早稲田大学大学院情報生産システム研究科

博 士 論 文 概 要

論 文 題 目

H.264/AVC 暗号化方式のアルゴリズムと ハードウエア設計

申 請 者

范 益波

情報生産システム工学専攻
マルチメディアシステム研究

２００９年１月

内容概要

H.264（MPEG-4 part10　Advanced Video Coding（AVC）とも呼ばれる）は，従来の動画圧縮技術と比較してより効率的な圧縮効率を実現する技術として，2003年に勧告された最新の動画圧縮規格である．現在、コンテンツ保護などを目的とした動画用暗号スキームが標準化のために提案されている．しかし，その多くはMPEG-1やMPEG-2/H.262, MPEG-4,H.263といった従来の動画圧縮規格用途向けであり，H.264/AVC向け暗号スキームはまだ数が少ない．

本論文では，H.264/AVC向けの新たな動画像暗号スキームを提案する．また，提案手法を実現する暗号モジュールのハードウェア設計も同時に提案する．この論文は以下の三つに貢献している．1)提案する暗号スキームは、より高いセキュリティとより低い計算コストを実現する．2)提案する暗号モジュール向けのスケーラブルハードウェアアーキテクチャは高いスケーラビリティを持つ．そのため，H.264/AVCに限らず他の動画圧縮規格に応用することができる．3)提案する暗号モジュールはAESとFLEX二つの暗号アルゴリズムを支持し、差分電力解析攻撃(DPA)対策を講じており，5種類のDPAを防止することができる．

本論文は以下の七つの部分で構成されている。

第1章[**Introduction**]では、動画像符号化システムの基本概念について紹介する．また，動画用暗号処理とそのアルゴリズムについて紹介する．H.264や，選択的なビデオ暗号化方法、暗号スキームに使用する共通鍵暗号AESなどについて紹介する．

第2章**[Selective Video Encryption Schemes]**では、従来の動画像暗号スキームについて説明する．従来手法はある暗号アルゴリズムを暗号スキームに応用している．従来手法の基本的な考え方は選択的な暗号アルゴリズムに基づいており，動画データの一部分を暗号化して、他のデータは暗号化しない．暗号化するデータを限定することで暗号処理にかかる時間を大幅に削減することができる一方，セキュリティの強度が落ちてしまうことが指摘されている．本章では，選択的な暗号アルゴリズムの持つ三つの主要な問題（セ

キュリティ問題、計算問題，応用問題）について議論する．

第3章**[Unequal Secure Encryption Scheme for H.264/AVC]**では、H.264/AVC向けの不等セキュリティ暗号化（USE）スキームについて提案する．このスキームは、従来の選択的な暗号アルゴリズムよりも高いセキュリティレベルを維持すると同時に、計算コストを削減することができる。USEは，重要度の高いデータを安全性の高い暗号アルゴリズムで暗号化し，一方で，重要度の低いデータを安全性が低い暗号アルゴリズムで暗号化する．すべてのデータを暗号化できるため、従来手法よりもセキュリティレベルを高めることができる．USEスキームについて以下に示す．

１）データの分類：三つのデータ分類方法（Data Partitioning、FMO，Parameter Extraction）を提案する．

２）安全レベルの定義：提案手法は5つの安全レベルを定義する．要求する安全性と計算量のバランスによって決まる．最低の安全レベルを0とし，その計算量は全文を暗号化する場合の計算量のわずか18％である．最高の安全レベルを3とする．その計算量は全文を暗号化する場合の計算量のわずか50％である．従来の選択的な動画像暗号化アルゴリズムと比較すると，提案手法は全文を暗号化して安全性を高める一方で、計算量を大幅に削減することができる。

３）多重モード暗号化モジュール：提案する暗号化モジュールは一つハートウェアで二種類の暗号化アルゴリズム（AESアルゴリズム，FLEXアルゴリズム）を使用する．AESは安全性が高い暗号アルゴリズムなので，重要度の高いデータを暗号化する．FLEXは提案する高速に暗号化できるアルゴリズムなので，重要度の低いデータを暗号化する．FLEXアルゴリズムはAESの5倍の速度で暗号化処理できる．さらにAES向けハードウェアを流用することができる。

第4章**[Hardware Design of AES]**では、スケーラブルなAESハードウェアアーキテクチャを提案する．動画圧縮規格の種類によって、ハードウェアのパフォーマンスの要求が異なるため、暗号ハードウェアのスケーラビリティが重要になる。提案するAESハードウェアアーキテクチャは、並列なデータ通路設計が使用し、コンフィギュラブルハードウェアモジュールを持っている設計が実現できる．実験結果によると、S-boxモジュール

を1個，MixColumnモジュールを1個使用した場合、暗号処理のスループットは７５Mbpsであるが，S-boxモジュール20個とMixColumnモジュールを4個使用した場合，暗号処理のスループットは2.4Gbpsに達する．従来のAESハードウェアアーキテクチャと比較し、提案手法によるスケーラブルなAESアーキテクチャは多種多様なAESハードウェアを設計でき、ハートウェアコストが低い、性能が高い、動画像暗号化システムに応用することが最も適する．

第5章**[DPA Attack on AES]**では、AESに対する強力なサイドチャンネル攻撃である差分電力解析攻撃(DPA)について紹介する．DPAは1998年、Paul Kockerらによって提案された．暗号デバイスの消費電力を解析して、暗号デバイス中の秘密鍵を盗み出す攻撃手法である．ハードウェアに関する専門知識がなくても攻撃することができ，しかもその成功率は高いとされている．DPAはAES以外にも多数の暗号デバイスを攻撃することができるため，現在の暗号システムの安全性に対する大きな脅威となっている．本章では、AESに対するDPAについて紹介し、DPA対策の重要性について示す．

第6章**[AES Design with DPA Countermeasure]**では、AES向け差分電力解析攻撃(DPA)を防ぐ方法について提案し、世界で初めてDPA対策方法がハードウェアを実装・評価する。本章では5つの対策方法について説明する．Independent ARK, Data Sliding, Subbyte Hiding, Simplified S-Box MaskingとRegisters Maskingである。これら5つの対策手法を使用すれば，AESハードウェアに対するDPAの計算複雑度は2^{12N}倍にも達する．そのためDPA対策として有効な手法となる．さらに、たとえこの中の1つもしくは2種類の対策方法が無効にされたとしても、他の防御手法により暗号デバイスの安全性も保つことができる．

次は，提案する5つの対策方法を実装したAESハードウェアアーキテクチャを実装・評価した．VDEC ROHM0.18CMOSライブラリを使用し，AES暗号テスト用チップを実装した．4つのAESハードウェアを実装した．：①AES0:　DPA対策を施していないAESハードウェア．スループットは51Mbps，面積は4678ゲート，クロック周波数は80MHzである．②AES1.0: DPA対策としてIndependent ARKとData Slidingを使用したAESハードウェア．スループットは75Mbps，面積は5500ゲート，クロック周波数は125MHzである．③AES1.1:　DPA対策としてSubbyte Hidingを使用したAESハードウェア．スループットとク

ロック周波数はAES1.0と同じ75Mbps, 125MHz, 面積は6244ゲートである. ④AES1.2: DPA対策としてSimplified S-Box MaskingとRegister Maskingを使用したAESハードウェア. スループットは45Mbps，面積は6834ゲート，クロック周波数は75Mhzである．また，提案手法によるDPA対策の有効性を検証するため，本論文ではSASEBOボードを利用したAESハードウェア向けDPA対策評価用のプラットフォームを提案する．このプラットフォームに基づいて、実機上での提案手法によるDPA対策を評価した．実験結果によると、提案手法によるDPA対策は、確実にDPAを防御することができる.

第七章**[Conclusion]**では、本論文についてまとめる.