AESにおける低消費電力アーキテクチャについて

池, 兼次郎
九州松下電器株式会社

萩原, 大輔
九州大学大学院システム情報科学府

櫻井, 幸一
九州大学システムLSI研究センター

安浦, 寛人
九州大学システムLSI研究センター

出版情報：コンピュータセキュリティシンポジウム2002論文集, pp.407-412, 2002-09. コンピュータセキュリティ研究会
バージョン：
権利関係：

AESにおける低消費電力アーキテクチャについて

池 兼次郎[1]　萩原 大輔[2]　櫻井 幸一[3]　安浦 寛人[3]

[1] 九州松下電器株式会社

[2] 九州大学 大学院システム情報科学府

[3] 九州大学 システムLSI研究センター

あらまし: 本稿ではAESにおけるアーキテクチャ・レベルでの低消費電力手法を検討する。まず、処理性能が等しい4つの基本的なアーキテクチャの消費電力を測定した結果、ラウンド関数における部分回路入力の信号確定時間のばらつきやグリッジ伝播により、本来の処理に寄与しない無駄な電力消費があることが分かった。このような電力消費を削減するため、ラウンド関数内にレジスタやANDゲートを挿入したところ、32bitバス幅のアーキテクチャにおいて、約2%のゲート数増大で、約24%の消費電力削減効果があることが分かった。本稿で述べる手法は回路レベル等の低消費電力手法と併用することにより、さらなる消費電力削減効果が得られる。

Hardware Architectures of AES for low power design

Kenjiro IKE[1]　Daisuke HAGIWARA[2]　Kouichi SAKURAI[3]　Hiroto YASUURA[3]

[1] Kyushu Matsushita Electric Co.,Ltd.

[1] Graduate School of Information Science and Electrical Engineering, Kyushu University

[3] System LSI Research Center, Kyushu University

Abstract: This paper deals with low power design of AES at arhitecture level. At first, we show the power dissipation about basic architectures of AES. On the basis of that results, we describe low power design methods about the round function.

1　はじめに

近年の回路設計において、低消費電力化は重要な課題の一つとなっている。その理由の一つとして、発熱に起因する、冷却コストやパッケージ・コストの増大、および回路の信頼性低下があげられる。また、バッテリ駆動の携帯機器では、機器の長時間利用あるいはバッテリの軽量化のために、回路の低消費電力化は必要不可欠である。次世代標準ブロック暗号であるAES[1]は、ICカードからネットワーク・バックボーンまで、幅広い用途に対する回路実装が予想されるが、どのような用途に実装される場合でも、要求性能を満足し、かつ消費電力を削減する方法を検討する必要があろう。

回路実装における低消費電力化手法は、アーキテクチャ(回路構成)レベルからデバイス・レベルまで、設計過程毎に様々な手法がこれまで提案されている[2]。AESにおける低消費電力化手法は、これまでトランジスタ・レベル[3]、回路レベル[4][5]について提案されている。いずれの手法もS–boxに着目し、S–boxの低消費電力化を図っている。しかし、S–box以外の回路を含めたAES回路全体のアーキテクチャ・レベルでの低消費電力化については、まだ検討されていない。

本稿ではAES回路のアーキテクチャ・レベルにおける低消費電力化手法について検討する。まず2章でCMOS回路における電力消費、エネルギー(電力量)消費の要因を述べる。3章でAESを基本的な4つのアーキテクチャで実装した場合の実装結果と消費電力を示し、消費電力削減のための方針を述べる。4章で実設計での使用頻度が高いと考えられるloop architectureにおけるラウンド関数の低消費電力化のための手法を検討する。5章でまとめと今後の方針を述べる。

本稿で述べる手法は回路レベル等の低消費電力化手法と併用することが可能であり、その場合さらなる消費電力削減が期待できる。

2　CMOS回路の電力消費

現在LSIで一般に使用されているCMOS回路における電力消費は、大きく3種類に分類できる。一つ目は回路中のダイオードやトランジスタのリーク電流に起因する静的(定常的)な電力消費、2つ目は

ゲートがスイッチングする際に発生する貫通電流に起因する電力消費、3 つ目はゲートがスイッチングする際に発生する負荷容量への充放電電流に起因する動的な電力消費である [6]。このうち、使用するプロセスが $0.1\mu m$ 以上である場合は動的な電力消費が支配的である [7]。動的な消費電力 P は以下のようにモデル化される。

$$P = f \cdot \sum_{k}^{M} \alpha_k C_k V_{DD}^2 \qquad (1)$$

式 (1) において、f は回路の動作周波数、M は回路中のゲート数、α_k はゲート g_k の 1 クロックサイクルのスイッチング回数、C_k はゲート g_k の負荷容量、V_{DD} は電源電圧をそれぞれ表している。

実際に発熱、バッテリ時間を決定するのは、電力の時間積分で表されるエネルギー (電力量) である。あるタスクの処理で消費されるエネルギー E は式 (1) の P を使用して、以下の式で与えられる。

$$E = T_{task} \cdot P = T_{task} \cdot f \cdot \sum_{k}^{M} \alpha_k C_k V_{DD}^2 \qquad (2)$$

式 (2) において、T_{task} はタスクの処理に要する時間を表している。

エネルギー E の削減のためには電源電圧 V_{DD} の削減が効果的であるが、V_{DD} を可変とする場合、DC–DC コンバータなどを実装しなければならないため、製造コストが上昇する。また、V_{DD} 削減により処理時間 T_{task} が増大するトレードオフがある [8]。本稿では、V_{DD} を固定の場合の消費エネルギー削減手法を検討する。ただし、本稿で述べる手法が V_{DD} 可変の場合にも適用可能であることは言うまでもない。

3 基本アーキテクチャの電力消費

アーキテクチャによる消費エネルギーの違いを調べるため、まず基本的なアーキテクチャの消費エネルギーを測定した。対象としたアーキテクチャは以下の通りである。

- loop architecture(32bit バス幅)(以下、LA32) — 図 1(a) 参照。shiftrows はレジスタ内で行っている。
- loop architecture(128bit バス幅) (以下、LA128) — 図 1(b) 参照。
- loop unrolling(以下、LU) — 図 1(c) 参照。
- loop unrolling with registers(以下、LUR) — 図 1(d) 参照。ラウンド毎のパイプライン処理が可能なアーキテクチャであるが、すべての暗号モードで動作することを前提として他のアーキテクチャとの比較を行うため、本稿では 1 ブロックの暗号化が終了するまで次のブロックの入力は行わない。

なお、loop architecture の鍵スケジュール部は on–the–fly 方式で実装している。

アーキテクチャの消費エネルギー比較にあたり、128bit 鍵長暗号化回路を各アーキテクチャで実装した。消費エネルギーの相対的な違いを調べるため、すべての回路は 100Mbps の処理性能 (スループット) で動作する。各アーキテクチャの動作周波数と 1 ブロック処理に要するサイクル数を表 1 に示す。

処理性能が等しい場合、1 ブロックを暗号化する処理時間 (式 (2) 中の T_{task}) が等しくなるため、平均消費電力を測定することにより消費エネルギーの相対的な違いが分かる。以下では、平均消費電力を比較の対象とする。本稿では V_{DD} 固定であるので、消費電力は $f \cdot \sum_{k}^{M} \alpha_k C_k$ に比例する。

表 1: 動作周波数・サイクル数 (@100Mbps)

アーキテクチャ	LA32	LA128	LU	LUR
動作周波数 (MHz)	34.5	8.6	0.78	8.6
サイクル数	44	11	1	11

論理合成は $0.35\mu m$CMOS スタンダード・セル・ライブラリを使用し、Synopsys 社の Design Compiler を用いて行った。S–box、mixcolumns などの部分回路は、事前に回路毎に面積最小の最適化による論理合成を行っており、回路全体の論理合成を行う際には、すべてのアーキテクチャで論理合成後の部分回路を共通に使用している。S-box はテーブル・ルックアップ方式で実装している。

消費電力は、論理合成後の HDL ネットリストと、SPICE ネットリストで記述された各セル・ライブラリの等価回路を使用して、Synopsys 社の回路シミュレータ nanosim を用いてトランジスタ・レベルで測定した。これにより、ゲート・レベルでの測定より精度の高い値を得ることができる。

各アーキテクチャのゲート数を表 2、消費電力を表 3 にそれぞれ示す。

以下では LA128 を基準として、それ以外のアーキテクチャとの消費電力の違いを検討する。

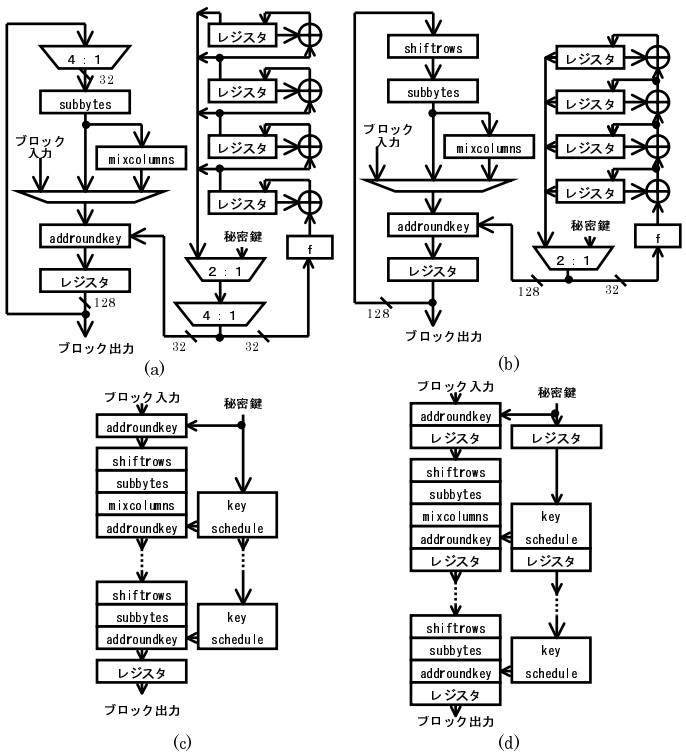

図 1: 基本アーキテクチャ

表 2: 基本アーキテクチャ実装結果 (ゲート数は 2 入力 NAND 換算)

部分回路	LA32 ゲート数	LA32 割合 (%)	LA128 ゲート数	LA128 割合 (%)	LU ゲート数	LU 割合 (%)	LUR ゲート数	LUR 割合 (%)
ラウンド関数	5,925	50.0	17,056	76.4	163,311	80.2	165,665	77.6
subbytes	3,670	31.0	14,194	63.5	147,889	72.6	141,701	66.4
レジスタ	832	7.0	832	3.7	832	0.4	9,152	4.3
その他	1,424	12.0	2,030	9.1	14,591	7.2	14,812	6.9
鍵スケジュール部	5,782	48.8	5,208	23.3	40,267	19.8	47,720	22.4
subword	3,506	29.6	3,512	15.7	35,996	17.7	35,408	16.6
レジスタ	832	7.0	832	3.7	—	—	8,320	3.9
その他	1,434	12.1	864	3.9	4,271	2.1	3,992	1.9
制御部等	143	1.2	72	0.3	—	—	72	0.0
合計	11,850	—	22,335	—	203,578	—	213,456	—

表 3: 基本アーキテクチャ消費電力計測結果

部分回路	LA32 消費電力 (mW)	LA32 割合 (%)	LA128 消費電力 (mW)	LA128 割合 (%)	LU 消費電力 (mW)	LU 割合 (%)	LUR 消費電力 (mW)	LUR 割合 (%)
ラウンド関数	73.9	80.4	35.5	75.5	306.7	98.3	42.1	76.7
subbytes	41.2	44.8	21.9	46.5	253.0	81.1	19.6	35.7
レジスタ	6.3	6.8	2.5	5.3	0.2	0.1	14.6	26.7
その他	26.5	28.8	11.1	23.7	53.7	17.2	7.9	14.3
鍵スケジュール部	17.1	18.6	11.4	24.2	5.2	1.7	12.6	23.1
subword	5.0	5.4	5.1	10.8	3.4	1.1	0.2	0.4
レジスタ	5.8	6.3	2.0	4.3	—	—	12.3	22.4
その他	6.3	6.9	4.3	9.1	1.8	0.6	0.1	0.3
制御部等	0.9	1.0	0.1	0.3	—	—	0.1	0.2
合計	91.9	—	47.0	—	312.1	—	54.9	—

LU との比較　LU の消費電力は LA128 の約 6.6 倍であった。これは、LU の回路内で本来の処理に寄与しないスイッチング (グリッジ) が大量に発生しているためである。クロックが立ち上がり、ブロック入力が変化した場合の、ラウンド 1 からラウンド 10 までの各ラウンド関数出力の 0 ビット目の信号変化の経過を図 2 に示す。後段のラウンドほどグリッジが多くなっている。

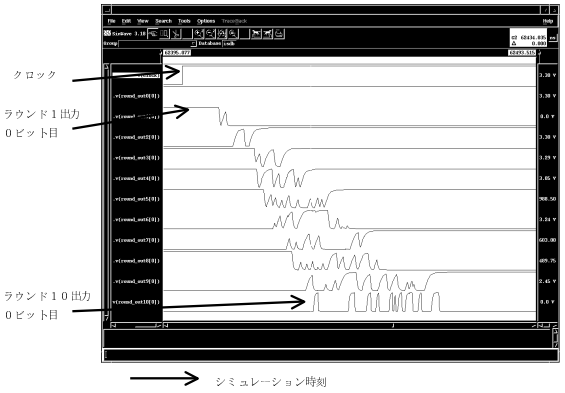

図 2: LU ラウンド出力信号波形

LU は回路入力 (ブロック入力、秘密鍵) から回路出力 (ブロック出力) の直前のレジスタまで、すべて組み合わせ回路で構成されているため、組み合わせ回路のゲート段数が非常に大きい。一般に、組み合わせ回路のゲート段数が大きい場合、後段にあるゲートほど、ゲート入力の信号値が確定するまでの時間にばらつきが生じるため、ゲート出力でグリッジが起こりやすい (図 3(a) 参照)。さらに、途中で発生したグリッジが次のゲートに伝播するため、回路全体でゲートのスイッチング回数 (式 (2) の α_k) が多くなり、消費電力増大につながる。

それに加えて、AES が strict avalanche criterion (SAC, 入力が 1bit 変化したときに、各出力ビットが変化する確率が 1/2) を満足していることが、消費電力増大につながっていると考えられる。AES は 3 ラウンドの実行で SAC を満足している [9]。このことは、あるラウンドの入力間の信号値確定時間にばらつきが生じたり、入力にグリッジが伝播した場合、3 ラウンド後のすべての信号に影響を与え、グリッジ発生の可能性が高いことを意味する。

ラウンド関数も、非線形変換を行う subbytes や拡散性が高い mixcolumns など、入力の変化が出力に大きく影響を与える関数により構成されている。つまり、ラウンド関数内の部分回路においても、入力の信号値確定時間のばらつきやグリッジの伝播が消費電力に与える影響が大きいといえる。

LUR との比較　消費電力は LUR が LA128 の 1.17 倍となっているが、主にレジスタが電力を消費しているためであり、組み合わせ回路の消費電力はむしろ減少している。LUR は AES を実行するために必要な組み合わせ回路のみ実装されており、LA128 におけるセレクタのような資源を共有するための回路が不要である。そのため、(1) セレクタ等の資源共有用回路による電力消費がない、(2) 各部分回路出力の負荷容量 (式 (1) の C_k) が少ない (例えば、LA128 において subbytes 出力は mixcolumns とセレクタに接続しているのに対し、LUR では mixcolumns にのみ接続している)、という 2 点から消費電力が削減される。

また、鍵スケジューリング部の組み合わせ回路の消費電力が非常に小さい。これは一旦拡大鍵が生成されれば秘密鍵が変わらない限り拡大鍵生成が不要であり、ゲートのスイッチングが起こらないためである。

LA32 との比較　LA32 の消費電力は LA128 の約 2 倍である。LA32 はラウンド関数の組み合わせ回路、特に subbytes の消費電力が大きくなっている。LA32 はレジスタと subbytes の間にセレクタが入っており、レジスタ出力からセレクタを伝播する間に生じる信号遅延のばらつきのため、subbytes でグリッジが発生する。さらに、subbytes より後段の回路は、subbytes での遅延のばらつきと subbytes でのグリッジにより、消費電力が大きくなる。

以上の比較から、アーキテクチャ・レベルでの消費電力削減には以下の点が重要と考えられる。

- 部分回路入力の信号値確定時間のばらつきや、回路入力へのグリッジ伝播を抑える。
- 部分回路出力の負荷容量を削減する。
- 鍵スケジュール部で 1 度作成した拡大鍵を保存する。

実際の設計においては動作周波数やゲート数に制約があるため、使用できるアーキテクチャは限られる。次章では、実設計での使用頻度が多いと考えられる LA32 と LA128 について、最小限の設計コスト (ゲート数、クロック等) 増大で、消費電力削減を図るための手法を検討する。

4　低消費電力手法

前章で消費電力削減のための方針を述べた。前章の結果より、電力削減効果が高いのは、ラウンド関数において、部分回路入力の信号値確定時間のばらつきや、回路入力へのグリッジ伝播を抑えることである。

上記課題のための手法としては、部分回路入力の前に AND ゲート、ラッチ、F/F 等を挿入し、信号値が確定するまで制御信号によって信号伝播を抑えることがあげられる (図 3(b))。

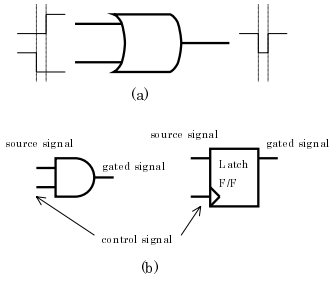

図 3: グリッジならびにグリッジ削減手法

以下では、LA32 と LA128 に対して AND ゲートとレジスタ (F/F) を挿入することによる消費電力削減効果を検討する。

LA32 への適用　前章の結果より、消費電力を削減するためには、subbytes 入力への信号値確定時間のばらつきを抑えるのが効果的である。そこで subbytes の直前にレジスタ (以下、レジスタ 1) を挿入する。ただし、処理性能が変わらないように図 1(a) からデータ・フローを一部変更する。また、AES では最終ラウンドを実行する際、mixcolumns の処理は不要であるが、図 1(a) の構成では、最終ラウンドにおいても mixcolumns でスイッチングが発生する。そこで、subbytes 出力と mixcolumns、セレクタの間に AND ゲートを挿入する (図 4(a) 参照)。

さらに、図 4(a) の構成に subbytes の直後にレジスタ (以下、レジスタ 2) を挿入し、subbytes の遅延ばらつきやグリッジによる無駄な電力消費を抑える構成も試みた (図 4(b))。レジスタ 2 を挿入した場合、処理性能を等しくするためには、(1) 動作周波数を 2 倍にする、(2) パイプライン動作させる (この場合動作周波数は 1.25 倍)、(3) 動作周波数はそのままで、レジスタ 2 にシステム・クロックの反転クロックを入力する (あるいは、レジスタ 2 をクロック立下り動作にする)、という 3 つの選択肢がある (図 4(c) 参照)。

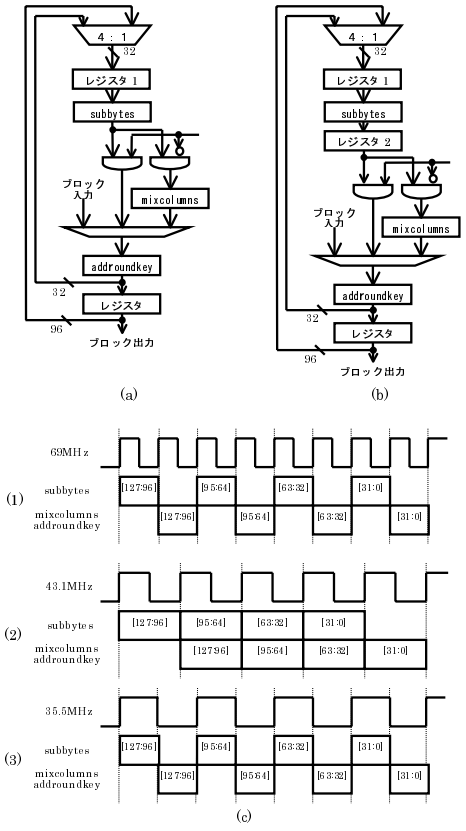

図 4: AND, レジスタ挿入

そこで、図 4(a)(以下 (a) と記す) と図 4(b) の 3 つの実現方法 (図 4(c) の (1),(2),(3)、以下それぞれ (b–1)、(b–2)、(b–3) と記す) について、処理性能 100Mbps となる回路を実装し、消費電力を測定した。(b–3) はレジスタ 2 に反転クロックを入力している。各アーキテクチャのゲート数、消費電力を表 4 に示す。

表 4: 適用結果

	ゲート数	消費電力 (mW)
LA32	11,850	91.9
(a)	12,052	69.0
(b–1)	12,709	80.6
(b–2)	12,226	68.4
(b–3)	12,198	63.9

(a) は LA32 と比較して約 2%のゲート数増大で、約 24%の消費電力削減となった。クロックに関する変更も無いため、消費電力削減効果が高い方法であるといえる。(b–2)、(b–3) は (a) に比べて消費電力

が削減されているものの、削減量は小さい。これは、レジスタ 2 出力以降の回路のゲート数が少なく、電力削減効果が上がらないためだと考えられる。(b–1) はクロックによるレジスタのスイッチング回数が多くなるため、(a) よりかえって増加する。

LA128 への適用　LA128 の場合、レジスタからの出力が直接 subbytes に入力されているため、(a) の構成は取りえない。また、LA128 では 1 クロックサイクルでラウンド関数の処理を行うので、パイプライン構成も取りえない。そのため選択肢としては (b–1) と (b–3) のみである。さらに、LA128 では最終ラウンドも 1 クロックサイクルで処理されるので、subbytes 出力と mixcolumns、セレクタの間に AND ゲートを挿入した場合も、消費電力削減効果がない。

LA128 において、(b–3) の構成 (ただし subbytes 後の AND ゲートは除く) で処理性能 100Mbps となる回路を実装し、消費電力を測定したところ、ゲート数は 23,119 と LA128 の約 4%増加に対し、消費電力は 43.4mW と LA128 の約 8%減少であった。理由は LA32 同様である。

5　おわりに

本稿では、AES のアーキテクチャ・レベルの消費電力削減手法として、ラウンド関数のデータパスに AND、レジスタを挿入することにより、不要なスイッチングを削減する方法を適用した結果を述べた。結果として、subbytes 入力の信号値確定時間のばらつき等を抑えることが最も効果的であることが分かった。

本稿では、アーキテクチャ・レベルにおける消費電力削減手法を検討するため、S–box 等の部分回路内の構成は固定とした。しかし、部分回路、特に S–box の回路構成を可変とし、部分回路内のレジスタ挿入を許す場合、より効果的なレジスタ挿入の解が得られる可能性がある。今後は、消費電力ならびにクロックサイクル、処理性能等の最適化を図るためのレジスタ挿入手法 (すなわち retiming 手法) を検討していきたい。

また、鍵スケジュール部の拡大鍵保存における消費エネルギー削減効果を検討したい。

謝辞

本研究の一部は東京大学大規模集積システム設計教育研究センター (VDEC) の協力で行われた。

参考文献

[1] Federal Information Processing Standards (FIPS) Publication 197. *Advanced Encryption Standard (AES)*. U.S. Department of Commerce/National Institute of Standard and Technology, 2001.

[2] J.M.Rabae and M.Pedram, editors. *Low Power Design Methodologies*. Kluwer Academic Publishers, 1996.

[3] 池, 櫻井, 安浦. Rijndael の LSI 実装における低消費電力化手法の提案. 信学技報 ISEC2001-33, 情処研報 01–CSEC–14–15, 2001.

[4] 森岡, 佐藤. AES の低消費電力回路のための論理設計方式の検討. コンピュータセキュリティシンポジウム 2001, pp. 307–312, 2001.

[5] S.Morioka and A.Satoh. An optimized S-Box circuit architecture for low power AES design. In *Workshop on Cryptographic Hardware and Embedded Systems 2002*, pp. 172–186, 2002.

[6] N.H.E. Weste and K.Eshraghian. *Principles of CMOS VLSI Design*. ADDISON–WESLEY PUBLISHING COMPANY, second edition, 1994.

[7] V.Tiwari, D.Singh, S.Rajgopal, G.Mehta, R.Patel, and F.Baez. Reducing power in high–performance microprocessors. In *35^{th} Design Automation Conference*, 1998.

[8] H.Yasuura and T.Ishihara. System LSI design methods for Low Power LSIs. *IEICE Trans. Electronics*, Vol. E83–C, No. 2, pp. 143–152, 2000.

[9] B.Preneel et al. Comments by the NESSIE Project on the AES Finalists. Public Comments on AES Candidate Algorithms – Round 2, 2000.