(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-292902
(P2005-292902A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	560E	5B017
H01L 21/822	G06F 12/14	540C	5F038
H01L 27/04	G06F 12/14	540P	5J104
H04L 9/10	H04L 9/00	621A	
	H01L 27/04	H	

審査請求 有　請求項の数 9　OL　（全 16 頁）

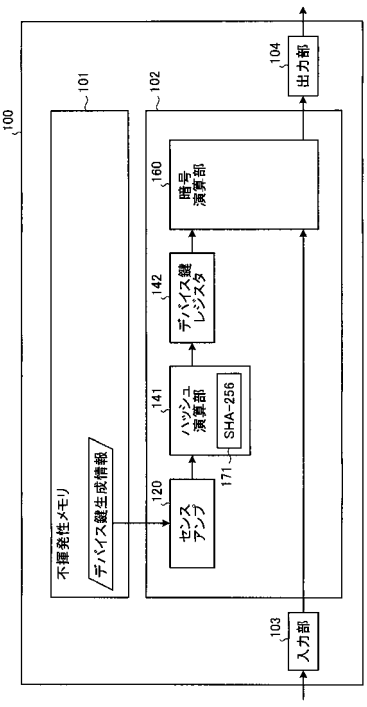
(21)出願番号　特願2004-102848 (P2004-102848)
(22)出願日　平成16年3月31日 (2004.3.31)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　橋本　幹生
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　藤田　忍
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　斉藤　好昭
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

最終頁に続く

(54)【発明の名称】半導体集積回路

(57)【要約】
【課題】第三者による情報の読み出しを防止することのできる半導体集積回路を提供する。
【解決手段】外部から隠匿すべきデバイス鍵を利用して、処理対象となる対象データに対して演算を施す集積回路１０２と、集積回路１０２に積層され、デバイス鍵生成情報を記憶している不揮発性記憶素子１０１とを備え、集積回路１０２は、不揮発性記憶素子１０１からデバイス鍵生成情報を読み出す読出手段１２０と、読出手段１２０からデバイス鍵生成情報を取得し、デバイス鍵生成情報に一方向性を有する演算を施し、デバイス鍵を生成するデバイス鍵生成手段１４１と、記対象データを取得する対象データ取得手段１６０と、デバイス鍵生成手段１４１によって生成されたデバイス鍵を利用して、対象データ取得手段が取得した対象データに対して演算を施す演算手段１６０とを有する。
【選択図】　図２



【特許請求の範囲】
【請求項１】
外部から隠匿すべきデバイス鍵を利用して、処理対象となる対象データに対して所定の主演算を施す集積回路と、
前記集積回路に積層され、かつ前記デバイス鍵を生成するときに利用すべきデバイス鍵生成情報を記憶している不揮発性記憶素子と
を備え、
前記集積回路は、
前記不揮発性記憶素子から前記デバイス鍵生成情報を読み出す読出手段と、
前記読出手段から前記デバイス鍵生成情報を取得し、前記デバイス鍵生成情報に一方向性演算を施し、デバイス鍵を生成するデバイス鍵生成手段と、
前記対象データを取得する対象データ取得手段と、
前記デバイス鍵生成手段によって生成された前記デバイス鍵を利用して、前記対象データ取得手段が取得した前記対象データに対して前記主演算を施す主演算手段と
を有することを特徴とする半導体集積回路。
【請求項２】
前記デバイス鍵生成手段によって生成された前記デバイス鍵を保持するデバイス鍵保持手段をさらに備えたことを特徴とする請求項１に記載の半導体集積回路。
【請求項３】
前記不揮発性記憶素子は、前記読出手段、前記デバイス鍵生成手段、前記対象データ取得手段、前記主演算手段および各手段の間を接続する接続部の上部に積層されていることを特徴とする請求項１または２に記載の半導体集積回路。
【請求項４】
前記主演算手段は、前記デバイス鍵を用いて前記対象データを暗号化することを特徴とする請求項１から３のいずれか一項に記載の半導体集積回路。
【請求項５】
前記主演算手段は、前記デバイス鍵を用いて前記対象データを復号することを特徴とする請求項１から４のいずれか一項に記載の半導体集積回路。
【請求項６】
前記主演算手段は、前記デバイス鍵を用いて前記対象データに対する署名を行うことを特徴とする請求項１から５のいずれか一項に記載の半導体集積回路。
【請求項７】
前記デバイス鍵生成手段は、単位演算回路を利用してデバイス鍵を生成し、
前記主演算手段は、前記デバイス鍵生成手段が前記デバイス鍵の生成を行っていないときに、前記単位演算回路を利用して前記第主演算を施すことを特徴とする請求項１から６いずれか一項に記載の半導体集積回路。
【請求項８】
前記不揮発性記憶素子の破壊を検出する記憶素子破壊検出手段と、
前記破壊検出手段が前記不揮発性記憶素子の破壊を検出した場合に、前記主演算手段による主演算を中止し、当該集積回路に保持されている情報を削除する制御手段と
をさらに備えたことを特徴とする請求項１から７のいずれか一項に記載の半導体集積回路。
【請求項９】
外部から隠匿すべきデバイス鍵を利用して、処理対象となる対象データに対して所定の主演算を施す集積回路と、
前記集積回路に積層され、前記デバイス鍵を生成するときに利用するデバイス鍵生成情報および予め定められたデバイス鍵暗号化情報により暗号化された暗号化済みデバイス鍵とを記憶している不揮発性記憶素子と
を備え、
前記集積回路は、

前記不揮発性記憶素子から前記デバイス鍵生成情報および暗号化済みデバイス鍵を読み出す読出手段と、
前記読出手段から前記デバイス鍵生成情報を取得し、前記デバイス鍵生成情報に一方向性演算を施し、前記デバイス鍵暗号化情報を生成するローカル鍵生成手段と、
前記読出手段から取得した前記暗号化済みデバイス鍵を、前記ローカル鍵生成手段から取得した前記デバイス鍵暗号化情報によって復号化し、前記デバイス鍵を生成するデバイス鍵生成手段と、
前記対象データを取得する対象データ取得手段と、
前記デバイス鍵生成手段によって生成された前記デバイス鍵を利用して、前記対象データ取得手段が取得した前記対象データに対して前記主演算を施す主演算手段と
を備えたことを特徴とする半導体集積回路。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、秘密情報を用いた演算を行う半導体集積回路に関するものである。

【背景技術】

【０００２】

従来、秘密情報を内蔵し、当該秘密情報に対する演算処理を行うＬＳＩ（Ｌａｒｇｅ Ｓｃａｌｅ Ｉｎｔｅｇｒａｔｉｏｎ）が利用されている。代表的なものとしては、ＩＣカードに基づく個人認証やデジタル放送向けの著作権保護向けＬＳＩが知られている。このような秘密情報は、秘密情報が暗号鍵でＬＳＩ固有である場合に、ＬＳＩデバイスに埋め込まれた暗号鍵との意味で、しばしばデバイス鍵と呼ばれる。以下、ＬＳＩに内蔵されるこのような秘密情報を、デバイス鍵と呼ぶこととする。デバイス鍵は基本的には製造者もしくはその関係者のみが知り得る情報である。したがって、ＬＳＩの利用者を含む第三者への漏洩を防止する必要がある。

【０００３】

近年では、ＬＳＩにおいて処理される情報の価値が大きくなってきている。これに伴って、デバイス鍵の不正な読み出しが問題となってきている。ＬＳＩは、ユーザ側に置かれる装置に内蔵されて利用される場合があり、この場合に特に問題となる。

【０００４】

デバイス鍵の不正な読み出し手段としては、ＬＳＩにプローブを接触させて動作状態の回路から電気的に情報を読み出す方法が知られている。

【０００５】

例えば、ＬＳＩは、秘密情報を利用した演算を行うとする。この場合、ＬＳＩが正常に動作しているときに、演算回路の適切な部位にプローブを適用すれば論理値を読み出すことができる。すなわち、攻撃者が秘密情報を取得することができる。

【０００６】

秘密情報が読み出されるのを防止するためには、以上のような読み出しを防止するための機構が要求されている。

【０００７】

プローブの適用を妨げる技術として、ＬＳＩチップ上部に特殊なコーティングを行う方法が知られている。ＬＳＩにおいては、半導体(シリコン)の上に金属の配線層を形成して回路が構成されている。この配線層は上面に露出している。したがって、チップの封止を開封し、配線層にプローブを適用される可能性がある。チップ上部にコーティングを行うことにより、このような読み出しを防止しようとするものである。

【０００８】

また、読み出し防止の機構を有する装置としては、半導体回路の上面にメモリ素子を積層した装置が知られている（例えば、特許文献１参照）。この装置は、メモリ素子に秘密情報を記憶している。また、パスワードのような認証情報の真偽を判定する認証回路を有している。そして、認証に成功した場合のみ、メモリ素子に記憶された秘密情報を読み出

すことができる。これにより、チップに格納された認証情報を攻撃者による読み出しから保護することができる。

【０００９】

【特許文献１】特開２００１－２７４３５５号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

チップ上部にコーティングを行う方法では、攻撃者がコーティングを取り除いてしまった場合には、回路は動作してしまう。すなわち、秘密情報の読み出しが可能になってしまい、この点が問題となっていた。

【００１１】

また、上述の装置においては、回路が動作するときには、秘密情報は回路に読み込まれ、さらに演算に利用される。このため、動作状態の回路にプローブを適用して秘密情報を読み出すことが可能であり、この点が問題となっていた。

【００１２】

本発明は、上記に鑑みてなされたものであって、上述のようなプローブを適用した情報の読み出しを防止することのできる半導体集積回路を提供することを目的とする。

【課題を解決するための手段】

【００１３】

上述した課題を解決し、目的を達成するために、本発明は、半導体集積回路であって、外部から隠匿すべきデバイス鍵を利用して、処理対象となる対象データに対して所定の主演算を施す集積回路と、前記集積回路に積層され、かつ前記デバイス鍵を生成するときに利用すべきデバイス鍵生成情報を記憶している不揮発性記憶素子とを備え、前記集積回路は、前記不揮発性記憶素子から前記デバイス鍵生成情報を読み出す読出手段と、前記読出手段から前記デバイス鍵生成情報を取得し、前記デバイス鍵生成情報に一方向性演算を施し、デバイス鍵を生成するデバイス鍵生成手段と、前記対象データを取得する対象データ取得手段と、前記デバイス鍵生成手段によって生成された前記デバイス鍵を利用して、前記対象データ取得手段が取得した前記対象データに対して前記主演算を施す主演算手段とを有することを特徴とする。

【００１４】

また、本発明は、半導体集積回路であって、外部から隠匿すべきデバイス鍵を利用して、処理対象となる対象データに対して所定の演算を施す集積回路と、前記集積回路に積層され、前記デバイス鍵を生成するときに利用するデバイス鍵生成情報および予め定められたデバイス鍵暗号化情報により暗号化された暗号化済みデバイス鍵とを記憶している不揮発性記憶素子とを備え、前記集積回路は、前記不揮発性記憶素子から前記デバイス鍵生成情報および暗号化済みデバイス鍵を読み出す読出手段と、前記読出手段から前記デバイス鍵生成情報を取得し、前記デバイス鍵生成情報に一方向性演算を施し、前記デバイス鍵暗号化情報を生成するローカル鍵生成手段と、前記読出手段から取得した前記暗号化済みデバイス鍵を、前記ローカル鍵生成手段から取得した前記デバイス鍵暗号化情報によって復号化し、前記デバイス鍵を生成するデバイス鍵生成手段と、前記対象データを取得する対象データ取得手段と、前記デバイス鍵生成手段によって生成された前記デバイス鍵を利用して、前記対象データ取得手段が取得した前記対象データに対して前記主演算を施す主演算手段とを備えたことを特徴とする。

【発明の効果】

【００１５】

本発明にかかる半導体集積回路は、不揮発性メモリに記憶されているデバイス鍵生成情報から生成されたハッシュ値をデバイス鍵とし、当該デバイス鍵を用いて暗号演算等を行う。当該半導体集積回路から秘密情報を読み出す攻撃が想定されるが、当該攻撃は、不揮発性メモリの破壊を伴う。この破壊に伴い、不揮発性メモリに保持されているデバイス鍵生成情報の一部が欠落する。したがって、一部が欠落したデバイス鍵生成情報から生成さ

れるハッシュ値であるデバイス鍵の値が異なるものとなってしまい、第三者は、正確なデバイス鍵の値を特定することができないという効果を奏する。

【００１６】

本発明は、上記に鑑みてなされたものであって、上述のようなプローブを適用した情報の読み出しを防止することのできる半導体集積回路を提供することを目的とする。

【発明を実施するための最良の形態】

【００１７】

以下に、本発明にかかる半導体集積回路の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【００１８】

（実施の形態１）

図１は、実施の形態１にかかる半導体集積回路１００の外観構成図である。半導体集積回路１００は、入力部１０３からの入力値に対してデバイス鍵を利用して演算を行い結果を出力部１０４に出力する。デバイス鍵は外部から隠匿すべきものであり、半導体集積回路内部においてはデバイス鍵生成情報として保持されている。そのため、実施の形態１にかかる半導体集積回路１００は、デバイス鍵およびデバイス鍵生成情報が攻撃者によって読み出されるのを防止するための構成を有している。以下、半導体集積回路１００の構成について説明する。

【００１９】

半導体集積回路１００は、半導体回路１０２と、半導体回路１０２の上面１０２ａに積層された不揮発性メモリ１０１とを備えている。デバイス鍵は、半導体回路１０２に保持されている。また、不揮発性メモリ１０１は、デバイス鍵の生成元の情報である原デバイス鍵生成情報を保持している。すなわち、デバイス鍵生成情報とはデバイス鍵を生成するときに利用する情報である。

【００２０】

このように、不揮発性メモリ１０１は、半導体回路の上面１０２aに積層され、半導体回路１０２の両端以外の領域を被覆している。半導体回路１０２の両端には、それぞれ入力部１０３および出力部１０４が形成されている。

【００２１】

入力部１０３および出力部１０４は、それぞれパッドとパッケージのリード線（図示せず）が接続されている。さらにパッドから半導体回路１０２の内部に向けて水平方向の配線（図示せず）が設けられている。

【００２２】

また、半導体回路１０２と不揮発性メモリ１０１の間には、後述するメモリと半導体回路のセンスアンプ接続のための垂直方向の配線１１１が多数設けられている。半導体回路１０２は、配線を介して不揮発性メモリ１０１に保持されているデバイス鍵生成情報を読み出す。

【００２３】

以下に説明するように不揮発性メモリ１０１に被覆された部分から内部情報を読み出すことは困難であり、以上の構成から、半導体回路１００は、入力部１０３および出力部１０４を有する一種のブラックボックスとみなすことができる。

【００２４】

半導体回路１０２は、演算回路、演算結果を一時的に保持する内部レジスタおよびこれらの要素間の接続線などの回路を有している。各種信号は、これらの回路の間を流れている。このため、侵害者がプローブを適用するにより情報を読み出すおそれがある。

【００２５】

本実施の形態における半導体回路１０２は、不揮発性メモリ１０１によって被覆されている。したがって、プローブを適用するためには不揮発性メモリ１０１を破壊しなければならない。また、仮に不揮発性メモリ１０１を破壊した場合には、不揮発性メモリ１０１に保持されている秘密情報の一部が欠落する。

【００２６】
本実施の形態にかかる半導体集積回路１００は、デバイス鍵生成情報を利用してデバイス鍵を生成する。したがって、不揮発性メモリ１０１に保持されているデバイス鍵生成情報の一部が欠落した場合にはデバイス鍵を生成することができない。このため、侵害者は、不揮発性メモリ１０１を破壊した場合には、デバイス鍵を特定することができない。以下、秘密情報の読み出しを防止するための機能構成について説明する。
【００２７】
図２は、実施の形態１にかかる半導体集積回路１００内部の機能構成を示す図である。半導体集積回路１００は、不揮発性メモリ１０１と、半導体回路１０２と、入力部１０３と、出力部１０４とを備えている。さらに、半導体回路１０２は、センスアンプ１２０と、ハッシュ演算部１４１と、デバイス鍵レジスタ１４２と、暗号演算部１６０とを有している。
【００２８】
不揮発性メモリ１０１は、複数のセルを有している。そして、複数のセルにわたってデバイス鍵生成情報を記憶している。センスアンプ１２０は、不揮発性メモリ１０１からデバイス鍵生成情報を逐次読み出し、ハッシュ演算部１４１に送る。すなわち、不揮発性メモリ１０１に保持されている複数のセルの情報を時分割的に読み出して、処理する。ハッシュ演算部１４１は、センスアンプ１２０から取得したデバイス鍵生成情報に対して、拡散性および一方向性を有する演算を行う。具体的には、ハッシュ演算部１４１は、ＳＨＡ－２５６計算機能１７１を有するハードウェアを有している。そして、当該ハードウェアによりハッシュ値が計算される。そして、演算により得られたハッシュ値、すなわちデバイス鍵をデバイス鍵レジスタ１４２に保持させる。
【００２９】
以上の処理は、半導体集積回路１００の初期化の際に行われる。そして、デバイス鍵レジスタ１４２は、再度初期化されるまで、ハッシュ演算部１４１から取得したデバイス鍵を保持する。
【００３０】
暗号演算部１６０は、入力部１０３を介して外部から処理対象となる対象データを取得すると、デバイス鍵レジスタ１４２に保持されているデバイス鍵を利用して、対象データに対して演算を施す。そして、演算結果を出力部１０４に送る。出力部１０４は、半導体集積回路１００の外部に演算結果を出力する。ここで、実施の形態にかかる暗号演算部１６０は、特許請求の範囲に記載の主演算手段と対象データ取得手段とを構成する。
【００３１】
なお、以下に述べる攻撃への対策から原秘密値を格納した不揮発性メモリは、上記センスアンプ１２０と、ハッシュ演算部１４１と、デバイス鍵レジスタ１４２と、暗号演算部１６０およびそれらの間の接続の全てを被覆することが望ましい。
【００３２】
以下、実施の形態１にかかる半導体集積回路１００が攻撃者によるデバイス鍵を特定するような攻撃からどのように保護するかを説明する。
【００３３】
攻撃者がデバイス鍵情報を取得する方法として、３つの方法が想定される。１番目の方法は、デバイス鍵レジスタ１４２に格納されたデバイス鍵値を直接読み出す方法である。２番目の方法は、デバイス鍵を生成するためのデバイス鍵生成情報の読み込み時に、デバイス鍵生成情報をセンスアンプ１２０から読み出す方法である。この場合、さらに、ハッシュ演算部１４１のハッシュアルゴリズムが既知であることを利用して間接的にデバイス鍵を特定する。３番目の方法は、センスアンプ１２０によりデバイス鍵生成情報の一部を特定し、これに基づいてデバイス鍵を特定する方法である。本発明ではセンスアンプ及びハッシュ演算部を全体にわたって被覆する不揮発性メモリ全体にデバイス鍵生成情報を保持することにより、これら３種類の攻撃のいずれをも困難にする効果がある。
【００３４】

まず、本発明の構成が１番目の方法による攻撃を防止できる理由を説明する。デバイス鍵レジスタ１４２に対して、プローブを適用してデバイス鍵レジスタに格納された値を直接読み出す攻撃が行われた場合を想定する。

【００３５】

このとき、ハッシュ演算部１４１に入力されるのは、デバイス鍵レジスタ上面を被覆するメモリセルがプローブ適用により破壊された結果の値である。したがって、デバイス鍵レジスタ１４２から読み出せるのは破壊されたデバイス鍵生成情報に対してハッシュ計算が行われた結果値である。

【００３６】

破壊後のデバイス鍵生成情報は、元来のデバイス鍵生成情報とは異なる情報である。さらに、破壊後のデバイス鍵生成情報に対して施されるハッシュ計算は拡散性を有する演算である。したがって、破壊後のデバイス鍵生成情報のハッシュ計算により得られる結果値は、本来のデバイス鍵生成情報から計算される正しいデバイス鍵の値とは全く違う値となる。従って、この攻撃を行っても攻撃者は本来のデバイス鍵の値に関して有効な情報を得ることができない。このため、攻撃者によってデバイス鍵が特定されるのを防止することができる。デバイス鍵レジスタ１４２と暗号演算部１６０との接続にもデバイス鍵値が出力されるが、この接続部分についても不揮発性メモリによって被覆されていれば、デバイス鍵レジスタの場合と同様に攻撃からデバイス鍵値を守ることができる。

【００３７】

また、一般にメモリセルの破壊やプローブの接触は半導体回路の動作に影響を与え、回路が保持する値に誤りを生じさせる。この誤りを回避することは極めて困難である。もし攻撃者がメモリ破壊を行わない状態で本半導体集積回路に電源を投入し、正しいデバイス鍵がデバイス鍵レジスタ１４２に格納されている状態で、不揮発性メモリを破壊してプローブを適用した場合、デバイス鍵レジスタ１４２の値に誤りが生じなければ攻撃者はデバイス鍵の値を取得できることになる。だが、前述のように動作状態の回路の近傍に破壊を行ったり、外部からプローブを接触させることは不可避的にデバイス鍵レジスタの値に誤りを生じ、デバイス鍵レジスタ１４２の値は破壊を受けるため攻撃者は正しいデバイス鍵の値を取得することは著しく困難である。

【００３８】

このように実施の形態１にかかる半導体集積回路１００は、不揮発性メモリ１０１に保持されているデバイス鍵生成情報に一方向性および拡散性を有するハッシュ演算を適用してデバイス鍵を生成するので、デバイス鍵生成情報の一部が欠落すると半導体集積回路において正しいデバイス鍵の値が生成されない。このため、デバイス鍵が特定されるのを防止することができる。

【００３９】

次に、２番目の方法による攻撃が防止できる理由について説明する。ハッシュ演算部のハッシュアルゴリズムが攻撃者にとって既知であるとすれば、攻撃者は直接デバイス鍵レジスタの値が得られなくても、正しいデバイス鍵生成情報を知ることにより、半導体集積回路以外の計算手段を用いてデバイス鍵値を計算することができる。デバイス鍵生成情報は、デバイス鍵の読み込み動作時において、ハッシュ演算部１４１またはセンスアンプ１２０にプローブを適用して値を逐次読み出すことができれば取得できる。

【００４０】

ところが、センスアンプ１２０は上面が不揮発性メモリ１０１に被覆されている。このため、センスアンプにプローブを適用すると必ずメモリセルの破壊が生じて正しいデバイス鍵生成情報は取得できない。なしにはプローブを適用して値を読み出すことはできず、正しいデバイス鍵生成情報は取得できない。破壊されたデバイス鍵生成情報にハッシュアルゴリズムを適用してデバイス鍵を計算しようとしても、ハッシュ演算の拡散性により、得られる値は正しいデバイス鍵とは全く異なった値となる。よって、本発明で導入された不揮発性メモリによるセンスアンプの被覆とハッシュ演算の拡散性により、２番目の攻撃方法も防止される。

【００４１】
３番目の方法による攻撃を防止する構成について説明する。３番目の方法は、２番目の方法の変形であり、一部が破壊されたデバイス鍵生成情報からハッシュアルゴリズムを利用して間接的にデバイス鍵を特定する方法である。この方法は、デバイス鍵レジスタからデバイス鍵を直接読み出す方法に比べてより強力な攻撃方法である。この攻撃方法と攻撃を防止する構成を詳述する。
【００４２】
一般にメモリは格子状に配線されたワード線、ビット線の交点にメモリセルがおかれ、ワード線で指定された列のメモリセルの内容が、それぞれのビット線に対応するセンスアンプで読み出される構成をとる。ここでは同一のビット線にα個のメモリセルが接続されているものとする。このとき、ビット線に接続されたセンスアンプ 120 にプローブを適用すれば、同一のビット線に接続されたα個のメモリセルの内容を全て観測できることが期待でき、攻撃が効率的である。
【００４３】
このような攻撃を防止する観点において、１個のセンスアンプ１２０の領域に１個のメモリセルに対応する領域が積層されているのが望ましい。この場合には、１つのセンスアンプ１２０に対してプローブを適用する場合に１つのメモリセルを破壊しなければならない。すなわち、攻撃者はデバイス鍵生成情報の総てを取得することはできず、多くのデバイス鍵生成情報を得ようとしてプローブを適用するセンスアンプの数を増やすほど、メモリセルの多くが破壊されてしまことになる。
【００４４】
プローブを適用するセンスアンプ１箇所あたり最低１個のメモリセルの破壊が必要であれば、ひとつのセンスアンプから読み取れるビット数は、同一のビット線に接続されたメモリセルのうち破壊した１個を除くα-1個である。センスアンプが１６個ある場合には、１６個のメモリセルを破壊しなければならない。この場合、失われた情報を補完するには総当りで２＾１６通りの検索が必要となる。
【００４５】
上述のようにプローブ適用によりメモリセルのデバイス鍵生成情報の一部が欠落する。しかし、デバイス鍵生成情報の一部が欠落していても、欠落部分のデータ量が小さい場合には、総当りにより欠落部分のデータを補完することが可能である。この点が依然として問題となる。
【００４６】
例えば、デバイス鍵生成情報が１２８ビットであって、α=8の場合、このメモリセル読み出しのためのセンスアンプの個数は１６個である。各センスアンプへのプローブ適用により、デバイス鍵生成情報のうち１６ビットが欠落して残りの１１２ビットが取得できる。デバイス鍵生成情報のうち欠落した１６ビットの情報については以下の方法で総当り探索することで秘匿情報であるデバイス鍵を特定することができる。
【００４７】
総当り方式による探索例として次の方法がある。まず不揮発性メモリ１０１を破壊する前に、半導体集積回路１００の入力部１０３に入力する暗号文と、当該暗号文に対する出力部１０４からの出力値である平文の組を入手しておく。そして、不揮発性メモリ１０１を破壊後、プローブ適用により読み出した１１２ビットのデバイス鍵生成情報に、残りの１６ビットがとりうる全ての値を組み合わせて列挙したデバイス鍵生成情報候補を生成する。さらにこのデバイス鍵生成情報候補について既知であるハッシュアルゴリズムによりハッシュ値を計算してデバイス鍵候補を生成する。
【００４８】
このデバイス鍵の候補を秘密鍵として、破壊前に入手した暗号文に対して暗号演算を施す。そして、演算結果と先に入手しておいた暗号文に対する平文とを照合する。照合結果が一致するまで全ての候補について総当りすることにより、秘密情報を特定することができる。なおこの過程で、暗号文と平文の組およびデバイス鍵生成情報の収集以外は攻撃対

象のチップを使わずに、別システムにおける計算で求めることができる。

【００４９】

上記の攻撃の所要時間は欠落したビット数ｎについて２＾ｎのオーダーで大きくなる。したがって欠落したビット数を大きくすることができればこの攻撃を実質的に不可能にすることができる。

【００５０】

実施の形態１にかかる半導体集積回路１００は、デバイス鍵生成にハッシュを使用している。このため、デバイス鍵生成情報のビット長は、デバイス鍵ビット長とは無関係に任意に大きく設定することができる。α＝８の場合において、デバイス鍵生成情報のビット長を１０２４ビットとすれば、センスアンプの個数は１２８個となる。すなわち、プローブ適用により１２８ビットのデバイス鍵生成情報が欠落する。このため、2^{128}通りの総当り検索がひつようとなり、いかに１回あたりのデバイス鍵照合を効率的に行ったとしても、総当りは実質的に不可能である。

【００５１】

このように、実施の形態１に係る半導体集積回路１００は、デバイス鍵の生成に拡散性と拡張性を持つハッシュを用いることにより、デバイス鍵生成情報の読み取りによる間接的なデバイス鍵特定の攻撃にも十分な耐性をもつことができる。上述のデバイス鍵に対する直接攻撃に耐性をもつこととあわせて、秘匿対象であるデバイス鍵の値を効果的に保護することができる。

【００５２】

このように、本発明においては前述の３種類の攻撃を防止できるだけでなく、デバイス鍵生成情報のビット長を長くすることにより攻撃をより困難にすることができるため、保護対象であるデバイス鍵を直接不揮発性メモリに格納する構成と比較して、デバイス鍵の解析がきわめて困難で安全な半導体装置を提供できる。

【００５３】

以上、本発明を実施の形態を用いて説明したが、上記実施の形態に多様な変更または改良を加えることができる。

【００５４】

そうした変更例としては、本実施の形態における半導体集積回路１００は、暗号演算にかかるデバイス鍵が第三者に特定されるのを避けるための構成であったが、半導体集積回路１００は、これ以外の機能に組み込んでもよい。

【００５５】

例えば、演算処理にかえて、署名生成処理を行ってもよい。また、逆に署名検証にかかる処理を行ってもよい。また、検証結果に基づいたエンターテイメントコンテンツやデータベースなど、別データへのアクセス制御にかかる処理をおこなってもよい。

【００５６】

この場合、不揮発性メモリはアクセス制御機能や別データの処理にかかる半導体回路も含めて被覆する。これにより、プローブの適用などを防止することにより、アクセス制御対象の情報を保護する等、第三者による秘密情報の特定を防止することができる。

【００５７】

（実施の形態２）

図３は、実施の形態２にかかる半導体集積回路１００の全体構成を示している。実施の形態２に係る半導体集積回路１００は、実施の形態１にかかるハッシュ演算部１４１が有するＳＨＡ－２５６計算機能１７１に変えて、演算制御部１７２を有している。ここで、演算制御部１７２と半導体回路１０２とは、共通の回路により構成されている。ハッシュ演算は、デバイス鍵レジスタ１４２にデバイス鍵を保持させた後は行われない。また、暗号演算は、デバイス鍵の設定が完了するまでは行われない。このように、ハッシュ演算と暗号演算とは時間的に排他的である。

【００５８】

そこで、実施の形態２にかかる半導体集積回路１００においては、１つの演算回路にお

いてハッシュ計算と暗号演算とを行うこととする。具体的には、演算制御部１７２は、暗号演算部１６０にデバイス鍵および入力データを出力する。さらに、演算制御部１７２は、暗号演算部１６０から暗号演算の結果を取得する。

【００５９】

なお、既存の暗号アルゴリズムを利用してハッシュ機能を実現する方法としては、共通鍵ブロック暗号やモジュロ演算がある。これらは、それぞれ国際規格ＩＳＯ／ＩＥＣ １０１１８－２および ＩＳＯ／ＩＥＣ １０１１８－４に記述されている。また、その他の暗号アルゴリズムやＭＡＣを適用してもよい。

【００６０】

このように、ハッシュ計算と外部入力に対する演算処理は時間的に排他的である。そこで、ハッシュ計算と外部入力に対する演算処理を同一の回路で行うことにより、スループットを低下させることなく、ハードウェア規模を削減することができる。

【００６１】

（実施の形態３）

次に実施の形態３にかかる半導体集積回路１００について説明する。実施の形態１および実施の形態２にかかる半導体集積回路１００においては、デバイス鍵の値はデバイス鍵生成情報のハッシュ計算結果が用いられていた。この方法では任意に選択した値もしくは外部から与えられた値をデバイス鍵として回路に組み込むことができない。半導体回路製造者が任意に選択した値もしくは外部から与えられた値をデバイス鍵として回路に組み込むには、ハッシュ値であるデバイス鍵値に対応するデバイス鍵生成情報を生成しなくてはならないが、これはハッシュ計算の一方向性により不可能である。これに対して、以下に説明する実施の形態３にかかる半導体集積回路１００においては、半導体回路製造者がデバイス鍵の値を任意に選択することができる。

【００６２】

図４は、実施の形態３にかかる半導体集積回路１００の全体構成を示している。実施の形態３にかかる半導体集積回路１００の不揮発性メモリ１０１は、デバイス鍵生成情報と暗号化済デバイス鍵を保持している。ここで、暗号化済デバイス鍵は、製造者により決定されたデバイス鍵を暗号化した情報である。

【００６３】

また、半導体回路１０２は、デバイス鍵復号化部１４４を備えている。半導体回路１０２においては、センスアンプ１２０は、不揮発性メモリ１０１から秘密情報および暗号化済デバイス鍵を読み出す。

【００６４】

ハッシュ演算部１４１は、デバイス鍵生成情報に対しハッシュ演算を施してハッシュ値を得る。実施の形態１にかかるセンスアンプ１２０においては、ハッシュ値はデバイス鍵として利用したが、実施の形態３にかかるセンスアンプ１２０においては、ハッシュ値は、製造者により決定されたデバイス鍵を暗号化および復号化するためローカル鍵として利用する。

【００６５】

デバイス鍵復号化部１４４は、センスアンプ１２０を介して不揮発性メモリ１０１から暗号化済デバイス鍵を取得する。デバイス鍵復号化部１４４は、さらにハッシュ演算部１４１からハッシュ値として得られたローカル鍵を取得する。

【００６６】

ここで、不揮発性メモリ１０１から取得した暗号化済みデバイス鍵は、ハッシュ演算部１４１により得られたローカル鍵を利用して、デバイス鍵を暗号化した情報である。デバイス鍵復号化部１４４は、暗号化済デバイス鍵をハッシュ演算部１４１から取得したローカル鍵を利用して復号化する。そして、復号化により得られたデバイス鍵をデバイス鍵レジスタ１４２に保持させる。

【００６７】

不揮発性メモリ１０１への暗号化済デバイス鍵の設定は、製造時に行われる。具体的に

は、製造者は半導体回路への情報書き込みの前に当該回路とは別のシステム上で次の準備作業を行う。まずデバイス鍵生成情報を任意に決定し、このデバイス鍵生成情報のハッシュ値を計算してローカル鍵とする。次に所定のデバイス鍵をローカル鍵で暗号化した暗号化済みデバイス鍵を計算する。当該回路とは別のシステム上でデバイス鍵生成情報と暗号化済みデバイス鍵がそれぞれ準備される。これらの情報が揮発性メモリ１０１に設定される。

【００６８】

このように、実施の形態３にかかる半導体集積回路１００においては、回路の動作時に使用されるデバイス鍵値を、製造者が製造時に任意に選択することができる。

【００６９】

実施の形態１および２においては秘匿対象であるデバイス鍵をプローブを適用した読み出しから守るために、デバイス鍵生成情報とハッシュ演算機能が使われていた。実施の形態３においては、秘匿対象であるデバイス鍵をプローブを適用した読み出しから守るために、デバイス鍵生成情報とハッシュ演算機能およびデバイス鍵生成情報から生成されるローカル鍵と復号機能がそれぞれ使われていることが、実施の形態１および２と実施の形態３の間の構成上の相違点である。

【００７０】

実施の形態３におけるデバイス鍵生成情報とローカル鍵は、実施の形態１におけるデバイス鍵生成情報とデバイス鍵の場合と同じメカニズムにより守られている。したがって、プローブ適用による攻撃が行われた場合にもローカル鍵は特定されず安全である。

【００７１】

実施の形態３における秘匿対象であるデバイス鍵は、不揮発性メモリ１０１上ではローカル鍵による暗号化により守られており、ローカル鍵が安全であるならば、たとえ暗号化済みデバイス鍵の値が読み出されてしまったとしても秘匿される。

【００７２】

実施の形態３においてデバイス鍵レジスタ１４２に対して直接プローブを適用する攻撃を考えた場合、プローブ適用によって破壊されたメモリセルが格納していた情報は、デバイス鍵生成情報か暗号化済みデバイス鍵のいずれかである。破壊されるメモリセルが格納していた情報がデバイス鍵生成情報である場合には、わずかのビット数の欠落でもローカル鍵レジスタの値は大きく変わる。したがって、デバイス鍵レジスタに格納される値は、この本来の値とは異なるローカル鍵で暗号化済みデバイス鍵を復号して得られた値である、すなわち、真のデバイス鍵の値とは全く異なる値である、このため、読み出されたとしても真のデバイス鍵特定のてがかりを与えず安全である。

【００７３】

また、プローブ適用によって破壊されたメモリセルが格納していた情報が暗号化済みデバイス鍵であった場合、デバイス鍵生成情報は破壊されない。このため、ローカル鍵の値は正しい値が保持される。しかし暗号化済みデバイス鍵のビットが欠落しているので、復号演算の拡散性により、復号の結果デバイス鍵レジスタに格納される値は真のデバイス鍵とは全く異なる値となる。したがって、読み出されたとしても真のデバイス鍵特定のてがかりを与えず安全である。以上のように攻撃者にデバイス鍵が読み取られるのを防止することができる。

【００７４】

実施の形態１にかかる半導体集積回路１００においては、デバイス鍵は、不揮発性メモリ１０１に保持させる秘密情報のハッシュ値であって、かつハッシュ演算は、一方向性の演算であるため、任意のデバイス鍵に対応する秘密情報を不揮発性メモリ１０１に保持させることができない。

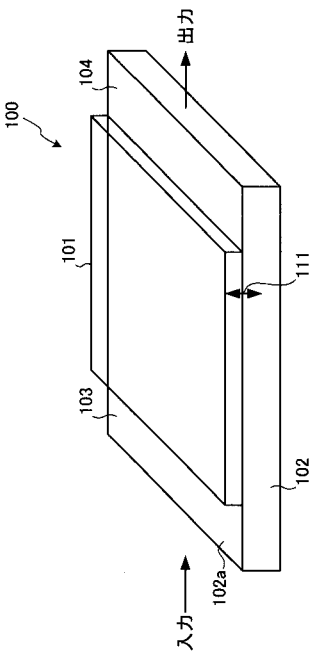
【００７５】

実施の形態３にかかる半導体集積回路１００においては、ハッシュ演算の一方向性および暗号演算を利用して攻撃者からの攻撃を困難にしつつ、任意のデバイス鍵を利用した暗号演算を行うことができる。

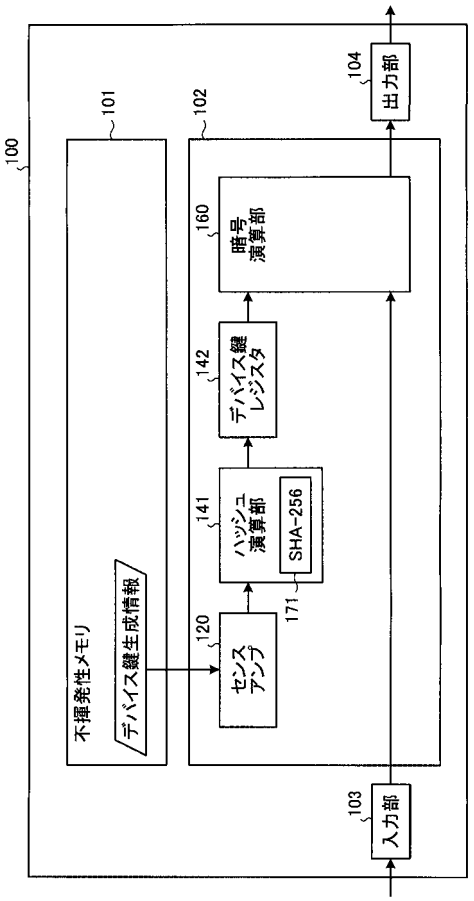
【００７６】
ＩＣカードなどにおいては、デバイス鍵が半導体集積回路１００の製造者以外の団体から発行される場合がある。例えば、クレジットカードや公共団体が使用するカードなどである。この場合には、外部団体が発行したデバイス鍵を製造時に回路に埋め込まなければならない。実施の形態３にかかる半導体集積回路１００によれば、このような場合であっても、製造者が任意のデバイス鍵を設定することができる。このように、デバイス鍵の値による制限を受けないので、汎用性を向上させることができる。
【００７７】
（実施の形態４）
不揮発性メモリ１０１の種類によっては、メモリセルの破壊を電気的に検出することが可能である。実施の形態４にかかる半導体集積回路１００は、メモリセルの破壊を電気的に検出することにより攻撃者からの秘密情報の読み出しをより効果的に防止する。
【００７８】
図５は、実施の形態４にかかる半導体集積回路１００の全体構成を示す図である。実施の形態４にかかるセンスアンプ１２０は、短絡検出回路１８１を有している。たとえば、ＭＲＡＭと呼ばれるメモリでは、２層の磁性層の間に極めて薄い絶縁層が置かれている。そして、この絶縁層を通して流れるトンネル電流が磁性層に記録された磁気の方向によって変化することで記憶が行われる。
【００７９】
つまり抵抗値を測定することで記録された値が読み出される。このとき、ＭＲＡＭセルにプローブ適用のため穴をあけるなどの加工を行うと絶縁層は破壊され、セルの抵抗値はきわめて低い値となる。すなわち短絡状態になる。
【００８０】
短絡状態は、メモリセルが機能しているときには起こり得ない。従って、正常状態と区別することができる。すなわち、短絡状態であるか否かを検出することにより、プローブ適用があったことを検出することができる。
【００８１】
短絡検出回路１８１は、メモリセルの抵抗値が短絡状態にあることを検出すると、演算を禁止する旨を示す信号をデバイス鍵レジスタ１４２および暗号演算部１６０に出力する。デバイス鍵レジスタ１４２および暗号演算部１６０は、短絡検出回路１８１から信号を受け取るとデバイス鍵など内部状態を消去し、処理を中断する。
【００８２】
したがって、このとき攻撃者がプローブ適用により読み出すことのできる情報は、メモリセルの破壊により一部が欠落したデバイス鍵生成情報である。具体的には、再度電源が投入され、初期化処理の過程で不揮発性メモリ１０１から読み出された欠落のあるデバイス鍵生成情報だけである。
【００８３】
このように、メモリセルが破壊された時点で、内部状態を初期化することにより、より確実に攻撃者によるデバイス鍵生成情報の読み出しを防止することができる。
【００８４】
図６は、実施の形態４にかかる半導体集積回路１００の処理を示すフローチャートである。初期化処理において、まず、センスアンプ１２０は、不揮発性メモリ中のセル内容を逐次読み出す（ステップＳ１００）。
【００８５】
このとき、短絡検出回路１８１は、短絡状態であるか否かを検出している。そして、短絡検出回路１８１が、短絡状態であることを検出しない間は（ステップＳ１０２，Ｎｏ）、ハッシュ演算部１４１は、センスアンプ１２０から秘密情報を取得し、ブロック単位でハッシュ演算を行う（ステップＳ１０４）。以上の処理をハッシュ演算が完了するまで繰り返す。そして、ハッシュ演算が完了すると（ステップＳ１０６，Ｙｅｓ）、ハッシュ値として得られたデバイス鍵をデバイス鍵レジスタ１４２に格納する（ステップＳ１０８）

。
【００８６】
そして、外部から処理対象となる対象データを取得すると（ステップＳ１１０，Ｙｅｓ）、暗号演算部１６０は、対象データに対してデイバス鍵を用いた演算を施す（ステップＳ１１２）、そして、出力部１０４が、処理後のデータを外部に出力する（ステップＳ１１４）。
【００８７】
一方、ステップＳ１０２において、短絡検出回路１８１が短絡状態であることを検出すると（ステップＳ１０２，Ｙｅｓ）、ハッシュ演算部１４１等は処理を中断する（ステップＳ１２０）。そして、これまでに蓄積されたデータが消去される（ステップＳ１２２）。以上で、半導体集積回路１００の処理が完了する。
【産業上の利用可能性】
【００８８】
以上のように、本発明にかかる半導体集積回路は、秘匿情報を利用した演算に有用であり、特に、外部からの攻撃を防止しつつ、秘匿情報を利用した演算を行うのに適している。
【図面の簡単な説明】
【００８９】
【図１】実施の形態１にかかる半導体集積回路１００の外観構成図である。
【図２】実施の形態１にかかる半導体集積回路１００内部の機能構成を示す図である。
【図３】実施の形態２にかかる半導体集積回路１００の全体構成を示す図である。
【図４】実施の形態３にかかる半導体集積回路１００の全体構成を示す図である。
【図５】実施の形態４にかかる半導体集積回路１００の全体構成を示す図である。
【図６】実施の形態４にかかる半導体集積回路１００の処理を示すフローチャートである。
【符号の説明】
【００９０】
１００　半導体集積回路
１０１　不揮発性メモリ
１０２　半導体回路
１０３　入力部
１０４　出力部
１１１　配線
１２０　センスアンプ
１４１　ハッシュ演算部
１４２　デバイス鍵レジスタ
１４４　デバイス鍵復号化部
１６０　暗号演算部
１７１　ＳＨＡ－２５６計算機能
１７２　演算制御部
１８１　短絡検出回路

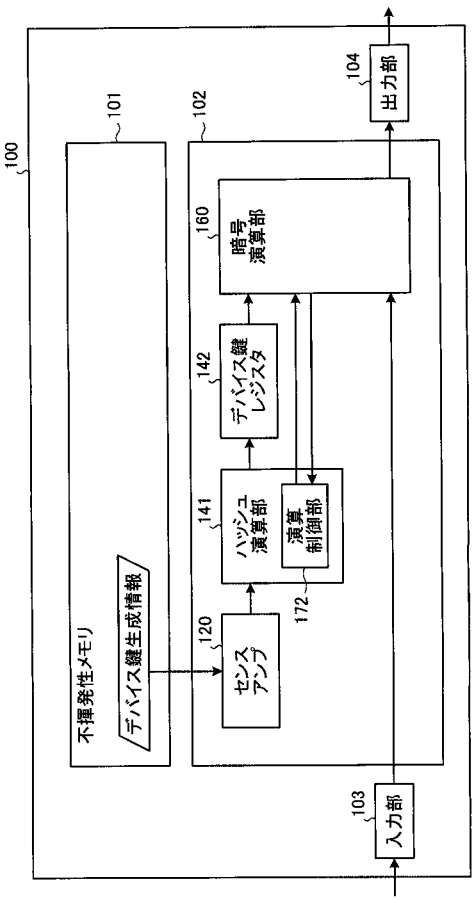
【図１】


100
101
102
102a
103
104
111
出力
入力

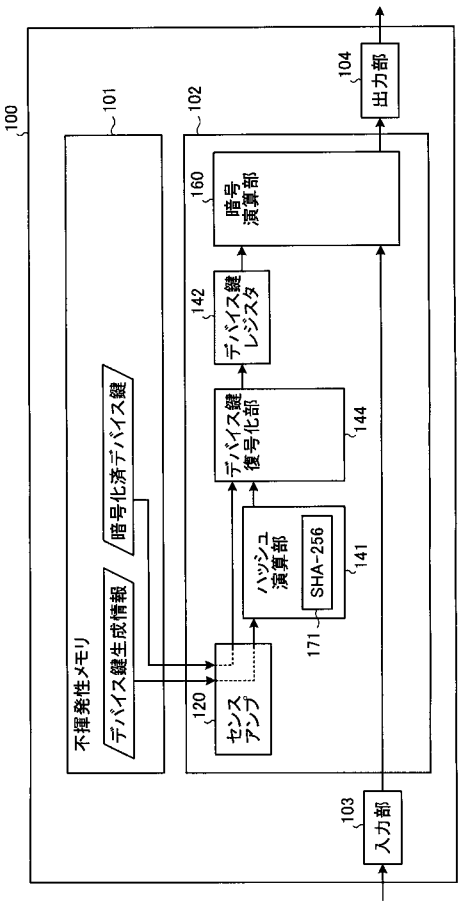
【図２】


100
101
不揮発性メモリ
デバイス鍵生成情報
102
104
出力部
160
暗号演算部
142
デバイス鍵レジスタ
141
ハッシュ演算部
SHA-256
171
120
センスアンプ
103
入力部

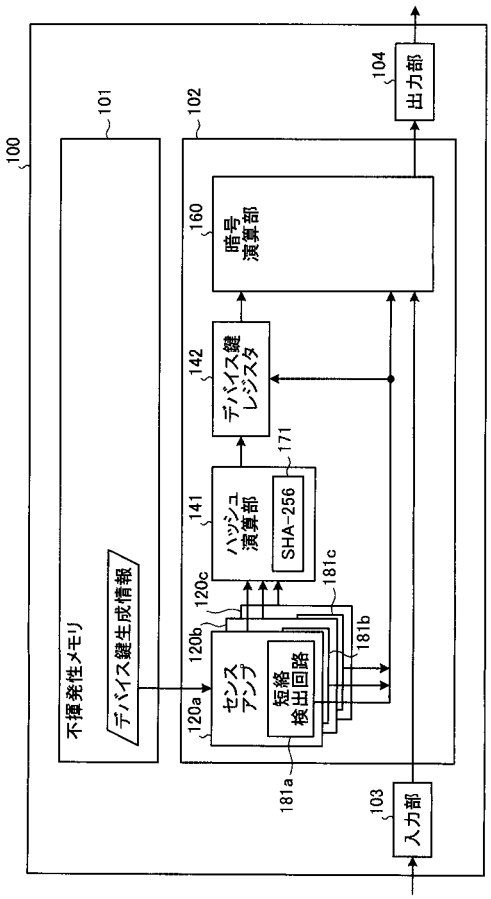
【図３】


100
101
不揮発性メモリ
デバイス鍵生成情報
102
104
出力部
160
暗号演算部
142
デバイス鍵レジスタ
141
ハッシュ演算部
演算制御部
172
120
センスアンプ
103
入力部

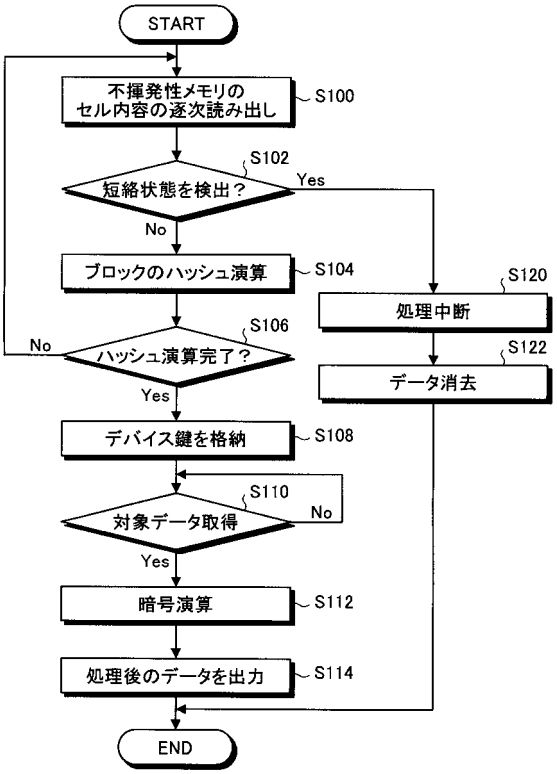
【図４】


100
101
不揮発性メモリ
デバイス鍵生成情報
暗号化済デバイス鍵
102
104
出力部
160
暗号演算部
142
デバイス鍵レジスタ
144
デバイス鍵復号化部
141
ハッシュ演算部
SHA-256
171
120
センスアンプ
103
入力部

【図５】


100
101
102
104
出力部
不揮発性メモリ
デバイス鍵生成情報
暗号演算部
160
デバイス鍵レジスタ
142
ハッシュ演算部
141
SHA-256
171
センスアンプ
120a
120b
120c
短絡検出回路
181a
181b
181c
103
入力部

【図６】


START
不揮発性メモリのセル内容の逐次読み出し
S100
短絡状態を検出？
S102
Yes
No
ブロックのハッシュ演算
S104
ハッシュ演算完了？
S106
No
Yes
処理中断
S120
データ消去
S122
デバイス鍵を格納
S108
対象データ取得
S110
No
Yes
暗号演算
S112
処理後のデータを出力
S114
END

フロントページの続き

(72)発明者　本山　雅彦
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考) 5B017 AA07 BA07 BA08 BB03 CA11 CA14
5F038 DF05 DF10 EZ20
5J104 AA01 AA16 EA04 EA15 EA16 EA20 JA03 NA02 NA37 NA39