システムLSI向け 暗号IP

Cryptographic IP for System LSIs

本山　雅彦　■ MOTOYAMA Masahiko
清水　秀夫　■ SHIMIZU Hideo
藤崎　浩一　■ FUJISAKI Koichi

東芝は，システムLSI分野で重要となってくる情報セキュリティ機能を実現するための暗号IP（Intellectual Property）を開発した。これにより，情報セキュリティ分野で標準的に用いられるすべての暗号アルゴリズムをIPとしてラインアップするとともに，暗号の基盤研究の成果を適用し，速度や実装面積などの性能に優れたIPや，世界最小規模のAES（Advanced Encryption Standard）用IPを実現した。これらのIPを利用することで，設計期間を短縮することができ，また，システムLSIの性能を向上できる。

Toshiba has developed a cryptographic intellectual property (IP) series, which is a key technology for information security and system LSIs. Almost all of the standard cryptographic algorithms are available in this series. High-performance or small-area implementation is achieved by applying the results of theoretical research on cryptography. The Advanced Encryption Standard (AES) IP, which has the smallest area as far as we know, is the representative result of this series. This cryptographic IP series can be used to reduce the design time and improve the performance of system LSIs.

1 まえがき

情報技術の急速な進歩に伴って，様々な分野で情報セキュリティ技術に対するニーズが高まってきている。特に，近年のインターネットの普及に従って，ネットワークを利用した様々なサービスが提供されるようになってきた。このようなサービスにおいては，サービスを行う側にとっても受ける側にとっても，その相手が正当な相手であるかどうかを確認できることが必要である。また，正当な相手であると確認できたときに，クレジットカード番号などの，第三者に盗聴されると大きな被害を被る可能性のある重要な情報を，両者の間で安全に通信できることが必要である。これを実現する技術が暗号技術であり，公開鍵暗号，共通鍵暗号，ハッシュ関数，乱数生成などの基本的な技術を組み合わせて，システム全体の安全性が実現される。

一方で，半導体技術が急速に進歩し，一つのチップ上にシステム全体を実現できるようになった。このようなLSIは，システムLSI[(1)]と呼ばれる。システムLSIは，CPUやメモリなどの様々な機能ブロックを用いて実現されるが，規模が大きいので，個々の機能ブロックを一から設計することは困難となってきている。このような問題を解決するために用いられているのがIPによる設計手法である。システムLSIにおけるIPとは，LSIを構成する機能ブロックを意味している。IPを使うことで，設計者は，既に実現されているIPをそのまま，あるいは小さな修正で使用でき，設計期間を短縮できる。

このように設計されたシステムLSIは，家電機器，情報機器，産業機器など様々な分野で様々な製品に組み込まれている。そして，これらの機器の多くは，ネットワークに接続されるようになってきている。ネットワークに接続された機器にとって情報セキュリティ機能は重要であり，これらの機器に用いられるシステムLSIにも，情報セキュリティ機能を実現するために暗号機能が必要となる。

東芝は，このような要求に対応するために，暗号基盤研究の成果をシステムLSI分野に適用して暗号IPシリーズを開発した（**図1**）。ここでは，この暗号IPシリーズの特長とその一つである世界最小規模のAES用IPの概要を述べる。

2 暗号機能の実現方法

暗号機能は，ソフトウェアによって実現する場合とハードウェアによって実現する場合がある。

ソフトウェアによる実現方法には，以下のような特徴がある。

(1) 実装コストが小さい　プログラムは，不揮発性メモリやROMなどの記憶装置に保存されているため，暗号処理専用のハードウェアを用意するより低コストである。

(2) 柔軟である　ソフトウェアで実現されているので，仕様の変更などがあった場合に，記憶装置に保存されているプログラムを修正することで対応できる。

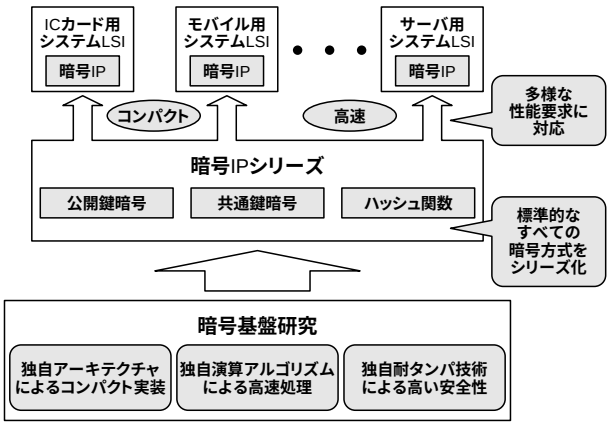

図1. 暗号IPシリーズ ― 暗号基盤研究の成果をシステムLSI分野に適用した。
Cryptographic IP series

⑶　処理が低速である　　CPUで実現されるため，専用のハードウェアに比べて低速である。処理手順を逐次的に処理していくため，処理時間が長くなる。

一方，ハードウェアで実現する場合は，ハードウェアコストが高く，柔軟性に欠けるが，高速であるというソフトウェアと逆の特徴がある。しかし，半導体技術の進歩によって大規模なLSIが実現できるようになってきたので，暗号処理に用いられるハードウェアのコストは，相対的に小さくなってきている。

3 システムLSI向け暗号IPシリーズ

当社は，暗号分野の基盤研究に注力してきている。その成果として，当社独自の共通鍵暗号Hierocrypt$_{TM}$，公開鍵暗号RSA(Rivest-Shamir-Adleman)の高速演算アルゴリズム[2]，共通鍵暗号AESのコンパクトな実装方式[3]を開発し，更に，これらの基盤研究の成果をシステムLSI分野に適用し，暗号IPシリーズを開発した。

3.1 暗号IPシリーズの目的と特長

暗号IPシリーズ開発の目的は，豊富なIPをラインアップしておくことで，暗号機能を必要とするシステムLSIの設計期間を短縮することである。また，高速に処理できるIPやコンパクトなIPなど高性能のIPを提供することで，システムの性能を向上することである。このような目的を達成するため，以下の方針で開発を行った。

⑴　標準的に利用される暗号機能をすべてIPとして実現する。

⑵　高速な処理速度，小さいゲート規模などの要求に対応できるIPを実現する。

情報セキュリティ分野では，以下に示す公開鍵暗号，共通鍵暗号，ハッシュ関数などを用いてセキュリティ機能が実現される。

⑴　公開鍵方式　　公開鍵と秘密鍵という2種類の鍵ペアが存在し，送信者は，送信者の公開鍵を用いて情報を暗号化し，受信者は，自身の秘密鍵を用いて情報を復号する方式である。デジタル署名も公開鍵暗号の一種として位置づけられる。公開鍵暗号では，RSA方式が広く利用されている。

⑵　共通鍵方式　　情報の送信者と受信者が共通の秘密鍵を持ち，送信者は，秘密鍵を用いて情報を暗号化し，受信者は，秘密鍵を用いて情報を復号する。共通鍵暗号方式では，DES(Data Encryption Standard)方式がもっとも利用されているが，今後は，新たに標準化されたAES方式への置き換えが進むと考えられている。

⑶　ハッシュ関数は，任意長のメッセージを圧縮し，固定長のダイジェスト情報を生成する関数であり，デジタル署名では，一方向性のハッシュ関数がRSAなどの暗号方式と組み合わせて用いられる。ハッシュ関数では，MD5(Message Digest 5)，SHA-1(Secure Hash Algorithm 1)などが広く使われている。

開発した暗号IPシリーズには，RSAや楕円(だえん)曲線暗号といった公開鍵暗号，DESやAESといった共通鍵暗号，MD5やSHA-1といったハッシュ関数など，標準的に用いられる方式のすべてが用意されている。このほかにも，当社独自の共通鍵暗号Hierocrypt$_{TM}$や次世代ハッシュ関数SHA-256など，将来において広く利用されることが予想される方式も用意した(**図2**)。

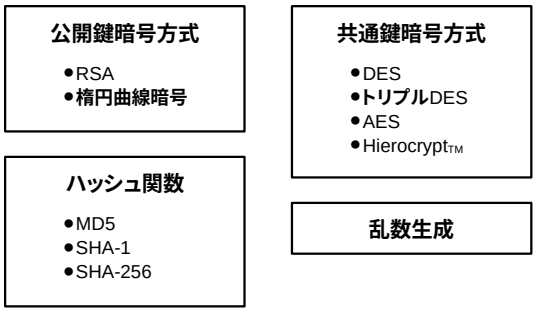

図2. 暗号IPシリーズのラインアップ ― 標準的に利用されるすべてのアルゴリズムを実現した。
Lineup of cryptographic IP series

また，アルゴリズムの豊富さだけではなく，その性能においても特長のあるIPをラインアップしている。例えば，Webサーバなどで高速なRSA処理を実現するIP，携帯機器で必要とされる小型化を実現した世界最小規模のAES用IPなどである。以下で，世界最小規模を実現したAES用IPについて述べる。

3.2 小型AES用IP

まず，背景となるAESについて簡単に説明する。AESは，米国政府の米国技術標準局（NIST：National Institute of Standards and Technology）が2001年に定めた共通鍵暗号アルゴリズムの標準である(4)。AESの仕様は，FIPS197（Federal Information Processing Standards 197）として出版されている。従来は，1976年に米国商務省が定めたDESが使われていたが，20年以上を経て安全性が問題になったため，代わりとなる新しい暗号が定められた。

AESの入力と出力（ブロックサイズ）は128 ビットである。AES以前は64 ビットブロック暗号が主流であったが，安全性と処理効率から長いブロック長となっている。鍵の長さは128，192，256 ビットの3種類から選ぶことができ，様々なセキュリティレベルに対応できるようになっている。

AESは，NIST主導の評価により高い信頼性が得られており，また，特許ライセンスの無償化も保証されているので，AESもDESと同様に広く普及することは十分考えられることである。そこで，当社は将来に備えて，高速処理が可能なIPや回路規模が小さなIPを準備しておくことにした。ここでは小型IPについて述べることにし，小型化の原理について技術的な解説を行う。

一般にハードウェアの性能は，処理速度（処理に要するクロック数と動作可能クロック周波数），回路規模，消費電力の三つで測られる。処理速度を高速化するための方針は，各部品がなるべく独自並列に動作するようにすることである。回路規模を小さくする場合の方針は，同じ回路を何度も使い回すことである。いずれの場合も，いくつかのレベルでの最適化を行うことになり，下記のレベルが考えられる。

⑴　上位レベル　　処理手順の見直しなど，回路の詳細に立ち入らないレベルでの最適化

⑵　中位レベル　　部品の共通化など，ある程度回路構成に立ち入ったレベルでの最適化

⑶　下位レベル　　部品そのものの最適化

各レベルを独立して行うこともできるが，各レベルは相互に関係し合っているので，複数を同時に最適化することもある。

図3はAESにおける暗号化変換の処理手順である。入力は暗号化したいメッセージ（平文）と鍵である。鍵は鍵処理により順次，拡大鍵に変換されていく。平文は，拡大鍵を使って非線形変換と線形変換を繰り返し適用され，最終的に暗号文に変換される。暗号文を復号するときは，図の手順を逆の順序で行う。

各部品（非線形変換，線形変換，鍵処理）の内容と，実施できる最適化については以下のとおりである。

⑴　非線形変換　　非線形変換はs-boxと呼ばれる8ビット入出力の表引きを行う。非線形変換の入力は128 ビットなので，そのままではs-boxに入力できない。そこで，128 ビットを8ビットづつ16個に区切って，各々s-boxにより変換する。

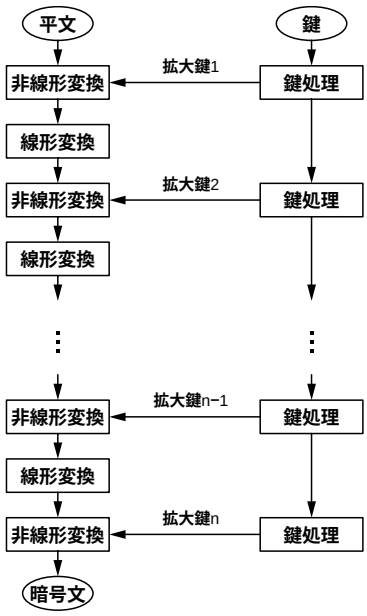

図3．AESの処理手順 ― 平文に非線形変換と線形変換を繰り返し作用させることで暗号化を行う。

Algorithm of AES

s-boxは乱数表のようなものと考えてよい。ハードウェア実装する際に表を自動合成すると，600ゲート程度が必要となり，これを16個実装すると回路規模が大きくなる。小型化するために，s-boxを時間的に共有する構成を用いた。

複数のデータを複数の処理回路で処理する並列処理方式と，一つの処理回路を複数のデータで時間的に分割して共有する時分割共有方式のようすを**図4**に示す。並列処理方式の場合，データごとに回路が必要になるので多くの回路が必要になるが，処理時間は短くなり，高速処理に適している。時分割共有する場合は，図4(b)のように一つの処理回路で，データを順次ベルトコンベアのように流し込むことになる。このように時分割共有は，処理時間が増えるが回路は一つとなり，小型化に適している。

またs-boxの変換表自体も等価な数学的表現を求めて，コンピュータを使った探索で複数ある等価表現の中から最適なものを選ぶことにより，300ゲート程度に圧縮できた。

⑵　線形変換　　線形変換は8ビット単位の並べ替えと，32 ビットごとの行列乗算によってできている。並べ替え自体は，ハードウェアでは結線により実現できるのでコ

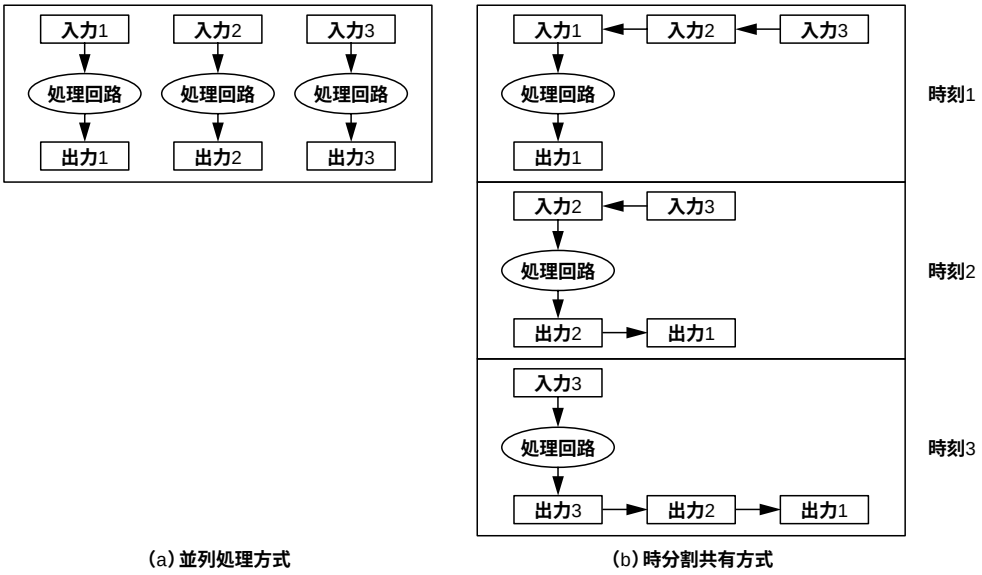

図4．並列処理と時分割共有処理の比較 ― 並列処理は高速な処理に，時分割共有処理は小型化に適している。
Parallel method and time-sharing method

ストはかからないが，行列乗算をいかに簡単に実現するかが問題になる。複雑な行列をより簡単な行列の積と和で表現することで回路を簡単にすることができた。ここでも，簡単な表現を求めるためにコンピュータによる探索を行った。

(3) 鍵処理　　鍵処理は，非線形変換と同じs-boxによる変換と，8ビット単位の並べ替えでできている。s-boxに関する最適化は，非線形変換と同じテクニックが使える。非線形変換と鍵処理でs-boxに関する処理を共有することで，更なる回路規模削減が可能となる。

以上の工夫により，仕様書のまま実装すると30kゲート程度必要となるAESを，約5kゲートで実現することができた。

4 あとがき

当社の暗号分野における基盤研究の成果をシステムLSIに適用し，暗号IPシリーズを開発した。このシリーズには，セキュリティ分野で標準的に利用されるすべての暗号方式がIPとしてラインアップされている。また，暗号処理を高速に行うことができ，サーバなどの用途に適したIP，回路規模が小さく携帯用機器に適したIP，当社独自の次世代暗号Hierocrypt$_{TM}$など特徴的なIPも含まれている。これらのIPシリーズを利用することにより，システムLSIの設計期間を短縮することや，性能を向上させることができる。

文　献

(1) 斎藤光男．半導体技術の進歩とシステムオンチップ．東芝レビュー．**57**，1，2002，p.38－42.
(2) 新保淳，ほか．高速RSA暗号LSI．東芝レビュー．**56**，7，2001，p.10－13.
(3) 清水秀夫，ほか．SPN型ブロック暗号の実装について．電子情報通信学会技術研究報告．**101**，311，2001，p.17－21.
(4) National Institute of Standards and Technology. "AES Home Page". <http://csrc.nist.gov/CryptoToolkit/aes/>，(accessed 2003-05-07)．

本山　雅彦　MOTOYAMA Masahiko
研究開発センター　コンピュータ・ネットワークラボラトリー
研究主務。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

清水　秀夫　SHIMIZU Hideo, D. Eng.
研究開発センター　コンピュータ・ネットワークラボラトリー
研究主務，工博。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，日本セキュリティ・マネジメント学会会員。

藤崎　浩一　FUJISAKI Koichi
研究開発センター　コンピュータ・ネットワークラボラトリー。
暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.