SASEBO-GII-AES 暗号 FPGA ボード

JIS X 19790 Non-Proprietary Security Policy

[第 0.96 版]

2012 年 2 月 8 日

（独）産業技術総合研究所
情報セキュリティ研究センター

目次

1. モジュール仕様

1.1 概要

SASEBO-GII-AES は，サイドチャネル攻撃標準評価プラットフォーム SASEBO-GII（Side Channel Attack Standard Evaluation Board – GII）の FPGA（Field Programmable Gate Array）上に 128 ビット共通鍵ブロック暗号である AES (Advanced Encryption Standard)回路を実装したマルチチップ組み込み型の暗号ハードウェアモジュールである．SASEBO-GII-AES は AES 暗号回路を実装する Virtex-5 LX30 または LX50(以下 FPGA1)と，制御回路用の Spartan-3A(以下 FPGA2)の 2 つの Xilinx 社製 FPGA を搭載している．図 1 と図 2 に SASEBO-GII-AES の概観とブロック図を示す．

図 2 で灰色に塗られた部分は，SASEBO-GII-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 FPGA1 には AES 暗号回路と USB インタフェース回路が，FPGA2 には信号線のドライバーが実装される．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 SPI-ROM である SPI-ROM1 および SPI-ROM2 から，ハードウェア設計情報が自動的にロードされる．ボードへの電力は USB ポートを通じて 5．0V が供給され，そこからボード内部で必要な 3.3V/2.5V/1.2V/1.0V の各電圧がレギュレータによって生成される．USB コントローラ(FT2232D)には 6MHz，FPGA2 には 24MHz のクロックが供給され，FPGA1 は FPGA2 を経由して 24MHz クロックが入力される．

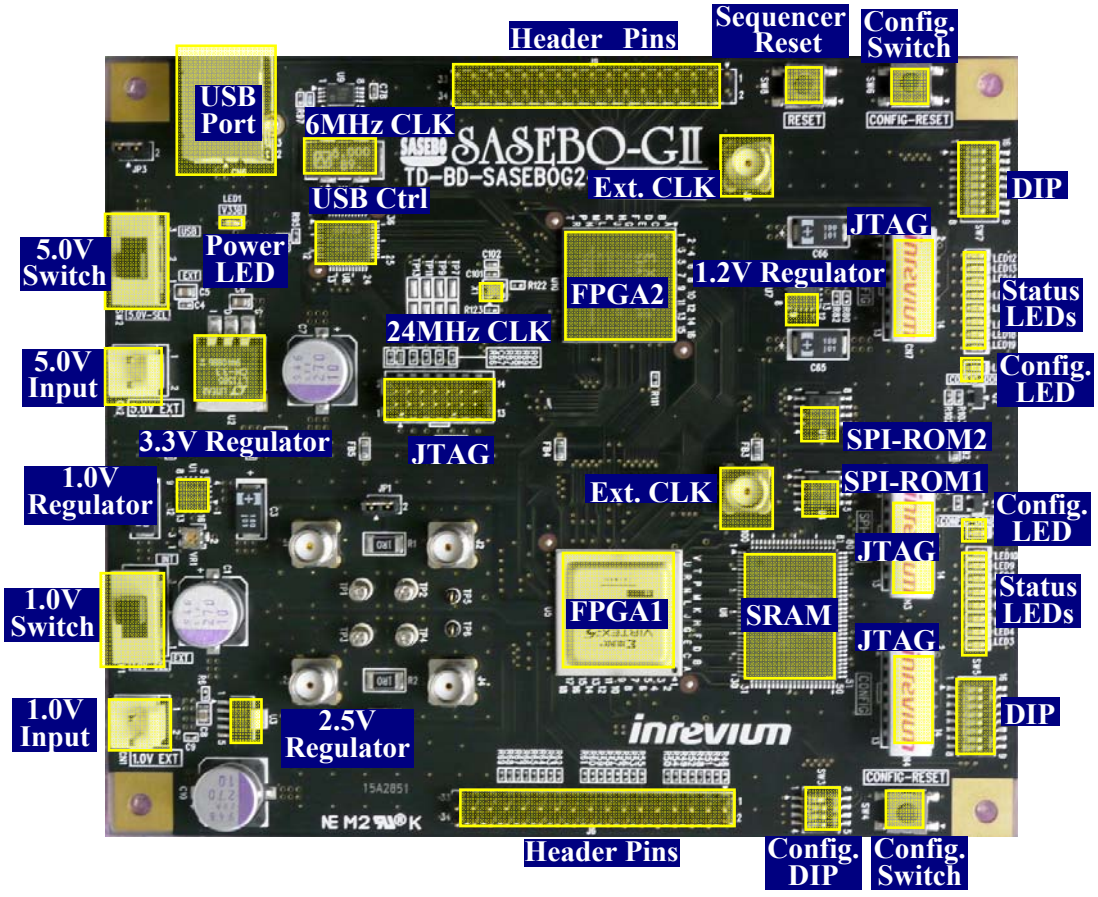

図 1　SASEBO-GII-AES の概観

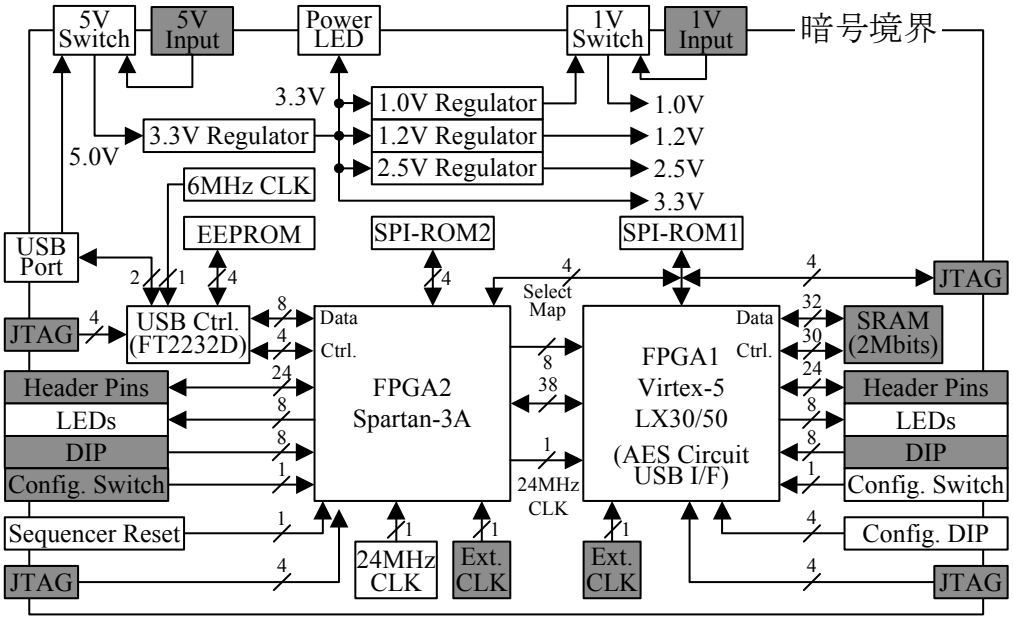

図 2　SASEBO-GII-AES のブロック図

暗号境界は図 1 および図 2 のボード全体で，主要コンポーネントは FPGA1 と FPGA2，そして各 FPGA に実装される回路設計情報を保持する SPI-ROM1 と SPI-ROM2 である．SASEBO-GII-AES 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 SASEBO-GII 仕様書 Version 1.0」で提供される．SPI-ROM1 内には AES 暗号回路，そして SPI-ROM1は USB インタフェースおよび AES 暗号回路のコントローラの回路設計情報を保持している．これらの回路設計情報の正当性の検証手順は別冊の「SASEBO-GII-AES 暗号 FPGA ボード仕様書 Version 1.0」の「4.2 コンフィギュレーションコードの正当性検証」を参照のこと．

FPGA1 と FPGA2 の間は，38 ビットの双方向データ用バスで接続されており，そのうち 8 本がデータ入出力用(FPGA2⇔FPGA1)，そして，残り 30 本のうち 4 本が制御用に使用される．外部の PC からは，FPGA1 の USB インタフェースを通じて FPGA1 の AES 暗号回路の対しコマンド/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 のボードの右上にあるシーケンサーリセットスイッチ SW8 または右下のコンフィグレーションスイッチ SW4 のいずれかを押すか，USB ポートを通じて 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．鍵をセットした直後には，読みだすことはできないがインタフェース回路のバッファにも鍵が残っている場合があるため，鍵が残っているかいないかにかかわらず，これらのバッファも全て上記のリセット処理と同時にゼロ化される．FPGA1 および FPGA2 には他の入出力デバイスとして，リセットスイッチ，コンフィグレーション用および汎用 I/O 用 DIP スイッチ，LED，ヘッダーピンがある．FPGA2 用コンフィグレーションスイッチ，そして汎用 I/O ポートに接続されている DIP スイッチとヘッダーピンは使用しない．LED はエラー状態を示す外部表示装置としての役割を持つ．電源は USB ポートから 5.0V が供給され，そこから全ての内部電源電圧が作られる．ボード上には 5.0V と 1.0V の外部電源入力ポートがあるが，これらは使用せず，1.0V 切り替え用のスイッチは内部電源側に固定する．5.0V 用スイッチは USB 側と外部電源側でオン/オフ切り替えに使用する．スイッチ，LED および各種ポートの詳細は「2. ポート及びインタフェース」を参照のこと．

SASEBO-GII-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．

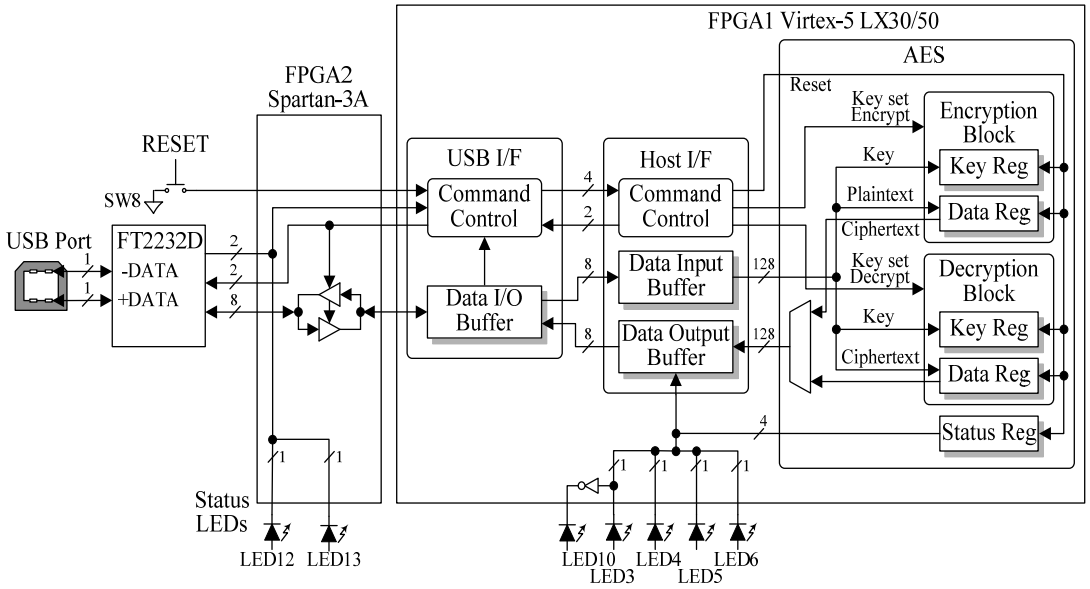

図 3 SASEBO-GII-AES 暗号 FPGA ボードの制御およびデータの流れ

図 3 は，SASEBO-GII-AES において，外部とのデータ入出力，制御入力，ステータス出力の経路の概略を示したものである．USB ポートに接続された PC からは，「2.ポート及びインタフェース」の図 5 に示す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 8 ビットずつ入力される．この信号は USB コントローラ FT2232D 経由で FPGA2 に渡され，そのまま通過して FPGA1 に入力される．そこで FPGA1 の USB インタフェース回路によって USB コントローラからコマンドとデータが読み取られ．さらに FPGA1 のホストインタフェース回路を通じて，鍵は AES 暗号回路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および復号ブロックの内部でのみ使用され，そこに保持されている唯一の CSP である鍵が外部に出力されるパスは存在しない．また，レジスタの内容は電源オフ，コマンドによるソフトウェアリセット，あるいは図 1 右上のシーケンサーリセットスイッチ SW8 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（復号）のコマンドが発行されると暗号化（復号）ブロックで処理が行われ，データレジスタに暗号文（平文）が得られた後に，図 6 の出力データフォーマットに従って入力とは逆向きの経路で USB ポートから PC へと結果が返される．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．なお 4 ビットのステータス情報は図 4 のように LED3~LED6 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 LED10 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-GII-AES-1.0 である．

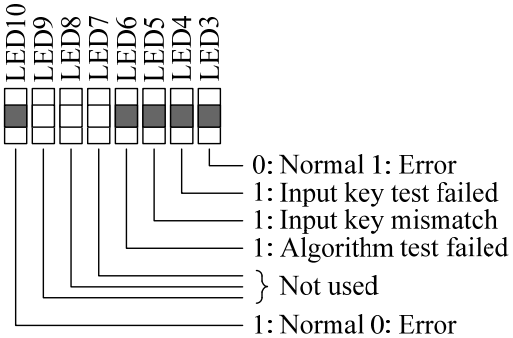

図 4 ステータス LED の意味

1.2 セキュリティレベル

SASEBO-GII-AES モジュールは表 1 に示した JIS X 19790 のセキュリティレベル 1 の要件を満たしている.

表 1 SASEBO-GII-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-GII-AES モジュールは, 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 (Electronic 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, ISO/IEC 18033-3 鍵長 128 ビット ECB (Electronic Code Book) モード

2. ポート及びインタフェース

表 3 に SASEBO-GII-AES の入出力インタフェースを, また図 5~6 にそのインタフェースを通して AES 暗号回路とやりとりされるコマンドおよびデータのフォーマットを示す. 主要なデータ入出力は USB ポートを通じて外部に接続された PC から制御する. 鍵およびデータの入出力, 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 6 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 暗号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 暗号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 6 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．なお，データ出力フォーマットのビット 4 は，アルゴリズムテストに入るときにセットされるので，エラーがあるかどうか確定していないテスト中もそれに応じて LED3 が点灯することになる．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 7 右側に示したように LED3~LED6 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 LED10 が発光する．

図 8 右端のコンフィグレーション用 DIP スイッチ SW3 は FPGA1 のコンフィグレーションのモードを切り替えるもので，ビット 1 を off（図 8 の下側），2~3 を on（上側）に設定することで（ビット 4 は未使用），SPI-ROM から FPGA1 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 FPGA1 へ回路設計情報は正しくロードされないが，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 および FPGA2 のコンフィグレーションが正常に終了すると，図 8 のように LED2（FPGA1 用）および LED11（FPGA2 用）が点灯し，FPGA1 ではそれに続いて回路機能の自己テストが行われ，正常であれば LED10 が点灯する．また，FPGA2 を通して LED12 と LED13 がそれぞれ USB コントローラ FT2232D の受信 FIFO 可能を示す RXF#と送信 FIFO への書き込みを許可する TXE#に接続され，書き込み許可を示す LED13 が点灯する．USB コントローラがデータを受信すると LED12 が点灯し，受信 FIFO の読み出しが可能となる．処理に対応して LED12 と LED13 が適宜点灯するが，処理は一瞬で完了するため，実際には LED13 が常時点灯している状態だけが目視で認識されることになる．

図 8 の両端にはコンフィグレーションスイッチ SW4（FPGA1 用）および SW6（FPGA2 用）があるが，SW6 は使用しない．なお，SW6 を押してしまった場合は，電源を再投入して再起動しなければならない．オペレータは電源オン以外にも SW4 の押下による再コンフィグレーションで，FPGA1 の自己テストを実行することができる．また図 8 左下のリセットスイッチ SW8 はシーケンサーのリセット用で，これの押下によっても FPGA1 と FPGA2 のシーケンサーが初期状態にリセットされ，自己テストが実行される．このとき，両 FPGA の再コンフィグレーションは行われない．

なお，ヘッダーピンおよび DIP スイッチ SW5 と SW7 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．

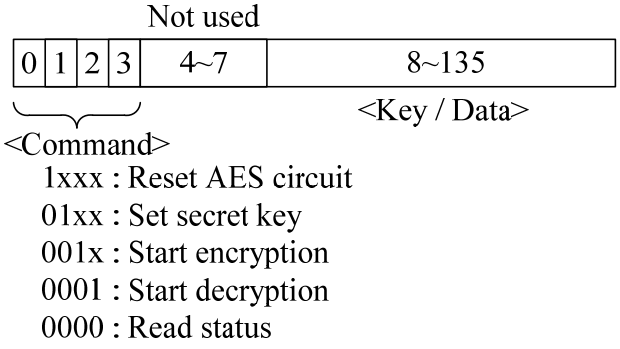

図 5　入力データフォーマット

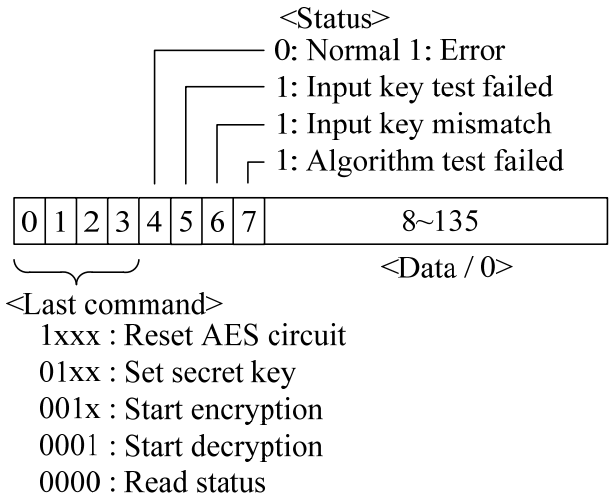

図 6　出力データフォーマット

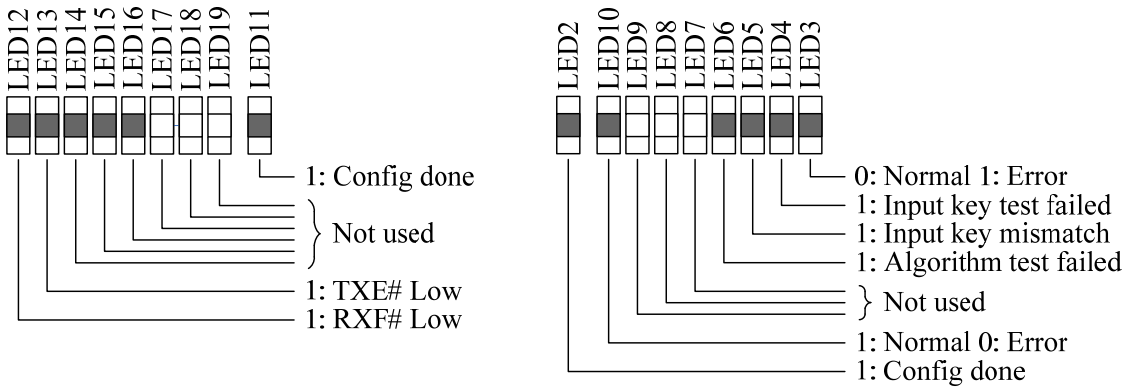

図 7　ステータス LED の意味

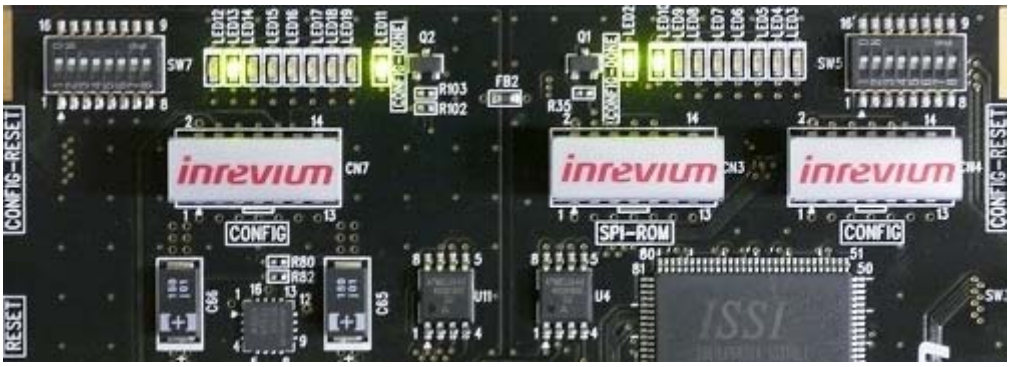

図 8　パワーアップ自己テスト正常終了時の状態

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	USB 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ビットのデータを入力する.
データ出力	USB 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)および暗号文/平文(128ビット)が, このポートから出力される.
制御入力	USB 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 および FPGA2 は, 回路設計情報をSPI-ROM1およびSPI-ROM2からそれぞれ再ロードするコンフィグレーションスイッチ SW4 およびSW6を有する. SW4を押すとFPGA1で回路設計情報のCRCエラーチェックが行われ, 正しくコンフィグレーションが行われると, AES 暗号回路でアルゴリズムテストが実行される. SW6の押下時は FPGA2 が正しくコンフィグレーションされた場合でも, ボードの状態が不定となるため, FPGA2 の再コンフィグレーションは電源の再投入によってのみ行うこととする. また, ボードの状態が不定でない場合であれば, いつでもハードウェアリセットスイッチ SW8 を押下することで, FPGA1 と FPGA2 のシーケンサーをリセットすることができる.
状態出力	電源 LED	電源がオンになり, 内部電源レギュレータが稼働するとLED1 が点灯する.
	USB 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.

		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，回路設計情報がFPGA1およびFPGA2に正しくロードされると，図 8 のようにLED2 および LED11 がそれぞれ点灯する．それに続いて，FPGA1でAES暗号回路のアルゴリズムテストが成功すると図 8 のようにステータス LED10 が点灯する．SW4 の押下では，FPGA1 の再コンフィグレーションだけが行われるが，両 FPGA にリセットがかかり，その後の状態に応じて LED が点灯する．またアルゴリズムテストおよび「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．なお，LED3 はエラーが確定していないアルゴリズムテスト中も点灯する． LED3: いずれかのテストにおいてエラー発生 LED4: 入力鍵による暗号化/復号テスト失敗 LED5: 鍵不一致 LED6: アルゴリズムテスト失敗 LED10: 正常状態 USBコントローラの受信FIFOにデータが溜まっている間，LED12 は点灯し，USB コントローラ送信 FIFO に空きがあれば LED13 が点灯するが，各処理は一瞬で終了するため，常にLED12 が消灯，LED13 が点灯しているように見える． LED12：USB 受信データあり LED13：USB 書き込み可
電源入力	USB ポート	USB ポートに供給される 5.0V 電源から，ボード上のレギュレータによって 3.3V，2.5V，1.2V，1.0V が生成され，FPGA1 側とFPGA2 側それぞれに供給される．
	5.0V 電源スイッチ	このスイッチ SW2 を“USB”側にセットすることで，USB ポートから5.0V 電源がボードに供給される．また“EXT”側にセットすることで電源がオフとなる．電源オフからオン状態に切り替えることで，FPGA1 と FPGA2 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 で回路設計情報のエラーチェックが行われ，それに続いて FPGA1 では AES 暗号回路のアルゴリズムテストが実行される．

3. 役割，サービス，及び認証

3.1 役割

SASEBO-GII-AES モジュールは，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，そして状態の取得を，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，その他の役割とメンテナンスインタフェースは

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. コマンドおよび鍵/平文/暗号文の入出力および状態出力は USB ポートを通じて 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-GII-AES モジュールは 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, AES 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.

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および復号回路で鍵のテストが自動的に行われる. また, リセット以外にもこのサービスを用いて 0 データを書き込むことで, 明示的に鍵のゼロ化も可能.
	AES 暗号化・復号	FPGA 内部からのみ参照	USB ポートからの平文または暗号文の入力により処理が開始される. 処理終了後直ちに, 暗号文または平文が, 直前に実行したコマンド 4 ビットおよびエラー状態 4 ビットとともに USB ポートから出力される. AES 鍵設定時には出力すべき暗号文・平文は存在しないが, ダミーの 0 データと上記の 8 ビットデータが. エラー状態の 4 ビットはボード上のステータス LED3~6 にも表示される.
	状態出力	なし	鍵テストとアルゴリズムテスト後のエラー状態を, 図 6 のフォーマット中の 4 ビットで USB ポートから出力する. 同じ 4 ビットの状態はボード上のステータス LED3~6 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	USB 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，AES 暗号回路の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＋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 SW4 を押下することで，SPI-ROM1 に格納された回路設計情報によって FPGA1 の回路が全て再構成され，鍵およ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 SW8 の押下によるリセット．FPGA1 のシーケンサーとレジスタがリセットされ，FPGA1 では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．
	回路設計情報完全性テスト	なし	電源オフ状態からオンにすることにより，各 FPGA のコンフィグレーションと同時に，回路設計情報のエラーチェックが自動的に 32 ビット CRC(FPGA1)および 22 ビット CRC(FPGA2)を用いて行われる．エラーがなければ，引き続きアルゴリズムテストが実行される．

4. 有限状態モデル

図 9 と図 10 にそれぞれ，FPGA1 上の AES 暗号回路および USB インタフェース回路の状態遷移図を示す．両者は共に 24MHz のシステムクロックに同期して動作している．図 9 で各状態から出ている矢印による状態 S0，S1，S2 への遷移は，それぞれ電源をオフ，図 8 左端の FPGA1 用コンフィグレーションスイッチ SW4 押下による再コンフィグレーション（リセット A），シーケンサーリセットスイッチ SW8 押下によるハードウェアリセット（リセット B）によって実行される．また，図 10 の各状態から出ている矢印による状態 S0，S1，T2 への遷移は，それぞれ電源をオフ，コンフィグレーションスイッチ SW4 押下による再コンフィグレーション（リセット A），シーケンサーリセットスイッチ SW8 押下によるハードウェアリセット（リセット B）によって実行される．状態 S0，S1，S11 は 2 つの図で共通である．

5V 電源スイッチ SW2 が“EXT”の「S0.電源オフ」状態から，“USB”側に切り替えオン状態にすると，電源用 LED1 が点灯する．なお，このとき FPGA1 内部コア用電源スイッチ SW1 は“INT”側に設定され，USB ケーブルによって SASEBO-GII-AES は外部 PC に接続されているものとする．LED1 が点灯しない場合は電源ケーブル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-GII-AES は電気的に動作しない．電源が入ると自動的に状態「S1.コンフィグレーション」に遷移し，FPGA1 および FPGA2 のコンフィグレーションのために，それぞれ SPI-ROM1 と SPI-ROM2 から回路設計情報が 32 ビットおよび 22 ビットの CRC 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，図 8 に示したように，コンフィグレーション成功を示す LED2 と LED11 がそれぞれ点灯する．なお FPGA2 は，FPGA1 と入出力ポートを結ぶ配線及びドライバーのみで構成されおり，レジスタやシーケンサーロジックは有していない．その後 FPGA1 において，AES 暗号回路と USB インタフェース回路がそれぞれ自動的に「S3 アルゴリズムテスト」と「T3.コマンド・データ待ち」に進む．なお，コンフィグレーションスイッチの押下により，電源がオンであればどの状態にあっても直ちに「S1.コンフィグレーション」に移行する．コンフィグレーション中にエラーがあると，「S11.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 SW4 押下によるリセット以外は受け付けなくなる．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 8 のシーケンサーリセットスイッチ SW8 押下によるハードウェアリセット（リセット B）は，「S0.電源オフ」「S1.コンフィグレーション」「S2.シーケンサーリセット」「S11.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 暗号回路と USB インタフェース回路はそれぞれ「S2.シーケンサーリセット」および「T2.シーケンサーリセット」からのリスタートとなる．さらに，AES 暗号回路が「S4.コマンド・データ入力待ち」または「S10.暗号回路停止」状態で，USB インタフェース回路が「T3.コマンド・データ入力待ち」状態にあるとき，ユーザはコマンド入力によるソフトウェアリセットを実行することができる．その後は，AES 暗号回路においてリセット B と同じく「S3.アルゴリズムテスト」が開始される．なお，このとき USB インタフェース回路にはリセットはかからない．

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），ハードウェアリセット（リセット B），またはソフトウェアリセット以外は受け付けない「S10.暗号回路停止」状態となる．このときエラーの発生を示す LED6 が点灯する．また，鍵テスト時にエラーが発生した場合も，「S10.暗号回路停止」状態となる．

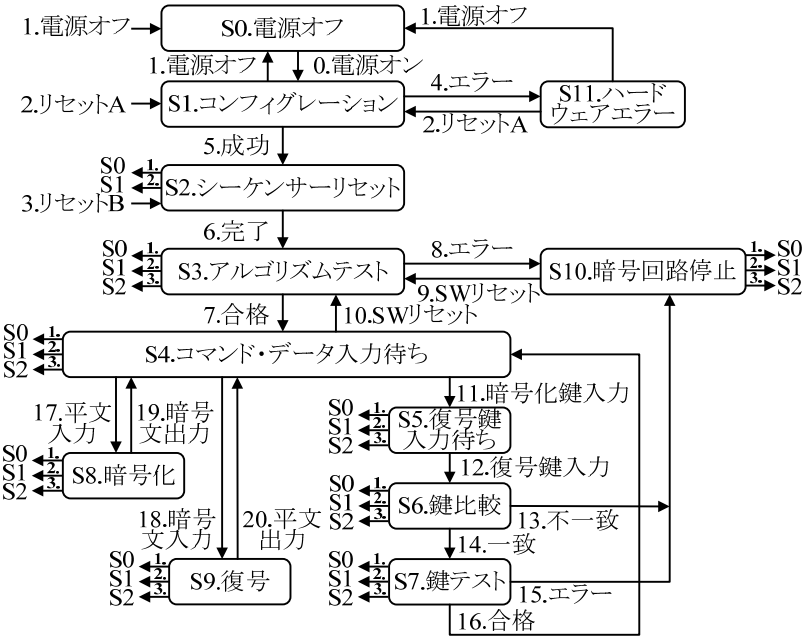

図9 AES暗号回路の状態遷移図

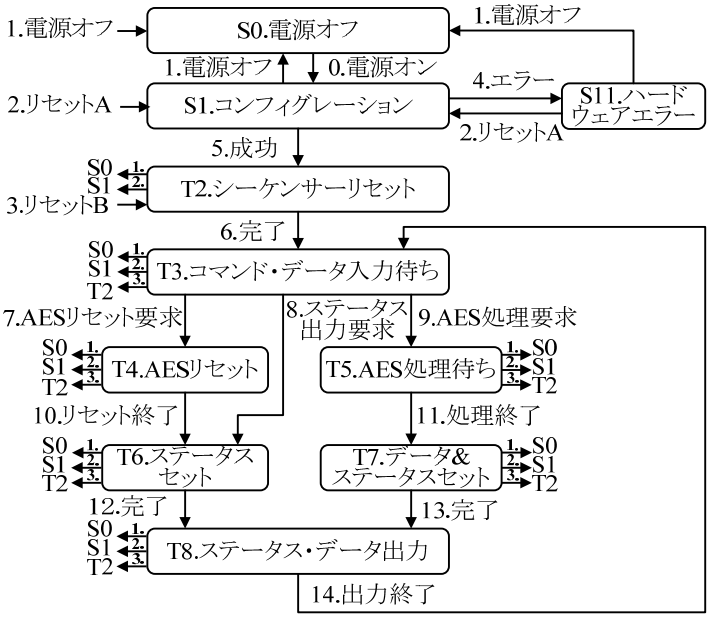

図10 USBインタフェース回路の状態遷移図

以下にAES暗号回路とUSBインタフェース回路の各状態S0~S11およびT2~T8の説明を記す.

●AES暗号回路

S0. 電源オフ

AES暗号回路とUSBインタフェース回路設計情報は, SPI-ROM1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は「S1.コンフィグレーション」に, 自動的に遷移する.

S1. コンフィグレーション

電源スイッチ SW2 を“EXT”から“USB”に切り替えて電源を投入するか，または電源オン状態においてコンフィグレーションスイッチ（図 8 の SW4）が押されると（リセット A）この状態に遷移し， SPI-ROM1 内の回路設計情報に対する CRC テストと同時に，FPGA1 に AES 暗号回路情報および後述の USB インタフェース回路情報がロードされる．ロードに成功すると LED2 が点灯し，FPGA1 の AES 暗号回路は「S2.シーケンサーリセット」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，「S11ハードウェアエラー」状態となる．

S2. シーケンサーリセット

FPGA1 のコンフィグレーション終了，または SW8 の押下によるハードウェアリセット（リセット B）によりこの状態に移行し，FPGA1 のシーケンサーにリセットがかかり，LED10 が消灯，LED3 が点灯する．自動的に「S3.アルゴリズムテスト」に遷移する．

S3. アルゴリズムテスト

「S2.シーケンサーリセット」からの自動遷移，またはコマンド入力によるソフトウェアリセットによってこの状態に遷移し，AES 暗号回路でアルゴリズムテストが実行される．テスト用の鍵とデータは事前に設定され SPI-ROM1 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，「S10.暗号回路停止」状態となる．また，テストに合格すると，LED10 が点灯，LED3 は消灯し「S4.コマンド・データ入力待ち」に自動的に遷移する．

S4. コマンド・データ入力待ち

USB インタフェース回路側からコマンドとデータが転送されるのを待っている状態．暗号化鍵入力コマンドとともに鍵が入力されると，「S5.復号鍵入力待ち」へ，また暗号化コマンドとともに平文が入力されると「S8.暗号化」へ，復号コマンドとともに暗号文が入力されると「S9.復号」へと遷移する．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 S8 と S9 へは遷移せずに，この状態にとどまる．なお， FPGA1 上の USB インタフェース回路からのデータ転送は 1 バイトずつ行われるので，それらが図 5 の 136 ビットのパケットとしてまとまった段階で次の状態へと遷移する．

S5. 復号鍵入力待ち

SASEBO-GII-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，遷移 11 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「S6.鍵比較」に遷移するように設計されている．しかし，USB 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がコピーされ，AES 暗号回路の暗号化鍵レジスタと復号鍵レジスタに順に保存されるため，実際には S5 で入力待ちとなって止まることはなく，S6 へすぐに遷移する．

S6. 鍵比較

「S4.コマンド・データ入力待ち」と「S5.復号鍵入力待ち」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「S7.鍵テスト」へ，異なっていれば「S10.暗号回路停止」となる．

S7. 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 128 ビットの 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「S4.コマンド・データ入力待ち」へ，また平文 0 に戻らなければ「S10.暗号回路停止」に遷移する．

S8. 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USBインタフェース回路に出力して「S4. コマンド・データ入力待ち」に戻る.

S9. 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USBインタフェース回路に出力して「S4.コマンド・データ入力待ち」状態に戻る.

S10. 暗号回路停止

「S3.アルゴリズムテスト」または「S7.鍵テスト」の結果が期待値と一致しないか，「S6.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. シーケンサーリセットスイッチ SW8 の押下によるハードウェアリセットか，USB ケーブルを経由したコマンド入力によるソフトウェアリセットによって，「S3.アルゴリズムテスト」を再始動することができる. なお，この状態で外部から図 5 のフォーマットに従ったコマンド・データが入力されると，AES 暗号回路が停止しているので出力されるデータ部分は無効であるが，図 6 のフォーマットに従ってステータスの出力が行われる.

S11. 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. FPGA1 用コンフィグレーションスイッチ SW4 押下（リセット A）による回路設計情報の再ロード，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 LED1 点灯	S1.コンフィグレーション
1	S0 以外の全ての状態	電源オフ	全電力遮断. 電源用 LED1 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 SW4 押下（リセット A）	FPGA1 のコンフィグレーション用 LED2 点灯せず	S1.コンフィグレーション
3	S0, S1, S2, S11 以外の全ての状態	シーケンサーリセットスイッチ SW8 押下（リセット B）	処理の停止	S2.シーケンサーリセット
4	S1.コンフィグレーション	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 LED2 点灯せず	S11.ハードウェアエラー
5	S1.コンフィグレーション	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 LED2 点灯	S2.シーケンサーリセット
6	S2.シーケンサーリセット	自動遷移	LED3 点灯しリセット完了	S3.アルゴリズムテスト
7	S3.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 LED10 点灯，LED3 消灯	S4 コマンド・データ入力待ち
8	S3.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 LED3 と LED6 点灯	S10.暗号回路停止
9	S10.暗号回路停止	ソフトウェアリセットコマンド発行	アルゴリズムテスト開始	S3.アルゴリズムテスト
10	S4.コマンド・データ	ソフトウェアリセットコ	アルゴリズムテスト開	S3.アルゴリズムテスト

	入力待ち	マンド発行	始	
11	S4.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	S5.復号鍵入力待ち
12	S5.復号鍵入力待ち	復号鍵入力（内部で自動的に暗号化鍵が復号鍵としてコピーされる）	復号鍵レジスタをセット	S6.鍵比較
13	S6.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 LED5 と LED3 点灯 LED10 消灯	S10.暗号回路停止
14	S6.鍵比較	鍵一致	鍵状態レジスタ「一致」	S7.鍵テスト
15	S7.鍵テスト	鍵テスト失敗	鍵状態レジスタ「無効」 鍵テスト失敗を示すステータス LED4 と LED3 点灯 LED10 消灯	S10.暗号回路停止
16	S7.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 LED10 点灯	S4.コマンド・データ入力待ち
17	S4.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	S8.暗号化
18	S4.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	S9.復号
19	S8.暗号化	暗号化終了	暗号文出力.	S4.コマンド・データ入力待ち
20	S9.復号	復号終了	平文出力.	S4.コマンド・データ入力待ち

●USB インタフェース回路

S0. 電源オフ

USB インタフェース回路と AES 暗号回路設計情報は，SPI-ROM1 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 は「S1.コンフィグレーション」に，自動的に遷移する．

S1. コンフィグレーション

電源スイッチ SW2 を“EXT”から“USB”に切り替えて電源を投入するか，または電源オン状態においてコンフィグレーションスイッチ（図 8 の SW4）が押されると（リセット A）この状態に遷移し， SPI-ROM1 内の回路設計情報に対する CRC テストと同時に，FPGA1 に AES 暗号回路情報および USB インタフェース回路情報がロードされる．ロードに成功すると LED2 が点灯し，FPGA1 の USB インタフェース回路「T2.シーケンサーリセット」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，「S11.ハードウェアエラー」状態となる．

T2. シーケンサーリセット

FPGA2 のコンフィグレーション終了後，または図 8 のシーケンサーリセットスイッチ SW8 が押されてハードウェアリセット（リセット B）がかかるとこの状態に遷移する．シーケンサーのリセット後，自動的に「T3.コマンド・データ入力待ち」に遷移する．

T3. コマンド・データ入力待ち

シーケンサーのリセットによって回路が初期状態となり，PC からの USB 経由によるコマンド・データ入力および FPGA1 上の AES 暗号回路に対するステータス・データ読出し要求を受け付けるようになる．PC からリセットコマンドを受けると「T4.AES リセット」へ，ダミーのデータとともにステータス読出し要求があると「T6.ステータスセット」へ，鍵またはデータとともに AES 暗号回路での処理要求があると「T5.AES 処理待ち」へ遷移する．

T4. AES リセット

ソフトウェアリセットが AES 暗号回路で終了するのを待つ．リセットが終了すると「T6.ステータスセット」状態となる．

T5. AES 処理待ち

鍵セット，または暗号化・復号処理が AES 暗号回路で終了するのを待つ．処理に先立ち，鍵セットでは鍵が，暗号化・復号ではデータが AES 暗号回路へ送られる．処理が終了するか処理が終了せずにタイムアウトすると「T7.データ&ステータスセット」状態となる．

T6.ステータスセット

AES 暗号回路が出力しているステータスがステータスレジスタにセットされ，ただちに「T8.ステータス・データ出力」状態に遷移する．

T7.データ&ステータスセット

AES 暗号回路が出力しているステータスとデータがステータスおよびデータレジスタにセットされ，ただちに「T8.ステータス・データ出力」状態に遷移する．

T8. ステータス・データ出力

USB コントローラへのデータ出力が可能であれば，AES 処理が行われた場合はステータスと結果を，ステータス出力要求の場合はステータスとダミーのデータを合わせて FPGA2，USB 経由で外部の PC へ出力する．出力が終了すると「T3.コマンド・データ入力待ち」に戻る．

S11. 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．FPGA1 用コンフィグレーションスイッチ SW4 押下（リセット A）による回路設計情報の再ロード，または電源オフ以外は受け付けない．

表 6 USB 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
0	S0.電源オフ	電源オン	電源用 LED1 点灯	S1.コンフィグレーション
1	S0 以外の全ての状態	電源オフ	全電力遮断．電源用 LED1 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 SW4 押下（リセット A）	FPGA1 のコンフィグレーション用 LED2 点灯せず	S1.コンフィグレーション
3	S0，S1，T2，S11 以外の全ての状態	シーケンサーリセットスイッチ SW8 押下（リセット B）	処理の停止	T2.シーケンサーリセット
4	S1.コンフィグレーシ	コンフィグレーション	FPGA1 のコンフィグ	S11.ハードウェアエ

	ョン	失敗	レーション用 LED2 点灯せず	ラー
5	S1.コンフィグレーション	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 LED2 点灯	T2.シーケンサーリセット
6	T2.シーケンサーリセット	自動遷移	リセット完了	T3.コマンド・データ入力待ち
7	T3.コマンド・データ入力待ち	AES リセット要求	なし	T4.AES リセット
8	T3.コマンド・データ入力待ち	ステータス出力要求	なし	T6.ステータスセット
9	T3.コマンド・データ入力待ち	AES 処理要求	なし	T5.AES 処理待ち
10	T4.AES リセット	リセット終了	なし	T6.ステータスセット
11	T5.AES 処理待ち	処理終了またはタイムアウト	なし	T7.データ&ステータスセット
12	T6.ステータスセット	自動遷移	AES 暗号回路からステータス読み出し	T8.ステータス・データ出力
13	T7.データ&ステータスセット	自動遷移	AES 暗号回路からデータとステータスの読み出し	T8.ステータス・データ出力
14	T8.ステータス・データ出力	出力終了	USB コントローラへのデータ書き込み	T3.コマンド・データ入力待ち

5. 物理的セキュリティ

SASEBO-GII-AES の主要コンポーネントで，暗号機能と USB インタフェース機能を有する FPGA1(Virtex-5 : XC5VLX30 または XC5VLX50) とコンフィギュレーション用 SPI-ROM1(AT45DB161D)，そして FPGA1 と USB コントローラ FT2232D，リセットスイッチ，クロック入力との間の配線情報を有する FPGA2(Spartan-3A: XC3S400A)とコンフィギュレーション用 SPI-ROM2 (AT45DB161D)は不透明な製品レベルのパッケージで封印されている．2 つの FPGA および 2 つの SPI-ROM はカバーでは囲まれていない．認証状態では 2 つの SPI-ROM の回路情報が書き換えられていないことを保証するために，全ての JTAG ポートには封止シールが貼られている．

6. 動作環境

SASEBO-GII-AES の利用は，ボード上の 2 つの FPGA に対して，2 つの SPI-ROM から回路設計情報がロードされ，クリプトオフィサは JTAG ポートにシールが貼られており，回路情報の書き換えがないことを確認した変更不可能な動作環境に限られるため，この要件は試験対象外である．

7. 暗号鍵管理

SASEBO-GII-AES モジュールは「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-GII-AES はコンフィグレーション時(図 9 の状態 S1)の「CRC テスト」, 内部で設定したデータを用いた AES 暗号回路の「アルゴリズムテスト」(図 9 の状態 S3), 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 S5~S7)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およびステータス LED がセットされる.

電源投入により FPGA1 には SPI-ROM1 から AES 暗号回路設計情報および USB インタフェース回路設計情報がロードされる. 回路設計情報は事前に 32 ビット CRC(CRC-32C. 生成多項式 $x^{32}+x^{28}+x^{27}+x^{26}+x^{25}+x^{23}+x^{22}+x^{20}+x^{19}+x^{18}+x^{14}+x^{13}+x^{11}+x^{10}+x^{9}+x^{8}+x^{6}+1$, 16 進表記 0x11edc6f41)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, FPGA1 にロードされるときに自動的に 32 ビット CRC 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. FPGA1 で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 SW4(FPGA1 のみ有効)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. FPGA1 のコンフィグレーションが成功すると, 図 8 に示したように LED2 が点灯する. その後, AES 暗号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「CRC 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 FPGA1 用コンフィグレーションスイッチ SW4 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 S3 において実行されるアルゴリズムテストの手順を図 11 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 11 の「Pass」に抜ける. テストが成功ならば図 8 に示したようにステータス LED10 が点灯し, また失敗した場合は LED6 と LED3 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.

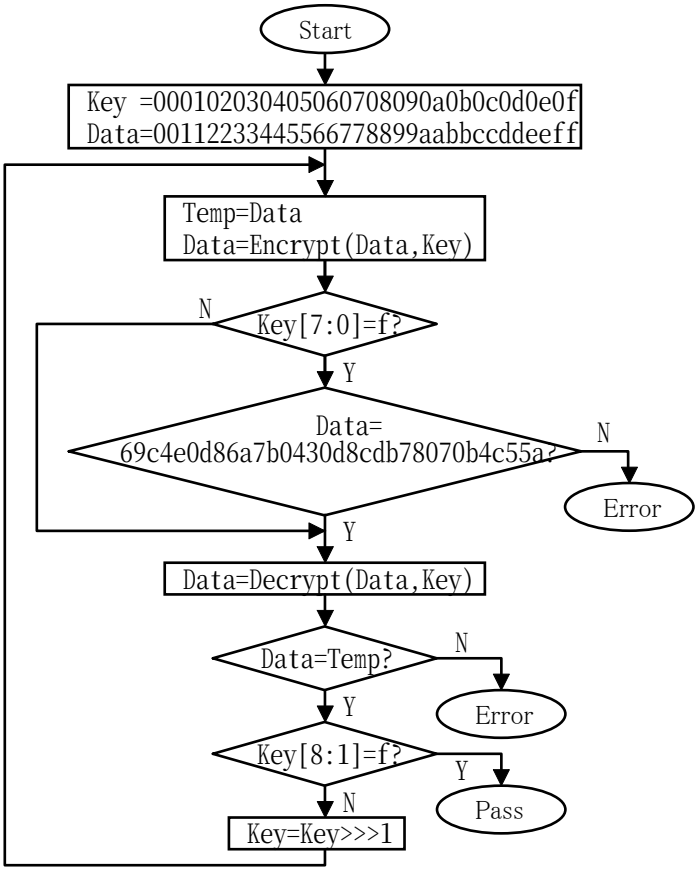

図11 SASEBO-GII-AESのアルゴリズムテスト

128 回の暗号化・復号に全てパスしたならば，図 9 で「S4.コマンド・データ入力待ち」となり，暗号化鍵と復号鍵が USB 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．USB 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「S6.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 LED5 と LED3 が点灯，LED10 が消灯し「S10.暗号回路停止」状態となる．2 つの鍵が一致したならば LED10 は点灯状態となり，「S7.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 LED10 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 LED4 と LED3 が点灯，LED10 が消灯し「S10.暗号回路停止」状態となる．

鍵テストに合格すると自動的に「S4.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

本要求事項は「SASEBO-GII-AES 設計保証文書 第一版」によって提供される．

9.2 配付及び運用

本要求事項は「SASEBO-GII-AES 設計保証文書 第一版」によって提供される.

10. その他の攻撃の対処

SASEBO-GII-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/AES