SASEBO-AES 暗号 FPGA ボード

FIPS140-2 Non-Proprietary Security Policy

Version 1.4

2007 年 11 月 12 日

東北大学・産業技術総合研究所
暗号ハードウェア開発プロジェクト

目次

1. モジュール仕様

1. 1 概要

SASEBO-AES は PowerPC プロセッサコアを内蔵した Xilinx 社の 2 つの FPGA (Field Programmable Gate Array) XC2VP7(以下 FPGA1)と XC2VP30(以下 FPGA2)を搭載したサイドチャネル攻撃評価用標準プラットフォームの FPGA ボード Side-channel Attack Standard Evaluation Board (以下 SASEBO)上に, 128 ビット共通鍵ブロック暗号 AES (Advanced Encryption Standard)をハードウェア実装し, データの暗号化及び復号を行うマルチチップ組込型の暗号ハードウェアモジュールである.

図 1 に SASEBO-AES の概観を, また図 2 にブロック図を示す. 図 2 で灰色に塗られた部分は, SASEBO-AES として未使用のコンポーネントを表している. 2 つの FPGA のうち図 1 及び 2 の左側の FPGA1 に AES 暗号回路とシリアルインタフェース回路が実装されており, 右側の FPGA2 は RS232C シリアルポートの信号をスルーして FPGA1 に渡している. それぞれの FPGA には電源オン後に, コンフィギュレーション用の EEPROM である EEPROM1(XCF08P)及び EEPROM2 (XCF16P)から, ハードウェア設計情報が自動的にロードされるが, FPGA2 は FPGA1 と RS232C ポート間の結線だけが定義されており, 論理回路は一切含まれていない. FPGA1 と FPGA2 では電源系統が左右に分離され, それぞれの電源入力端子に 3.3V を接続し, FPGA1 Power Selector を左側(INT)に, Main Power Switch を下側(ON)にスライドさせることで, レギュレータからそれぞれの FPGA に I/O 用 2.5V, コア用 1.8V の電力が供給される. なお, クロックも両者で独立しており, 2 つのオシレータから基板の左右に別々に 24MHz が供給されるが, コンフィグレーション終了後の暗号処理時に FPGA2 はクロックを使用しない.

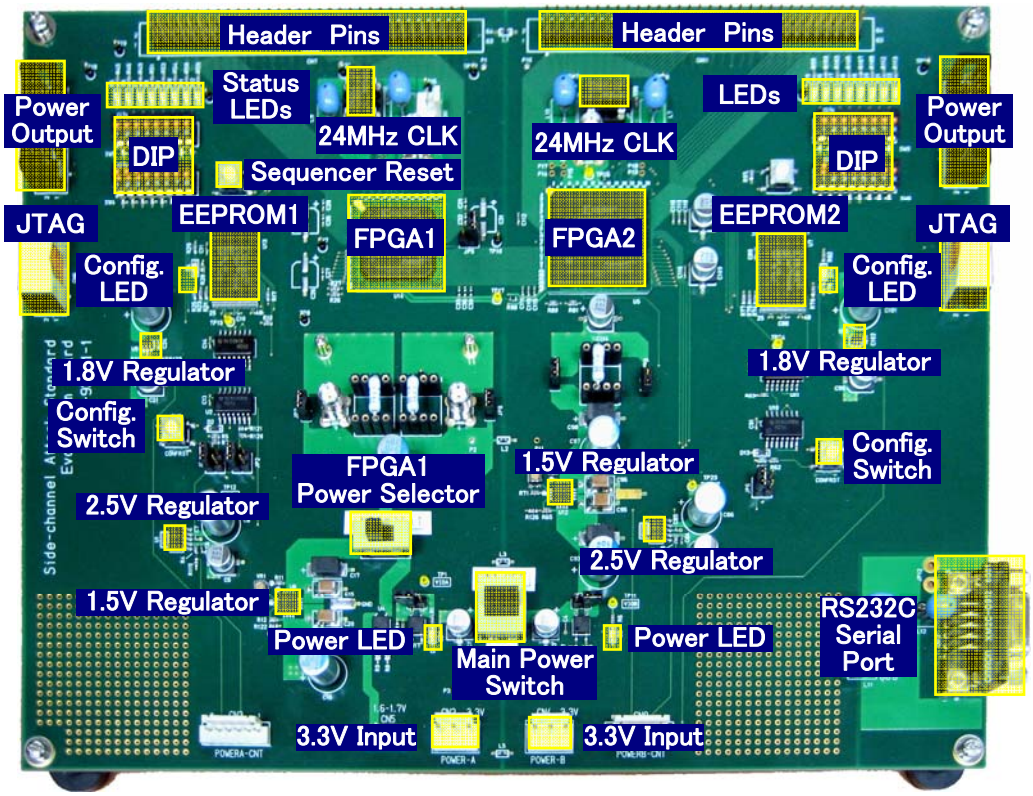


図 1 Side-channel Attack Standard Evaluation Board (SASEBO)の概観

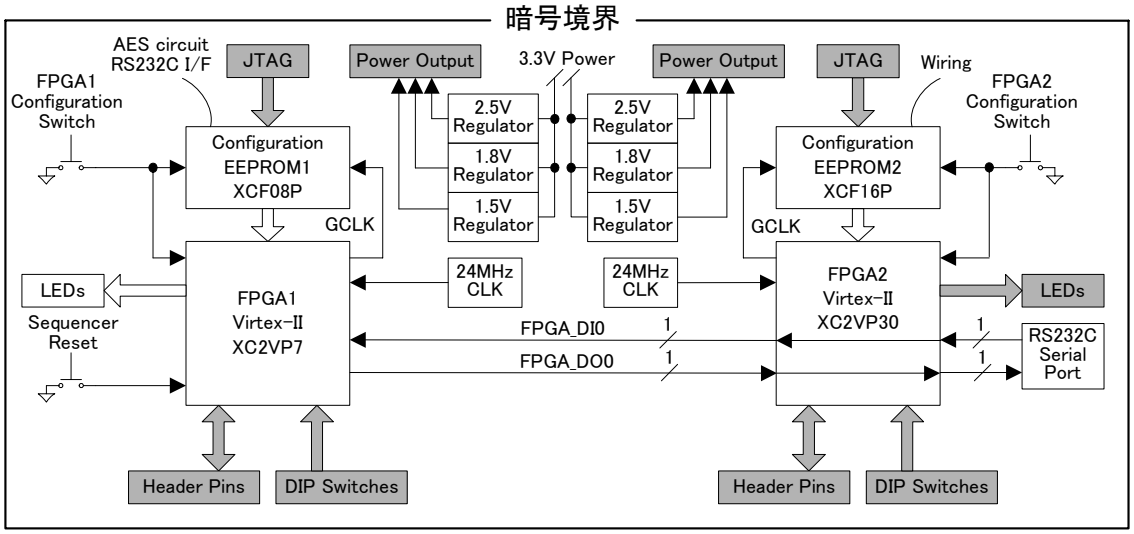


図 2 SASEBO-AES 暗号 FPGA ボードのブロック図

暗号境界は図 1 及び図 2 のボード全体で，主要コンポーネントは FPGA1 と AES ハードウェア及びシリアルインタフェース回路情報を保持する EEPROM1 の 2 つである．SASEBO に含まれる全てのコンポーネントと回路図は別冊の「サイドチャネル攻撃用標準評価基板仕様書」で提供される．

EEPROM1 内の AES ハードウェア設計情報は，「4．有限状態モデル」の章の図 9 で状態 S2～S6 として示された動作テスト，AES 暗号化・復号処理，そして状態 T1～T5 のシリアルインタフェース回路を含んでいる．

回路情報を保持する EEPROM1 及び入出力ポートの結線情報のみを保持する EEPROM2 用の JTAG 端子には，第三者による設計情報の改ざんを防止するために，剥がすと痕跡の残るセキュリティシールが貼られている．FPGA1 と FPGA2 の間は，データ入力(FPGA1←FPGA2)及び出力(FPGA1→FPGA2)用として，それぞれ 1 本ずつの信号線で結ばれており，入力線はコマンド及び秘密鍵・データが，出力線はステータス及びデータがシリアルに転送される．また外部の PC からは，RS232C ポートを通じて FPGA1 に対してこれらのコマンド/ステータス，鍵/データ入出力制御を行うことができる．FPGA1 に入力された秘密鍵は内部レジスタに保持され，FPGA1 の外部に出力されることはなく，また図1のボードの左側にある 2 つのプッシュスイッチ(Sequencer Reset 及び Config Switch)のいずれかを押すか，シリアルインタフェースを通じて Reset コマンドを与えるか，あるいは電源をオフにすることでゼロ化される．FPGA1 に接続された LED はエラー状態を示す外部表示装置としての役割を持ち，LED2 に接続された LED は未使用である．詳細は「2．ポート及びインタフェース」を参照のこと．FPGA1 及び FPGA2 には他の入出力デバイスとして，電源出力，DIP スイッチ，ヘッダーピンを持つ．SASEBO-AES は様々な回路を後から実装できる汎用の FPGA ボードに AES 暗号回路を実装したものであり，EEPROM1 と EEPROM2 の内容を書き換えて他の用途として用いる場合に，その制御や外部回路を付加するためにこれらの入出力デバイスが用意されている．従って，今回は不要であるこれらのデバイスは SASEBO-AES では使用しておらず，図 2 では灰色のボックスとして示されている．

SASEBO-AES は共通鍵暗号 AES を使用しているので暗号化と復号は同じ 128 ビットの秘密鍵を使用するが，暗号化と復号で回路を分離しかつそれぞれのレジスタに同じ鍵をセットしている．これはレジスタへの鍵設定時に動作エラーが生じると被害が甚大なため，暗号化と復号の両回路で正しく暗号化→復号の処理が行われるかどうかを内部で自動的にテストするためである．

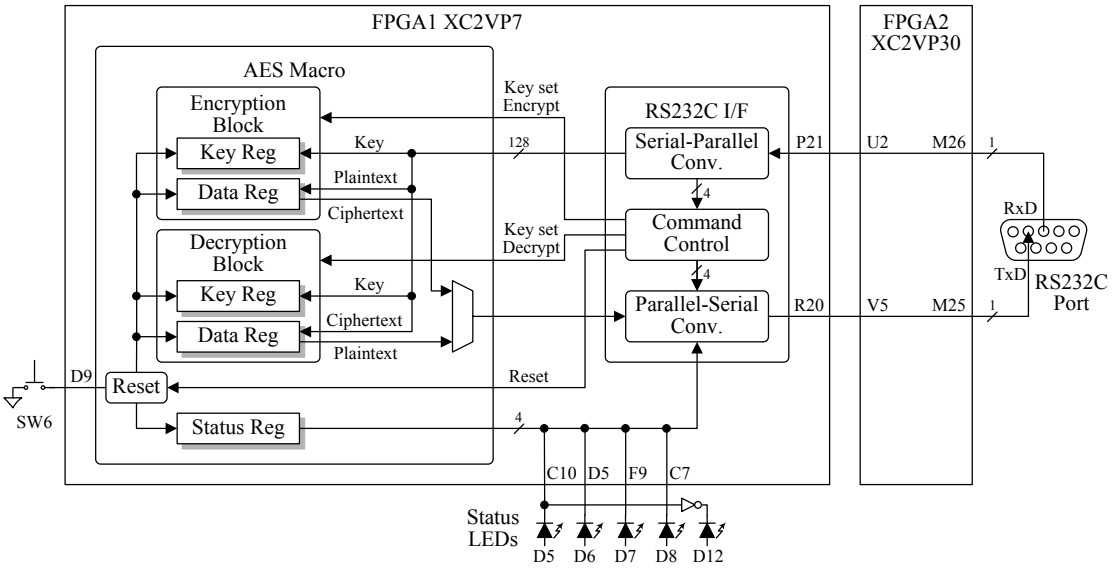


図 3 SASEBO-AES 暗号 FPGA ボードの制御及びデータの流れ

図 3 は，SASEBO-AES において，外部とのデータ入出力，制御入力，ステータス出力が SASEBO-AES においてどのような経路で行われるか，その概略を示したものである．FPGA1 及び FPGA2 の入出力線には，それぞれの FPGA で定義されている I/O ピン番号を振ってある．また，リセットスイッチ SW6 とステータス LED の D5～D8,D12 はボード上に印字されている部品番号である．外部からの制御は，RS232C シリアルポートにつないだ PC 等の一台の外部端末及びボード上のリセットスイッチによって行われ，SASEBO-AES は単一オペレータ動作モードにおいて機能する．RS232C の RxD ピンには，「2．ポート及びインタフェース」の図 4 で詳解する入力データフォーマットに従って，コマンド，鍵，平文または暗号文が 1 ビットずつ入力される．この信号は RS232C インタフェース回路のパラレルーシリアル変換回路を通じて，コマンドとデータが分離され，鍵は AES マクロの暗号化ブロックと復号ブロックそれぞれの鍵レジスタへ，また平文は暗号化ブロックのデータレジスタへ，暗号文は復号ブロックのデータレジスタへと書き込まれる．鍵レジスタは暗号化及び復号ブロックの内部でのみ使用され，その情報が外部に出力されることはない．また，レジスタの内容はコマンドによるソフトウェアリセット，あるいはスイッチ SW6 の押下によるハードウェアリセットによってゼロ化される．

暗号化のコマンドが発行されると暗号化ブロックで処理が行われ，データレジスタに暗号文が得られた後にパラレルーシリアル変換回路を通り，図 5 の出力データフォーマットに従って RS232C ポートの TxD ピンから 1 ビットずつ出力される．このとき，データの先頭にはコマンドの種類を示す 4 ビットのコマンド情報とエラー状態を示す 4 ビットのステータス情報が付加される．復号時には復号ブロックによる処理が終わるとデータレジスタに平文が得られるので，暗号化と同様，コマンドとステータスと共に RS232C ポートから 1 ビットずつ出力される．なお 4 ビットのステータス情報は D5~D8 の 4 つの LED にも同じものが出力される（ビットが 1 のとき発光）．またエラーがない場合には D12 が発光する．

本セキュリティポリシーに記載されている暗号モジュールのバージョンは，SASEBO-AES-G1.1 である．

1．2 セキュリティレベル

SASEBO-AES は表 1 に示した JCMVP 暗号モジュールセキュリティ要件のセキュリティレベル 1 の要件を満たしている．なお、電磁妨害／電磁両立性（EMI/EMC）に関する事項は選択しない。

表 1　SASEBO-AES のセキュリティ要件

セキュリティ要件	レベル
暗号モジュール仕様	1
暗号モジュールのポート及びインタフェース	1
役割，サービス，及び認証	1
有限状態モデル	1
物理的セキュリティ	1
動作環境	N/A
暗号鍵管理	1
自己テスト	1
設計保証	1
その他の攻撃の対処	N/A

1．3 オペレーションモード

SASEBO-AES は，FIPS-197 で規定され，国際標準規格 ISO/IEC18033-3 に採用された 128 ビットブロック暗号 Advanced Encryption Standard (AES)の暗号化・復号をサポートしている．鍵長は 128 ビット，またオペレーションモードは ECB (Electric Code Book)のみである．また承認されていないセキュリティ機能は使用していない．したがって本暗号モジュールは，常に承認された動作モードにおいて機能する．

表 2　承認アルゴリズム

アルゴリズム	仕様
AES	FIPS 197 鍵長 128 ビット ECB (Electric Code Book)　モード

2．ポート及びインタフェース

表 3 に SASEBO-AES の入出力インタフェースを，また図 4~5 にそのインタフェースを通して AES 回路とやりとりされるコマンド及びデータのフォーマットを示す．主要なデータ入出力は RS232C シリアルポートを通じて外部に接続された PC から制御する．鍵及びデータの入出力，ステータスの読み出しは，4 ビットの入力コマンドで制御する．CSP である秘密鍵は，いずれのインタフェースからも出力されることはない．

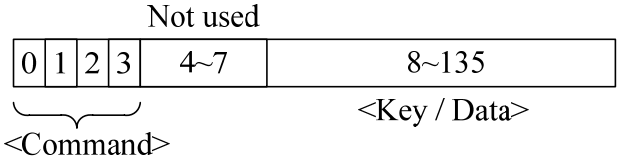
データの入出力は常に 136 ビット単位で行われる．入力データは図 4 に示したように，先頭 4 ビットがコマンド，次の 4 ビットが未使用，そして最後の 128 ビットが秘密鍵または平文(暗号化時)/暗号文（復号時）となる．ビット 0 の値が 1 のときは AES 回路のリセットなので，128 ビットの鍵や平文/暗号文を入力する必要はないが，この場合もデータフォーマットを統一するためにダミーの 128 ビットデータを付加して 136 ビットとする．ビット 0~3 で複数ビットの値 1 となっていた場合のコマンドの優先順位は，「リセット＞秘密鍵セット＞暗号化＞復号」である．またビット 0~3 の値が全て 0 の場合は，AES 回路は何の処理も行わないので，現在のエラー状態を示すステータスだけを読み出すこ

とになる.

出力データフォーマットは図 5 に示したように, その直前に実行したコマンド 4 ビットに続いて, ステータス 4 ビット, そして 128 ビットの暗号文(暗号化)/平文(復号)である. エラーが発生していなければステータスビットは全て 0 となる. また, 暗号化と復号以外のコマンドでは返すべき暗号文あるいは平文がないが, データ長を 136 ビットに統一するため, ステータスの後は 128 ビットの 0 が続けて出力される. なお 4 ビットのステータス情報は図 6 のように D5~D8 の 4 つの LED にも同じものが出力される(ビットが 1 のとき発光). またエラーがない場合には D12 が発光する.

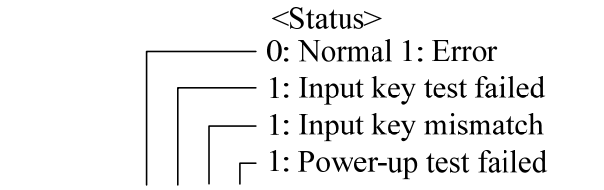
FPGA1 と FPGA2 にはそれぞれ DIP スイッチ SW4 と SW8 が接続されているが, これは SASEBO-AES 製造時の EEPROM への回路設計情報書き込み時の JTAG 入力切り替え, 及び書き込まれた情報を FPGA にロードする目的で使用される. 各 DIP スイッチのビット 1~3 を on, それ以外を off に固定した状態(ビット 6~8 は未使用)で, EEPROM から FPGA に回路情報がロードされ暗号化・復号処理が行えるようになっている. その他の設定では FPGA への回路設計情報のロード動作は保障されないが, 回路設計情報の書き換えや誤動作による CSP の漏洩等の危険性はない. 電源オン後に FPGA1 及び FPGA2 のコンフィグレーションが正常に終了すると, 図 7 のようにそれぞれの EEPROM の横の LED(D4 及び D14)が点灯する. また, 図 8 のコンフィグレーションスイッチを押すことで, FPGA の再コンフィグレーションを行うことがきる. SW2 を押下すると, FPGA1 と FPGA2 の双方が, また SW7 を押下すると, FPGA2 だけが再コンフィグレーションされる. 従って, オペレータは電源オン以外にも SW2 の押下により, 自己テストを実行することができる.

なお, ヘッダーピン及びディップスイッチ SW5 と SW9 は未使用であり, いずれの FPGA の入出力信号もアサインされていない.



<Command>
1xxx : Reset AES circuit
01xx : Set secret key
001x : Start encryption
0001 : Start decryption
0000 : Read status

図 4 入力データフォーマット



<Last command>
1xxx : Reset AES circuit
01xx : Set secret key
001x : Start encryption
0001 : Start decryption
0000 : Read status

図 5 出力データフォーマット

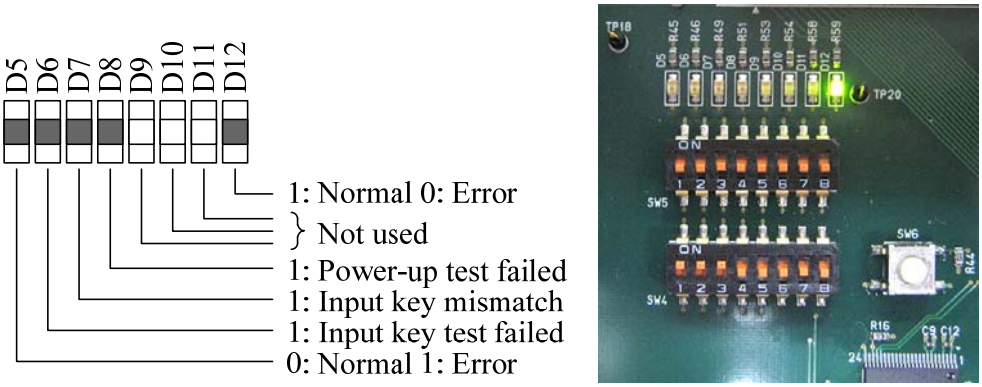


図 6　ステータス LED の意味とパワーアップ自己テスト正常終了時の状態
右写真のスイッチ SW6 は FPGA1 のシーケンサーのリセット用

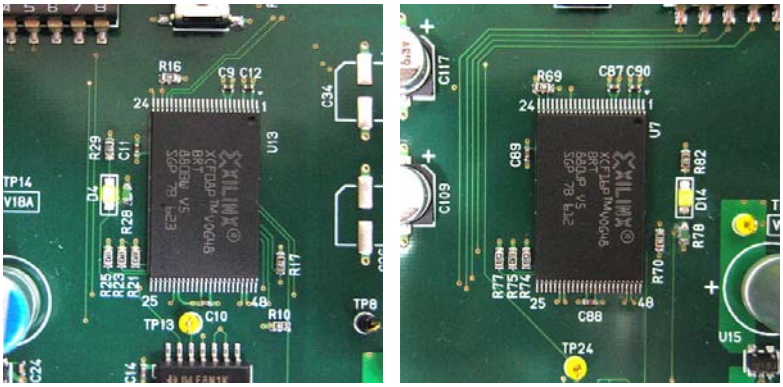


図 7　2 つの EEPROM，XCF08P(左)と XCF16P（右）の LED，D4 と D14 が点灯

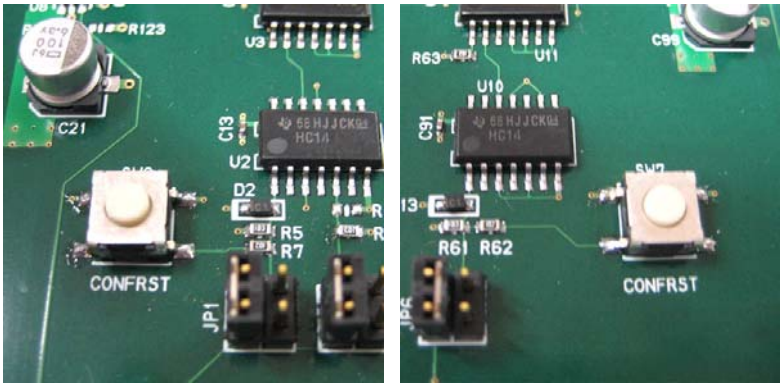


図 8　コンフィグレーションスイッチ SW2(左)と SW7(右)

表 3　入出力インタフェース

インタフェース	ポート/スイッチ	説明
データ入力	RS232C シリアルポート	8ビットのコマンド(内上位4ビットのみ使用)に続いて128ビットの鍵または平文/暗号文をセットとした136ビットのデータを1ビットずつ入力する.
データ出力	RS232C シリアルポート	リセット, 鍵セット, 暗号化/復号の処理が終わると, その結果に応じたステータス(実行したコマンド 4 ビット+エラー状態 4 ビット)及び暗号文/平文(128 ビット)が, このポートから 1 ビットずつ出力される.
制御入力	RS232C シリアルポート	鍵入力, 暗号化, 復号, リセット, 状態出力の各コマンドを 4 ビットで指定する. このコマンドビットは上記データ入力時の136ビットの先頭4ビットである.
	リセットスイッチ	FPGA1 及び FPGA2 は, 回路設計情報(FPGA2 は結線情報のみ)を EEPROM から再ロードするコンフィグレーションスイッチ SW2 及び SW7 を有する. SW2 を押すと FPGA1 と FPGA2 の双方のコンフィグレーションが, SW7 を押すと FPGA2 だけのコンフィグレーションが行われる. コンフィグレーション後は両 FPGA で回路設計情報の完全性テストが行われ, それに続いて FPGA1 ではアルゴリズムテストが実行される. また FPGA1 は回路のシーケンサーをリセットするスイッチも有し, これが押された場合はアルゴリズムテストだけが実行される.
状態出力	RS232C シリアルポート	136ビット出力の先頭から5~8ビット目の4ビットで, 内部のエラー状態を出力する.
	LED	電源オンまたはコンフィグレーションスイッチが押され, 正常に回路設計情報が各 FPGA に正しくロードされると, 図 7 のように EEPROM 横の LED D4 及び D14 が点灯する. それに続く, アルゴリズムテストが成功すると図 6 のようにステータス LED 右端 D12 が点灯する. またアルゴリズムテスト及び「8.自己テスト」で後述の鍵テストの結果に応じて次の LED が点灯する. D5: いずれかのテストにおいてエラー発生 D6: 入力鍵による暗号化/復号テスト失敗 D7: 鍵不一致 D8: アルゴリズムテスト失敗 D12: 正常状態
電源ポート	SASEBO への 3.3V 直流電源ポート	FPGA1 側と FPGA2 側それぞれに供給され, この電源電圧から内部電源の 1.5V, 1.8V, 2.5V が生成される.

3. 役割，サービス，及び認証

3．1 役割

SASEBO-AES は，表 4 に示したように，ユーザ役割として AES の 128 ビット秘密鍵の設定，データの暗号化・復号，状態の取得、そしてソフトウェアリセットを，またクリプトオフィサ役割としてゼロ化とそれに続くアルゴリズムテストをサポートしている．また，その他の役割は有さない．なお，ユーザ役割とクリプトオフィサ役割を区別するための認証手段は有しておらず，役割は利用するサービスにより暗黙的に区別される．

3．2 サービス

表 4 にユーザ役割とクリプトオフィサ役割それぞれのサービスを示す．コマンド及び鍵/平文/暗号文の入出力及び状態出力は RS232C シリアルインタフェースを通じて 1 ビットずつおこなわれる．また，状態出力はステータス LED にも表示される．コマンド発行後は AES 暗号回路で直ちに処理が行われ，処理終了後は自動的にデータが出力される．なお，一旦マクロ内のレジスタに書き込まれた鍵は読み出すことはできない．

3．3 CSP の定義とアクセス

SASEBO-AES は 128 ビットの AES 秘密鍵だけを CSP として保持する．秘密鍵はユーザによってモジュール内の FPGA1 のレジスタに書き込まれ，暗号回路はレジスタ内の秘密鍵を参照して暗号化あるいは復号を行う．レジスタ内の秘密鍵は FPGA1 の外に読み出すことはできず，レジスタの値はユーザの鍵の変更による書き込み，あるいはクリプトオフィサによる鍵・データゼロ化によってのみ変更することができる．秘密鍵のゼロ化は，電源オフオン，コンフィグレーションスイッチ SW2 の押下，シーケンサーリセットスイッチ SW6 の押下又はソフトウェアリセットによって行うことができる．

表 4 役割とサービス

役割	サービス	CSP へのアクセス	備考
ユーザ役割	AES 鍵設定	書き込み	128ビットの暗号化鍵を設定する．これにより内部では暗号化及び復号回路で鍵のテストが自動的に行われる．
	AES 暗号化・復号	FPGA 内部からのみ参照可	平文または暗号文の入力により処理が開始される．処理が終わった暗号文(暗号化処理)または平文(復号処理)はシリアルインタフェースを経由してリクエストなしに直ちに出力される．この暗号文/平文出力のヘッダーとして，直前に実行したコマンド4ビット及びエラー状態 4 ビットも出力される．
	状態出力	なし	アルゴリズムテスト，鍵比較及び鍵テスト後のエラー状態を，図5のフォーマット中の4ビットでシリアルインタフェース経由から出力する．同じ 4 ビットの状態はボード上のステータスLEDでも表示される．

	ソフトウェアリセット ＋アルゴリズムテスト	ゼロ化	シリアルインタフェース経由のコマンド入力による AES 暗号回路のリセット. シーケンサーとレジスタがリセットされ, アルゴリズムテストが自動的に実行される. 鍵をレジスタに残したままでアルゴリズムテストが単独実行されることはない.
クリプト オフィサ役割	コンフィグレーション&回路設計情報完全性テスト ＋アルゴリズムテスト	ゼロ化	ボード上のコンフィグレーションスイッチ SW2 を押すことで, EEPROM1 に格納された回路設計情報に対する完全性テストが実行され FPGA1 の回路が全て再構成され, 鍵及びデータはゼロ化される. 引き続き自動的にアルゴリズムテストも実行される.
	ハードウェアリセット ＋アルゴリズムテスト	ゼロ化	ボード上のシーケンサーリセットスイッチ SW6 の押下によるリセット. シーケンサーとレジスタがリセットされ, アルゴリズムテストが自動的に実行される. 鍵をレジスタに残したままでアルゴリズムテストが単独実行されることはない.

4. 有限状態モデル

図 9 に SASEBO-AES の状態遷移図を示す. FPGA2 はシリアルポートと FPGA1 を結ぶ結線情報のみを有し, ステートマシーンを持たないため, この図は AES 暗号回路とシリアルインタフェース回路を含む FPGA1 における状態遷移を表したものである. AES 暗号回路はボードのシステムクロックと同じ 24MHz で動作しており, シリアルインタフェース回路はそれを分周したクロック 115.2KHz で動作している.

「S0.電源オフ」状態において, 主電源スイッチ SW1 をオンに, FPGA1 の電源切り替えスイッチ SW3 を INT にすると, 電源用 LED が点灯する. 点灯しない場合は外部電源の不具合もしくは内部レギュレータの損傷などが考えられ, SASEBO-AES は電気的に動作しない. 電源が入ると自動的に状態「S1.コンフィグ＆完全性テスト」に遷移し, FPGA1 のコンフィグレーションのために EEPROM1 から回路設計情報が 16 ビットの CRC による完全性テストを受けながらロードされる. その結果, エラーがなければコンフィグレーション成功を示す LED が点灯する. その後, AES 暗号回路とシリアルインタフェース回路はそれぞれ自動的に「S2.アルゴリズムテスト」と「T1.コマンド入力待ち」に進む. なお, Configuration Switch 押下(状態遷移図のリセット A)により, 電源がオン中はどの状態にあっても直ちに「S1.コンフィグ&完全性テスト」に移行する. コンフィグレーション中にエラーがあると, 「S10.ハードウェアエラー」状態となり, 電源オフか図 8 のコンフィグレーションスイッチ SW2 押下によるリセット以外は受け付けない. なお, これ以外のいずれの状態にあっても, 電源オフは無条件で実行可能である.

また, 図 6 のシーケンサーリセットスイッチ SW6 押下によるハードウェアリセット(状態遷移図のリセット B)も, 「S0.電源オフ」と「S10.ハードウェアエラー」状態以外の FPGA1 の全てのステートで実行することができる. リセット B の後は FPGA の再コンフィグレーションは行われず, AES 暗号回路は「S2.アルゴリズムテスト」から, シリアルインタフェース回路は「T1.コマンド入力待ち」からのリスタートとなる. さらに, AES 暗号回路が「S3.コマンド＆データ入力待ち」状態にあるとき, ユーザはシリ

アルインタフェース回路を通してコマンドによるソフトウェアリセット(状態遷移図のリセット C)を実行することができる. その後はリセット B と同じく「S2.アルゴリズムテスト」が開始される.

AES 暗号回路はアルゴリズムテスト中にエラーが見つかったならば, 電源オフ, 再コンフィグレーション(リセット A), ハードウェア/ソフトウェアリセット(リセット B/C) 以外は受け付けない「S9.停止」状態となる. このときエラーの発生を示す LED が点灯する. また, 鍵比較と鍵テスト時にエラーが発生した場合も,「S9.停止」状態となる. この状態においてもシリアルインタフェース回路は動作しているが, 鍵設定, 暗号化及び復号のコマンドを受け取っても, AES 回路が停止しているため, そのエラー状態だけを返すことになる.

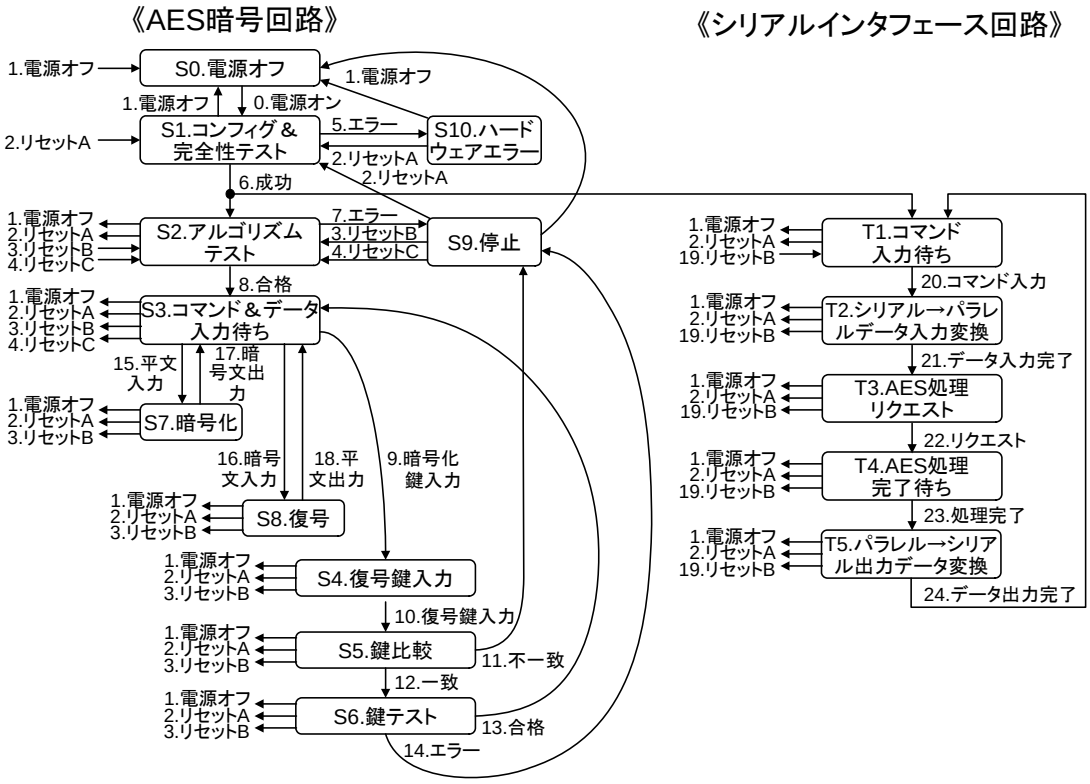


図9 SASEBO-AESの状態遷移図

以下に AES 暗号回路とシリアルインタフェース回路の各状態 S0~S11 及び T1~T16 の説明を記す.

●AES 暗号処理回路

S0. 電源オフ

暗号回路設計情報はそれぞれ EEPROM1 内部に保持されており, FPGA1 には回路設計情報やデータが何もロードされていない状態. 電源オンによって FPGA1 および FPGA2 は「S1.コンフィグ&完全性テスト」に, 自動的に遷移する.

S1. コンフィグ&完全性テスト

EEPROM1 内のコードに対する CRC チェックによる完全性テストと同時に FPGA1 に暗号回路設計情報がロードされる. ロードに成功すると対応する LED が点灯し「S2.アルゴリズムテスト」に自動的に移行する. 何らかのハードウェアエラーが発生すると,「S10.ハードウェアエラー」状態となる. (EEPROM2 と FPGA2 に対しても同様の処理が行われる)

S2. アルゴリズムテスト

電源オンまたは電源オン状態でコンフィグレーションスイッチ(図 8 の SW2)が押されて(リセット A) FPGA1 のコンフィグレーションが成功すると，AES 暗号回路が自動的にアルゴリズムテストを開始する．また SASEBO-AES 起動後に，ハードウェアリセット(図 6 のシーケンサーリセットスイッチ SW6)の押下（リセット B）あるいは 136 ビット入力データの先頭ビットを 1 にセットすることによるソフトウェアリセットリセット(リセット C)によってもアルゴリズムテストが開始される．テスト用の鍵とデータは事前に設定され EEPROM1 に保持されているものが使用される．テスト中に期待されるデータが生成されない場合はエラーとなり，「S9.停止」状態となる．また，テストに合格すると，「S3.コマンド＆データ入力待ち」状態に自動的に遷移する．

S3. コマンド＆データ入力待ち

暗号化鍵入力コマンドとともに鍵が入力されると，「S4.復号鍵入力」状態へ，また暗号化コマンドとともに平文が入力されると「S7.暗号化」状態へ，復号コマンドとともに暗号文が入力されると「S8.復号」状態へ遷移する．ただし，暗号化鍵と復号鍵がセットされていないときには，平文あるいは暗号文が入力されても S7 と S8 へは遷移せずに，この状態にとどまる．またこの状態にあるとき，ステータスの読み出し，そして暗号化及び復号によって暗号文または平文が生成されていれば，シリアルインタフェース回路を通してそれらを読み出すことができる．

S4. 復号鍵入力

SASEBO-AES は共通鍵暗号 AES を用いているので暗号化と復号で同じ秘密鍵を使用する．しかし，CSP である秘密鍵が FPGA 内部の鍵レジスタの故障などにより誤った処理が行われるのを避けるため，S3 の暗号化鍵入力に続いて同じ鍵を復号鍵として入力し，それらによって正しく暗号化→復号が行われるかどうかをこの後でチェックする．AES 暗号回路の制御回路は復号鍵が入力されると，復号回路内の鍵レジスタにセットした後に次の状態「S5.の鍵比較」に遷移するように設計されている．しかし，シリアルインタフェース回路は外部から入力された一つの秘密鍵を，暗号化鍵及び復号鍵として AES 暗号回路に連続して入力するため，実際には S4 で入力待ちとなって止まることはなく，S5 へすぐに遷移する．

S5. 鍵比較

「S3.コマンド＆データ入力待ち」状態と「S4.復号鍵入力」状態において入力され，2 つのレジスタにセットされた暗号化鍵と復号鍵が比較され，両者が一致していれば「S6.鍵テスト」へ，異なっていれば「S9.停止」状態となる．

S6. 鍵テスト

暗号化鍵と復号鍵が一致したときに，暗号化鍵で 0 データを暗号化し，その暗号文を復号鍵で復号して元の平文 0 に戻るかどうかをチェックする．処理が正しく行われれば「S3.コマンド＆データ入力待ち」状態へ，また平文 0 に戻らなければ「9.停止」状態に遷移する．

S7. 暗号化

暗号化回路が暗号化鍵を用いて平文を処理し，処理が終了すると暗号文を出力して「S3.コマンド＆データ入力待ち」に戻る．

S8. 復号

復号回路が復号鍵を用いて暗号文を処理し，処理が終了すると平文を出力して「S3.コマンド＆データ入力待ち」状態に戻る．

S9. 停止

「S2.アルゴリズムテスト」または「S6.鍵テスト」の結果が期待値と一致しないか，「5.鍵比較」で暗号化鍵と復号鍵が不一致のときに，この状態となる．リセットスイッチを押すことで,「S2.アルゴリズムテスト」を再始動することができる．

S10. ハードウェアエラー

電源オン後，FPGA1 のコンフィグレーションに失敗すると，この状態となる．コンフィグレーションスイッチ押下による回路コードの再ロードまたは電源オフ以外は受け付けない．

表 5 AES 暗号処理回路の状態遷移のトリガとなる入力と遷移後の出力

	現在の状態	入力	出力	次の状態
0	S0.電源オフ	電源オン	電源用 LED 点灯	S1.コンフィグ＆完全性テスト（FPGA1 側）
1	S0 以外の全ての状態	電源オフ	全電力遮断．電源用 LED 消灯	S0.電源オフ
2	S0，S1 以外の全ての状態	コンフィグレーションスイッチ SW2 押下	FPGA1 のコンフィグレーション用 LED D4 点灯せず	S1.コンフィグ＆完全性テスト
3	S0，S1，S2，S10 以外の全ての状態	Sequencer Reset スイッチ押下	アルゴリズムテスト開始	S2.アルゴリズムテスト
4	S3.コマンド＆データ入力待ち及び S9.停止	ソフトウェア Reset コマンド発行	アルゴリズムテスト開始	S2.アルゴリズムテスト
5	S1.コンフィグ＆完全性テスト	コンフィグレーション失敗	FPGA1 のコンフィグレーション用 LED D4 点灯せず	S10.ハードウェアエラー
6	S1.コンフィグ＆完全性テスト	コンフィグレーション成功	FPGA1 のコンフィグレーション用 LED D4 点灯	S2.アルゴリズムテスト
7	S2.アルゴリズムテスト	アルゴリズムテスト失敗	アルゴリズムテスト失敗を示すステータス LED D5 と D8 点灯	S9.停止
8	S2.アルゴリズムテスト	アルゴリズムテスト成功	ステータス LED D12 点灯	S3 コマンド＆データ入力待ち
9	S3.コマンド＆データ入力待ち	暗号化鍵入力	暗号化鍵レジスタをセット	S4.復号鍵入力
10	S4.復号鍵入力	復号鍵入力（シリアルインタフェース回路が自動的に暗号化鍵を復号鍵にコピーして入力）	復号鍵レジスタをセット	S5.鍵比較
11	S5.鍵比較	鍵不一致	鍵状態レジスタ「不一致」 鍵比較失敗を示すステータス LED D5 と D7 点灯 LED D12 消灯	S9.停止

12	S5.鍵比較	鍵一致	鍵状態レジスタ「一致」	S6.鍵テスト
13	S6.鍵テスト	鍵テストが失敗	鍵状態レジスタ「無効」 鍵テスト失敗を示すステータスLED D5とD6 点灯 LED D12 消灯	S9.停止
14	S6.鍵テスト	鍵テスト成功	鍵状態レジスタ「有効」 正常状態を示すステータスLED D12 点灯	S3.コマンド＆データ入力待ち
15	S3.コマンド＆データ入力待ち	鍵がセットされている状態で平文入力	暗号化開始	S7.暗号化
16	S3.コマンド＆データ入力待ち	鍵がセットされている状態で暗号文入力	復号開始	S8.復号
17	S7.暗号化	暗号化終了	データ有効フラグをセット	S3.コマンド＆データ入力待ち
18	S8.復号	復号終了	データ有効フラグをセット	S3.コマンド＆データ入力待ち

●シリアルインタフェース回路

S0. 電源オフ

インタフェース回路コードは EEPROM1 内部に保持されており, FPGA1 には回路設計情報が何もロードされていない状態. 電源オンによってFPGA1 およびFPGA2 は「S1.コンフィグ&完全性テスト」に, 遷移する.

S1 .コンフィグ&完全性テスト

EEPROM2 内のコードに対する CRC チェックと同時に FPGA2 に暗号回路設計情報がロードされる. ロードに成功すると対応する LED が点灯し「T1.コマンド入力待ち」に移行する. 何らかのハードウェアエラーが発生すると,「S10.ハードウェアエラー」状態となる. (EEPROM1 と FPGA1 に対しても同様の処理が行われる)

T1. コマンド入力待ち

FPGA1 のコンフィグレーション終了後または, Sequencer Reset スイッチ押下後に, この状態に移行する. ソフトウェアリセット(リセット C)は AES 暗号回路のためのものであり, シリアルインタフェース回路がそれによってリセットされることはない. またコマンドパケットは 8 ビット(内上位 4 ビットのみ使用)で, 全て AES 暗号回路の制御用である. シリアルインタフェース回路はRS232C シリアルポートとAES 暗号回路をつなぐためのプロトコル変換回路として機能している. シリアルポートから 8 ビットのコマンドパケットを受け取ると,「T2.シリアル→パラレルデータ入力変換」状態に遷移する.

T2. シリアル→パラレルデータ入力変換

AES 暗号回路は鍵, 平文, 暗号文を 128 ビットブロックで受け取るため, シリアルインタフェースから 1 ビットずつ入力されるデータはひとまず内部の 128 ビットバッファに蓄積される. AES にソフトウェアリセットをかける場合にはデータは不要であるが, インタフェースを簡単にするた

め，このときも 8 ビットのコマンドに続いてダミーのデータ 128 ビットを受け取る．データが 128 ビットそろった時点で，「T3.AES 処理リクエスト」状態に移行する．

T3. AES 処理リクエスト

128 ビットバッファに溜まっているデータと共に，AES 暗号回路に各種コマンドを印加する．このとき AES 回路にエラーがなく「S7.データ入力待ち」状態にあるかどうかのチェックは行わない．シリアルインタフェース回路の動作クロックは AES 回路のおよそ 1/200 であり，シリアルデータ入力に百数十クロックを要するため，AES 回路が正常動作しているのであれば，リクエストをかける時には既に「S7.データ入力待ち」状態に移行しているからである．またエラー状態であれば，AES 回路にリクエストをかけても何の処理も実行されず，ユーザはデータの前に出力されるステータス情報でエラーの発生を知ることができる．なお，AES 回路におけるエラーの発生は LED にも表示される．リクエスト出力処理が完了すると，「T4.AES 処理完了待ち」状態に移行する．

T4. AES 処理完了待ち

AES 回路の処理が終了したことを示すステータスを確認したならば，「T5.パラレル→シリアルデータ出力変換」状態に移行する．

T5. パラレル→シリアルデータ出力変換

AES 回路が出力する処理結果 128 ビットとステータス 8 ビットをシリアルインタフェース回路内の 136 ビットバッファに転送し，1 ビットずつ RS232C ポートから出力する．ステータスの上位 4 ビットは「T1.コマンド入力待ち」で入力したコマンドそのままで，下位 4 ビットが実際のステータスとなる．リセットや鍵入力コマンドでは出力すべき処理結果はないが，そのときもダミーのデータを 128 ビット出力する．その後，「T1.コマンド入力待ち」状態に移り，次のコマンドの受付が許可される．

表 6 シリアルインタフェース回路の状態遷移のトリガとなる入力と遷移後の出力

	現在の状態	入力	出力	次の状態
6	S1.コンフィグ＆完全性テスト	コンフィグレーション成功	FPGA2 のコンフィグレーション用 LED 点灯	T1.コマンド入力待ち
19	T1 以外の全ての状態	Sequencer Reset スイッチ押下	処理の停止	T1.コマンド入力待ち
20	T1.コマンド入力待ち	8 ビットコマンド入力	データ入力開始	T2．シリアル→パラレルデータ入力変換
21	T2．シリアル→パラレルデータ入力変換	128 ビットデータ入力完了	リクエスト出力処理開始	T3．AES 処理リクエスト
22	T3．AES 処理リクエスト	リクエスト出力処理完了	リクエスト出力	T4．AES 処理完了待ち
23	T4．AES 処理完了待ち	AES 暗号回路の処理完了	ステータス及びデータ出力開始	T5．パラレル→シリアルデータ出力変換
24	T5．パラレル→シリアルデータ出力変換	データ出力完了	8 ビットステータス＋128 ビットデータ出力	T1.コマンド入力待ち

5. 物理セキュリティ

SASEBO-AES の主要コンポーネントで，暗号機能を有する FPGA1(XC2VP7)とコンフィギュレーション用 EEPROM1(XCF08PVOG48C)，そして FPGA1 と RS232C ポートを結ぶ FPGA2(XC2VP30)とコンフィギュレーション用 EEPROM2(XCF16PVOG48C)は不透明な製品レベルのパッケージで封印されている．二つの LSI はカバーでは囲まれていない．また EEPROM1 及び EEPROM2 に記録されている回路設計情報の改ざんを防ぐために，書込み端子である JTAG 端子ははがすと痕跡の残るシールによって封止されている．ユーザ及びクリプトオフィサは，モジュールの使用前に，ボード上の 2 つの EEPROM(XCF08P と XCR16P)の回路設計情報が書き換えられていないことを，改ざん防止シールの状態で確認する．

6. 動作環境

SASEBO-AES は汎用としてのインタフェースを有する AES 暗号アクセラレータハードウェアモジュールであるため，この要件は試験対象外である．

7. 暗号鍵管理

SASEBO-AES は「3.3 CSP の定義とアクセス」で述べたように，128 ビットの AES 秘密鍵を使用する．秘密鍵はユーザによって暗号化されない平文の状態で FPGA 内の秘密鍵レジスタに書き込まれる．一旦書き込まれた鍵は外部に読み出すことはできない．秘密鍵はユーザがいつでも書き換えることが可能である．また，リセットによってゼロ化することもできる．

8. 自己テスト

SASEBO-AES は CRC による回路設計情報の「完全性テスト」(図 9 の状態 S1)，内部で設定したデータを用いた AES 回路の「アルゴリズムテスト」(図 9 の状態 S2)，入力した鍵が正しく設定されていることをチェックする「鍵テスト」（図 9 の状態 S3~S6）の 3 つのテストが適宜行われ，その結果に応じてステータスレジスタ及びやステータス LED がセットされる．

電源投入により FPGA1 と FPGA2 には，それぞれ EEPROM1 及び EEPROM2 から AES 回路設計情報及びシリアルインタフェース回路設計情報がロードされる．それぞれの回路設計情報は事前に CRC16 によって計算されたエラー検出コードが付加されており，各 FPGA にロードされるときに自動的に CRC16 を除いた部分から再度エラー検出コードが計算され，最後にロードされる事前計算の値との比較を行うことで完全性テストが実行される．設計情報にエラーが検出された場合は，コンフィグレーションスイッチ SW2 の押下か，または電源オフしか受け付けないエラー状態となる．コンフィグレーションが成功すると，図 7 に示したように LED D4 と D14 が点灯する．その後，AES 回路では自動的に鍵を変えながら暗号化と復号を繰り返すアルゴリズムテストが開始される．この「完全性テスト」と「アルゴリズムテスト」を合わせた「自己テスト」は，電源オフオンあるいはコンフィグレーションスイッチ SW2 の押下によっていつでも明示的に実行することが可能である．

図 9 の状態 S2 において実行されるアルゴリズムテストの手順を図 10 に示す．ここでは，鍵と平文を所定の値に初期化した後に暗号化→復号でデータが復元できるかどうかの検査を，鍵を 1 ビットずつ右巡回シフトしながら 128 回繰り返す．初回 (鍵の最下位バイトが Key[7:0]=f) だけは，

FIPS-197「ADVANCED ENCRYPTION STANDARD (AES)」の Appendix C.1 でサンプルデータとして使用されている鍵，平文，暗号文の既知のデータを用いて検査を行うが，2 回目以降の繰り返しにおいて，平文入力は前回の暗号文出力を用いる．128 パターンの鍵全てに対して暗号化・復号・比較という一連のテストが成功すると，127 回の巡回シフトによって Key[8:1]=f となるので，このときテストのループを終了し，図 10 の「Pass」に抜ける．テストが成功ならば図 6 に示したようにステータス LED の D12 が点灯し，また失敗した場合は D5 と D8 が点灯し，電源オフ，再コンフィグレーション，ソフトウェア/ハードウェアリセットしか受け付けない状態となる．

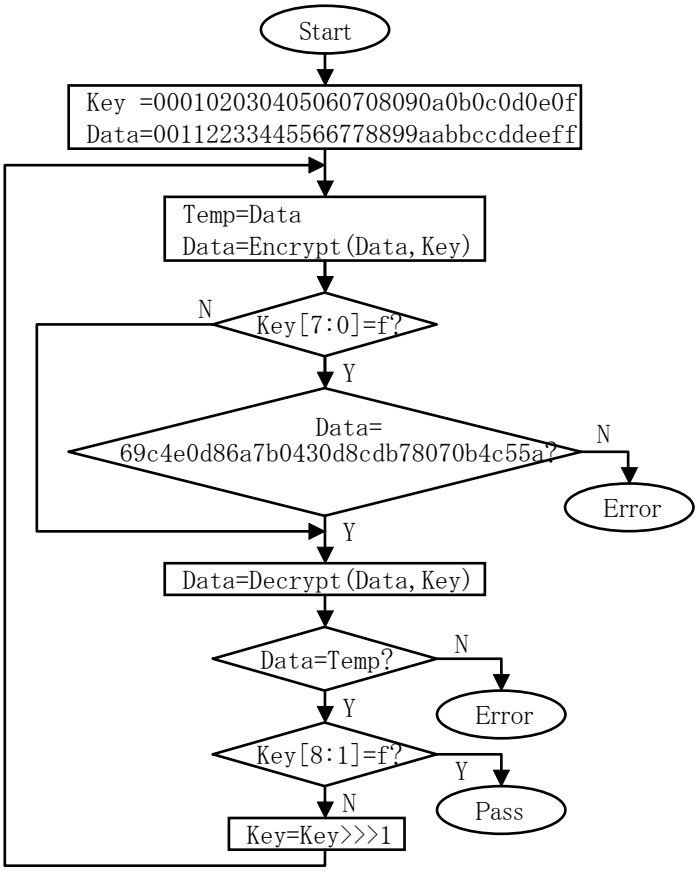


図10　SASEBO-AESのアルゴリズムテスト

128 回の暗号化・復号に全てパスしたならば，図 9 で「S3.コマンド＆データ入力待ち」となり，暗号化鍵と復号鍵がシリアルインタフェース回路から続けて入力されると鍵テストが実行される．シリアルインタフェース回路は同一の鍵を暗号化鍵と復号鍵として AES ハードウェアマクロに 2 度入力するが，図 9 ではその同一の鍵に対して「S5.鍵比較」が実行されている．これは暗号化と復号のレジスタが故障していた場合に，誤った鍵で処理が行われることを防ぐためである．鍵比較の結果，不一致であれば LED　D5 と D7 が点灯，D12 が消灯し「S9.停止」状態となる．2 つの鍵が一致したならばD12 は点灯状態となり，「S6.鍵テスト」に移行し，暗号化回路モジュールが 0 データを暗号化し，それに続いて復号回路モジュールは暗号化回路が出力した暗号文を復号する．その復号の結果が 0 になれば,それぞれのモジュールに正しく鍵が設定され，正しく動作していることを示すステータス LED D12 は点灯した状態を維持する．また，このテストに失敗するとステータス LED D5 と D6 が点灯，D12 が消灯し「S9.停止」状態となる．

鍵テストに合格すると自動的に「S3.コマンド＆データ入力待ち」状態に移り，通常の暗号化，復号，そして新たな鍵の設定が可能となる．

9. 設計保証

9．1 構成管理

SASEBO-AESの暗号境界内の暗号モジュールに関連する構成要素を図11及び以下に列挙する. これらはユーザ及びクリプトオフィサに全て公開される.

- SASEBO FPGA ボード Side-channel Attack Standard Evaluation Board 3-93961-1
- FPGA1 に実装される AES 暗号回路と RS232C インタフェース回路及び FPGA2 の結線情報を記述した Verilog-HDL ソースコード
- 上記 Verilog-HDL ソースコードを FPGA1 及び FPGA2 にマッピングするためのピンアサイン情報（ucf ファイル）
- 上記回路情報を EEPROM1 及び EEPROM2 に書き込める形にしたバイナリファイル FPGA1_V1.1.mcs 及び FPGA2_V1.0.mcs
- SASEBO-AES 暗号 FPGA ボード FIPS140-2 Non-Proprietary Security Policy Version 1.4 2007 年 11 月 12 日 （本ドキュメント）
- SASEBO-AES 暗号 FPGA ボード仕様書 Version 1.3 2007 年 11 月 12 日
- サイドチャネル攻撃用標準評価基板仕様書 第 1 版 2007 年 3 月 30 日

SASABO FPGA ボードの品名・品番「Side-channel Attack Standard Evaluation Board 3-93961-1」はボード上に印刷されていることで確認できる. FPGA1 に実装される Verilog-HDL のソースコード（.v 及び.ucf ファイル）のバージョン管理は, コード内のヘッダー部分に記述された日付及びバージョン番号により管理されている. mcfファイルはファイル名のVx.xがバージョン番号を示している, また, 各ドキュメントの管理は日付とバージョン番号によって行われている.

図11 SASEBO-AESの構成

9．2 配付及び運用

SASEBO-AES はボード上の EEPROM に記録された回路設計情報の改ざんを防止するために, その情報の入力端子である JTAG 端子にはがすと痕跡の残るシールを貼っている. クリプトオフィサはこのシールがはがされていないことを確認した後,「SASEBO-AES 暗号 FPGA ボード仕様書」に従って初期設定を行うことで, 暗号化・復号が実行可能となる.

10. その他の攻撃の対処

SASEBO-AES はその他の攻撃に対する対策は施されていない.

11. 参考文献

[1] NIST, “Advanced Encryption Standard (AES) FIPS Publication 197,” Nov. 2001.
http://csrc.nist.gov/ publications/fips/fips197/ fips-197.pdf
[2] The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)
http://csrc.nist.gov/cryptval/aes/AESAVS.pdf