暗号アルゴリズムのハードウェア実装技術

鈴木大輔*

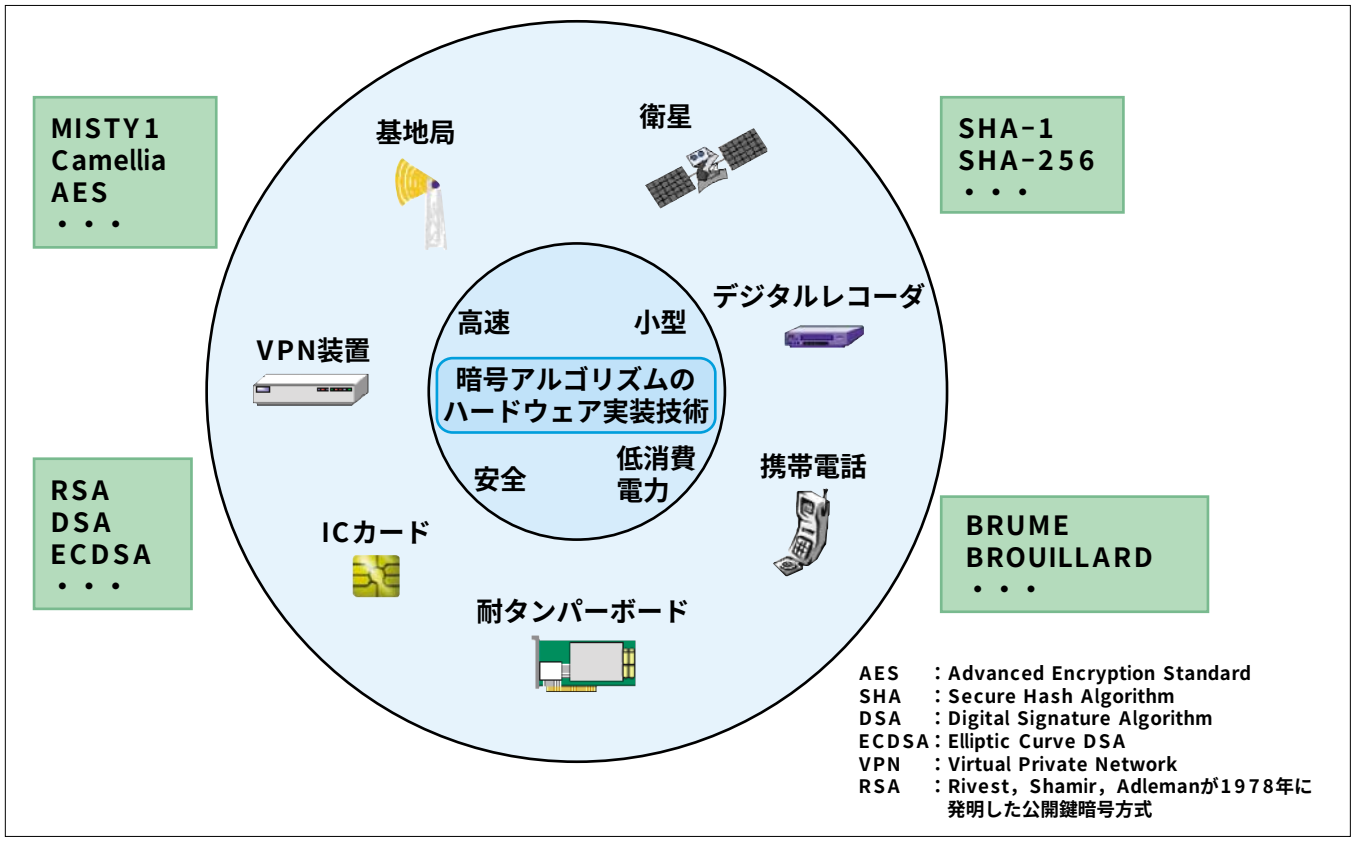
Hardware Implementation for Cryptographic Algorithm

Daisuke Suzuki

要　旨

近年，小型機器やデバイス単体が通信機能を持つことによってセキュリティ機能が不可欠となりつつある。また，ネットワークの高速化に伴い，SSL(Secure Socket Layer)等で必要な暗号化処理をより効率的に装置内で処理することが求められている。従来の高速化手法としては，ASIC(Application Specific Integrated Circuit)やDSP(Digital Signal Processor)を用いたアクセラレーションが一般的である。しかしながら，ASICの開発はコストが高く，セキュリティの要件上，アルゴリズムやそのパラメータが変更されうる暗号処理に対し，柔軟性に乏しい。またDSPを用いた処理方式は，ソフトウェアをベースに構築可能なため，柔軟性は高いが，ASICと比較すると処理性能は劣る。柔軟性と性能を満たす解決策として，FPGA(Field Programmable Gate Array)を用いた処理方式が提案されている。FPGAは，開発コストが低く，回路の変更が可能なため柔軟性が高い。また，容易に実動作までの実現が可能である。三菱電機はセキュリティ機能の中でも処理が重いとされる公開鍵(かぎ)暗号系の処理をFPGA上で専用LSI並みの高速処理を可能とするハードウェア実装技術を開発した。当社が試作したべき乗剰余演算回路は512ビットのべき乗剰余演算を約0.26msで処理可能である。これは，筆者が知る限り，FPGAによるべき乗剰余演算回路としては世界最速である。また，回路規模は4,000slices程度であり，Virtex−4(注1)シリーズで最小の論理規模のFPGA上でも実装可能である。この技術によって様々な機器で低コストに暗号処理のアクセラレーションが可能となる。

(注1)　Virtexは，Xilinx, Inc. の登録商標である。



暗号アルゴリズムのハードウェア実装技術とアプリケーションへの展開

ICカード等の小型機器から携帯基地局向けの高速通信機器まで，暗号アルゴリズムのハードウェア実装技術は幅広く展開されている。

*情報技術総合研究所