(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 8 月 16 日(16.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/108016 A1

(51) 国際特許分類:
H04N 7/173 (2011.01)

(21) 国際出願番号: PCT/JP2011/052782

(22) 国際出願日: 2011 年 2 月 9 日(09.02.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社(**FUJITSU LIMITED**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 内田　好昭(**UCHIDA, Yoshiaki**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内 Kanagawa (JP).

(74) 代理人: 酒井　宏明(**SAKAI, Hiroaki**); 〒1006020 東京都千代田区霞が関三丁目２番５号　霞が関ビルディング　酒井国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

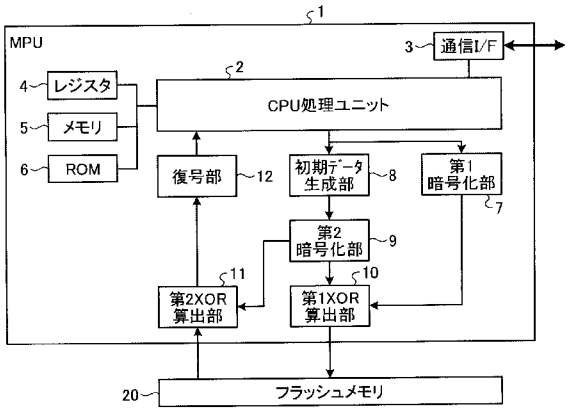
— 国際調査報告（条約第 21 条(3)）

WO 2012/108016 A1

(54) **Title**: INFORMATION PROCESSING DEVICE IN EMBEDDED DEVICE, METHOD OF PROCESSING INFORMATION AND INFORMATION PROCESSING PROGRAM

(54) 発明の名称 : 組み込み機器における情報処理装置、情報処理方法及び情報処理プログラム

[図1]



2	CPU processing unit	8	Initial data generating unit
3	Communication I/F	9	Second encrypting unit
4	Resistor	10	First XOR calculating unit
5	Memory	11	Second XOR calculating unit
6	ROM	12	Decoding unit
7	First encrypting unit	20	Flash memory

(57) **Abstract**: MPU (1) according to the present invention encrypts a confidential value using a given encryption key. Further, if the confidential value is an initial value which is written upon initialization of a flash memory (20) storing the encrypted value, the MPU (1) converts the encrypted value to a value that is reconvertible and independent from the encrypt key. Then, the MPU (1) stores the converted value in the flash memory (20). Hereby, the MPU (1) makes it virtually impossible to analyze the encryption, and thereby improving its tamper resistance.

(57) 要約: ＭＰＵ（１）は、秘匿する値を所定の暗号鍵を用いて暗号化する。また、ＭＰＵ（１）は、秘匿する値が、暗号化された値を格納するフラッシュメモリ（２０）の初期化時に書込まれる初期値である場合には、暗号化された値を、逆変換可能であって暗号鍵に依存しない値に変換する。その後、ＭＰＵ（１）は、変換した値をフラッシュメモリ（２０）に格納する。このため、ＭＰＵ（１）は、暗号の解析を事実上不可能にし、抗タンパー性を向上させることができる。

明　細　書

発明の名称 ：

組み込み機器における情報処理装置、情報処理方法及び情報処理プログラム

技術分野

[0001] 本発明は、組み込み機器における情報処理装置、情報処理方法及び情報処理プログラムに関する。特に秘匿データを管理する小規模な管理ユニットであって、ＭＰＵとフラッシュメモリを有するものに関する。またこのような暗号化方法を内蔵したＭＰＵに関する。

背景技術

[0002] 従来、秘匿するべき情報をフラッシュメモリ等の不揮発性メモリに格納する際、これを暗号化し、暗号化した情報を格納することで、不揮発性メモリに格納された情報の悪意による解析を困難にする技術が知られている。このような技術の一例として、著作権によって保護される動画などのＡＶ（Ａｕｄｉｏ　Ｖｉｄｅｏ）データの管理ユニットにおいて、暗号鍵や複製可能な回数等の管理情報を暗号化し、暗号化した管理情報を不揮発性メモリに格納する技術が知られている。

[0003] 図１０は、暗号化した管理情報を不揮発性メモリに格納するＭＰＵを説明するための図である。図１０に示す例では、管理ユニットのＭＰＵは、管理ユニット固有の暗号鍵を用いて情報を暗号化する暗号化部と、暗号化された情報を復号化する復号部とを有する。なお、これらの暗号化部や復号部は、論理回路またはプログラムによりＭＰＵ内部に構成するものとする。また、ＭＰＵは、管理情報を格納するためのフラッシュメモリと接続されている。

[0004] このようなＭＰＵは、管理情報をフラッシュメモリに格納する場合には、暗号化部を用いて、管理情報を暗号化し、暗号化した管理情報をフラッシュメモリに格納する。また、ＭＰＵは、復号部を用いて、フラッシュメモリに格納された管理情報を復号化する。また、ＭＰＵは、復号化した管理情報か

ら暗号鍵（復号鍵）を取得し、この鍵を使って、別に取得した暗号化済ＡＶデータを復号する。その後、ＭＰＵは、通信Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）を介して、復号化したＡＶデータをＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）やＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）等の本体に送信する。

先行技術文献

特許文献

[0005] 特許文献1：特開２０００－３４１６３２号公報

特許文献2：特開平０７－２２５５５１号公報

発明の概要

発明が解決しようとする課題

[0006] しかし、上述した暗号化した管理情報をフラッシュメモリ等の不揮発性メモリに格納する技術では、暗号化した管理情報をそのまま不揮発性メモリに格納する。このため、暗号化前の管理情報を容易に推定することができる場合には、攻撃者は、暗号化前の管理情報と、暗号化後の管理情報とを用いて、全数攻撃により暗号鍵を取得することができる。結果として、耐タンパー性を満たせないという問題があった。

[0007] 図１１は、ＡＶデータの管理情報の一例を説明するための図である。図１１に示す例では、管理情報は、複数の格納領域を有し、各格納領域には、２ｂｙｔｅの管理番号、４ｂｙｔｅの管理ＩＤ、２ｂｙｔｅの許可フラグ、１ｂｙｔｅのコピー回数、３ｂｙｔｅの有効期限、３６ｂｙｔｅの名前、１６ｂｙｔｅの暗号鍵が格納される。ここで、管理情報に格納される暗号鍵とは、管理対象であるＡＶデータを復号化するための復号（暗号）鍵である。

[0008] 例えば、ＭＰＵは、不揮発性メモリのデータを初期化する場合には、管理情報の各格納領域に「０」を格納した初期値を生成する。そして、ＭＰＵは、生成した初期データを暗号化し、暗号化した初期データをそのまま不揮発性メモリに格納する。このため、不揮発性メモリに格納された管理情報を解析しようとする攻撃者は、不揮発性メモリのデータを初期化し、不揮発性メ

モリのデータを解析した場合には、全ての格納領域に「０」が格納された初期値を暗号化した値を取得することができる。

[0009] ここで、攻撃者は、不揮発性メモリのデータを初期化した際に、各格納領域に「０」が格納された管理情報が初期値として生成されることを容易に推定できる。このため、攻撃者は、推定された初期値と、初期値を暗号化した値とを用いて、暗号鍵を解析するための全数攻撃を行うことができる。つまり、攻撃者は、初期値のように推定が容易な管理情報を暗号化した値が不揮発性メモリに格納されていた場合には、管理情報を暗号化する暗号鍵の解析を容易に行う事ができる。

[0010] このように、ＭＰＵが暗号化した管理情報をそのまま不揮発性メモリに格納した場合には、管理情報を暗号化するための暗号鍵の解析が容易となるので、耐タンパー性を悪化させてしまう。結果として、管理情報を暗号化する暗号鍵の解析を容易にし、耐タンパー性を悪化させてしまう。

[0011] 本願に開示の技術は、一側面では、暗号鍵の解析を困難にし、耐タンパー性を改善する。

課題を解決するための手段

[0012] 一側面では、本発明の情報処理装置は、秘匿する値を所定の暗号鍵を用いて暗号化する。また、情報処理装置は、秘匿する値が、暗号化された値を格納する記憶装置の初期化時に書込まれる初期値である場合には、暗号化された値を、逆変換可能であって秘匿する値を暗号化した暗号鍵に依存しない値に変換する。その後、情報処理装置は、変換した値を記憶装置に格納する。

発明の効果

[0013] 本願に開示の技術は、一つの態様によれば、暗号鍵の解析を困難にし、耐タンパー性を改善する。

図面の簡単な説明

[0014] [図1]図１は、実施例１に係るＭＰＵを説明するための図である。

[図2]図２は、実施例１に係るフラッシュメモリに格納されるデータの一例を説明するための図である。

[図3]図３は、従来のフラッシュメモリに格納される初期データを説明するための図である。

[図4]図４は、従来のＭＰＵが管理情報を操作する単位を説明するための図である。

[図5]図５は、従来のフラッシュメモリに格納されるデータの一例を説明するための図である。

[図6]図６は、従来のセキュアユニットの一例を説明するためのシーケンス図である。

[図7]図７は、従来のセキュアユニットがフラッシュメモリに格納した管理情報の一例を説明するための図である。

[図8]図８は、実施例２に係るＭＰＵを説明するための図である。

[図9]図９は、情報処理プログラムを実行するＬＳＩの一例を説明するための図である。

[図10]図１０は、暗号化した管理情報を不揮発性メモリに格納するＭＰＵを説明するための図である。

[図11]図１１は、ＡＶデータの管理情報の一例を説明するための図である。

発明を実施するための形態

[0015] 以下に添付図面を参照して本願に係る情報処理装置、情報処理方法及び情報処理プログラムについて説明する。

実施例 1

[0016] 以下の実施例１では、図１を用いて、著作権で保護された動画等のＡＶデータに係る管理情報を管理するＭＰＵの一例を説明する。図１は、実施例１に係るＭＰＵを説明するための図である。なおＭＰＵ１は、例えば、暗号化されたＡＶデータの復号化を行うセキュアユニットや小さな組み込みユニット等に設置されるＭＰＵであるものとする。

[0017] また、フラッシュメモリに保存される管理情報には、ＡＶデータの暗号化や復号化を行うための暗号鍵、ＡＶデータの名称、ＡＶデータを複製することができる許可回数等の情報が格納されているものとする。例えば、管理情

報は、ＡＶデータに係る管理番号、ＡＶデータに係る管理ＩＤ、複製許可フラグ、ＡＶデータを複製することができる許可回数、有効期限、ＡＶデータの名前、ＡＶデータを復号化するための暗号鍵等をレコードとして有する。

[0018] 図１に示すように、ＭＰＵ１は、ＣＰＵ（Central Processing Unit）処理ユニット２、通信Ｉ／Ｆ（Interface）３、レジスタ４、メモリ５、ＲＯＭ（Read Only Memory）６を有する。また、ＭＰＵ１は、第１暗号化部７、初期データ生成部８、第２暗号化部９、第１ＸＯＲ算出部１０、第２ＸＯＲ算出部１１、復号部１２を有する。また、ＭＰＵ１は、外部のフラッシュメモリ２０と接続される。

[0019] 通信Ｉ／Ｆ３は、ＡＶデータの再生を行うＰＣ（Personal Computer）やＳＴＢ（Set Top Box）とＡＶデータの送受信を行うインターフェースであり、ＰＣＩ（Peripheral Component Interconnect）バスやＵＳＢ（Universal Serial Bus）等が適用される。また、通信Ｉ／Ｆ３は、公開鍵暗号方式等を用いて、ＡＶデータに係る管理情報を管理するサーバと通信し、ＡＶデータに係る管理情報を受信する。

[0020] レジスタ４は、ＣＰＵ処理ユニット２が用いる一時記憶装置である。また、メモリ５は、ＣＰＵ処理ユニット２が用いるメモリである。また、ＲＯＭ６は、ＣＰＵ処理ユニット２が実行する処理のプログラムが格納されている。

[0021] ＣＰＵ処理ユニット２は、ＡＶデータの管理情報を管理する。具体的には、ＣＰＵ処理ユニット２は、通信Ｉ／Ｆ３を介して、ＡＶデータを復号するための暗号鍵等の管理情報を取得した場合には、取得した管理情報を第１暗号化部７へ送信する。また、ＣＰＵ処理ユニット２は、取得した管理情報を格納するフラッシュメモリ２０のメモリアドレスを第１暗号化部７に送信する。また、ＣＰＵ処理ユニット２は、初期データを生成させるトリガ信号を初期データ生成部８に送信する。

[0022] また、ＣＰＵ処理ユニット２は、通信Ｉ／Ｆ３を介して、ＳＴＢ等からコンテンツＩＤと暗号化されたコンテンツとを受信した場合には、管理情報の

取得要求と受信したコンテンツＩＤが示す管理情報が格納されたメモリアドレスを復号部１２へ送信する。また、ＣＰＵ処理ユニット２は、初期データを生成させるトリガ信号を初期データ生成部８へ送信する。その後、ＣＰＵ処理ユニット２は、第２ＸＯＲ算出部１１および復号部１２を介して、復号された管理情報を受信した場合には、受信した管理情報を用いて、受信したコンテンツを復号化する。その後、ＣＰＵ処理ユニット２は、通信Ｉ／Ｆ３を介して、複合化したコンテンツをＰＣやＳＴＢへ送信する。

[0023] また、ＣＰＵ処理ユニット２は、通信Ｉ／Ｆ３を介して、初期化する管理情報が通知された場合には、管理情報の初期値である初期データを生成する。また、ＣＰＵ処理ユニット２は、通知された情報が示す管理情報が格納されたフラッシュメモリ２０のメモリアドレスを判別する。そして、ＣＰＵ処理ユニット２は、生成した初期データと判別したメモリアドレスとを第１暗号化部７へ送信する。また、ＣＰＵ処理ユニット２は、初期データを生成させるトリガ信号を初期データ生成部８に送信する。

[0024] 例えば、ＣＰＵ処理ユニット２は、初期化する管理情報が格納されたメモリアドレスとして「０ｘ００」、「０ｘ８」、「０ｘ１０」を判別する。また、ＣＰＵ処理ユニット２は、フラッシュメモリ２０のメモリアドレス「０ｘ００」に格納する初期データとして、１６進数のデータ「Ｅ０、００、００、００、００、００、００、００」を生成する。

[0025] また、ＣＰＵ処理ユニット２は、フラッシュメモリ２０のメモリアドレス「０ｘ０８」と「０ｘ１０」に格納する初期データとして、１６進数のデータ「００、００、００、００、００、００、００、００」を生成する。そして、ＣＰＵ処理ユニット２は、判別したメモリアドレスと、各メモリアドレスに格納される初期データとを第１暗号化部７へ送信する。

[0026] 第１暗号化部７は、秘匿する情報を所定の暗号鍵を用いて暗号化する。具体的には、第１暗号化部７は、ＣＰＵ処理ユニット２からＡＶデータの管理情報とフラッシュメモリ２０のメモリアドレスとを取得する。すると、第１暗号化部７は、所定の暗号鍵を用いて、取得したＡＶデータの管理情報を暗

号化する。その後、第１暗号化部７は、暗号化した管理情報と取得したメモリアドレスとを第１ＸＯＲ算出部１０へ送信する。

[0027] 同様に、第１暗号化部７は、ＣＰＵ処理ユニット２から初期データを受信した場合には、所定の暗号鍵を用いて、受信した初期データを暗号化する。そして、第１暗号化部７は、暗号化した初期データを第１ＸＯＲ算出部１０へ送信する。

[0028] ここで、第１暗号化部７が用いる暗号鍵については、任意の方式および任意の長さの暗号鍵が適用される。以下の説明では、第１暗号化部７は、ＭＵＬＴＩ２やＣＡＳＴ－１２８などの８バイトをブロック長とする暗号方式を用いて、ＥＣＢ（Electronic CodeBook）モードで管理情報および初期データの暗号化を行うものとする。なお、暗号鍵の方式及び暗号鍵の長さ、処理モードについては、これに限定されるものではない。

[0029] 例えば、第１暗号化部７は、ＣＰＵ処理ユニット２から、メモリアドレス「０ｘ００」に格納する初期データとして、「Ｅ０、００、００、００、００、００、００、００」を取得する。このような場合には、第１暗号化部７は、取得した初期データ「Ｅ０、００、００、００、００、００、００、００」をＥＣＢモードで８ｂｙｔｅごとに暗号化したデータ「１２０１、０４ＡＦ、９８Ａ３、３１Ｂ３」を算出する。

[0030] また、第１暗号化部７は、メモリアドレス「０ｘ０８」、「０ｘ１０」に格納する初期データ「００、００、００、００、００、００、００、００」を取得する。このような場合には、第１暗号化部７は、取得した「００、００、００、００、００、００、００、００」を暗号化したデータ「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を算出する。

[0031] その後、第１暗号化部７は、取得したメモリアドレス「０ｘ００」、「０ｘ０８」、「０ｘ１０」と、算出したデータ「１２０１、０４ＡＦ、９８Ａ３、３１Ｂ３」、「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を第１ＸＯＲ算出部１０へ送信する。

[0032] 初期データ生成部８は、初期データを生成し、生成した初期データを第２

暗号化部９へ送信する。具体的には、初期データ生成部８は、ＣＰＵ処理ユニット２から初期データを生成させるトリガ信号を受信した場合には、初期データを生成し、生成した初期データを第２暗号化部９へ送信する。

[0033] 例えば、初期データ生成部８は、フラッシュメモリの各メモリアドレスに格納する初期データとして、１６進数のデータ「００、００、００、００、００、００、００、００」を作成する。そして、初期データ生成部８は、生成した初期データと受信したメモリアドレスとを第２暗号化部９へ送信する。

[0034] 第２暗号化部９は、第１暗号化部７が用いる暗号鍵と同一の暗号鍵を用いて、初期データを暗号化し、暗号化した初期データを第１ＸＯＲ算出部１０および第２ＸＯＲ算出部１１へ送信する。具体的には、第２暗号化部９は、初期データ生成部８から初期データを受信した場合には、第１暗号化部７が用いる暗号鍵と同一の暗号鍵を用いて、受信した初期データを暗号化する。その後、第２暗号化部９は、暗号化した初期データを第１ＸＯＲ算出部１０および第２ＸＯＲ算出部１１に送信する。

[0035] 例えば、第２暗号化部９は、初期データ生成部８から、初期データとして、「００、００、００、００、００、００、００、００」を受信する。このような場合には、第２暗号化部９は、第１暗号化部７と同一の暗号鍵を用いて、受信した各初期データを暗号化する。

[0036] つまり、第２暗号化部９は、取得した「００、００、００、００、００、００、００、００」を暗号化したデータ「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を算出する。その後、第２暗号化部９は、算出したデータ「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を第１ＸＯＲ算出部１０および第２ＸＯＲ算出部１１へ送信する。

[0037] 第１ＸＯＲ算出部１０は、第１暗号化部７によって暗号化された情報を加工し、第１暗号化部７が用いた暗号鍵に依存しない情報であって、かかる暗号鍵に依存しない情報から第１暗号化部７によって暗号化された情報に逆変換可能な情報に変換する。そして、第１ＸＯＲ算出部１０は、変換した情報

をフラッシュメモリ２０に格納する。

[0038] 具体的には、第１ＸＯＲ算出部１０は、第１暗号化部７から暗号化された管理情報と管理情報を格納するメモリアドレスとを取得する。また、第１ＸＯＲ算出部１０は、第２暗号化部９から暗号化された初期データを取得する。そして、第１ＸＯＲ算出部１０は、暗号化された管理情報と暗号化された初期データとの排他的論理和を取った情報を算出する。その後、第１ＸＯＲ算出部１０は、フラッシュメモリ２０が有する記憶領域のうち、取得したメモリアドレスに算出した値を格納する。

[0039] 図２は、実施例１に係るフラッシュメモリに格納されるデータの一例を説明するための図である。例えば、図２に示す例では、第１ＸＯＲ算出部１０は、第１暗号化部７の暗号結果として、メモリアドレス「０ｘ００」に格納する管理情報の暗号結果「１２０１、０４ＡＦ、９８Ａ３、３１Ｂ３」を受信する。また、第１ＸＯＲ算出部１０は、第１暗号化部７の暗号結果として、メモリアドレス「０ｘ０８」、「０ｘ１０」に格納する管理情報の暗号結果「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を受信する。

[0040] また、第１ＸＯＲ算出部１０は、第２暗号化部９から、暗号化された初期データ「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を受信する。そして、第１ＸＯＲ算出部１０は、第１暗号化部７によって暗号化された各メモリアドレスに格納する管理情報と、第２暗号化部９によって暗号化された初期データとの排他的論理和をビットごとに取った情報を算出する。

[0041] この結果、第１ＸＯＲ算出部１０は、メモリアドレス「０ｘ００」に格納するメモリデータとして、「０Ｂ３５、Ａ０Ｂ３、８Ａ３Ｂ、８１Ａ０」を算出する。そして、第１ＸＯＲ算出部１０は、算出したデータ「０Ｂ３５、Ａ０Ｂ３、８Ａ３Ｂ、８１Ａ０」をフラッシュメモリ２０のメモリアドレス「０ｘ００」に格納する。

[0042] また、第１ＸＯＲ算出部１０は、メモリアドレス「０ｘ０８」、「０ｘ１０」に格納するメモリデータとして、「００００、００００、００００、００００」を算出する。そして、第１ＸＯＲ算出部１０は、算出したデータ「

００００、００００、００００、００００」をフラッシュメモリ２０のメモリアドレス「０ｘ０８」、「０ｘ１０」に格納する。

[0043] このように、第１ＸＯＲ算出部１０は、ＭＰＵ１が管理情報の初期化を行う場合には、第１暗号化部７が初期データを所定の暗号鍵で暗号化した値を取得する。また、第１ＸＯＲ算出部１０は、ＭＰＵ１が管理情報の初期化を行う場合には、第２暗号化部９が初期データを第１暗号化部７が用いる暗号鍵と同一の暗号鍵を用いて暗号化した値を取得する。そして、第１ＸＯＲ算出部１０は、第１暗号化部７および第２暗号化部９から取得した情報の排他的論理和を取った情報を算出し、算出した値をフラッシュメモリ２０に格納する。

[0044] この結果、第１ＸＯＲ算出部１０は、第１暗号化部７および第２暗号化部９から取得した情報同士の排他的論理和を取った場合には、管理情報と同じビット数の情報であって、全てのビットが「０」の情報を算出することとなる。つまり、第１ＸＯＲ算出部１０は、同じ暗号鍵を用いて暗号化した初期データ同士の排他的論理和を算出することによって、暗号鍵に依存しない情報を算出する。このため、第１ＸＯＲ算出部１０は、初期データを暗号化した値ではなく、管理情報と同じビット数の情報であって、全てのビットが「０」の情報をフラッシュメモリ２０の初期化するメモリアドレスに格納する。

[0045] このような場合には、攻撃者は、フラッシュメモリ２０を解析した際に、従来技術における暗号化された初期データを取得することができない。このため、攻撃者は、暗号化する前の初期データを容易に推定できる場合であっても、それに対応する暗号化された初期データを取得することができないので、管理情報を暗号化する暗号鍵を全数攻撃により解析することがきわめて困難である。

[0046] また、初期データ以外の部分については、暗号化前の情報を推定することは難しい。このため、攻撃者は、初期データ以外の部分について暗号化された情報を用いて、暗号鍵を全数攻撃により解析できないと考えられる。結果

として、ＭＰＵ１は、フラッシュメモリ２０に格納された管理情報の解析を困難にし、耐タンパー性を向上させることができる。

[0047] 一方、従来技術を実装したＭＰＵ（以下、従来のＭＰＵと称する）は、暗号化した値をそのままフラッシュメモリに格納する。このため、従来のＭＰＵは、物理的に厳密にタンパーフリーに構成しない限り、外付けされたフラッシュメモリから攻撃者が暗号化後の値を取得することを防ぐことができない。

[0048] 以下、このような従来のＭＰＵについての詳細を説明する。例えば、図３は、従来のフラッシュメモリに格納される初期データを説明するための図である。図３に示す例では、初期データとして、全ての格納領域に「ａｌｌ＿０」を示す情報が格納されている。従来のＭＰＵは、このような管理情報を十分に秘匿するため、各管理情報の「ａｌｌ＿０」を暗号化した値をフラッシュメモリに格納する。

[0049] ここで、上記の説明では、従来のＭＰＵが便宜上ＥＣＢモードを使う例を説明したが、暗号技術においては、特に初期データのような典型的なデータに対する暗号の強度を高める方法としてＥＣＢでなくＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）などのモードを使うことが知られている。これは、あるブロックの暗号結果が直前のブロックのデータや暗号結果に依存するようにするものである。

[0050] 図４は、従来のＭＰＵが管理情報を操作する単位を説明するための図である。図４に示す例では、管理情報２の暗号は、ＣＢＣモードを適用した場合には、直前のデータである管理情報１に依存することになる。

[0051] 実際には、ＡＶデータの再生や複製に伴って、複製許可回数を減らすなど管理情報を更新することがある。たとえば管理情報1に対応するＡＶデータをダビングしたとき、ダビング許可回数を１だけ減じるごとくである。この場合、管理情報１を更新する必要があり、その結果管理情報２、したがって管理情報３も再暗号化しなくてはならなくなる。これは好ましくない実装である。

[0052] そこで、管理情報の暗号鍵を、管理番号ごとに異なるようにする方法がある。例えば、ＭＰＵがもつ暗号鍵に管理情報を書き込むメモリアドレスを組み合わせるなどである。図４に示す例では、管理番号ごとに個別の暗号鍵を用いる例を示した。この方法によれば、「ａｌｌ＿０」のような初期データに対する暗号結果は管理番号により変化する。

[0053] しかしながら、特定の管理番号ないしメモリアドレスについては、特定の暗号鍵を使っていることは同様である。特定の管理番号に注目して攻撃する場合には、その初期データ（「ａｌｌ＿０」など）と、その管理番号に対する暗号鍵で暗号化した結果が得られるので、これを用いてその管理番号に対する暗号鍵を推定する全数攻撃が可能となる。

[0054] このように従来のＭＰＵは、管理情報を暗号化してフラッシュメモリに格納するものの、物理的に厳密にタンパーフリーに構成しない限り、外付けされたフラッシュメモリから攻撃者が暗号化後の値を取得することを防ぐことができない。結果、容易に推定できる値を暗号化してフラッシュメモリに格納した場合には、攻撃者は、推定し易い値に係る暗号化前の値と暗号化後の値とを取得することができ、容易に全数攻撃を行う事ができる。

[0055] 例えば、従来のＭＰＵは、図５に示すように、ＣＰＵからみた値のデータとして、初期データ「Ｅ５、００、００、００、００、００、００、００」を暗号化した値「１２０１、０４ＡＦ、９８Ａ３、３１Ｂ３」をメモリアドレス「０ｘ００」に格納する。また、従来のＭＰＵは、ＣＰＵからみた値のデータとして、初期データ「００、００、００、００、００、００、００、００」を暗号化した値「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」をメモリアドレス「０ｘ０８」、「０ｘ１０」に格納する。図５は、従来のフラッシュメモリに格納されるデータの一例を説明するための図である。

[0056] このため、攻撃者は、フラッシュメモリを解析することによって、「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」が初期データ「００、００、００、００、００、００、００、００」を暗号化した値であると推定することができる。結果として、攻撃者は、推定される初期データ「００、００、００、

００、００、００、００、００」と取得した値「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」から、暗号鍵の全数攻撃を容易に行う事ができる。結果、従来の技術は、耐タンパー性の問題がある。

[0057] また、従来の技術は、暗号化した初期データをそのままフラッシュメモリに格納するので、長い鍵長を有する暗号鍵や、強固な暗号方式を採用したとしても、暗号化された初期データが攻撃者に取得された場合には、暗号鍵の全数攻撃を可能としてしまう。つまり、従来のＭＰＵは、暗号鍵方式等によらず、全数攻撃を防げないという問題があった。

[0058] 一方、本発明のＭＰＵ１は、暗号方式や暗号鍵の長さによらず、暗号化後に保存した初期データを暗号鍵によらない値とすることができる。このため、全数攻撃によっても、攻撃者による暗号鍵の推定をきわめて困難とする。これにより耐タンパー性を向上させることができる。

[0059] 図１に戻って、第２ＸＯＲ算出部１１は、第１暗号化部７が用いる暗号鍵と同一の暗号鍵を用いて暗号化した値と、第１ＸＯＲ算出部１０によってフラッシュメモリ２０に格納された情報との排他的論理和を取った情報を算出する。そして、第２ＸＯＲ算出部１１は、算出した値を復号部１２へ送信する。

[0060] 具体的には、第２ＸＯＲ算出部１１は、復号部１２からフラッシュメモリ２０のメモリアドレスを取得した場合には、フラッシュメモリ２０に格納された情報のうち、取得したメモリアドレスに格納された情報を取得する。つまり、第２ＸＯＲ算出部１１は、第１暗号化部７によって暗号化された管理情報と、第２暗号化部９によって暗号化された初期データとの排他的論理和を取った情報を取得する。

[0061] また、第２ＸＯＲ算出部１１は、第２暗号化部９が第１暗号化部７が用いた暗号鍵と同一の暗号鍵で暗号化された初期データを取得する。そして、第２ＸＯＲ算出部１１は、フラッシュメモリ２０から取得した情報と第２暗号化部９から取得した情報との排他的論理和を取った情報を算出する。

[0062] つまり、第２ＸＯＲ算出部１１は、暗号化された管理情報と暗号化された

初期データとの排他的論理和に対して、さらに暗号化された初期データとの排他的論理和を取った情報を算出する。この結果、第２ＸＯＲ算出部１１は、第１暗号化部７によって暗号化された管理情報を算出する。その後、第２ＸＯＲ算出部１１は、算出した値、つまり、第１暗号化部７によって暗号化された管理情報と同じ情報を復号部１２へ送信する。

[0063] 復号部１２は、第１暗号化部７が用いた暗号鍵と同一の暗号鍵を用いて、第２ＸＯＲ算出部１１によって算出された情報を復号する。具体的には、復号部１２は、ＣＰＵ処理ユニット２からフラッシュメモリ２０のメモリアドレスを受信した場合には、受信したメモリアドレスを第２ＸＯＲ算出部１１に通知する。そして、復号部１２は、第２ＸＯＲ算出部１１から、通知したメモリアドレスに格納された情報と第２暗号化部９によって暗号化された初期データとの排他的論理和を取った情報を受信する。

[0064] つまり、復号部１２は、第２ＸＯＲ算出部１１から、第１暗号化部７によって暗号化された管理情報を取得する。そして、復号部１２は、第１暗号化部７によって用いられた暗号鍵を用いて、暗号化された管理情報を復号する。

[0065] 例えば、復号部１２は、第２ＸＯＲ算出部１１によって算出された情報「１２０１、０４ＡＦ、９８Ａ３、３１Ｂ３」を復号した場合には、「Ｅ５、００、００、００、００、００、００、００」を取得する。そして、復号部１２は、取得した「Ｅ５、００、００、００、００、００、００、００」をＣＰＵ処理ユニット２に送信する。

[0066] また、復号部１２は、第２ＸＯＲ算出部１１によって算出された情報「１９３４、Ａ４１Ｃ、１２９８、Ｂ０１３」を復号した場合には、「００、００、００、００、００、００、００、００」を取得する。そして、復号部１２は、取得した「００、００、００、００、００、００、００、００」をＣＰＵ処理ユニット２に送信する。

[0067] このように、第２ＸＯＲ算出部１１は、フラッシュメモリ２０に格納された管理情報を取得する場合には、フラッシュメモリ２０に格納された情報と

初期データを暗号化した値との排他的論理和を取った情報を算出する。そして、復号部１２は、第２ＸＯＲ算出部１１によって算出された情報を復号する。このため、ＭＰＵ１は、フラッシュメモリ２０に格納された情報を、正確に復号することができる。

[0068] また、ＭＰＵ１は、ＣＰＵ処理ユニット２とフラッシュメモリ２０とを接続する回路上に各部７～１２を有する。このため、ＭＰＵ１は、フラッシュメモリ２０に暗号化された情報が格納されていることを考慮したプログラムをＣＰＵ処理ユニット２に実行させずとも、適切に動作することができる。

[0069] 例えば、通信Ｉ／Ｆ３、ＣＰＵ処理ユニット２、第１暗号化部７、初期データ生成部８、第２暗号化部９、第１ＸＯＲ算出部１０、第２ＸＯＲ算出部１１、復号部１２とは、電子回路である。ここで、電子回路の例として、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路、またはＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などを適用する。また、各部７～１２は、ＰＬＡ（Programmable Logic Array）やゲートアレイなどの論理回路を適用してもよい。

[0070] このように、ＭＰＵ１は、フラッシュメモリ２０に暗号化された情報を格納する場合には、情報を暗号化した暗号鍵と同一の暗号鍵で暗号化した初期データとの排他的論理和を算出し、算出した排他的論理和をフラッシュメモリ２０に格納する。このため、ＭＰＵ１は、フラッシュメモリ２０に初期データを格納する場合には、すべてのビットが「０」の情報をフラッシュメモリ２０に格納するので、攻撃者に初期データに対応する暗号結果を秘匿することができる。これにより、この方式では攻撃者が全数攻撃を用いて、情報を暗号化する暗号鍵を算出することを防ぎ、高タンパー性を改善することができる。

[0071] 次に、図を用いて、著作権によって保護されるＡＶデータを暗号化して配信するサーバから、ＡＶデータを復号するための暗号鍵を受信し、受信した暗号鍵を管理するセキュアユニットにＭＰＵ１を適用する例について説明す

る。

[0072] 図６は、セキュアユニットの一例を説明するためのシーケンス図である。図６に示す例では、サーバ３０は、公開鍵暗号方式に基づく秘密鍵ＫＨＳと公開鍵ＫＰＳを有する。また、セキュアニット５０は、ユニットごとに固有の秘密鍵ＫＨ１と公開鍵ＫＰ１を有する。また、図６に示す例では、セキュアユニット５０は、ＭＰＵ１を有し、ＭＰＵ１を用いて、暗号化した値をフラッシュメモリに格納するものとする。

[0073] 図６に示す例では、ＡＶデータをサーバ３０から受信する受信機４０が、購入するＡＶデータをコンテンツＩＤにより指定する（ステップＳ１）。すると、サーバ３０は、ユーザの認証や課金処理を行うとともに、自己の公開鍵であるＫＰＳとセキュアユニット５０が有する認証データの要求とをセキュアユニット５０に要求する（ステップＳ２）。

[0074] 次に、セキュアユニット５０は、ＫＰ１と認証データとをＫＰＳで暗号化し、暗号化したＫＰ１と認証データとをサーバ３０へ送信する（ステップＳ３）。サーバ３０は、暗号化した認証データを復号化し、認証データを検証する（ステップＳ４）。次に、サーバ３０は、コンテンツの暗号鍵ＣＫを生成し、要求されたコンテンツのコンテンツＩＤとともに生成したＣＫをＫＰ１で暗号化してセキュアユニット５０へ送信する（ステップＳ５）。

[0075] 次に、セキュアユニット５０は、コンテンツＩＤとＣＫとを取得した場合には、ＭＰＵ１を用いて、取得したコンテンツＩＤとＣＫとを暗号化する（ステップＳ６）。そして、セキュアユニット５０は、ＭＰＵ１を用いて、セキュアユニットごとに固有の暗号鍵で暗号化したコンテンツＩＤと暗号化したＣＫとを含む管理情報をフラッシュメモリに格納する（ステップＳ７）。ここでは管理情報の暗号方式としてＡＥＳ（１２８ビット）を用いており、そのことが知られているとする。

[0076] また、サーバ３０は、ＣＫで暗号化したコンテンツを受信機４０に送信する（ステップＳ８）。すると、受信機４０は、受信したコンテンツを自装置のＨＤＤ（Hard Disk Drive）等に保存する（ステップＳ９）。なお、受信

機４０が受信したコンテンツは、セキュアユニット５０に送信されたＣＫによって暗号化されており、ＣＫはセキュアユニット５０のみに存在するため、セキュアユニット５０なしではコンテンツを復号できない。

[0077] 受信機４０は、受信したコンテンツを再生する場合には、ＣＫによって暗号化されたコンテンツを読み出すとともに（ステップＳ１０）、セキュアユニット５０にコンテンツＩＤを指定して、暗号化されたコンテンツの復号を要求する（ステップＳ１１）。すると、セキュアユニット５０は、コンテンツＩＤを手掛かりに用いて、フラッシュメモリに格納されたＣＫを読み出して復号し、このＣＫを用いて、暗号化されたコンテンツを復号する。

[0078] また、セキュアユニット５０は、ランダムな乱数ＥＫを生成し、生成したＥＫを用いてコンテンツを暗号化し、暗号化したコンテンツと受信機４０のＡＶ出力部が持つ公開鍵ＫＰＤで暗号化したＥＫを受信機４０へ返信する（ステップＳ１２）。その後、受信機４０のＡＶ出力部分は秘密鍵ＫＨＤによって、ＥＫを復号し、生成したＥＫを用いて受信したコンテンツを復号し、内部解析を困難にしつつ、復号したコンテンツの映像出力を行う（ステップＳ１３）。

[0079] このようなシステムにおいて、攻撃者は、コンテンツの複製や不正利用を行おうとする場合には、セキュアユニット５０によってフラッシュメモリに格納された情報を解析し、ＣＫを解読しようとする。例えば、セキュアユニット５０がＭＰＵ１ではなく、従来のＭＰＵを用いてコンテンツを暗号化したＣＫを一つだけ保存した場合には、フラッシュメモリに、図７に示すデータを格納する。なお、図７は、従来のセキュアユニットがフラッシュメモリに格納した管理情報の一例を説明するための図である。

[0080] ここで、図７に示すデータにおいて「１２、Ｃ１、Ｄ９、１１、０２、Ａ０、９８、９９、２５、Ｃ１、８Ｃ、９３、４３、１２、４７、１０」という情報が反復している。このため、攻撃者は、この反復している情報が、初期データとしてよく使われる「ａｌｌ　０」を１６ｂｙｔｅの暗号鍵で暗号化したものだと容易に仮定することができる。

[0081] すると、攻撃者は、「ａｌｌ　０」をＡＥＳ－１２８ｂｉｔで暗号化した際に、この反復したデータを算出する暗号鍵を検索するだけで、フラッシュメモリに格納されたＣＫを取得することができると考えられる。また、攻撃者は、「ａｌｌ　０」を様々な暗号鍵で暗号化した辞書を用いることによって、容易に暗号鍵を算出することができると考えられる。

[0082] 一方、図６に示したシステムにおいて、セキュアユニット５０に実施例１に係るＭＰＵ１を適用した場合には、図７中の反復する情報、つまり、初期データを暗号化した値の部分には、暗号鍵に依存しない情報、つまり「０」が格納される。このため、攻撃者は、初期データの推定が容易な場合にも、暗号化された初期データを取得することができず、ＣＫを暗号化した暗号鍵を全数攻撃により算出することができない。結果として、ＭＰＵ１は、耐タンパー性を向上させることができる。

[0083] ［実施例１の効果］

上述したように、ＭＰＵ１は、管理情報を所定の暗号鍵を用いて暗号化する。そして、ＭＰＵ１は、秘匿する値がフラッシュメモリ２０の初期化時に書込まれる初期データである場合には、暗号化された管理情報を、逆変換可能であって、暗号鍵に依存しない情報になるように変換する。その後、ＭＰＵ１は、変換した情報をフラッシュメモリ２０に格納する。つまり、ＭＰＵ１は、管理情報を暗号化した際に用いた暗号鍵と一対一で対応しない情報をフラッシュメモリ２０に格納する。

[0084] このため、ＭＰＵ１は、暗号化した管理情報の初期データを攻撃者から秘匿することができる。結果として、ＭＰＵ１は、攻撃者が全数攻撃を用いて暗号鍵を解析する処理を事実上不可能にし、僅かなコストで耐タンパー性を向上させることができる。

[0085] また、ＭＰＵ１は、第１暗号化部７が所定の暗号鍵を用いて暗号化した管理情報と、第２暗号化部９が第１暗号化部７と同一の暗号鍵を用いて暗号化した所定の情報との排他的論理和を取った情報をフラッシュメモリ２０に格納する。このため、ＭＰＵ１は、暗号化された管理情報を容易に秘匿するこ

とができる。

[0086] つまり、暗号化された管理情報を秘匿する方法として、第１暗号化部７が管理情報を暗号化した値を監視し、推定が容易な管理情報を暗号化した値を検出し、検出された情報のビットを「０」や所定の情報に置き換える処理等を行ってもよい。しかし、第１暗号化部７が管理情報を暗号化した値を全て監視する処理は、計算コストが大きくなる。

[0087] 一方、ＭＰＵ１は、暗号化した管理情報と、暗号化した初期データとの排他的論理和を取るだけで暗号化された管理情報の初期データを容易に秘匿することができる。この結果、ＭＰＵ１は、第１暗号化部７が暗号化した値を監視せずともよく、暗号化された管理情報を容易に秘匿することができる。

[0088] このように、ＭＰＵ１は、管理情報の初期データをフラッシュメモリ２０に格納する場合には、初期データを暗号化した値を攻撃者から秘匿することができる。結果として、ＭＰＵ１は、攻撃者が暗号化された初期データと推定される初期データとから暗号鍵を解析する処理を困難にし、耐タンパー性を向上させることができる。

[0089] また、ＭＰＵ１は、初期データをフラッシュメモリ２０に格納する場合には、典型的には、対応するフラッシュメモリ２０の格納領域すべてのビットに「０」を格納することとなる。従来技術であれば「０」を暗号化した結果をフラッシュメモリに書き込むことになるが、これは暗号鍵に依存する。本発明を適用すると暗号鍵によらず「０」を書き込めばよいので、フラッシュメモリ単体であらかじめ書き込んでおくことができる。このため、ＭＰＵ１を組み込んだ製品を製造する際に、フラッシュメモリ２０をクリアする処理を省略することができる。

[0090] つまり、従来のＭＰＵを組み込んだ製品は、製造時に初期データを暗号化した値をフラッシュメモリに書込む処理を行う。しかし、従来のＭＰＵを組み込んだ製品は、ＭＰＵが用いる暗号鍵が製品ごとに異なるため、同一の値をフラッシュメモリに格納できない。このため、製造時に全ての製品においてフラッシュメモリの初期化をおこなうこととなり、製造時のコストが上が

ってしまう。

[0091] しかし、ＭＰＵ１を組み込んだ製品は、ＭＰＵが用いる暗号鍵が製品ごとに異なった場合でも、フラッシュメモリ２０のビットをすべて「０」にするだけでよい。この結果、ビットをすべて「０」にしたフラッシュメモリを全ての製品に適用すれば初期化を行う必要がなくなるので、製造コストを下げることができる。

[0092] また、ＭＰＵ１は、第２暗号化部９によって暗号化された情報と、フラッシュメモリ２０に格納された情報との排他的論理和を取った情報を算出する。そして、ＭＰＵ１は、第１暗号化部７が用いた暗号鍵と同一の暗号鍵を用いて、算出した値を復号する。このため、ＭＰＵ１は、攻撃者から秘匿した情報を適切に読み出すことができる。

実施例 2

[0093] これまで本発明の実施例について説明したが実施例は、上述した実施例以外にも様々な異なる形態にて実施されてよいものである。そこで、以下では実施例２として本発明に含まれる他の実施例を説明する。

[0094] （１）初期データ生成部８および第２暗号化部９について

上述したＭＰＵ１の初期データ生成部８は、初期データとしてオールゼロのデータを生成していた。しかし、実施例はこれに限定されるものではなく、初期データ生成部８は、他の値を有する初期データを生成してもよい。

[0095] また、ＭＰＵ１は、第１暗号化部７と同じ暗号鍵を用いて、初期データを暗号化する第２暗号化部９を有していた。しかし、実施例は、これに限定されるものではなく、例えば、ＭＰＵ１は、初期データ生成部８と第２暗号化部９との代わりに、第１暗号化部７と同じ暗号鍵を用いて初期データを暗号化した値を記憶するレジスタを有してもよい。以下、このようなレジスタを有するＭＰＵ１ａについて説明する。

[0096] 図８は、実施例２に係るＭＰＵを説明するための図である。図８に示す例では、実施例２に係るＭＰＵ１ａは、ＭＰＵ１と同様に、通信Ｉ／Ｆ３、レジスタ４、メモリ５、ＲＯＭ６、第１暗号化部７、第１ＸＯＲ算出部１０、

第２ＸＯＲ算出部１１、復号部１２を有する。また、ＭＰＵ１ａは、初期データ生成部８と第２暗号化部９との代わりに、レジスタ１３を有する。なお、ＭＰＵ１ａが有する各部３～７、１０～１２は、ＭＰＵ１が有する各部３～７、１０～１２と同様の機能を発揮するものとする。

[0097] ＣＰＵ処理ユニット２ａは、実施例１に係るＣＰＵ処理ユニット２と同様の機能を有する。さらに、ＣＰＵ処理ユニット２ａは、初期データを第１暗号化部７に送信した場合には、暗号化された初期データをラッチするトリガ信号をレジスタ１３に送信する。また、ＣＰＵ処理ユニット２ａは、初期データを生成させるトリガ信号に変えて、暗号化された初期データを出力されるトリガ信号をレジスタ１３へ送信する。

[0098] レジスタ１３は、揮発性のメモリである。また、レジスタ１３は、第１暗号化部７と同じ暗号鍵を用いて、所定の情報を暗号化した値をあらかじめ記憶する。具体的には、レジスタ１３は、暗号化された初期データをラッチするトリガ信号をＣＰＵ処理ユニット２ａから受信した場合には、第１暗号化部７が出力した情報をラッチする。つまり、レジスタ１３は、第１暗号化部７によって暗号化された初期データをラッチする。

[0099] そして、レジスタ１３は、暗号化された初期データを出力させるトリガ信号をＣＰＵ処理ユニット２ａから受信した場合には、初期データを暗号化した値を第１ＸＯＲ算出部１０と第２ＸＯＲ算出部１１へ送信する。

[0100] このように、ＭＰＵ１ａは、第１暗号化部７と同一の暗号鍵を用いて初期データを暗号化した値をあらかじめ記憶するレジスタ１３を有する。そして、ＭＰＵ１ａは、第１暗号化部７よって暗号化された管理情報と、レジスタ１３に格納された情報との排他的論理和を取った情報をフラッシュメモリ２０に格納する。

[0101] このため、ＭＰＵ１ａは、初期データ生成部８と第２暗号化部９を不要とすることができる。このため、ＭＰＵ１ａをＦＰＧＡ（Field-Programmable Gate Array）で作成した場合には、ＭＰＵ１と比較して暗号化ユニットの数を減らすことができる。また、ＭＰＵ１ａは、ＭＰＵ１と比較して、回路

規模を小さくすることができる。

[0102] また、ＭＰＵ１ａは、初期データを暗号化した値を揮発性のメモリであるレジスタ１３に格納する。このため、ＭＰＵ１ａは、攻撃者によって分解等された場合にも、レジスタ１３に暗号化された初期データが自然に消去されるため、攻撃者に暗号化された初期データを秘匿することができる。

[0103] （２）排他的論理和を取る情報について

上述したＭＰＵ１は、第１暗号化部７が所定の暗号鍵を用いて暗号化した管理情報と、第２暗号化部９が第１暗号化部７と同じ暗号鍵を用いて暗号化した初期データとの排他的論理和を取った情報を算出した。また、ＭＰＵ１ａは、第１暗号化部７が所定の暗号鍵を用いて暗号化した管理情報と、レジスタ１３に格納された情報、つまり、第１暗号化部７が暗号化した初期データとの排他的論理和を取った情報を算出した。

[0104] しかし、実施例は、これに限定されるものではない。つまり、ＭＰＵは、所定の暗号鍵を用いて暗号化した管理情報と排他的論理和を取る情報として、初期データ以外の情報を第１暗号化部７と同じ暗号鍵を用いて暗号化した値を用いてもよい。

[0105] このようなＭＰＵの一例として、管理情報を初期化する場合には、初期化する管理情報が格納されたメモリアドレスに応じた情報をフラッシュメモリ２に格納するＭＰＵ１ｂについて説明する。例えば、ＭＰＵ１ｂが有するＣＰＵ処理ユニット２ｂは、初期化する管理情報を示す情報が通知された場合には、初期化する管理情報が格納されたフラッシュメモリ２０のメモリアドレスに応じた情報を生成する。

[0106] また、ＣＰＵ処理ユニット２ｂは、初期データ生成部８ａに対して、初期データを生成させるトリガ信号を送信するとともに、初期化する管理情報が格納されたメモリアドレスを初期データ生成部８へ送信する。つまり、ＣＰＵ処理ユニット２ｂは、初期データ生成部８ａに対して、初期データを生成させるトリガ信号を送信するとともに、アクセスするフラッシュメモリ２０のメモリアドレスを初期データ生成部８ａに送信する。

[0107] 初期データ生成部８ａは、初期データを生成させるトリガ信号とメモリアドレスとを受信した場合には、ＣＰＵ処理ユニット２ｂと同様に、受信したメモリアドレスに応じた情報を生成する。そして、初期データ生成部８ａは、生成した初期データを第２暗号化部９へ送信する。

[0108] この結果、ＭＰＵ１ｂは、所定の暗号鍵を用いて管理情報を暗号化するとともに、管理情報を暗号化した暗号鍵と同じ暗号鍵を用いて、管理情報を格納するメモリアドレスに応じた情報を暗号化する。そして、ＭＰＵ１ｂは、管理情報を暗号化した値と、メモリアドレスに応じた情報を暗号化した値との排他的論理和を取った情報をフラッシュメモリ２０に格納する。このため、ＭＰＵ１ｂは、管理情報を初期化する際に、管理情報が格納されたメモリアドレスごとに異なる初期データが格納される場合にも、適切に暗号化された初期データを攻撃者から秘匿することができる。

[0109] なお、ＣＰＵ処理ユニット２ｂおよび初期データ生成部８ａがメモリアドレスに応じた情報を生成する方法の一例としては、メモリアドレスと１６ワードの情報とを対応付けたテーブルメモリをＭＰＵ１ｂ内に設置する。そして、ＣＰＵ処理ユニット２ｂおよび初期データ生成部８は、アクセスするメモリアドレスと対応付けられた１６ワードの情報を出力する。

[0110] また、管理情報には、初期データ以外にも、攻撃者が容易に推定することができる情報が含まれる場合がある。このような情報を暗号化した値をそのままフラッシュメモリ２０に格納した場合には、攻撃者に暗号鍵を容易に解析されてしまう。このような問題を解決するため、ＭＰＵは、管理情報に含まれる情報であって、推定が容易な情報を暗号化した値と管理情報を暗号化した値との排他的論理和を取ってもよい。以下、このような処理を行うＭＰＵ１ｃについて説明する。

[0111] 例えば、ＭＰＵ１ｃは、管理情報を所定の暗号鍵で暗号化するとともに、管理情報を暗号化した暗号鍵を用いて、管理情報の一部であって推定が容易な情報を暗号化する。そして、ＭＰＵ１ｃは、管理情報を暗号化いた情報と、管理情報の一部であって推定が容易な情報を暗号化した値との排他的論理

和を取った情報をフラッシュメモリ２０に格納する。

[0112] このため、ＭＰＵ１ｃは、フラッシュメモリ２０に格納される暗号化された管理情報のうち、暗号化前の情報を攻撃者が容易に推定することができる部分については、「０」を格納することとなる。結果として、ＭＰＵ１ｃは、暗号化された管理情報のうち、暗号化前の情報を攻撃者が容易に推定することができる部分を攻撃者から秘匿することができ、耐タンパー性を高めることができる。

[0113] （３）暗号鍵について

上述したＭＰＵ１は、ＡＥＳ暗号方式の１２８ｂｉｔ長の暗号鍵を用いて、管理情報と初期データとをＥＣＢモードで暗号化していた。しかし、実施例はこれに限定されるものではなく、例えば、ＣＢＣモードやカウンタモードで暗号化してもよい。また、ＭＰＵ１は、ＤＥＳ（Data Encryption Standard）暗号方式やトリプルＤＥＳ暗号方式等、任意の暗号方式および鍵長を用いて暗号化を行うことができる。つまり、ＭＰＵ１は、任意の暗号化方式を用いて暗号化を行う事ができる。なお、本願に開示された暗号化装置、暗号化方法および暗号化プログラムは、暗号そのものを強化する手法を否定するものではなく、強化された任意の暗号アルゴリズムと併用することができる。

[0114] （４）管理情報について

上述したＭＰＵ１は、管理情報の一例として、著作権で保護されるＡＶデータの管理情報を暗号化した。しかし、実施例はこれに限定されるものではなく、他の情報についても適用可能である。また、ＭＰＵ１は、管理情報を暗号化する前に推定困難な秘密の値と排他的論理和をとった情報を算出し、算出した値を暗号化した値と初期データを暗号化した値との排他的論理和を取ることで、初期データ以外の管理情報の推定を困難にしてもよい。また、ＭＰＵ１は、ＰＣやＳＴＢ以外にも、秘匿する情報を扱う多様の装置に接続、設置してよい。

[0115] （５）プログラム

ところで、実施例１に係るＭＰＵ１、および実施例２に係るＭＰＵ１ａ～１ｃは、ハードウェアを利用して各種の処理を実現する場合を説明した。しかし、実施例はこれに限定されるものではなく、あらかじめ用意されたプログラムをＬＳＩ（Large Scale Integration）が実行することによって実現するようにしてもよい。そこで、以下では、図９を用いて、暗号化された初期値を逆変換可能であって、暗号鍵に依存しない値に変換し、変換した値をメモリに格納する情報格納プログラムを実行するＬＳＩの一例を説明する。図９は、情報処理プログラムを実行するＬＳＩの一例を説明するための図である。

[0116] 図９に例示されたＬＳＩ１００は、ＲＯＭ（Read Only Memory）１３０、ＣＰＵ（Central Processing Unit）１４０、がバス１７０で接続される。また、ＬＳＩ１００は、外部の半導体メモリ、ＰＣ、ＳＴＢと情報の送受信を行うＩ／Ｏ(Input Output)１６０がバス１７０で接続される。

[0117] ＲＯＭ１３０には、取得プログラム１３１、変換プログラム１３２、格納プログラム１３３があらかじめ保持される。ＣＰＵ１４０が各プログラム１３１～１３３をＲＯＭ１３０から読み出して実行することによって、図９に示す例では、各プログラム１３１～１３３は、暗号化プロセス１４１、変換プロセス１４２、格納プロセス１４３として機能するようになる。なお、各プロセス１４１～１４３は、図１に示した各部７～１０と同様の機能を発揮する。また、各プロセス１４１～１４３は、実施例２に係るＭＰＵ１ａ～１ｃと同等の機能を発揮するようにすることも可能である。

符号の説明

[0118] １　ＭＰＵ

２　ＣＰＵ処理ユニット

３　通信Ｉ／Ｆ

４　レジスタ

５　メモリ

６　ＲＯＭ

７　第１暗号化部

８　初期データ生成部

９　第２暗号化部

１０　第１ＸＯＲ算出部

１１　第２ＸＯＲ算出部

１２　復号部

２０　フラッシュメモリ

３０　サーバ

４０　受信機

５０　セキュアユニット

請求の範囲

[請求項1] 秘匿する値を所定の暗号鍵を用いて暗号化する暗号化部と、

前記秘匿する値が、前記暗号化部によって暗号化された値を格納する記憶装置の初期化時に書込まれる初期値である場合には、前記暗号化部によって暗号化された値を、逆変換可能であって前記暗号化部が用いた暗号鍵に依存しない値に変換する変換部と、

前記変換部によって変換された値を前記記憶装置に格納する格納部と、

を有することを特徴とする情報処理装置。

[請求項2] 前記変換部は、前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて、前記記憶装置の初期化時に書込まれる初期値を暗号化した値と、前記暗号化部によって暗号化された値との排他的論理和を変換後の値とすることを特徴とする請求項１に記載の情報処理装置。

[請求項3] 前記変換部は、前記初期値を前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて暗号化した値を揮発性のメモリにあらかじめ格納し、当該揮発性のメモリに格納された値と前記暗号化部によって暗号化された値との排他的論理和を変換後の値とすることを特徴とする請求項１又は２に記載の情報処理装置。

[請求項4] 前記変換部は、前記格納部が値を格納する記憶装置のメモリアドレスに応じた初期値を生成するブロックを有し、このブロックが生成した値を前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて暗号化した値と、前記暗号化部によって暗号化された値との排他的論理和を変換後の値とすることを特徴とする請求項１又は２に記載の情報処理装置。

[請求項5] 前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて前記初期値を暗号化した値と、前記格納部によって記憶装置に格納された値との排他的論理和を算出し、前記暗号化部によって用いられた暗号鍵と同一の暗号鍵を用いて、該算出した排他的論理和の値を復号する復号部を

さらに有することを特徴とする請求項２に記載の情報処理装置。

[請求項6] 前記変換部は、前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて推定が容易な値を暗号化した値と、前記暗号化部によって暗号化された値との排他的論理和を変換後の値とすることを特徴とする請求項１に記載の情報処理装置。

[請求項7] 前記変換部は、前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて、前記推定が容易な値を暗号化した値を揮発性のメモリにあらかじめ格納し、当該揮発性のメモリに格納された値と前記暗号化部によって暗号化された値との排他的論理和を変換後の値とすることを特徴とする請求項６に記載の情報処理装置。

[請求項8] 前記暗号化部が用いる暗号鍵と同一の暗号鍵を用いて前記推定が容易な値を暗号化した値と、前記格納部によって記憶装置に格納された値との排他的論理和を算出し、前記暗号化部によって用いられた暗号鍵と同一の暗号鍵を用いて、該算出した排他的論理和の値を復号する復号部をさらに有することを特徴とする請求項６に記載の情報処理装置。

[請求項9] 秘匿する値を格納する記憶装置に、所定の暗号鍵を用いて暗号化された値を格納する情報処理装置によって実行される情報処理方法であって、

前記秘匿する値を前記所定の暗号鍵を用いて暗号化した値を取得し、

前記秘匿する値が前記記憶装置の初期化時に書込まれる初期値である場合には、前記取得した値を、逆変換可能であって、前記所定の暗号鍵に依存しない値に変換し、

前記変換した値を前記記憶装置に格納することを特徴とする情報処理方法。

[請求項10] 秘匿する値を格納する記憶装置に、所定の暗号鍵を用いて暗号化された値を格納する情報処理装置によって実行される情報処理プログラ

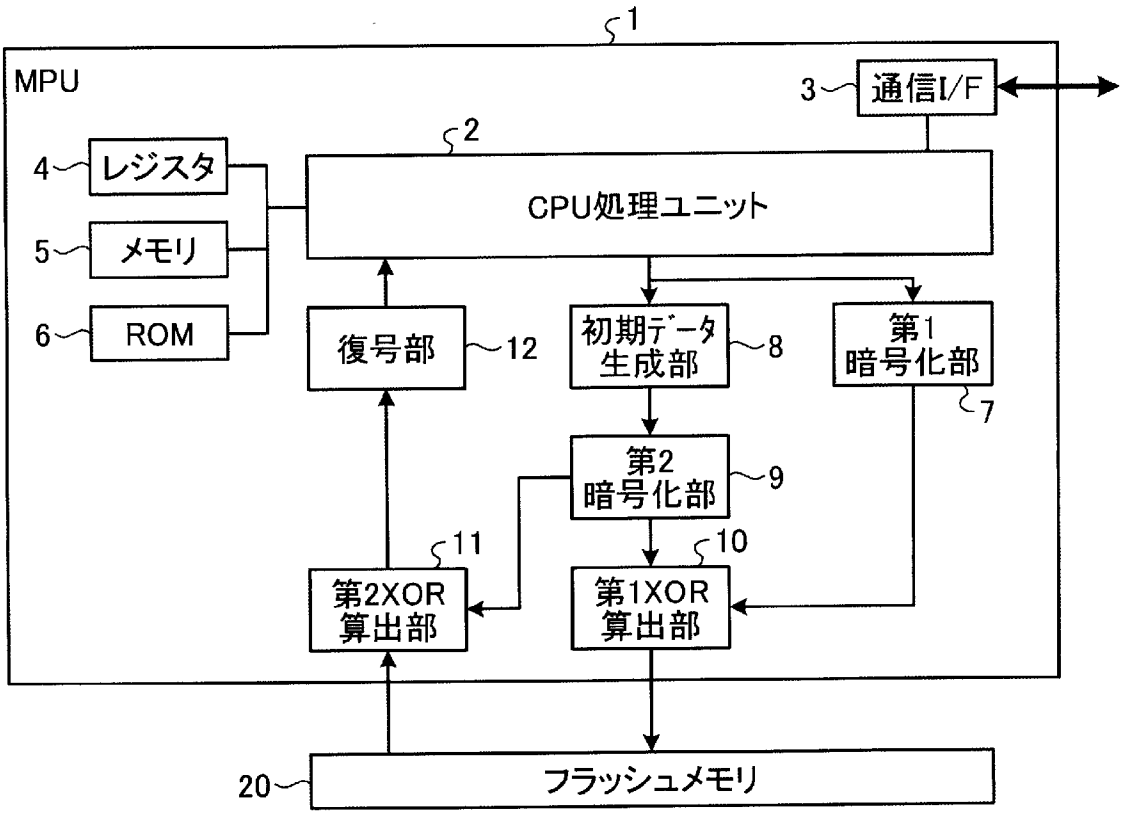
ムであって、

前記秘匿する値を前記所定の暗号鍵を用いて暗号化した値を取得し、

前記秘匿する値が前記記憶装置の初期化時に書込まれる初期値である場合には、前記取得した値を、逆変換可能であって、前記所定の暗号鍵に依存しない値に変換し、

前記変換した値を前記記憶装置に格納することを特徴とする情報処理プログラム。

[図1]


1
MPU
3
通信I/F
2
4
レジスタ
5
メモリ
6
ROM
CPU処理ユニット
復号部
12
初期データ生成部
8
第1暗号化部
7
第2暗号化部
9
11
10
第2XOR算出部
第1XOR算出部
20
フラッシュメモリ

[図2]

アドレス	0x00	0x08	0x10
第1暗号化部の暗号結果	1201, 04AF, 98A3, 31B3	1934, A41C, 1298, B013	1934, A41C, 1298, B013
第2暗号化部の暗号結果	1934, A41C, 1298, B013	1934, A41C, 1298, B013	1934, A41C, 1298, B013
メモリデータ	0B35, A0B3, 8A3B, 81A0	0000, 0000, 0000, 0000	0000, 0000, 0000, 0000
CPUからみた値	E5, 00, 00, 00, 00, 00, 00, 00	00, 00, 00, 00, 00, 00, 00, 00	00, 00, 00, 00, 00, 00, 00, 00

[図3]

管理番号	管理ID	許可フラグ	コピー回数	有効期限	名前	暗号鍵
0	all 0	all 0	all 0	all 0	all 0	all 0
1	all 0	all 0	all 0	all 0	all 0	all 0
2	all 0	all 0	all 0	all 0	all 0	all 0
3	all 0	all 0	all 0	all 0	all 0	all 0
4	all 0	all 0	all 0	all 0	all 0	all 0

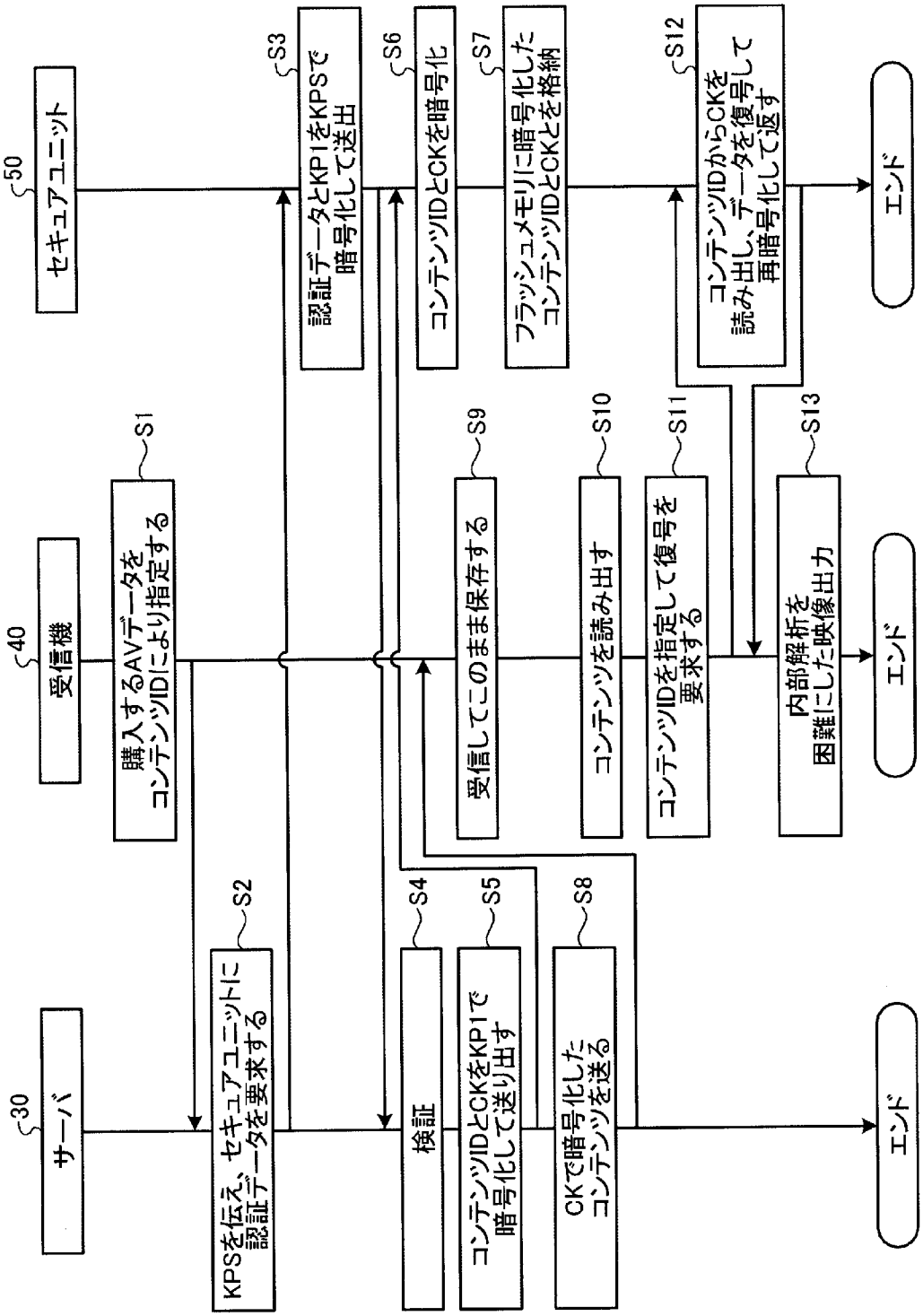
[図4]

管理番号	管理ID	許可フラグ	コピー回数	有効期限	名前	暗号鍵
0	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
1	aのID	aのフラグ	aの複製回数	2011/10/20	xxxx	xaaaaax
2	bのID	bのフラグ	bの複製回数	2012/6/20	xxxx	xbbbbbx
3	cのID	cのフラグ	cの複製回数	2011/4/20	xxxx	xcccccx
4	all 0	all 0	all 0	all 0	all 0	all 0

[図5]

アドレス	0x00	0x08	0x10
メモリデータ	1201, 04AF, 98A3, 31B3	1934, A41C, 1298, B013	1934, A41C, 1298, B013
CPUから みた値	E5, 00, 00, 00, 00, 00, 00, 00	00, 00, 00, 00, 00, 00, 00, 00	00, 00, 00, 00, 00, 00, 00, 00

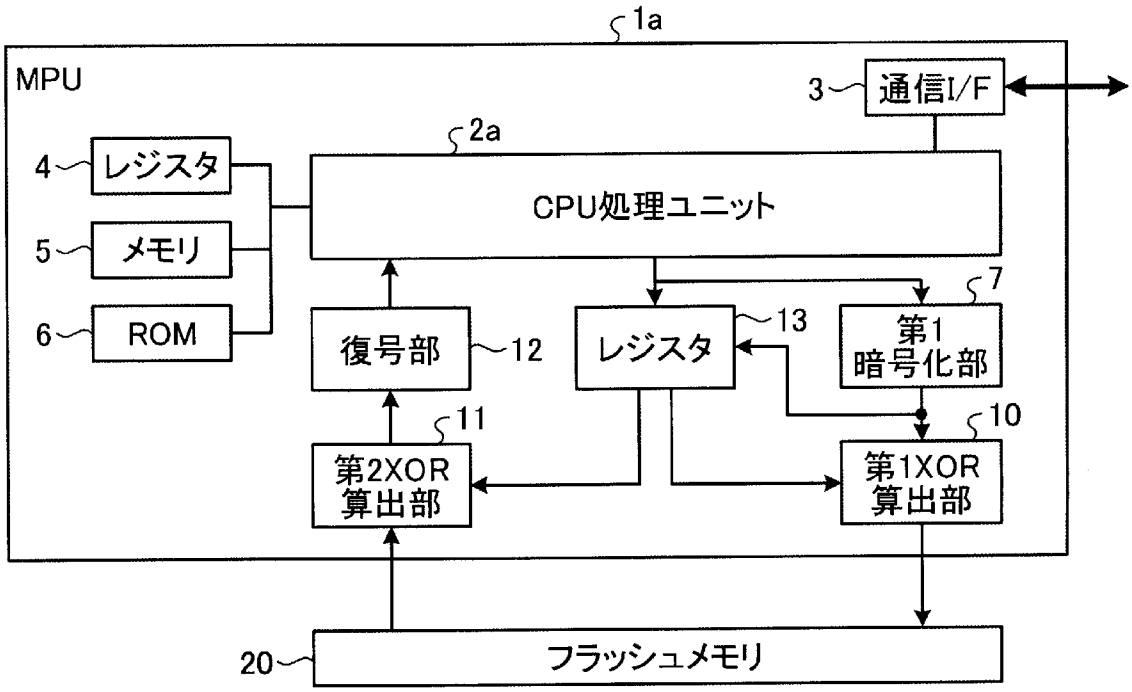
[図6]


50
セキュアユニット
40
受信機
30
サーバ
S1
購入するAVデータを
コンテンツIDにより指定する
S2
KPSを伝え、セキュアユニットに
認証データを要求する
S3
認証データとKP1をKPSで
暗号化して送出
S4
検証
S5
コンテンツIDとCKをKP1で
暗号化して送り出す
S6
コンテンツIDとCKを暗号化
S7
フラッシュメモリに暗号化した
コンテンツIDとCKとを格納
S8
CKで暗号化した
コンテンツを送る
S9
受信してこのまま保存する
S10
コンテンツを読み出す
S11
コンテンツIDを指定して復号を
要求する
S12
コンテンツIDからCKを
読み出し、データを復号して
再暗号化して返す
S13
内部解析を
困難にした映像出力
エンド
エンド
エンド

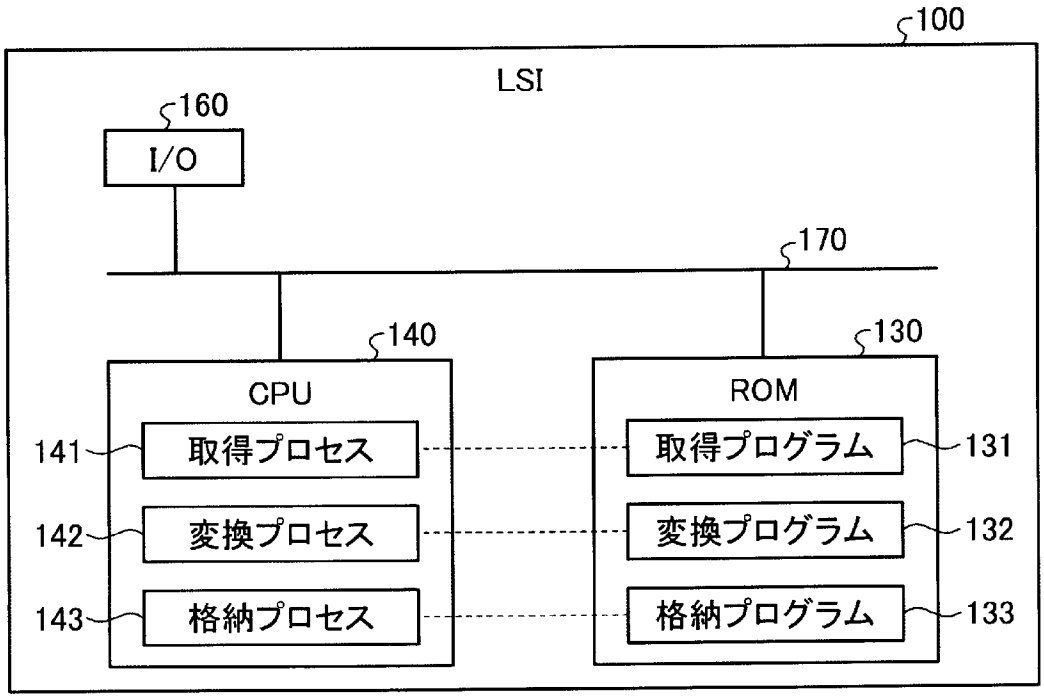
[図7]

Offset	データ
0	67 12 03 14 FE 19 13 32 7E 19 0A 13 47 11 04 9A 09 98 34 74 13 45 01 13 ED 8A 19 63 13 01 4C 7B
20	78 13 42 A3 9C 32 57 BA 19 14 78 A3 A4 B1 94 14 13 94 27 60 13 87 13 41 B4 92 C4 0A 42 14 05 89
40	1C EA 10 2C F8 C0 C4 30 EB 09 1A D1 C0 E2 F8 05 12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10
60	12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10 12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10
80	1C EA 10 2C F8 C0 C4 30 EB 09 1A D1 C0 E2 F8 05 12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10
A0	12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10 12 C1 D9 11 02 A0 98 99 25 C1 8C 93 43 12 47 10

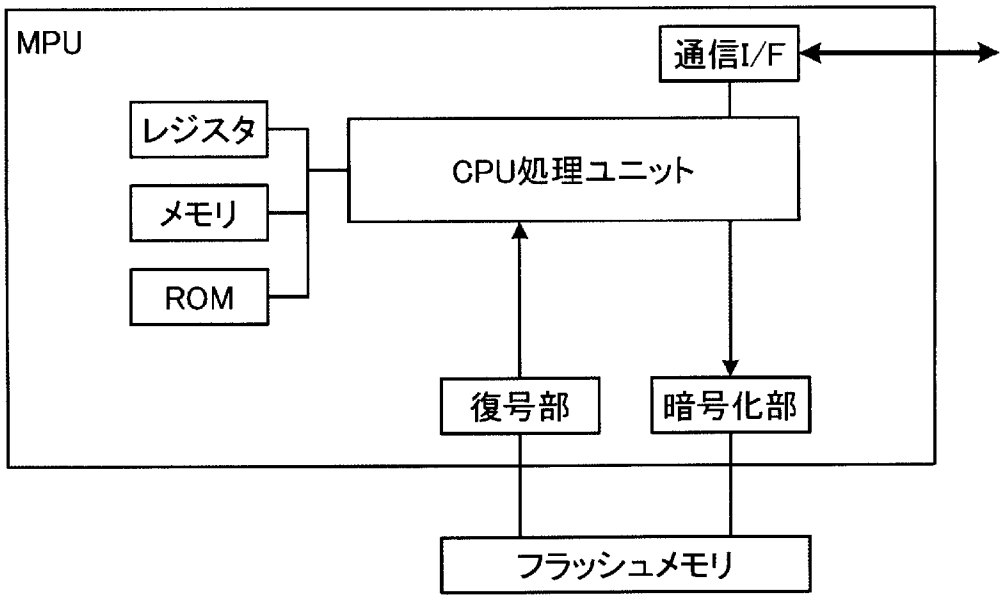
[図8]


1a
MPU
3
通信I/F
2a
4
レジスタ
5
メモリ
6
ROM
CPU処理ユニット
7
復号部
12
レジスタ
13
第1
暗号化部
11
10
第2XOR
算出部
第1XOR
算出部
20
フラッシュメモリ

[図9]


100
LSI
160
I/O
170
140
130
CPU
ROM
141
取得プロセス
取得プログラム
131
142
変換プロセス
変換プログラム
132
143
格納プロセス
格納プログラム
133

[図10]



[図11]

field type	管理番号	管理ID	許可フラグ	コピー回数	有効期限	名前	暗号鍵
byte size	2	4	2	1	3	36	16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/052782

A. CLASSIFICATION OF SUBJECT MATTER
H04N7/173(2011.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N7/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 5-130098 A (Hitachi, Ltd.), 25 May 1993 (25.05.1993), paragraphs [0013] to [0014], [0021] (Family: none)	1-10
X	JP 10-164049 A (Sony Corp.), 19 June 1998 (19.06.1998), paragraphs [0050] to [0051]; fig. 6 & US 6363148 B1	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February, 2011 (23.02.11)	08 March, 2011 (08.03.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０５２７８２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04N7/173(2011.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04N7/173

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ｘ	JP 5-130098 A（株式会社日立製作所）1993.05.25, 段落【００１３】－【００１４】、【００２１】 （ファミリーなし）	１－１０
Ｘ	JP 10-164049 A（ソニー株式会社）1998.06.19, 段落【００５０】－【００５１】、【図６】 & US 6363148 B1	１－１０

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２３．０２．２０１１	０８．０３．２０１１

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｃ　３７８３
矢野　光治
電話番号　０３－３５８１－１１０１　内線　３５４１