

(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2010-9135

(P2010-9135A)

(43) 公開日 平成22年1月14日(2010.1.14)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/24 (2006.01)	G06F 12/14 530P	5B017
G06F 21/20 (2006.01)	G06F 15/00 330E	5B285
G09C 1/00 (2006.01)	G06F 12/14 530D	5J104
	G09C 1/00 650A	
	G09C 1/00 640E	
審査請求 未請求 請求項の数 13 O L (全 13 頁)		

(21) 出願番号 特願2008-164874 (P2008-164874)
(22) 出願日 平成20年6月24日 (2008. 6. 24)

(71) 出願人 504378124
スパンション エルエルシー
アメリカ合衆国 カリフォルニア州 94
088-3453 サニーベイル デグウ
イン ドライブ 915
(74) 代理人 100099324
弁理士 鈴木 正剛
(74) 代理人 100108604
弁理士 村松 義人
(74) 代理人 100111615
弁理士 佐野 良太
(72) 発明者 杉本 智
福島県会津若松市高久工業団地2番 S p
ansion Japan株式会社内

最終頁に続く

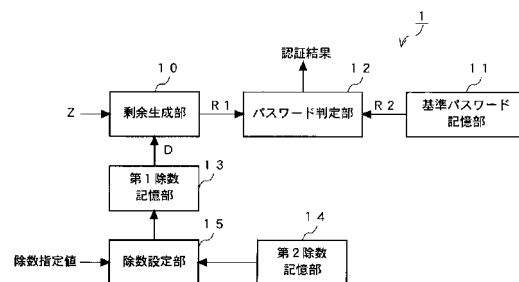
(54) 【発明の名称】 認証装置、認証方法、コンピュータプログラム

(57) 【要約】

【課題】 除算を用いた認証処理において除数の秘匿性を高めた認証装置を提供する。

【解決手段】 除算に用いられる除数Dを記憶可能な揮発性の第1除数記憶部13と、外部から入力される入力数値Zを第1除数記憶部13に記憶される除数Dで除算したときの剰余R1を生成する剰余生成部10と、基準パスワードR2を記憶する基準パスワード記憶部11と、剰余生成部10で生成された剰余R1と基準パスワード記憶部11に記憶された基準パスワードR2とを比較して、一致すると、認証したこと表示認証信号を出力するパスワード判定部12と、を備える認証装置1である。除数Dは、剰余生成部10により剰余R1が生成される前に第1除数記憶部13に記憶され、パスワード判定部12により認証信号が出力されると第1除数記憶部13から消去される。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

所定の第 1 数値を記憶するための揮発性の第 1 記憶部と、
外部から入力される入力数値を前記第 1 記憶部に記憶された前記第 1 数値で除算した場合の剰余を生成する剰余生成部と、
所定の第 2 数値データを記憶する第 2 記憶部と、
前記剰余生成部で生成された前記剰余と前記第 2 記憶部に記憶された前記第 2 数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ、前記入力数値を認証しないことを表す非認証信号を出力する比較部と、を備えており、

10

前記第 1 数値は、前記剰余生成部により前記剰余が生成される前に前記第 1 記憶部に記憶され、前記比較部により前記認証信号が出力されると前記第 1 記憶部から消去される、認証装置。

【請求項 2】

前記入力数値は複数バイトで表されており、
前記第 2 記憶部は、前記第 2 数値を複数記憶しており、
前記剰余生成部は、前記入力数値を、所定のバイト数毎に前記第 1 数値で除算した場合の複数の剰余を生成し、
前記比較部は、前記複数の剰余を前記複数の第 2 数値と比較して、すべて一致すると、前記認証信号を出力する、
請求項 1 記載の認証装置。

20

【請求項 3】

前記第 1 記憶部は各々異なる複数の第 1 数値を記憶可能であり、
前記剰余生成部は、前記入力数値を、前記所定のバイト数毎に、前記第 1 記憶部に記憶される 2 以上の前記第 1 数値のそれぞれで除算した場合の複数の剰余を生成する、
請求項 2 記載の認証装置。

【請求項 4】

前記剰余生成部は、前記入力数値を、1 バイト又は 2 バイト毎に、2 以上の前記第 1 数値のそれぞれで除算した場合の複数の剰余を生成する、
請求項 3 記載の認証装置。

30

【請求項 5】

前記剰余生成部は、前記入力数値を、前記所定のバイト数毎に異なる前記第 1 数値で除算した場合の複数の剰余を生成する、
請求項 3 記載の認証装置。

【請求項 6】

前記 2 以上の前記第 1 数値同士の乗数は、前記入力数値よりも大きい、
請求項 3～5 のいずれか 1 項記載の認証装置。

【請求項 7】

前記 2 以上の前記第 1 数値は、少なくとも 1 つが素数である、
請求項 6 記載の認証装置。

40

【請求項 8】

所定の数値を前記除数で除算した場合の剰余を表すテーブルを備えており、
前記剰余生成部は、前記テーブルを参照して前記入力数値と前記除数とから前記剰余を読み出す、
請求項 3～5 のいずれか 1 項記載の認証装置。

【請求項 9】

前記第 1 数値の候補となる第 3 数値を記憶する第 3 記憶部と、
外部から入力される第 4 数値と前記第 3 記憶部に記憶された前記第 3 数値とを比較して、一致すると、当該第 3 数値を前記第 1 数値として前記第 1 記憶部に記憶させる除数設定部と、を更に備える、

50

請求項 1～8 のいずれか 1 項記載の認証装置。

【請求項 10】

前記第 3 記憶部は揮発性メモリであり、前記第 1 記憶部に前記第 1 数値が記憶されると、前記第 3 記憶部に記憶された前記第 3 数値が消去される、
請求項 9 記載の認証装置。

【請求項 11】

前記第 1 記憶部、前記剰余生成部、前記第 2 記憶部、及び比較部は、同一の半導体装置として構成される、
請求項 1～8 のいずれか 1 項記載の認証装置。

【請求項 12】

除算に用いられる第 1 数値を記憶可能な揮発性の第 1 記憶部と、所定の第 2 数値データを記憶する第 2 記憶部とを備えた装置により実行される方法であって、

前記装置が、

前記第 1 記憶部に前記第 1 数値を記憶させる段階と、

前記装置の外部から入力される入力数値を前記第 1 記憶部に記憶させた前記第 1 数値で除算した場合の剰余を生成し、この剰余と前記第 2 記憶部に記憶された前記第 2 数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ前記入力数値を認証しないことを表す非認証信号を出力する段階と、

前記第 1 数値を前記第 1 記憶部から消去する段階と、を含む、

認証方法。

【請求項 13】

除算に用いられる第 1 数値を記憶可能な揮発性の第 1 記憶部と、所定の第 2 数値データを記憶する第 2 記憶部とを備えたコンピュータシステムに、

前記第 1 記憶部に前記第 1 数値を記憶させる処理、

前記コンピュータシステムの外部から入力される入力数値を前記第 1 記憶部に記憶させた前記第 1 数値で除算した場合の剰余を生成し、この剰余と前記第 2 記憶部に記憶された前記第 2 数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ前記入力数値を認証しないことを表す非認証信号を出力する処理、

前記第 1 数値を前記第 1 記憶部から消去する処理、

を実行させるコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、例えばフラッシュメモリにおけるパスワード認証のように、外部から入力されたパスワードを認証することで、当該フラッシュメモリなどの装置へのアクセスを許可する認証技術に関する。

【背景技術】

【0002】

フラッシュメモリへのデータの書き込み、読み出しなどのアクセスには、パスワード認証を伴うものがある。例えば、フラッシュメモリに内蔵される認証装置が、フラッシュメモリにアクセスするためのメモリコントローラから送られたパスワード（以下、「被パスワード」という。）と、フラッシュメモリに記憶されたパスワード（以下、「基準パスワード」という。）とを比較することで認証動作を行う。認証装置は、2つのパスワードが一致すれば、パスワードを認証してメモリコントローラからのフラッシュメモリへのアクセスを許可し、一致しなければフラッシュメモリへのアクセスを許可しない。

【0003】

特許文献 1 は、このような従来の認証装置の一例である。特許文献 1 の図 7 には、ホスト機器から送られた被パスワードと、基準パスワードとを比較して認証動作を行うマルチメディアカードが開示されている。

【0004】

10

20

30

40

50

メモリコントローラなどの外部装置から送られる被パスワードと、基準パスワードとにより認証を行う方法では、例えば、フラッシュメモリから基準パスワードが直接読まれることで、簡単に被パスワードが外部に知られることになる。そのために、基準パスワードが読まれても被パスワードが外部に知られないように、様々な対策がとられている。

【0005】

特許文献2は、このような対策の一つである。特許文献2には、外部から入力された数値（以下、「入力数値」という。）を素数で除算したときの剰余の一部を被パスワードとして用いた認証動作に関する発明が開示されている。このような構成では、基準パスワードからは被パスワード（剰余の一部）しかわからず、その元となる入力数値が不明である。そのために、入力数値が漏洩する可能性は低い。

特許文献2の発明では、基準パスワードの他に、除数が漏洩することを防止することが重要である。除数と基準パスワードにより、入力数値が特定できるからである。しかし、特許文献2では、除数となる素数が端末に格納される。そのために、端末から除数が漏洩する可能性がある。

また、フラッシュメモリのような半導体装置に内蔵された認証装置に特許文献2の発明を用いようとする、処理負荷が重くなり認証処理に時間がかかってしまう。そのために、もっと簡単に秘匿性の高い認証処理が必要である。

【特許文献1】特開2005-11151号公報

【特許文献2】特開平6-289781公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明は、このような問題に鑑みて、除算を用いた認証処理において除数の秘匿性を高めた認証装置を提供することを主たる課題とする。

【課題を解決するための手段】

【0007】

以上の課題を解決する本発明の認証装置は、所定の第1数値を記憶するための揮発性の第1記憶部と、外部から入力される入力数値を前記第1記憶部に記憶された前記第1数値で除算した場合の剰余を生成する剰余生成部と、所定の第2数値データを記憶する第2記憶部と、前記剰余生成部で生成された前記剰余と前記第2記憶部に記憶された前記第2数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ、前記入力数値を認証しないことを表す非認証信号を出力する比較部と、を備えている。この認証装置では、前記第1数値が、前記剰余生成部により前記剰余が生成される前に前記第1記憶部に記憶され、前記比較部により前記認証信号が出力されると前記第1記憶部から消去される。

【0008】

本発明の認証装置では、第1記憶部が揮発性であるために、第1数値が、認証の開始時に第1記憶部に記憶され終了時に消去される。そのために、認証処理時以外では、第1記憶部に第1数値が記憶されない。このような構成であるので、第1数値が外部に漏洩する危険性が従来よりも大幅に低くなり、入力数値の除算時に除数となる第1数値の秘匿性が向上する。

【0009】

本発明の認証装置は、前記入力数値が複数バイトで表される場合に、例えば、前記第2記憶部が前記第2数値を複数記憶し、前記剰余生成部が、前記入力数値を、所定のバイト数毎に前記第1数値で除算した場合の複数の剰余を生成し、前記比較部が、前記複数の剰余を前記複数の第2数値と比較して、すべて一致すると、前記認証信号を出力するように構成されていてもよい。

さらに、前記第1記憶部が各々異なる複数の第1数値を記憶可能である場合には、例えば、前記剰余生成部が、前記入力数値を、前記所定のバイト数毎に、前記第1記憶部に記憶される2以上の前記第1数値のそれぞれで除算した場合の前記複数の剰余を生成するよ

10

20

30

40

50

うに構成されてもよい。

例えば、前記剰余生成部は、前記入力数値を、1バイト又は2バイト毎に、2以上の前記第1数値のそれぞれで除算して、前記複数の剰余を生成する。

また、前記剰余生成部は、前記入力数値を、前記所定のバイト数毎に異なる前記第1数値で除算した場合の複数の剰余を生成するように構成されてもよい。

前記2以上の前記第1数値同士の乗数は、好適には、前記入力数値よりも大きく、更に好適には、少なくとも1つが素数である。

以上のような構成により、複数の剰余を複数の第2数値と比較して認証する必要がある。従来は、被パスワード、基準パスワードがそれぞれ1つずつであったので、上記の構成を備えることで従来よりも第2数値の秘匿性が向上する。また、第1数値を複数用いる場合には、第1数値の秘匿性も更に向上する。

10

【0010】

本発明の認証装置は、所定の数値を前記除数で除算した場合の剰余を表すテーブルを備えていてもよい。この場合、前記剰余生成部は、前記テーブルを参照して前記入力数値と前記除数とから前記剰余を読み出す。除算処理を行わず、テーブルの参照により剰余が得られるので、大量の剰余を生成する場合でも認証処理を高速に行うことができる。

【0011】

本発明の認証装置は、前記第1数値の候補となる第3数値を記憶する第3記憶部と、外部から入力される第4数値と前記第3記憶部に記憶された前記第3数値とを比較して、一致すると、当該第3数値を前記第1数値として前記第1記憶部に記憶させる除数設定部と、を更に備えていてもよい。

20

このような構成では、第1数値が第3数値と第4数値とが一致した場合にのみ、第1記憶部に記憶される。そのために、第4数値がそれ自体パスワードになり、第1数値の秘匿性が更に向上する。なお、第3記憶部を揮発性として、第1記憶部に第1数値が記憶されると第3記憶部の第3数値を消去するようにしてもよい。このような構成では、第3数値が漏洩する可能性を低くすることができる。

【0012】

本発明の認証装置において、例えば前記第1記憶部、前記剰余生成部、前記第2記憶部、及び比較部は、同一の半導体装置として構成される。

【0013】

本発明の認証方法は、除算に用いられる第1数値を記憶可能な揮発性の第1記憶部と、所定の第2数値データを記憶する第2記憶部とを備えた装置により実行される方法である。前記装置が、前記第1記憶部に前記第1数値を記憶させる段階と、前記装置の外部から入力される入力数値を前記第1記憶部に記憶させた前記第1数値で除算した場合の剰余を生成し、この剰余と前記第2記憶部に記憶された前記第2数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ前記入力数値を認証しないことを表す非認証信号を出力する段階と、前記第1数値を前記第1記憶部から消去する段階と、を含む。

30

【0014】

本発明のコンピュータプログラムは、除算に用いられる第1数値を記憶可能な揮発性の第1記憶部と、所定の第2数値データを記憶する第2記憶部とを備えたコンピュータシステムに、前記第1記憶部に前記第1数値を記憶させる処理、前記コンピュータシステムの外部から入力される入力数値を前記第1記憶部に記憶させた前記第1数値で除算した場合の剰余を生成し、この剰余と前記第2記憶部に記憶された前記第2数値とを比較して、一致すると、前記入力数値を認証したこと表す認証信号を出力し、一致しなければ前記入力数値を認証しないことを表す非認証信号を出力する処理、前記第1数値を前記第1記憶部から消去する処理、を実行させるコンピュータプログラムである。

40

【発明の効果】

【0015】

以上のような本発明では、除数となる第1数値が認証の開始時に第1記憶部に記憶され

50

、終了時に消去されるために、認証処理時以外では、第1記憶部に第1数値が記憶されない。このような構成であるので、第1数値が外部に漏洩する危険性が従来よりも大幅に低くなり、第1数値の秘匿性が向上する。

【発明を実施するための最良の形態】

【0016】

以下、図面を参照して本発明の実施形態を説明する。

【0017】

図1は、本実施形態の認証装置1の構成図である。

認証装置1は、剰余生成部10と、基準パスワード記憶部11と、パスワード判定部12と、第1除数記憶部13と、第2除数記憶部14と、除数設定部15とを備えている。認証装置1は、例えば、認証装置1の外部にある図示しない外部装置から、認証を必要とする装置（この実施形態では、フラッシュメモリ）へのアクセスを許可するために設けられる。認証装置1は、例えば認証を必要とするフラッシュメモリなどの装置に内蔵される。認証装置1は、外部装置から入力された入力数値Zを除算して得られる剰余R1を被パスワードとして認証を行う。入力数値Zが認証されると、外部装置からフラッシュメモリへのアクセスが許可される。認証装置1は、例えば1つの半導体装置に、フラッシュメモリとともに設けられる。また、認証装置1は、CPU（Central Processing Unit）、揮発性メモリ、及び不揮発性メモリが本発明のコンピュータプログラムを読み込んで実行することで構成されてもよい。

【0018】

剰余生成部10は、入力数値Zを除数Dで除算して、剰余R1を生成する。入力数値Zは、複数バイト（Byte：1バイトは例えば0～16）で表される。剰余R1は、1個でもよいが、好適には複数生成される。例えば、入力数値Zを1バイト毎に除数Dで除算して、入力数値Zのバイト数と同数の剰余R1を生成する。また、複数の異なる除数Dで入力数値Zを除算して、除数Dの個数と同数の剰余R1を生成してもよい。さらに、これらを組み合わせて、入力数値Zを1バイト毎に複数の異なる除数Dにより除算して、1バイト毎に除数Dの個数と同数の剰余R1を生成してもよい。

【0019】

基準パスワード記憶部11は、基準パスワードR2を記憶する不揮発性メモリである。基準パスワード記憶部11は、例えば、フラッシュメモリの記憶領域の一部に設けられる。基準パスワードR2は、認証装置1の製造者側で予め記憶されていてもよく、ユーザにより書き込まれてもよい。なお、基準パスワード記憶部11がフラッシュメモリの場合には、認証装置1の終了時、或いは認証動作終了時に、基準パスワードR2が基準パスワード記憶部11から消去されるようになっていてもよい。基準パスワード記憶部11への基準パスワードR2の書き込みについては後述する。

【0020】

パスワード判定部12は、剰余生成部10で生成された剰余R1と、基準パスワード記憶部11から取得する基準パスワードR2とを比較する比較器である。比較結果は、認証結果として外部装置に出力される。剰余R1が複数ある場合には、基準パスワードR2も複数用意して、それぞれ比較する。剰余R1と基準パスワードR2とがすべて一致する場合には、認証結果として入力数値Zを認証したことを表す認証信号が出力される。一つでも一致しないものがある場合には、認証結果として入力数値Zを認証しないことを表す非認証信号が出力される。

【0021】

第1除数記憶部13は、剰余生成部10で除算に用いられる除数Dを一時記憶する揮発性メモリである。除数Dは、本実施形態では、後述の除数設定部15により第2除数記憶部14から書き込まれる。除数Dは、認証装置1の起動時、或いは認証動作開始時に、第1除数記憶部13に書き込まれ、認証装置1の終了時、或いは認証動作終了時に第1除数記憶部13から消去される。

第2除数記憶部14は、除数Dの候補となる除数候補値が複数記憶される揮発性メモリ

である。除数候補値は、認証装置の外部にある図示しない装置から書き込まれる。除数候補値は、認証装置 1 の起動時、或いは認証動作開始時に第 2 除数記憶部 1 4 に書き込まれ、認証装置 1 の終了時、或いは認証動作終了時に第 2 除数記憶部 1 4 から消去される。

除数設定部 1 5 は、図示しない入力装置により入力される除数指定値と、第 2 除数記憶部 1 4 に記憶された除数候補値とを比較して、一致した場合に、当該除数候補値を除数 D として第 1 除数記憶部 1 3 に書き込む。除数設定部 1 5 は、認証動作終了時に、第 1 除数記憶部 1 3 に記憶された除数 D を消去する。除数 D は、外部からの入力により決められるので、パスワードと同様に秘匿性が高くなる。また、認証動作終了時に除数 D を第 1 除数記憶部 1 3 から消去するために、除数 D が第 1 除数記憶部 1 3 から直接読み取られないことがない。

10

【0022】

認証装置 1 は、基準パスワード R 2 を剰余 R 1 と比較することで認証を行う構成である。そのために、基準パスワード R 2 が漏洩しても、そこから剰余 R 1 の元となる入力数値 Z を知ることは困難である。上記の通り除数 D 自体の秘匿性が高いためである。

なお、認証装置 1 は、第 1 除数記憶部 1 3、第 2 除数記憶部 1 4、及び除数設定部 1 5 を用いずに、外部装置から剰余生成部 1 0 に、直接、除数 D が入力されるようになっていてもよい。

【0023】

認証装置 1 は、例えば以下のような運用が可能である。

【0024】

20

(i) 認証装置 1 は、例えば、複数バイトで表される入力数値 Z を、1 バイト毎に 2 つの除数 D により除算して算出される剰余 R 1 により認証を行う。例えば、入力数値 Z が「FFFFFFFF」(HEX) で表され、除数 D が (3, 7) の場合には、剰余 R 1 (0, 1) が、入力数値 Z のバイト数と同数の 8 組算出される。パスワード判定部 1 2 は、基準パスワード記憶部 1 1 から基準パスワード R 2 として 2 つの数値の組を 8 組読み出して、剰余 R 1 と比較する。パスワード判定部 1 2 は、剰余 R 1 と基準パスワード R 2 とがすべて一致する場合に認証信号を出力する。この例では 2 つの除数 D により剰余 R 1 を算出したが、更に多くの除数 D を用いてもよく、また、逆に 1 つの除数 D による除算であってもよい。

【0025】

30

(ii) 認証装置 1 は、例えば、複数バイトで表される入力数値 Z を、所定のバイト数毎に 2 つの除数 D で除算することで算出される剰余 R 1 により認証を行う。例えば、入力数値 Z が「FFFFFFFF」(HEX) で表され、これを 2 バイト毎に除数 D (5, 53) で除算する場合には、剰余 R 1 (0, 43) が 4 組算出される。パスワード判定部 1 2 は、基準パスワード記憶部 1 1 から基準パスワード R 2 として 2 つの数値の組を 4 組読み出して、剰余 R 1 (0, 43) と比較する。パスワード判定部 1 2 は、剰余 R 1 と基準パスワード R 2 とがすべて一致する場合に認証信号を出力する。この例では 2 つの除数 D により剰余 R 1 を算出したが、更に多くの除数 D を用いてもよく、また、逆に 1 つの除数 D による除算であってもよい。

【0026】

40

(iii) 認証装置 1 は、例えば、複数バイトで表される入力数値 Z を、所定のバイト数毎に異なる除数 D で除算することで算出される剰余 R 1 により認証を行う。例えば、入力数値 Z がある「8576ACEF」(HEX) を、上位 4 バイトには除数 D として (5, 7)、下位 4 バイトには除数 D として (3, 7) を用いて除算する。剰余 R 1 は、上位 4 バイト「8576」の各バイトを除数 D (5, 7) で除算した場合の剰余である (3, 1)、(0, 5)、(2, 0)、(1, 6) と、下位 4 バイト「ACEF」の各バイトを除数 D (3, 7) で除算した場合の剰余である (1, 3)、(0, 5)、(2, 0)、(0, 1) と、になる。パスワード判定部 1 2 は、基準パスワード記憶部 1 1 から基準パスワード R 2 として 2 つの数値の組を 8 組読み出して、剰余 R 1 と比較する。パスワード判定部 1 2 は、剰余 R 1 と基準パスワード R 2 とがすべて一致する場合に認証信号を出力する。

50

この例では2つの除数Dにより剰余R1を算出したが、更に多くの除数Dを用いてもよく、また、逆に1つの除数Dによる除算であってもよい。

【0027】

上記の(i)、(ii)、(iii)の例では、複数量出される剰余R1がすべて基準パスワードR2と一致した場合にのみ、入力数値Zが認証され、一つでも一致しないものがあると、入力数値Zが認証されない。そのために、基準パスワードR2が多数必要になる。基準パスワードR2を不正に入手しようとする者は、多数の基準パスワードR2が必要になるために、基準パスワードR2の入手が困難になる。そのために基準パスワードR2の秘匿性が従来よりも向上する。

【0028】

図2は、除数Dと入力数値Zとの関係から算出される剰余R1を表す図である。

入力数値Zを1バイト毎に乗数Dで除算すると、剰余は周期的になる。この周期を考慮すると、除数Dは、「入力数値Z<複数の除数D同士の乗数」の関係にあるものが好適である。このような関係にあると、複数の除数Dのそれぞれから得られる剰余が、同じになる周期を延ばすことができ、同じ剰余の組み合わせとなる入力数値Zを少なくすることができるため、セキュリティの強化を図ることができる。なお、図2中の斜線Aは、この線よりも右側では除数Dに関わらず剰余R1が同じになるために、本実施形態では好適ではないことを表す線である。

最も好適なものは、「入力数値Z<複数の除数D同士の乗数」、且つ入力数値Zに最も近い素数同士の乗数の組み合わせである。例えば、入力数値Z=15であれば、除数Dは(3, 7)が最も好適になる。この場合、使用可能な剰余R1は「3~15」の13通りと比較的多く、且つ剰余の組み合わせ(0, 1)は、入力数値Z=15のときのみである。なお、入力数値Z=15で除数Dが(3, 5, 7)の場合も、剰余R1が「3~15」の13通りであるが、除算回数が多くなり、処理に時間がかかる。また、回路規模も大きくなる。

次に好適なものは、「入力数値Z<複数の除数Dの乗数」、且つ入力数値Zに最も近い素数とそれ以外の数の乗数の組み合わせである。例えば、入力数値Z=15であれば、除数Dは(4, 5)である。この場合、使用可能な剰余R1は「4~15」の12通りである。

図2の右端は、これらの組み合わせの一致性を表している。「#OK」の部分は非推奨な剰余である。剰余としてこれらの値を使用すると、剰余の組み合わせや入力数値Zが同じ数値になり、パスワードやそれに準ずる剰余の設定値として望ましくない。

【0029】

なお、認証装置1は、図2のような除数Dと入力数値Zとから算出される剰余R1を、テーブルとして保持していてもよい。このようなテーブルを保持すると、剰余生成部10で除算を行う必要が無くなり、剰余生成部10は、除数Dと入力数値Zとからテーブルを参照して剰余R1を出力すればよい。この場合、除算するよりも高速に大量の剰余R1を生成することができる。

【0030】

図3は、基準パスワード記憶部11に基準パスワードR2となる剰余データを書き込む処理のタイミングチャートの例示図である。基準パスワード記憶部11への剰余データの書き込みは、例えば図示しないメモリコントローラのようなもので行う。なお、第2除数記憶部14に除数候補値となる数値を書き込む処理も同様である。

以下、基準パスワードR2を書き込む処理を例に説明する。

【0031】

図3では、認証装置1の外部から、基準パスワードR2になる剰余データとともにコード1~コード17が入力される。コード1~コード17は、認証装置1が設けられるフラッシュメモリにアクセスするための、予め決められたコードである。コードの組み合わせにより、各種コマンドが形成される。

コード1~コード3及びコード10~コード12は、基準パスワードR2の入力を認証

10

20

30

40

50

装置 1 に指示する基準パスワード入力コマンドを形成する。基準パスワード入力コマンドにより、基準パスワード記憶部 11 への剰余データの入力が可能になる。

コード 4～コード 6 及びコード 13, 14 は、剰余データ入力コマンドを形成しており、剰余データとともに入力される。剰余データ入力コマンドにより、剰余データが基準パスワード R2 として基準パスワード記憶部 11 に書き込まれる。

コード 7～コード 9 及びコード 15～コード 17 は、基準パスワード R2 の入力の終了を認証装置 1 に指示する基準パスワード入力終了コマンドを形成する。基準パスワード入力終了コマンドにより、基準パスワード R2 として基準パスワード記憶部 11 に書き込んだ剰余データが確定する。入力されたコードに一つでも間違いがあれば、基準パスワード R2 として基準パスワード記憶部 11 に書き込んだ剰余データが消去される。

このように、コード 1～コード 17 がすべて正当なコードの場合にのみ、剰余データが基準パスワード R2 として、基準パスワード記憶部 11 に記憶される。

【0032】

図 4 は、パスワード入力からデータの読み出しまでの処理のタイミングチャートの例示図である。

図 4 では、入力数値 Z と除数 D とが同時に入力されている。パスワード判定部 12 は、この入力数値 Z をこの除数 D で除算したときの剰余 R1 を基準パスワード R2 と比較する。比較の結果、一致する場合にデータの保護領域の保護状態が解除されて、保護領域へのアクセスが可能になる。

【0033】

図 4 では、アクセスするアドレスとともに、コード 20～コード 25、コード 30～コード 40、コード 50～コード 55、除数 D、入力数値 Z となるパスワード PWD0～PWD7 が入力される。

コード 20～コード 25 は、保護領域へアクセスを認証装置 1 に指示するパスワード入力コマンドを形成する。パスワード入力コマンドにより、認証装置 1 に入力数値 Z 及び除数 D が入力可能になる。

コード 30～コード 40 は、除数 D 及びパスワード PWD0～PWD7 とともに入力される。パスワード PWD0～PWD7 は、入力数値 Z である。コード 30～コード 40 は、フラッシュメモリにアクセスのためにパスワードを解除するためのパスワード解除コマンドを形成している。パスワード PWD0～PWD7 を除数 D で除算したときの剰余 R2 が基準パスワード R2 と一致した場合にのみ、データの読み出しや書き込みが可能になる。コード 35 に次いで入力されるアドレスに対応したデータにアクセス可能になり、パスワードによって保護されたデータの読み出しが可能になる。

コード 50～コード 55 は、フラッシュメモリにパスワードを再びかけてアクセスを不許可にするためのパスワード解除終了コマンドを形成する。コード 50～コード 55 により、パスワードの解除状態を停止し、パスワードロック状態に戻る。

このように、コード 20～コード 25、コード 30～コード 40、コード 50～コード 55 がすべて正当なコードであり、パスワード PWD0～PWD7 を除数 D で除算した結果得られる剰余 R1 が基準パスワード R2 と一致する場合のみ、データの読み出しや書き込みが可能になる。

【図面の簡単な説明】

【0034】

【図 1】 本実施形態の認証装置 1 の構成図である。

【図 2】 除数と入力数値との関係から算出される剰余を表す図である。

【図 3】 基準パスワード記憶部に基準パスワードを書き込む処理のタイミングチャートの例示図である。

【図 4】 パスワード入力からデータの読み出しまでの処理のタイミングチャートの例示図である。

【符号の説明】

【0035】

10

20

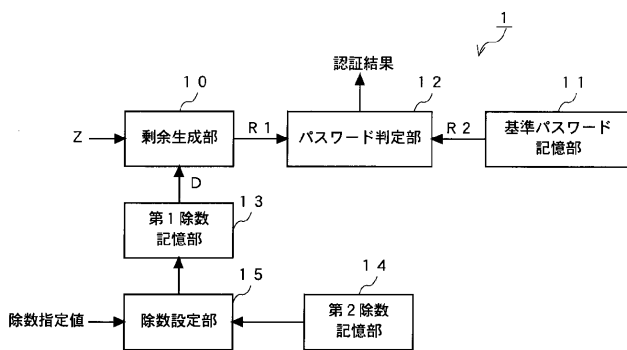
30

40

50

1…認証装置、10…剰余生成部、11…基準パスワード記憶部、12…パスワード判定部、13…第1除数記憶部、14…第2除数記憶部、15…除数設定部

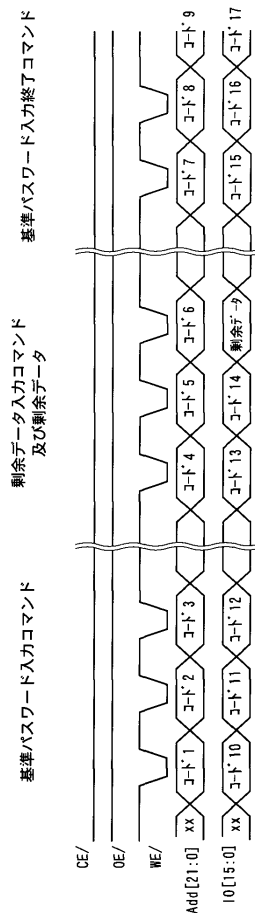
【 図 1 】



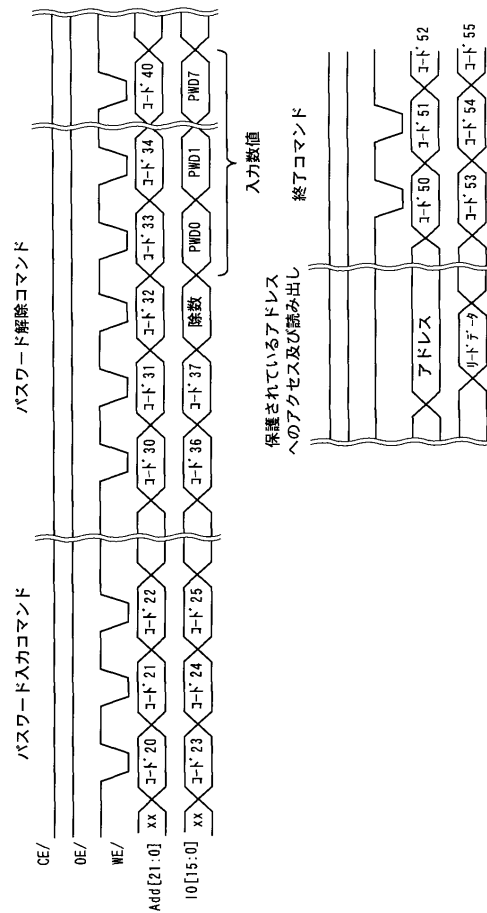
【図 2】

[illegible]

【図 3】



【図 4】



【手続補正書】

【提出日】平成21年1月28日(2009.1.28)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】0028

【補正方法】変更

【補正の内容】

【0028】

図2は、除数Dと入力数値Zとの関係から算出される剰余R1を表す図である。

入力数値Zを1バイト毎に除数Dで除算すると、剰余は周期的になる。この周期を考慮すると、除数Dは、「入力数値Z<複数の除数D同士の乗数」の関係にあるものが好適である。このような関係にあると、複数の除数Dのそれぞれから得られる剰余が、同じになる周期を延ばすことができ、同じ剰余の組み合わせとなる入力数値Zを少なくすることができるため、セキュリティの強化を図ることができる。なお、図2中の斜線Aは、この線よりも右側では除数Dに関わらず剰余R1が同じになるために、本実施形態では好適ではないことを表す線である。

最も好適なものは、「入力数値Z<複数の除数D同士の乗数」、且つ入力数値Zに最も近い素数同士の乗数の組み合わせである。例えば、入力数値Z=15であれば、除数Dは(3, 7)が最も好適になる。この場合、使用可能な剰余R1は「3~15」の13通りと比較的多く、且つ剰余の組み合わせ(0, 1)は、入力数値Z=15のときのみである。なお、入力数値Z=15で除数Dが(3, 5, 7)の場合も、剰余R1が「3~15」の13通りであるが、除算回数が多くなり、処理に時間がかかる。また、回路規模も大きくなる。

次に好適なものは、「入力数値Z<複数の除数Dの乗数」、且つ入力数値Zに最も近い素数とそれ以外の数の乗数の組み合わせである。例えば、入力数値Z=15であれば、除

数 D は (4 , 5) である。この場合、使用可能な剰余 R 1 は「 4 ~ 1 5 」の 1 2 通りである。

図 2 の右端は、これらの組み合わせの一致性を表している。「 # 0 K 」の部分は非推奨な剰余である。剰余としてこれらの値を使用すると、剰余の組み合わせや入力数値 Z が同じ数値になり、パスワードやそれに準ずる剰余の設定値として望ましくない。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】 0 0 3 3

【補正方法】変更

【補正の内容】

【 0 0 3 3 】

図 4 では、アクセスするアドレスとともに、コード 2 0 ~ コード 2 5、コード 3 0 ~ コード 4 0、コード 5 0 ~ コード 5 5、除数 D、入力数値 Z となるパスワード P W D 0 ~ P W D 7 が入力される。

コード 2 0 ~ コード 2 5 は、保護領域へアクセスを認証装置 1 に指示するパスワード入力コマンドを形成する。パスワード入力コマンドにより、認証装置 1 に入力数値 Z 及び除数 D が入力可能になる。

コード 3 0 ~ コード 4 0 は、除数 D 及びパスワード P W D 0 ~ P W D 7 とともに入力される。パスワード P W D 0 ~ P W D 7 は、入力数値 Z である。コード 3 0 ~ コード 4 0 は、フラッシュメモリにアクセスのためにパスワードを解除するためのパスワード解除コマンドを形成している。パスワード P W D 0 ~ P W D 7 を除数 D で除算したときの剰余 R 1 が基準パスワード R 2 と一致した場合にのみ、データの読み出しや書き込みが可能になる。コード 3 5 に次いで入力されるアドレスに対応したデータにアクセス可能になり、パスワードによって保護されたデータの読み出しが可能になる。

コード 5 0 ~ コード 5 5 は、フラッシュメモリにパスワードを再びかけてアクセスを不許可にするためのパスワード解除終了コマンドを形成する。コード 5 0 ~ コード 5 5 により、パスワードの解除状態を停止し、パスワードロック状態に戻る。

このように、コード 2 0 ~ コード 2 5、コード 3 0 ~ コード 4 0、コード 5 0 ~ コード 5 5 がすべて正当なコードであり、パスワード P W D 0 ~ P W D 7 を除数 D で除算した結果得られる剰余 R 1 が基準パスワード R 2 と一致する場合のみ、データの読み出しや書き込みが可能になる。

フロントページの続き

(72)発明者 加藤 健太

福島県会津若松市高久工業団地2番 Spansion Japan株式会社内

Fターム(参考) 5B017 AA03 BA05 CA11

5B285 AA04 BA08 CA41 CA42 CB02 CB52 CB58

5J104 AA07 AA32 AA41 EA03 EA08 EA26 KA01 NA05 NA06 NA38