審 査 の 結 果 の 要 旨

氏　　名　　ベンジャミン　ステファン　デブリン

本論文は「Dual Pipeline Self Synchronous Circuits for High Performance, Energy Minimum, and Error Robust Operation (耐誤動作特性を有する低電力・高性能二重パイプライン型自己同期回路)」と題し、特性バラツキが避けがたい先端集積回路に向いている回路形式の一つである自己同期回路の高性能化および低消費電力化、高信頼動作について研究したもので、英文で記述され六章より構成されている。

第一章は Introduction（序論）であり、研究の背景である先端集積回路におけるバラツキ問題を述べ、従来の大域クロックを用いる同期式回路と遅延無依存の非同期式回路について優劣を論じ、関連研究を参照しつつ非同期式回路の一つである自己同期回路を研究した理由を明らかにしている。

第二章は Gate-level Dual Pipeline Self Synchronous Circuits（ゲートレベル二重パイプライン型自己同期回路）と題し、本研究で用いている二線信号方式と二重パイプライン型自己同期回路について述べている。ビット単位の終了検出回路を用いた細粒度のゲートレベルパイプライン方式が高信頼と高性能を同時に実現できる方式であることを論じ、差動カスコード電圧論理回路（DCVSL）を用いた場合のプリチャージ時間のオーバヘッドを隠蔽できることを述べている。

第三章は Energy Minimum and Robust Operation（最小エネルギおよびロバスト動作）と題し、まず低電圧動作に関し分析し先端技術に特有のパラメータばらつきによる遅延の不確定性とリーク電流の問題に対する解としてゲート粒度でのレベルキーパ回路の最適化と自動パワーゲーティング回路の有効性について述べている。次に先端技術特有のソフトエラー耐性問題への解としてセルフチェック回路と自己同期ウォッチドッグ回路を提案しその有効性を論じている。

第四章は Self Synchronous FPGA（自己同期 FPGA）と題し、本研究で提案する回路方式を FPGA（フィールドプログラマブル・ゲートアレイ）に適用する方法と実験結果について述べている。FPGA を構成するルックアップテーブルや配線用ブロック等の各回路要素について述べ、65nm の CMOS を用いて試作した結果を示し 1.8V から 0.72V の広い電圧範囲で動作することを実証し 1.2V では約 3GHz のスループットが得られたことを述べている。また、低電圧向け設計による自己同期パワーゲーティング回路により約 7 倍の電力効率が得

られること、0.6V 動作では 27fJ の高い演算電力効率が達成できたこと、さらに優れた耐電源雑音特性が得られたことを述べている。

第五章は Self Synchronous RSA Crypto Engine（自己同期 RSA 暗号エンジン）と題し、本研究の自己同期方式を公開暗号法の一つ RSA 暗号エンジンに応用し、ASIC（特定用途向け集積回路）として実現した実験結果について述べている。この SSRSA（自己同期 RSA）は 40nmCMOS 技術を用いて 0.4V から 1.3V の広い電源電圧で動作するものでこれまでの実現例に比べ約 3 倍の速度を有していることを述べている。さらにこの ASIC は各種の電力分析を用いたサイドチャンネル攻撃に対し充分な耐性を有することを示している。また改良の上再試作した ASIC では 0.28V までの低電圧動作が実現できたことを述べている。

第六章は Conclusion（結論）であり本論文の成果をまとめている。

以上要するに、本論文は先端半導体技術に適した回路方式として自己同期回路による新たな細粒度二重パイプライン回路方式を提案し、FPGA および RSA 暗号エンジンに適用することでその低電圧高速動作と耐バラツキ性能、耐ソフトエラー性能さらに耐電力分析攻撃性能を実験的に示したものであり、電子工学の進歩に貢献することが少なくない。

よって本論文は博士（工学）の学位請求論文として合格と認められる。