C-014

Handel-Cによる暗号処理ボードSEBSW-2への暗号回路の実装・評価

Implementation and evaluation of cryptographic circuits for SEBSW-2 with Handel-C

古市　洋希[†]　山内　剛[‡]　梶崎　浩嗣[†]　岩井　啓輔[†]　黒川　恭一[†]
[†]防衛大学校情報工学科　[‡]防衛庁陸上自衛隊

1. はじめに

大量のデータを高速に暗号化するために，多くのセキュリティシステムにて共通鍵暗号方式が用いられている。しかし，近年の計算機性能の向上や暗号解読技術の進歩により，同じ暗号方式を継続して使用することは安全でない。そこで，我々は暗号方式と鍵をダイナミックに変更可能な暗号処理ボード SEBSW-2（SEcret-key Block cipher SWitcher）を開発し[1]，Verilog-HDL を用いて CRYPTREC において次世代共通鍵暗号の候補となっている暗号アルゴリズム（3-DES，MISTY1，Hierocrypt-L1，Camellia，AES 等）の実装を行い，その性能を評価した。[2] SEBSW-2 はコアとして FPGA（XCV300）を持つ。これにより，ハードウェア実装された暗号アルゴリズムをダイナミックに変更することが可能であるとともに，高速動作が可能である。また，新しい暗号アルゴリズムの導入も容易である。しかしながら，その暗号アルゴリズムに対応した回路自体は HDL によって記述されており，その作成には多大な労力が必要となっていた。

これに対して，近年システムレベル設計手法と呼ばれる C 言語ベースの設計技術が向上しており，HDL より抽象度の高い，C 言語を拡張した言語を用いることにより容易にハードウェアを設計することが可能になっている[3]。現在の暗号アルゴリズム等に何らかの理由で変更しなければならない必要性が生じた場合，このような言語及びツールを使用することで，より迅速かつ容易にアルゴリズム等が変更可能になる。暗号回路の設計にこの様な手法を用いることで，新しい暗号アルゴリズムの導入期間の短縮が期待でき，現在までその環境の整備を行ってきた[4]。

本稿では，この環境を用いて SEBSW-2 において利用可能な暗号回路を実装し，開発期間の短縮を図るとともに，その性能等を評価する。また，HDL で設計した場合との性能等の比較を行う。

2. 暗号処理ボードSEBSW-2の概要

2.1 要求される仕様

SEBSW-2 は，汎用の IBM PC 互換機同士が，頻繁に暗号方式や鍵を交換しながら通信することによって，データ等の保障を得ることを目的とした DCCS（Dynamically Changeable Cipher System）の中核を成す PCI ベースの暗号処理ボードである。このシステムは，自衛隊における暗号通信，特に航空機等に搭載することを想定したものであり，そのために求められる仕様は以下のとおりである。

(1) 航空機搭載を想定し，軽量かつ低消費電力であること
(2) 暗号方式の変更時には，ボードレベルでのハードウェアの変更が少ないこと
(3) 公開もしくは非公開の共通鍵ブロック暗号の暗号化及び復号ができること

これらは，再構成可能素子である FPGA を使用することにより解決できる。

2.2 SEBSW-2の構成

暗号処理ボード SEBSW-2 は，PCI コントローラ，SRAM，FPGA，ネットワークコントローラ，コンフィグレーションコントローラの 5 つのブロックで構成されており，それぞれ 32-bit データバスと 32-bit アドレスバスとで接続されている。さらに，様々な機器との接続のため，インターフェイスとして PCI や USB インターフェイスを想定している。PCI インターフェイスを持つ暗号処理ボードのブロック図を図 1 に示す。

図 1 中，下段左は，PCI bus とのインターフェイスを行う PCI コントローラを表しており，PCI bus と Local bus の信号の送受信を行う。その右の SRAM は FPGA の構成データを一時的に蓄えるためのものである。右から 2 番目は SEBSW-2 のコアである FPGA を表し，構成データを変更することによって異なる暗号アルゴリズムの処理を行う。下段右端のネットワークコントローラは，Ethernet 等の外部ネットワークへデータを送受信するためのコントローラである。上段のコンフィグレーションコントローラは，一時的に SRAM に蓄えられた FPGA の構成データを FPGA へ転送するための機能を果たし，CPLD（XC95108）を用いて実装している。

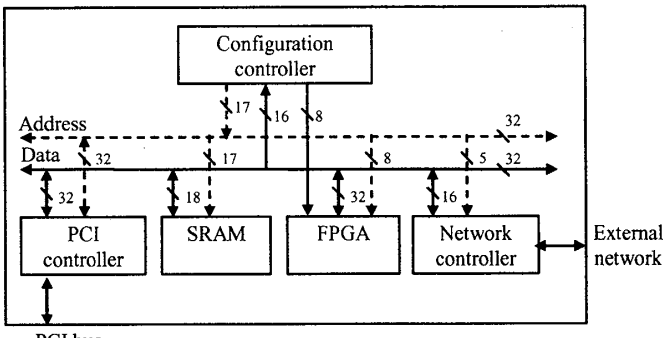

図1：SEBSW-2のブロック図

3. 開発環境

今回構築した開発環境を以下にまとめる。まず，開発言語として Handel-C 言語を用い，実装するターゲットは Xilinx 社 XCV300-PQ240-4 とした。また，論理合成，配置配線及びシミュレーションは Celoxica 社の DK2 デザインスイートを利用した。配置配線については，Xilinx 社 ISE Foundation 5.1 を使用した。

4. 暗号アルゴリズムの実装

4.1 実装アーキテクチャ

多くのブロック暗号は，基本的な関数を繰り返す逐次的なアルゴリズムである。このような暗号回路の実装方法としては，以下の 3 種類のアーキテクチャが考えられる。

(1) Fully loop unrolled
(2) Pipeline
(3) Loop

(1)は，F 関数全てを実現するアーキテクチャであり，回路規模が大きくなるが，処理速度は比較的速い（図 2）。
(2)は，(1)をパイプライン化したアーキテクチャであり，スループットは最も大きくなる。
(3)は，F 関数 1 ラウンド分のみを実装して，それをループさせることにより実現するアーキテクチャであり，スループットは小さくなるが，回路規模を小さできる。(図 3)。

SEBSW-2 への実装には，ターゲットデバイスが Xilinx 社の XCV300-PQ240-4 であるため，回路規模としてスライス数 3,072 以下に収める必要がある。そこで，ループアーキテクチャを選択して回路規模を抑えるとともに，できる限り高速化を図ることとした。

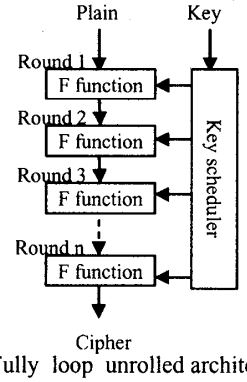

図2：Fully loop unrolled architecture

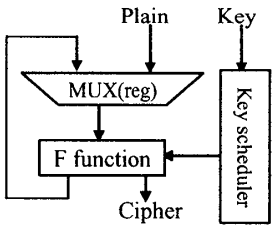

図3：Loop architecture

4.2 暗号アルゴリズムの設計

暗号アルゴリズムの実装にあたり，今回は整備した環境の確認を兼ねて，代表的なブロック暗号である 3-DES，AES，MISTY1 を取り上げ実装した。

4.2.1 3-DES

DES は，Feistel 構造で，64-bit の平文と 64-bit の鍵を元に，16 段の同一の変換が繰り返し行われるブロック暗号である。3-DES は，鍵を 3 個用意し，DES を 3 段組み合わせたものである。本研究では，1 段の変換を 16 回ループさせた DES を 3 回ループする設計とした。S-BOX はメモリを用いた表引きで実装した。

4.2.2 AES

AES は，SPN 構造の 128-bit ブロック暗号であり，ShiftRows, SubBytes, MixColumns, AddRoundKey により構成されている。SubBytes では 8-bit 単位の S-BOX が 16 個必要であり，鍵生成で必要な S-BOX は 4 個である。また，鍵生成は On the Fly 方式である。実装については，3-DES と同様に，1 段の変換を 10 回ループさせ，S-BOX についてはすべてメモリを用いた表引きで実装した。

4.2.3 MISTY1

MISTY1 は，Feistel 構造の 128-bit の暗号化鍵を持つ 64-bit ブロック暗号であり，繰り返される F 関数は FO 関数と FL 関数により構成されている。また，FO 関数は FI 関数を 3 回繰り返す構造であり，FI 関数には S9，S7 と呼ばれる S-BOX により構成されている。推奨される段数は 8 段であることから，8 段とした。8 ラウンド後の出力までに S-BOX は S9,S7 合わせて合計 72 回使用される。設計については，同様に 8 段ループとし，S-BOX はメモリを用いた表引きで実装した。

5. 実装結果及び評価

Handel-C による実装結果を表 1 に，HDL による実装結果を表 2 に示す。スライス数については，本研究で用いたアルゴリズムすべてにおいて HDL で設計したほうが，小さなものとなった。また，動作周波数は，MISTY1 を除き HDL のほうが高くなった。全体的に Handel-C による実装のほうが劣るものの，SEBSW-2 に求められる要件や開発期間等を考慮すると問題がないといえる。

MISTY1 において，動作周波数が向上した理由については，現在検討中であるが，回路の記述方法によっては，HDL と同様またはそれ以上の性能を出すことが可能であるといえる。

表 1 Handel-C による実装結果

Algorithm	Area [Slices]	f_{MAX} [MHz]	開発期間 [h]
3-DES	2,409	24.826	48
AES	2,606	21.417	20
MISTY1	2,341	34.727	8

表 2 HDL による実装結果

Algorithm	Area [Slices]	f_{MAX} [MHz]	開発期間 [h]
3-DES	917	48.024	48
AES	2,305	27.585	40
MISTY1	2,283	19.108	40

6. おわりに

本稿では，整備したシステムレベル設計手法を用いて SEBSW-2 において利用可能な暗号回路のうち代表的な 3-DES，AES，MISTY1 を実装し，その性能等を評価した。また，HDL で設計した場合との性能等の比較を行い，システムレベル設計言語の使用による SEBSW-2 の開発期間の短縮について示した。今後の課題としては，さらに様々な暗号アルゴリズムを実装し回路削減や高速化の手法を導くことが挙げられる。

なお，本研究は東京大学大規模集積システム設計教育研究センターを通し，Celoxica 社の協力で行われたものである。

参考文献

[1] 梶崎浩嗣，黒川恭一：“暗号処理ボード SEBSW-2 の設計と性能評価”,信学技報 VLD2002-123,CPSY2002-76,2002
[2] 山内剛，梶崎浩嗣，黒川恭一：“暗号処理ボード SEBSW-2 への暗号回路の実装”,FIT2003，C-034，2003
[3] http://www.celoxica.co.jp
[4] 古市洋希，山内剛，岩井啓輔，梶崎浩嗣，黒川恭一：“Handel-C による暗号処理ボード SEBSW-2 への暗号回路の実装”,情報処理学会第 66 回全国大会，1Y-6，2004