暗号アルゴリズム「Hierocrypt-L1」

詳細評価（HW実装評価）レポートサマリー

本報告は、ブロック暗号アルゴリズム Hierocrypt-L1 のハードウェア実装評価を行ったものである。評価方針としては、SBOX、乗算器、加算器、ラウンド関数等といった基本的な機能を実現している個々のパーツ(以下、primitive)の評価(回路規模、処理速度等)を実施することによりアルゴリズム全体の性能を見積る方法で評価を行い、また、個々の primitive においては、実際の LSI 作成に則した条件を付加して評価を行うことを前提にしている。この方針のもとに、評価期間の制約から、特定のアルゴリズムだけを最適化することはせずに、アルゴリズムを全て実装（回路規模は大きくても構わない）し、クリティカルパス長の短縮（処理速度向上）を重視して評価を行った。

本報告で用いる評価環境は、我々が H/W 評価経験のある三菱 0.35μm CMOS ASIC ライブラリを用い、回路記述には Verilog-HDL、Synthesis には Design Compiler を用い、回路規模(ゲート数)およびクリティカルパス長、処理速度等の性能見積を行った。

以上のような条件で評価した結果、以下のような結果となった。なお、アルゴリズムの処理速度を見積るため、本報告ではクリティカルパスに鍵スケジュールは含まれていないことに注意する。

	回路規模[Gate]	クリティカルパス[ns]
データランダマイズ部	278130	70.13
鍵スケジュール部	95397	42.38
アルゴリズム全体	373526	70.13

回路規模[Gate]	クリティカルパス[ns]	処理速度[Mbps]
373526	70.13	912.59

Hierocrypto-L1 は、約 912Mbps の処置速度であることから、64 ビット暗号として Triple-DES と比較した場合、高速なアルゴリズムであると言える。しかし、回路規模に関しては、Triple-DES と比較した場合、約 373Kgate と大きいアルゴリズムであり、小型化実装を考慮したとしても、IC カードや携帯端末などの小型なデバイスを使用するアプリケーションには向いていないアルゴリズムであると考えられる。