ノート

非同期式設計によるFPGA向け低消費電力システムの開発

岡部　忠[*1)]　　入月　康晴[*1)]　　金田　泰昌[*1)]

Development of low power system for fpgas using asynchronous circuit design

Tadashi Okabe[*1)], Yasuharu Irizuki[*1)], Yasuaki Kaneda[*1)]

キーワード：非同期式設計，FPGA，消費電力
Keywords：Asynchronous circuit design, FPGA, Power consumption

1.　はじめに

近年ではシステムの基盤デバイスとしてFPGA（Field Programmable Gate Array）を用いたシステム開発が多くなされている。FPGAは半導体の微細化によりデバイス自体の消費電力は低減されているが，ASIC（Application Specific Integrated Circuit）等の他デバイスと比較すると充分な水準とはいえない。そこで本研究では，デジタル回路の主流な設計法である同期式設計ではなく，非同期式設計によってFPGA応用回路の消費電力低減を試みる。本研究では，システムの消費電流と処理時間を実測し，非同期式設計の有効性を確認したので報告する。

2.　非同期式設計

2．1　デジタル回路設計手法　デジタル回路の設計手法は同期式設計と非同期式設計に区別される。同期式設計はFF（フリップフロップ）やレジスタ等の順序回路のデータ取り込みをクロック信号の遷移を基準として制御する。一方，非同期式設計は個々の順序回路のデータ取り込みをクロックの様な単一の信号の遷移で制御するのではなく，順序回路間でハンドシェイクし，個々の順序回路向けに局所的なクロックの遷移を使って制御する。

デジタル回路を設計する場合には同期式設計を用いるのが通例である。非同期式設計が使われない理由として，同期式設計と比較して設計自体が難しく，設計ツールやFPGA等のプログラマブルデバイスが同期式設計を推奨しているためである。しかしながら，先行研究や一部の製品に対しては非同期式設計が用いられており，同期式設計よりも回路性能が向上するといった報告がなされている[(1)(2)]。

先行研究の多くは対象がASICに限られ，FPGA等のプログラマブルデバイスでの非同期式設計に関する先行研究は少ない[(3)]。本稿では，同期式設計が推奨されるFPGAを対象デバイスとして，FPGA向けの汎用設計ツールと非同期式設計を使い，ブロック暗号のAES（Advanced Encryption Standard）[(4)]を用いた暗号処理システムを構築した。

2．2　4相束データ方式　非同期式設計手法はデジタル回路の黎明期から研究されてきているが，かつては非同期式設計を使うと局所的なクロックラインにグリッチが発生し，正しく動作しないことから敬遠されていた。しかしながら，近年では非同期式設計も様々な手法が提案されている。本稿では回路のタイミング制御が比較的容易な4相束データ方式を採用した。

この手法を用いると，同期式設計の回路アーキテクチャを大幅に変更する事なく設計でき，非同期式設計特有の遅延の見積もりの煩雑さや回路のタイミング収束の問題を比較的容易に解決できる。この方式は同期式設計された回路のクロックラインを非同期式向けハンドシェイク信号に置換するだけであり，容易に設計や実装が可能である。また，束データ方式では制御信号の立ち上りあるいは立ち下りの一方のみを使う4相方式と両遷移のエッジを使う2相方式がある。

本稿では，試作に用いるFPGA内部の順序回路が立ち上がりと立ち下がりの両エッジに対応したものでないという制約と設計の簡便さの観点から，2相方式ではなく4相方式を採用した。本稿で使用した4相束データ方式のパイプラインのブロック図を図1に，プロトコルを図2に示す。束データ方式の設計において図1にあるCが記載されたセルはMullerのC素子と呼ばれるものであり，束データ方式に限らず他の方式の非同期式設計でも使われている[(1)(2)]。本稿で用いた図1のパイプラインは一般的な4相束データ方式のパイプラインとは破線内のハンドシェイク回路部分が異なる[(1)~(3)]。これを用いたのは，ハンドシェイク回路の制御が容易でFPGAの実装に適しているためである[(6)~(8)]。図2にある様に，REQとACKのハンドシェイク信号を組み合わせた4種類の信号遷移（図2の中の円で囲まれた部分）を経てデータバス上のデータが有効である事を順序回路に通知してデータの転送が行われる。

事業名　平成22,23年度　基盤研究
[*1)]情報技術グループ

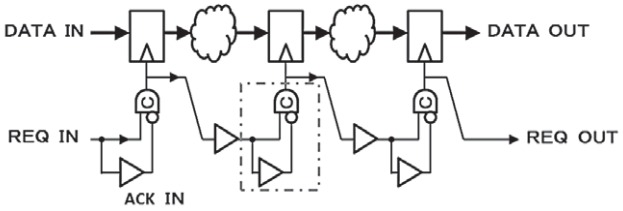

図1.　本稿で用いた4相束データ方式のパイプライン

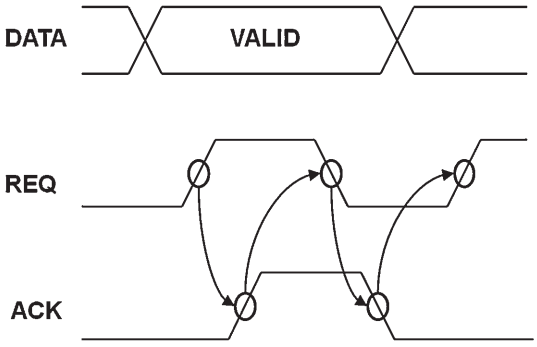

図2.　4相束データ方式のデータ伝送プロトコル

3.　試作と評価

3. 1　試作システム　本節では，試作システムについて述べる。図3のブロック図にあるシステムを試作した。システム全体に占める非同期式回路部分の回路規模が小さいと消費電力評価の点で同期式と非同期式の差異が結果として得にくいため，本研究では暗号化IPとしてブロック暗号のAES[4]を用いた。これを用いる事でシステムの8割以上を非同期式設計回路で占有でき，性能評価結果の判別が容易になる。本研究のAESは，定型の処理（図3にあるRound部分）を繰り返す型のアーキテクチャとして試作している[8]。

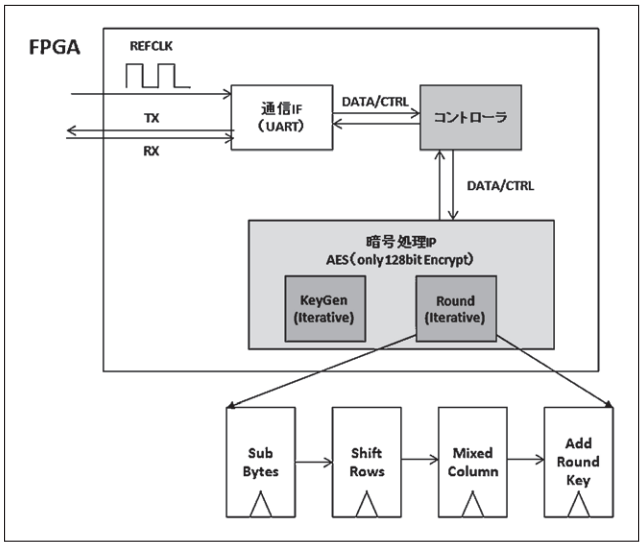

図3.　試作暗号処理システムのブロック図

3. 2　結果と考察　暗号化IPとしてAESを同期式設計と非同期式設計で設計し，周辺機器としてUART（Universal Asynchronous Receiver Transmitter）と暗号処理の制御回路を同期式設計で構築したシステムをFPGAに実装し，表1の結果を得た。表1では，図3のUARTを経由してFPGA外部からテストデータを入力し暗号化処理を行わせた際のFPGAコアの電源ラインを流れる直流電流を，設計手法別に測定している。設計手法は同期式設計と2. 2節で述べた4相束データ方式の非同期式設計を用いた。

表1から，同期式設計は多くの電流を消費している事がわかる。更に，非同期式AESの方が，同期式AESよりも処理時間が短く，消費電流の低減も両立できている。また非同期式設計では遅延回路部分やハンドシェイク回路部に回路リソースを要するため，回路規模の点では同期式設計の方が非同期式設計よりも回路規模を抑えられている。非同期式設計されたAESコアでは各FF間の遅延素子を変える事で処理性能を上昇させる事や性能を維持しながら更に消費電力を低減させる事も柔軟に調整できる。

表1.　評価結果

	消費電流［mA］	処理時間［ns］	回路規模［Slice］
同期式	82.00	945	2,801
非同期式	17.67	480	3,117

4.　まとめ

本稿では，ブロック暗号であるAESを用いた暗号処理システムを例に挙げ，同期式設計向けデバイスであるFPGAを使ってシステムを構築する場合にも，非同期式設計により設計されたデジタル回路の方が消費電力を大きく抑えられる事を紹介した。更に，消費電力だけでなく処理速度の向上も同時に達成できる事を報告した。今後，非同期式設計が広く産業へ応用される事を期待したい。

（平成25年7月12日受付，平成25年8月9日再受付）

文　献

(1) Sparso, J., Furber S. : “Principles of Asynchronous Circuit Design”, Kluwer Academic Publishers (2001)
(2) 齋藤寛：「FPGAを対象とした束データ方式による非同期式回路の設計」，信学技法，Vol.110，pp.157-162 (2011)
(3) 齋藤寛：「非同期式回路の設計技術」，IEICE Trans. Fundamentals, Vol.3，No.3，pp.64-70 (2010)
(4) “Specification for the ADVANCED ENCRYPTION STANDARD”, Federal Information Processing Standards Publication, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (2012)
(5) 岡部忠：「束データ方式による非同期式回路のFPGA実装とその性能評価」，信学技法，Vol.111，No.31，pp.37-42 (2011)
(6) 岡部忠，金田泰昌，入月康晴：「非同期式設計によるブロック暗号回路の性能評価」，電子情報通信学会2012年総合大会講演論文集，D-18-6 (2012)
(7) 岡部忠：「非同期式設計によるFPGA向け省電力化手法」，第14回3都市FPGAカンファレンス2011東京招待講演予稿集 (2012)
(8) 岡部忠：「非同期式設計によるFPGA向け低消費電力化手法」，JPCA showアカデミックプラザ2012講演論文集 (2012)