
(2)　Q_L が “0” から “1” へ遷移する状態の消費電力を $\beta C_L V^2$ とする．
(3)　Q_L が “1” から “0” へ遷移する状態の消費電力を $\gamma C_L V^2$ とする．
(4)　Q_L が “1” に保持している状態の消費電力を

表 1 二線式論理の符号例
Table 1 An examples of dual-rail logic code.

Input value $(in, \overline{in})$	Logical value	State
"00"	Valid "-"	Inactive
"01"	False "0"	Active
"10"	True "1"	Active
"11"	Valid "-"	-

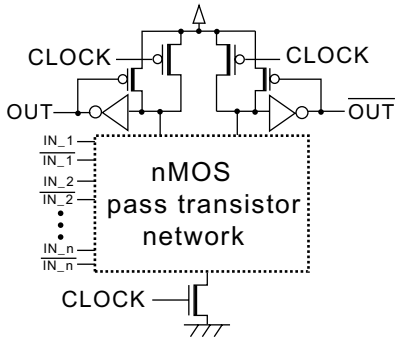

図 5 二線式 n-MOS の基本ゲート構成
Fig. 5 A structure of dual-rail n-MOS dynamic logic circuit.

$\delta C_L V^2$ とする．

CMOS で回路を構成する場合は，Q_L が "0" から "1"，または "1" から "0" へと変化する (2) と (3) の場合のみ動的な電力消費が発生し，(1) と (4) では動的な電力消費は発生しない．つまり，$\beta = \gamma = \frac{1}{2}$，$\alpha = \delta = 0$ と考えることができる．一般に CMOS 回路は出力値が変化する場合のみ電力消費が発生し，変化しない場合は電力消費が発生しないため低電力であるといえる．しかし，入力信号のパターンにより出力信号がつねに変動する場合は，消費電力が変動する．本論文ではすべての状態遷移において，NOT ゲートの例であれば $\alpha = \beta = \gamma = \delta = const.$ となる固有電力消費を実現しようとするものである．この手法を次節に説明する．

3.3 固有電力消費モデル

本節では，まず固有電力消費アーキテクチャに採用する二線式論理を説明し，次に固有電力消費モデルについて述べる．

固定電力アーキテクチャは二線式 n-MOS を用いる．二線式論理は 2 本の線を用いて論理を伝達する方式である[5),8),10)]．**表 1** に符号の割当ての例を示す．符号として "00" は演算を行ってない状態である．符号 "01" に論理値 "0" を，符号 "10" に論理値 "1" を割り当てる．符号 "11" は無効とする．

二線式 n-MOS の基本ゲート構成を**図 5** に示す[10)]．

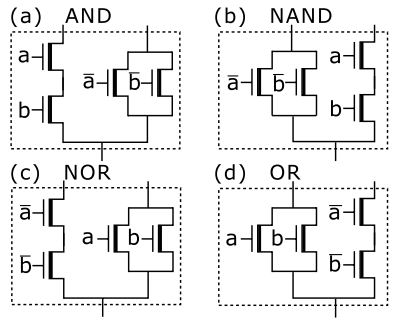

図 6 各ゲートの構成要素．(a) AND，(b) NAND，(c) NOR，(d) OR
Fig. 6 Circuit structures of (a) AND, (b) NAND, (c) NOR, (d) OR gates.

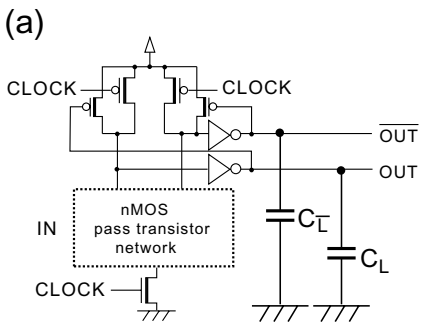

図 7 二線式 n-MOS ゲートの電力消費モデル．(a) トランジスタモデル，(b) 出力ノードの状態遷移
Fig. 7 Power dissipation model (dual-rail n-MOS). (a) transistor model, (b) transition probability of output Q_L, $Q_{\overline{L}}$.

演算部は nMOS パストランジスタを用いて論理を構成する[5),8),10),11)]．**図 6** に nMOS パストランジスタを用いたゲート（AND，NAND，NOR，OR）の例を示す．パストランジスタは CMOS と比較して配線容量が少ない性質があるため，ゲート遅延時間は短く消費電力は低い[8)~10)]．

図 7 は二線式 n-MOS で構成したゲートのモデルである．(a) は負荷容量 C_L，$C_{\overline{L}}$ を考慮したトランジ

表 2 出力ノードの状態遷移と消費電力（NAND ゲート）
Table 2 Transition and power dissipation of output nodes (NAND gate).

Logical Value (Logical value)	Single rail CMOS (Static)		Dual-rail n-MOS (Dynamic)	
	(Q_L)	Consumption Power	($Q_L, Q_{\overline{L}}$)	Consumption Power
Fales to Fales	"0" to "0"	0	"01" to "00" to "01"	$C_{LD}V^2$
Fales to True	"0" to "1"	$\frac{1}{2}C_{LC}V^2$	"01" to "00" to "10"	$C_{LD}V^2$
True to Fales	"1" to "0"	$\frac{1}{2}C_{LC}V^2$	"10" to "00" to "01"	$C_{LD}V^2$
True to True	"1" to "1"	0	"10" to "00" to "10"	$C_{LD}V^2$

スタモデル，(b) は C_L に蓄えられる電荷を Q_L，同様に $C_{\overline{L}}$ の電荷を $Q_{\overline{L}}$ とする場合の状態遷移を示した図である．図 7 (b) の e_1 および e_3 の矢印はエバリュエーションを表し，e_2 および e_4 はプリチャージを表す．ここで，固定電力を実現するために e_1，e_2，e_3 および e_4 の電力消費をすべて同一にする必要がある．つまり，キャパシンタンス C_L と $C_{\overline{L}}$ の大きさが等しければよい．

表 2 は CMOS と二線式 n-MOS の消費電力と出力の論理値（符号）の遷移をまとめたものである．両方式では負荷容量が異なると仮定しているので，CMOS の負荷容量を C_{LC} [F]，二線式 n-MOS の 1 線あたりの負荷容量を C_{LD} [F] とする．これらの変数を用いて消費電力を記述する．CMOS では出力の論理値とキャパシタンスの電荷の値が 1 対 1 に対応する．二線式ダイナミック論理は前回の評価値を，プリチャージを経由して再評価する必要があるため，符号が "xx" → "00" → "xx" と変化する．符号が 1 つ変化するたびにキャパシタンスの電荷が充電または放電されるため，消費電力は $\frac{1}{2}C_{LD}V^2$ [J] となる．2 回の符号変化で 1 回の状態遷移完了となるため，すべての状態遷移は一定の $C_{LD}V^2$ [J] の消費電力となる．

4. 実　　験

本章では固有電力消費アーキテクチャを 64 ビットの DES のデータパスに実装し，入力信号の変化にともなう電力消費パターンを測定した結果を示し，考察を述べる．

4.1 電力消費の評価指標

電力消費パターンの評価指標として，消費電力と電流波形の振幅誤差の 2 つを用いる．

4.1.1 消 費 電 力

従来の CMOS 実装では，入力信号のパターンによっては演算器の中間ノードまたは出力ノードのスイッチングが発生しないことがあるため，消費電力が大きく変動する．提案する方式は逆につねに一定電力が発生する．そこで，測定した消費電力を最小値，最大値，平均値，分散の統計処理を行うことで定量的に評価することにした．分散が小さいほど消費電力のばらつきが小さく，つねにある範囲内の一定の消費電力を示しているといえる．

4.1.2 電流波形の振幅誤差

電流波形の振幅誤差は演算器の電流を観測し，統計処理を行って算出する．具体的には 1 演算サイクルの電流波形を同一グラフ上にプロットし，その誤差を求めることにした[12]．HSPICE シミュレーションで過渡解析の時間刻みを 0.05 nS に設定した場合，たとえば時間間隔 5 nS の解析では 100 点の測定が得られる．そこで，i 回目のシミュレーションの任意時刻 t の時点での電流値を $\mathrm{Ii}(t)$ とするとき，N 個の $\mathrm{Ii}(t)$ に対して各々統計処理を行い，このときの電流波形の振幅誤差 $Err\_(t)$ を以下のように定義する．

$Err\_(t) = (\mathrm{Max}(\mathrm{I}(t))$ - $\mathrm{Min}(\mathrm{I}(t)))$

ただし

$\mathrm{Max}(\mathrm{I}(t)) = \mathrm{Max}((\mathrm{Ii}(t))$ for all i's

$\mathrm{Min}(\mathrm{I}(t)) = \mathrm{Min}(\mathrm{Ii}(t))$ for all i's

$i = 1, 2, \ldots, N$

4.2 実 験 方 法

演算器（DES のデータパス）を設計し，入力信号の変化にともなう消費電力を測定する．**図 8** は DES 演算の基本単位であり，**図 9** は DES の非線形変換 $f(R_{n-1}, K_n)$ を示す[14]．DES 演算は非線形演算を繰り返す処理が主であり，演算の大多数は EXOR 演算が占める．そのため本実験では図 9 に示す非線形演算を行う EXOR 演算を主とするアルゴリズムをデータパスとして実装し，その電力消費の測定を行う．入力信号は乱数を用いて 100 パターン生成し，測定データは統計的に処理を行う．実験では 0.6 μm CMOS 設計ルールのデータを用いて，電流波形と消費電力を Star HSPICE で測定する．入力ベクトル生成と測定データの統計処理はオブジェクト指向スクリプト言語である Ruby ver. 1.4.6（Sun Ultra2，CPU: 200 MHz × 2，Memory: 512 Mbyte，OS: Solaris 7）を用いる．

4.3 実験結果と考察

表 3 に 64 ビットの DES の消費電力とその分散を示す．提案手法の消費電力の平均値は従来手法と比較

表 3 消費電力の測定結果（電源電圧：3.3 V，動作周波数：200 MHz）
Table 3 Experimental results on consumption power (3.3 V, 200 MHz).

Function		Power (mW)			Variance
		Min.	Average	Max.	(S^2)
64-bit DES	Conventional	20.39	24.10	26.15	2.956
	Proposed	29.74	29.83	30.00	0.008

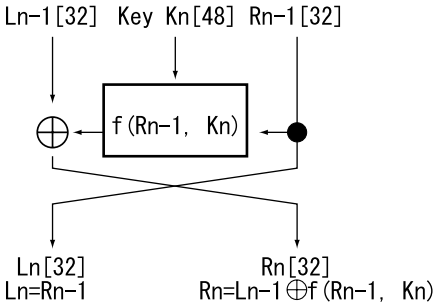

図 8 DES 暗号化の基本演算
Fig. 8 Basic unit of DES algorithm.

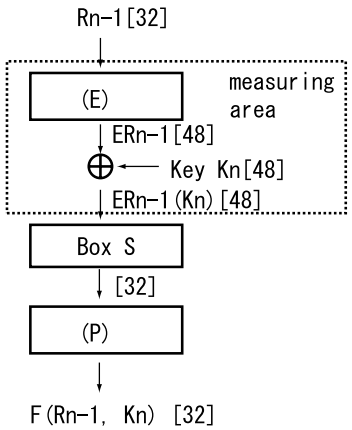

図 9 DES の非線形変換 f(R_{n-1}, K_n)
Fig. 9 Non-linear f(R_{n-1}, K_n) of the DES.

して 24%増加している．消費電力が単純に 2 倍とならないのは DES が EXOR ゲートを主とした実装であること，二線式ダイナミック回路は負荷容量が小さい N-MOS の構成が主であること，従来手法（CMOS）の稼動率は入力データによって大きく変化することがあげられる．**図 10**，**図 11** は消費電流 I(t) の重ね合わせ波形の最大振幅 Max(I(t)) と最小振幅 Min(I(t)) を示す．**図 12** は振幅誤差 $Err\_(t)$ を示す．図 12 より従来手法と提案手法は振幅誤差の違いが明らかであり，電力消費パターンに差があることが読み取れる．以上より，提案した手法は実験データより消費電力の分散が小さく振幅誤差が小さいといえるため，従来の一線式 CMOS での実装と比較して電力消費の変動が小さく固有の電力消費であるといえる．つまり電力消費パ

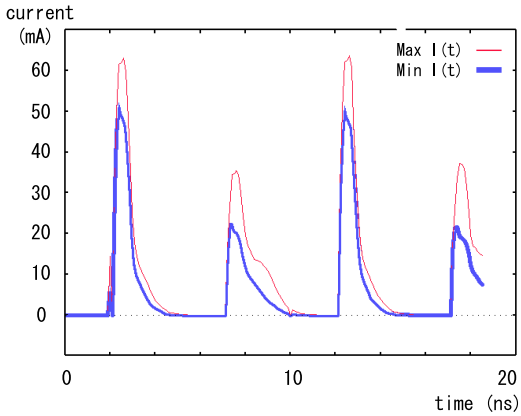

図 10 電流波形（従来）
Fig. 10 Current curves (conventional).

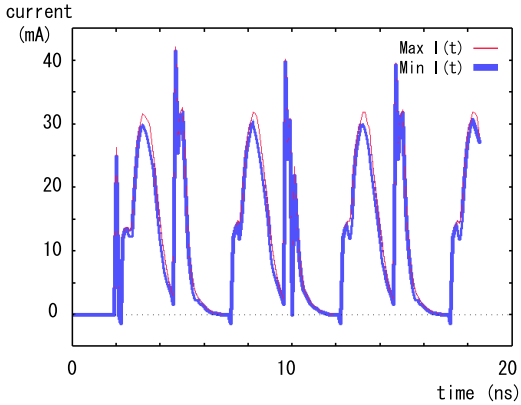

図 11 電流波形（提案）
Fig. 11 Current curves (Proposed).

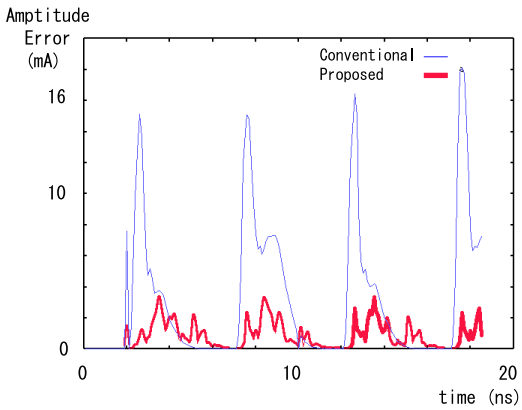

図 12 電流波形の振幅誤差
Fig. 12 Amptitude error of the current curves.

ターンが相対的に固有化されているため，電力消費解析が困難となる．以上より，本提案手法は暗号 VLSI プロセッサの実装に適していることが確認できた．

5. おわりに

本論文では，演算処理内容にかかわらずつねに一定の電力消費パターンを示す固有電力消費アーキテクチャを提案し，二線式ダイナミック回路網を用いて符号変化にともなう電力消費の詳細を検討した．本提案の固有電力消費アーキテクチャを採用して，64 ビット DES データパスを 0.6 μm 設計ルールで設計した．提案する構成と従来の一線式 CMOS で実装した場合とを比較し，提案手法の方が電力消費の解析が困難になることを定量的に評価した．結論として，我々の提案する固有電力消費アーキテクチャが電力消費からの暗号解読を困難にするという点で，安全な暗号 VLSI プロセッサ向きであることが示された．

今後はより大規模回路への適用と，振幅誤差を小さくするためにより精度の高いモデルの確立が必要である．

参考文献

1) Kuroda, T.: Overview of Low-Power ULSI Circuit Techniques, *IEICE Trans. Electoron.*, Vol.E78-C, No.4, pp.344–343 (1995).
2) 桜井貴康：2010 年の LSI と低消費電力技術，信学技報，ICD 99-56, pp.65–72 (1999).
3) Yasuura, H. and Ishihara, T.: System LSI Design Methods for Low Power LSIs, *IEICE Trans. Electron.*, Vol.E83-C, No.2, pp.143–152 (2000).
4) Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, *Proc. CRYPTO '99*, pp.388–397 (1999). http://www.cryptography.com/dpa/Dpa.pdf
5) 松原裕之，渡邊孝博，中村維男：低電力のための細粒度電力制御 Cooled Logic アーキテクチャ，第 13 回回路とシステム（軽井沢）ワークショップ，No.C4-2, pp.545–548 (2000).
6) Ishihara, T. and Yasuura, H.: Programmable Power Management Architecture for Power Reduction, *IEICE Trans. Electron.*, Vol.E81-C, No.9, pp.1473–1480 (1998).
7) Ishihara, T. and Yasuura, H.: Experimental Analysis of Power Estimation Models of CMOS VLSI Circuits, *IEICE Trans. Fundamentals*, Vol.E80-A, No.3, pp.480–486 (1997).
8) Zimmermann, R. and Fichtner, W.: Low-Power Logic Styles: CMOS Versus Pass-Transistor Logic, *IEEE Journal of Solid-State Circuits*, Vol.32, No.7, pp.1079–1090 (1997).
9) Song, B., Furui, M., Yoshida, Y., Onoye, T. and Shirakawa, I.: Low-Power Scheme of NMOS 4-Phase Dynamic Logic, *IEICE Trans. Electron.*, Vol.E82-C, No.9, pp.1772–1776 (1999).
10) Weste, N.H.E. and Eshraghian, K.: *Principles of CMOS VLSI Design*: *A System Perspective*, 2nd Ed., Addison-Wesley (1993).
11) Harris, D. and Horowitz, M.A.: Skew-Tolerant Domino Circuits, *IEEE International Solid-State Circuits Conference*, SP 25.7, pp.422–423 (1997).
12) 中野 健，永田達也：ステップ応答波形重ね合わせによる 1 Gbit/s 高速信号伝送系のジッタ評価法，1999 信学総大，分冊 5, No.C-12-28, p.126 (1999).
13) 田中 聡，石藤智昭：RF-ID タグに向けた CMOS アナログ回路の応用，第 13 回回路とシステム（軽井沢）ワークショップ論文集，No.Ba2, pp.217–222 (2000).
14) 三谷政昭：共通鍵暗号-DES 暗号の構成とその応用，*Interface*, No.6, pp.166–170 (2000).

(平成 12 年 9 月 22 日受付)
(平成 13 年 2 月 1 日採録)

松原 裕之

昭和 49 年生．平成 8 年山口大学工学部知能情報システム工学科卒業．平成 10 年東北大学大学院情報科学研究科博士課程前期修了．現在，同大学大学院情報科学研究科博士課程後期に在学中．低電力 VLSI の研究に従事．電子情報通信学会，IEEE-CS 各会員．

渡邊 孝博（正会員）

昭和 25 年生．昭和 49 年山口大学工学部電気工学科卒業．昭和 51 年同大学院修士課程修了．昭和 54 年東北大学大学院博士課程単位取得退学．同年（株）東芝入社，LSI-CAD の研究開発に従事．平成 2 年山口大学工学部知能情報システム工学科助教授．現在に至る．工学博士．電子情報通信学会会員．

中村　維男（正会員）

昭和 19 年生．昭和 47 年東北大学大学院工学研究科博士後期課程修了．工学博士．昭和 47 年同大学工学部助手．昭和 53 年同大学助教授．昭和 63 年同大学大学院情報科学研究科教授．現在に至る．平成 6 年よりスタンフォード大学客員教授併任．研究分野は，計算機アーキテクチャ．COOL Chips 組織委員長．電子情報通信学会，日本機械学会，IEEE 各会員．