

LSI IPデザイン・アワード応募書類表紙(企業)

タイトル： 暗号技術を容易に実装できるセキュリティIPコア

技術分野： 暗号

応募者： 北村公一 鈴木孝一郎 古川輝幸 大越 智

所属機関： NECマイクロシステム株式会社 コア開発事業部 IPソリューションセンター

1. 研究・開発の目的・狙い(100字程度)

ネットワークのセキュリティ向上のために暗号技術の利用は必須になってきているが、その実装は容易ではない。そこで、暗号アルゴリズムの規格に精通していなくても、SOC に暗号技術を容易に実装できるセキュリティ IP コアの開発を行った。

2. 研究・開発の概要(箇条書き)

1) 利用分野： ネットワークのセキュリティ

2) 特徴： i) ディスクリプタによるプログラマブルなセキュリティIPコア

ii) トータルなセキュリティコアだけでなく、演算エンジン単体のコアも提供

3) 種類：ソフトウェアVC

4) 規模：約600kGate(0.18um)

5) 性能：DES:1.2Gbps TripleDES:400Mbps AES:1.2Gbps MD5:850Mbps

SHA1:850Mbps 1024bitべき乗剰余：40ms (クロック周波数133MHzの時)

3. 訴求点および効果：(100字程度および図表)

暗号の基本演算(TripleDES, AES, SHA1, べき乗剰余等)の連続処理をディスクリプタに記述することで、より複雑な暗号アルゴリズム(DSA, RSA等)を実現するIPコアを開発した。その結果、暗号アルゴリズムの規格に精通していなくても、ディスクリプタを記述する事で、ハードウェアの変更なしに各種暗号技術や新規アルゴリズムの暗号技術を容易に利用する事が可能となった。

暗号技術を容易に実装できるセキュリティ IP コア

NEC マイクロシステム株式会社 コア開発事業部 IP ソリューションセンター
北村公一 鈴木孝一郎 古川輝幸 大越 智

1. 新規性

本 IP の特徴は、演算の種類と、演算するデータの格納領域情報を記述したディスクリプタ（後述）を連結し、シーケンサで自動的に一連の処理を行うようにプログラムできる点である。この機能により、演算器単独では実現できない手続き、たとえば電子署名のひとつである DSA(Digital Signature Algorithm)や、RSA の高速化手法の一つである CRT(Chinese Remainder Theorem)などを実現できる。

また、新規の暗号アルゴリズムや、独自の暗号アルゴリズムを実装する際にも、ディスクリプタに対するプログラムを変更することで、ハードウェアの変更なしに暗号アルゴリズムを実現できる。

図 1 に本 IP のブロック図を示す。

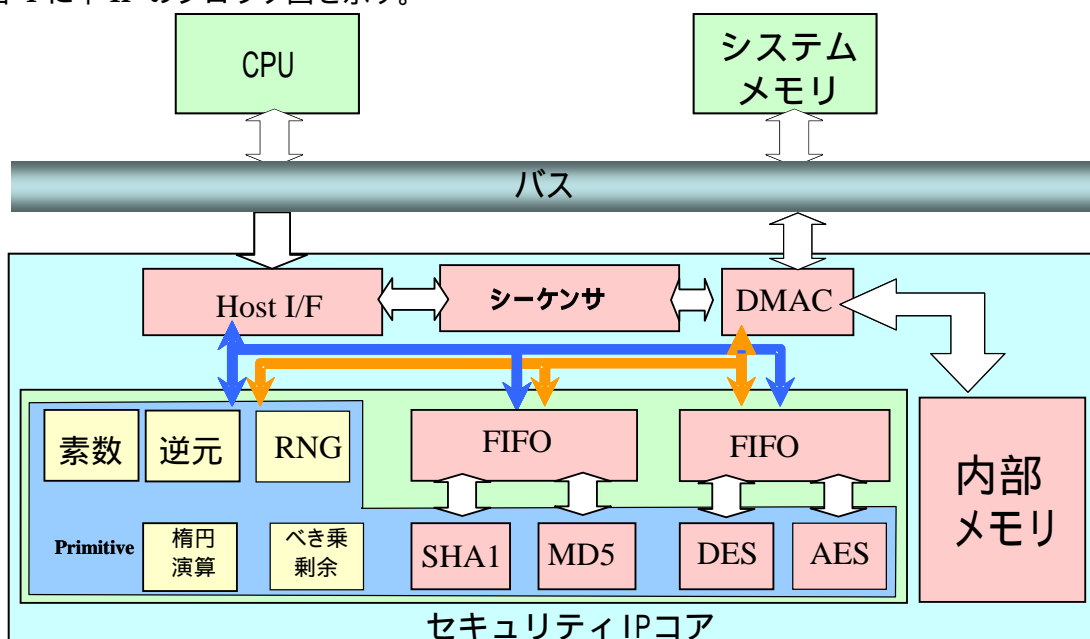


図 1 セキュリティ IP コア ブロック図

1.1. 単独のディスクリプタ(AES)

ディスクリプタとは、演算の種類と入力・出力データの格納領域情報等を指定し、演算を自動的に行うための記述である。

ディスクリプタはシステムメモリに置かれ、本 IP 内のシーケンサ(図 1 参照)により参照される。例として、図 2、表 2 に AES のディスクリプタを示す。シーケンサは、表 1 に示す動作を行うことで、暗号処理を行う。

表 1 単独のディスクリプタ(AES)を処理するシーケンサの手順

DMA を起動し、ディスクリプタが置かれたアドレス(DMACFG レジスタに格納)のデータを取得 ディスクリプタをデコード DMA を起動、DATAIN, DATAOUT, KEY を AES に対して与える。 AES 演算 DMA を起動、AES の演算結果を DATAOUT へ DMA 転送 branch Address が 0 なので処理終了。

ここで示した例は AES のディスクリプタだが、他の演算のディスクリプタのフォーマットも、UNIT と branch Address フィールドは共通、それ以後は各演算固有のフィールドとなっている。

				UNIT(0001)
branch Address				-
			SZ	MOD E
DATASIZE				
*DATAIN				I M
*DATAOUT				I M
*KEY				I M
*IV				I M

図 2 ディスクリプタの例(AES ディスクリプタ)

表 2 AES ディスクリプタフィールド

Name	Description
UNIT	ディスクリプタが起動する演算ユニットを指定する。AES ならば 0001
branch Address	16 バイトアラインされた次のディスクリプタのアドレス。0 を設定すると、最後のディスクリプタであることを表す。
SZ	キーのサイズの選択 00:128 ビット 01:192 ビット 10:256 ビット
MODE	AES のモードの選択を行う。 00:EBC モード 01:CBC モード
E	入力データを encrypt するか、decrypt するかを切り替える。 0: Decrypt 1: Encrypt
DATASIZE	AES を行うデータサイズのワード数を指定する。
DATAIN	AES を行う入力データが置いてあるメモリへのポインタ。
IM	DATAIN/DATAOUT の参照先を切り替える。 0:外部メモリ 1:セキュリティ IP コア内のメモリ
DATAOUT	AES を行った結果を出力するメモリへのポインタ
KEY	AES を行う際の KEY を格納してあるメモリへのポインタ。KSIZE に応じたキーが格納されている領域を指定すること。0 が設定されると、以前に設定されたキーを継続して使う。
IV	初期化ベクタが格納されているメモリへのポインタ。0 に設定されると、以前に設定された IV を継続して使う。

1.2. 内部メモリへのアクセス

セキュリティ向上のため、鍵情報などを本 IP 外部に置かず、演算できるように内部メモリを用意し、ここに重要なデータを保存しておくことができる。この内部メモリは、外部から直接読み出しができない構造であり、唯一、ディスクリプタの参照としてのみアクセスできる。図 2 の例では、DATAIN、DATAOUT、KEY、IV フィールドの LSB の IM フィールドで、演算に関連するデータの格納場所を、内部メモリにするか、システムメモリにするかを指定する。IM がセットされていれば、内部メモリ、リセットされていれば、システムメモリへアクセスする。

1.3. 連結したディスクリプタ(CRT)

シーケンサは、ディスクリプタを連続に処理する機能を持つ。図 3 に、RSA の復号を加速するために使われる CRT(Chinese Remainder Theorem)のディスクリプタ記述の例を示す。シーケンサは、このディスクリプタ記述にしたがって連続実行する。表 3 に連結したディスクリプタの動作を示す。

表 3 連結したディスクリプタ(CRT)の動作

DMA を起動し、ディスクリプタが置かれたアドレス(DMACFG レジスタに格納)のデータを取得
ディスクリプタをデコード
DMA を起動、ディスクリプタにかかれたアドレスから必要なデータを DMA 転送
ディスクリプタに書かれた演算を実行
DMA を起動、演算結果をディスクリプタに書かれたアドレスへ DMA 転送
branch Address が 0 なら処理終了、0 でないなら DMACFG レジスタに branch Address の値を設定し、へ戻る

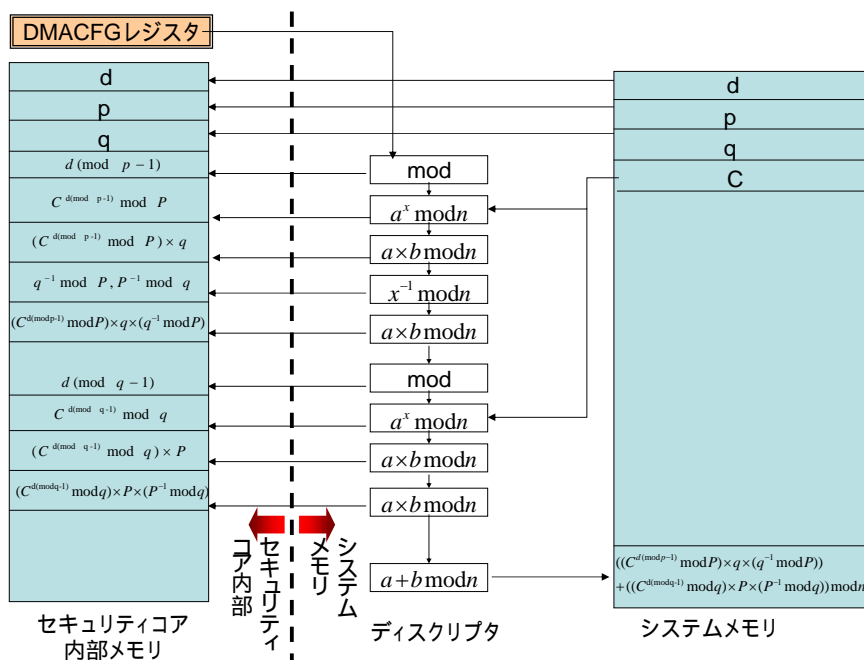


図 3 ディスクリプタによる CRT 演算

1.4. ディスクリプタの制御

本 IP では、ディスクリプタの連結をリンクリストで行う。また、シーケンサをディスクリプタ単位で停止し、ディスクリプタの再構成を行うことができる。これにより、現在処理中のシーケンスより優先順位が高い要求が発生した場合(たとえば通信では、通常、送信パケットデータの暗号化中にパケットを受信した場合、受信パケットの復号は送信よりも優先する)、ディスクリプタの処理を一時停止し、ディスクリプタのリンクリストの先頭に受信データの処理のためのディスクリプタを追加し、処理を続行することで求める処理が実現できる。

2. 有用性

AV などのデジタルコンテンツ、インターネット上での電子決済、電子政府での個人情報管理など、通信を利用したサービスが整備されている。一方、それらシステムの間を突いたネット犯罪は急増し続けており、暗号技術はネット犯罪を防止するための要となる技術である。また、さらに強固な暗号アルゴリズムの研究がなされ、ネット犯罪防止のために進化を続けている。

技術的な視点から見て、暗号 IP がその他の IP と大きく違う点は、アルゴリズムの複雑さにある。その他の IP がインテグレータやドライバ開発者にとって理解できるのに対し、数学的な原理を基礎としている暗号 IP の振る舞いは、技術者にとって理解することが難しく、それゆえにドライバの開発も困難である。

本 IP は、SOC に容易に実装できると共に、各種暗号アルゴリズムに対し柔軟に対応するためのプログラマブルな機能を持つため、SOC に組み込んだ後に、新規の暗号アルゴリズムにも対応することが可能となる。

3. 実用性

本 IP は、共通鍵暗号エンジン(DES,AES)、公開鍵暗号エンジン(RSA、楕円)、ハッシュ演算エンジン(MD5,SHA1)と乱数・素数発生器を基本演算器として持ち、DMA コントローラと内部メモリをディスクリプタ方式のシーケンサでコントロールすることで、より複雑な暗号アルゴリズムを実現する暗号プロセッサである(図 1)。公開鍵エンジンのビット幅は最適化を考慮し、パラメータ化した。

共通鍵暗号エンジン(DES,AES)とハッシュ演算エンジン(MD5,SHA1)は、大量のデータ処理を考慮し、入力段に FIFO を装備した。共通鍵暗号エンジン(DES,AES)に関しては、出力段にも FIFO を装備した。これらの FIFO は格納段数の最適化を考慮し、パラメータ化した。これにより、SOC に最適な FIFO を実装することが可能となる。

ハッシュ演算エンジン(MD5,SHA1)は、IPv6 等で使う鍵つきハッシュ(HMAC)機能も搭載している。本 IP のスペックを表 4 に、ブロック図を図 1 に示す。これらの演算エンジンは、顧客の要求するシステムに必要なものだけを抜き出して提供することも可能である。

表 4 セキュリティ IP コアの各演算エンジンの機能と性能

演算エンジン	機能	性能
TripleDES	FIPS46-3 準拠、EBC,CBC モード	400Mbps@133MHz
AES	FIPS 197 準拠	1.2GBps@133MHz(128bitKey)
MD5	RFC1321 準拠 RFC2104 準拠 HMAC	850MBps@133MHz
SHA1	FIPS 180-1 準拠 RFC2104 準拠 HMAC	850MBps@133MHz
べき乗剰余	最大 2048bit 長の RSA、Diffie-Helman 鍵交換 FIPS186-2 の DSA に対応	約 40ms/133MHz (1024bit 時)

4. 品質

本 IP は、C 言語設計・検証・動作合成環境で設計を行っている。各基本演算器は次に示す検証を実施した。

- ・ 動作合成可能な C 言語での検証
- ・ RTL での検証

暗号アルゴリズムの中でも、特にべき乗剰余演算器は非常に長いシミュレーション時間が必要になる。たとえば、1024bit のべき乗剰余演算の平均的演算速度は、実時間で 40ms@133MHz かかる。一般に、RTL(Verilog-HDL,VHDL)シミュレーションの実行速度は 10Hz ~ 100Hz といわれており、この速度だと実時間で 40ms(133MHz)かかるべき乗剰余の演算は、約 148 時間(シミュレーション速度を 100Hz

で計算)かかることになる。そのため、RTL シミュレーションで網羅的な検証することは現実的ではなく、主に信号のタイミングの検証が中心となる。

同様の検証を合成可能な C 言語で行うと、約 1 分で実行できるため、網羅的に検証することができた。本 IP のべき乗剰余演算器に関しては、約 100 種類のテストパターンを作成し、検証を実施した。ユーザには、検証済みの合成可能な C 言語から、動作合成ツールを用いて生成した RTL を提供する。

5. 完成度、親和性

本 IP の提供物件には、高速シミュレーションのための SystemC ビヘイビアモデル(Cycle-true モデル)が含まれる。SystemC ビヘイビアモデルは、ARM モデルを CPU としたシステム上で、約 100KHz のシミュレーション速度が確保できることを確認した(Pentium 3GHz, Linux マシン)。このシステム・レベルでの RTL シミュレーションは演算器単体シミュレーション(4章参照)以上に現実的ではない。

100KHz の SystemC シミュレーションでは、1 回のべき乗剰余の演算が約 53.2 秒となるので、Diffie-Hellman 鍵交換アルゴリズムや RSA 暗号アルゴリズムを実際の手順で動かすことが可能なオーダーである。

この SystemC ビヘイビアモデルは、AMBA AHB CLI(AMBA が提供する Cycle-true モデルのための SystemC インタフェース)に対応しているため、顧客の SystemC 検証環境にインテグレートしてシステム検証を行うことも可能である。

SystemC シミュレーションで、本 IP と他ブロック間のトランザクションの検証を行い、システムパフォーマンスの見積もりと改善を、シミュレーションの段階で行うことができる。

また、ドライバの開発をすることも可能であるため、ハードウェア設計とソフトウェア設計を並行して進めることができる。

ディスクリプタによる制御は、ドライバの記述を容易にする特徴もある。各エンジンを単独で扱う場合、データの受渡しや演算エンジンの切り替えなど、各エンジンの単独動作を管理する必要がある。しかし、ディスクリプタ記述を利用することで、各エンジンの動作を事前に記述、エンジンの連動動作は本 IP が保証することで、一連の処理が可能となる。

最後に、当社は、組み込みサポート、ドライバ開発サービスなど、本 IP を利用したトータルソリューションを提供する。また、顧客の要求仕様に合わせた本コアのカスタマイズも行っている。

6. 提供物件

- ・ 合成可能な RTL
- ・ サイクルアキュレートな SystemC 検証モデル
- ・ ユーザーズマニュアル
- ・ サンプルドライバ
- ・ テストベクター一覧

LSI IP デザイン・アワード/チェック・シート企業部門ハード設計資産

- 1) タイトル
暗号技術を容易に実装できるセキュリティ IP コア
- 2) IP 名
SECURE-IP
- 3) 応募者
社名 NEC マイクロシステム株式会社
応募者名 北村公一 鈴木孝一郎 古川輝幸 大越 智
連絡先 NEC マイクロシステム株式会社 コア開発事業部 IPソリューションセンター

〒211-0063 神奈川県川崎市中原区小杉町1丁目403番53号 NEC小杉ビル
TEL: 044-722-8389 FAX: 044-733-8735
- 4) 応募部門
課題部門
- 5) IP の提供形態
VerilogHDL,VHDL
- 6) 実績 (製品化やライセンス状況など)
 - ・ ASSP 製品に DES,AES,MD5,SHA1,べき乗剰余演算器を IPsec の一部として実装
 - ・ ASIC 製品に DES を実装。評価完了。
- 7) 合成可能な EDA 環境
Synopsys 社 Design Compiler
- 8) 検証レベル (論理シミュレーションや FPGA、Si 試作など)
 - ・ 機能合成可能な C 記述による動作検証
 - ・ RTL シミュレーション
- 9) 提供可能物
 - ・ 合成可能な RTL
 - ・ サイクルアキュレートな SystemC 検証モデル
 - ・ ユーザーズマニュアル
 - ・ サンプルドライバ
 - ・ テストベクター一覧
- 10) VSIA 準拠状況
未対応
- 11) 特許の有無
無し
- 12) 特許調査の有無
現時点で特許侵害なしと判断
- 13) サポート体制
コア開発者による直接サポートを提供する。
 - ・ SOC への組み込みサポート
 - ・ ドライバ開発サービス
 - ・ カスタマイズサービス