氏名	アンダレス ザルディ アチヴァー（あんだれす ざるでぃ あちう゛ぁー）
博士の専攻分野の名称	博士（工学）
学位記番号	第 17062 号
学位授与年月日	平成14年3月25日
学位授与の要件	学位規則第4条第1項該当 工学研究科情報システム工学専攻
学位論文名	A Study on Performance Enhancement of Symmetric Key Cryptography and its VLSI Implementation （共通鍵暗号の性能向上手法とVLSI化設計に関する研究）
論文審査委員	（主査） 教授 白川 功 （副査） 教授 村上 孝三　教授 藤岡 弘　教授 西尾章治郎 教授 赤澤 堅造　教授 薦田 憲久　教授 下條 真司

論文内容の要旨

本論文は、共通鍵暗号の性能向上手法とそのVLSI化設計に関する研究の成果をまとめたものであり、以下の6章により構成した。

第1章では、共通鍵暗号の実装手法について述べ、本研究の背景と目的を明らかにするとともに研究内容と成果について概説した。

第2章では、共通鍵暗号の基本特性と暗号解読手法の原理について述べ、暗号モードの必要性を記述した。

第3章では、共通鍵暗号を用いた暗号処理の高速化設計を実現する高性能暗号モードを考案し、その実行アルゴリズムについて記述した。さらに、暗号解読試行に対する耐性の向上を目的としたさまざまな暗号モードの特長を活用することにより、本暗号モードが暗号解読試行に対する耐性を損なうことなく暗号処理速度の向上が実現できることを示した。

第4章では、差分解読法および線形解読法を用いた暗号解読試行に対する耐性の評価および出力値の相関性に関する評価を通じて、本暗号モードの暗号強度解析を行った。本暗号モードにより、従来の暗号モードと比較して十分に高い暗号強度が得られることを示した。

第5章では、本暗号方式をソフトウェアおよびハードウェアで実装し、処理速度と実装効率に関する評価を行った。共通鍵暗号に本暗号モードを適用することにより、低い実装コストで高い性能向上が実現できることを示した。

第6章では、本研究で得られた成果を要約し、今後に残された課題について述べた。

論文審査の結果の要旨

本論文は、共通鍵暗号の高性能化を実現する新しい暗号モードを考案し、その処理速度、暗号強度、および実装効率について評価を行った結果をまとめたものであり、以下の主要な結果を得ている。

(1)共通鍵暗号の処理速度の向上に有効な実行アルゴリズムとしての暗号モードを考案している。本暗号モードは、ブロック暗号処理の再帰呼び出しおよびストリーム暗号処理機構を利用することにより、暗号化に必要なブロッ

ク暗号処理の回数を4分の1に削減している。さらに、暗号強度の向上を目的として広く用いられている暗号モードの処理機構を活用することより、暗号強度を損なうことなく処理速度の大幅な向上を実現している。

(2)本暗号モードの最大差分確率および最大線形確率を解析し、差分解読法および線形解読法によって高い暗号強度が保持できることを示している。さらに、本暗号モードは、ブロック暗号の出力値により生成する非線形テーブルを活用することによって、出力値の相関性を用いた暗号解読試行に対して高い暗号強度が保持できることを示している。

(3)共通鍵暗号に本暗号モードを適用した暗号システムの実装を行い、その実装効率について評価を行っている。本暗号システムをソフトウェアにより実装した場合、暗号処理速度を共通鍵暗号の約2倍まで高速化することが可能である。また、本暗号モードを実現するアクセラレータコアを設計し、ソフトウェアで実装した共通鍵暗号に本アクセラレータコアを用いることにより、暗号処理速度を共通鍵暗号の4倍まで高速化することが可能である。さらに、本暗号システムをハードウェアで実装し、1チップ内に集積化することにより、共通鍵暗号コアの約2倍である1.32Gbpsのスループットが実現できることを示している。

以上のように、本論文は共通鍵暗号の高性能化とそのVLSI化設計に関して多くの有用な研究成果をあげており、共通鍵暗号の実装技術の発展に寄与するところが大きい。よって本論文は博士論文として価値あるものと認める。