(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5930619号
(P5930619)
(45)発行日　平成28年6月8日(2016.6.8)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.　F I
H04L 9/36 (2006.01)　H04L 9/00 685

請求項の数 7 (全 12 頁)

(21)出願番号　特願2011-142243(P2011-142243)
(22)出願日　平成23年6月27日(2011.6.27)
(65)公開番号　特開2013-9276(P2013-9276A)
(43)公開日　平成25年1月10日(2013.1.10)
審査請求日　平成26年6月26日(2014.6.26)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　石川　学
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　熊取谷　昭彦
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号処理装置

(57)【特許請求の範囲】
【請求項１】
暗号化データに対して復号処理を行う復号処理手段と、
前記復号処理手段で復号処理された前記暗号化データの認証処理を行う認証処理手段と、
前記復号処理手段で復号処理された前記暗号化データの認証を行うために必要なパラメータを算出するパラメータ算出手段と、
前記算出されたパラメータおよび前記復号処理手段で復号処理された前記暗号化データを用いて前記認証処理手段への入力データを形成する入出力データ形成手段を有し、
前記復号処理手段は、前記暗号化データの最後のブロックから復号処理を行い、
前記入出力データ形成手段は、前記最後のブロックを用いて前記復号処理手段への入力データを形成し、前記最後のブロックの復号処理後、前記復号処理手段で復号処理された前記最後のブロックを用いて前記認証処理手段への入力データを形成することを特徴とする暗号処理装置。
【請求項２】
前記復号処理手段は、前記暗号化データの最後から２番目のブロックをイニシャルベクタとして、前記最後のブロックを復号処理することを特徴とする請求項１に記載の暗号処理装置。
【請求項３】
前記算出されたパラメータは、前記暗号化データのパディングデータのデータ長に関連

付いたパラメータであることを特徴とする請求項１もしくは２に記載の暗号処理装置。
【請求項４】
前記入出力データ形成手段は、前記認証処理手段で得られたＭＡＣ値と、前記復号処理手段で得られたＭＡＣ値とを比較することを特徴とする請求項１乃至３の何れか１項に記載の暗号処理装置。
【請求項５】
前記パラメータ算出手段は、１パケットまたは１データグラムごとに、前記パラメータの算出を行うことを特徴とする請求項１乃至４の何れか１項に記載の暗号処理装置。
【請求項６】
さらに、前記入出力データ形成手段への入出力データの転送を制御する入出力データ転送手段を有し、
前記入出力データ形成手段は、さらに、前記復号処理手段で処理されたデータ、あるいは、前記認証処理手段で処理されたデータを一時保持するための中間データ保持手段を有する特徴とする請求項１乃至５の何れか１項に記載の暗号処理装置。
【請求項７】
前記復号処理および認証処理は、ＳＳＬ／ＴＬＳレコードプロトコル処理であることを特徴とする請求項１乃至６の何れか１項記載の暗号処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号処理装置に関するものである。
【背景技術】
【０００２】
近年、各種デジタル機器をネットワークに接続し、機器間でデータ通信を行なうことが多くなり、インターネット上でデータ通信を行う機会も増加している。このようなネットワーク上でのデジタル機器間の通信においては送受信するデータの盗聴や改竄の可能性があり、これらの盗聴や改竄からデータ通信の安全性を守るための通信プロトコルが必要になる。このような通信プロトコルとして暗号化・復号機能と認証機能を備えたＩＰｓｅｃやＳＳＬ／ＴＬＳなどが標準技術として広く使われている。
従来このような通信暗号処理はソフトウエアにより実現されることが多かった。しかしネットワーク上のデータ通信におけるデータ量が年々増加しており、かつ、リアルタイム性を要求されるケースが多いことから通信暗号処理の高速化が求められている。
このため、通信暗号処理をハードウエア化し、通信暗号処理における暗号化・復号処理と認証処理を並列化することにより高速化する手法が用いられている。特許文献１では、ＳＳＬ／ＴＬＳ受信処理において暗号化・復号処理と認証処理を並列化する手法が提案されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１０－５７１２３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１では、ＳＳＬ／ＴＬＳ受信処理において、認証パラメータを算出するための復号処理、ペイロード・データの復号処理と認証処理を一括してハードウエア処理できなかった。これらの処理を行うにはソフトウエア処理、ハードウエア処理の切替、ハードウエア処理の設定、ソフトウエア処理、データ転送等を順次処理する必要があり、高速化の妨げになっていた。
【課題を解決するための手段】
【０００５】

上記課題を解決するため、データの転送回数を従来より削減し、復号処理と認証処理との並列化処理の高速化を目的とする。

本発明に係る暗号処理装置は、暗号化データに対して復号処理を行う復号処理手段と、

前記復号処理手段で復号処理された前記暗号化データの認証処理を行う認証処理手段と、

前記復号処理手段で復号処理された前記暗号化データの認証を行うために必要なパラメータを算出するパラメータ算出手段と、前記算出されたパラメータおよび前記復号処理手段で復号処理された前記暗号化データを用いて前記認証処理手段への入力データを形成する入出力データ形成手段を有し、前記復号処理手段は、前記暗号化データの最後のブロックから復号処理を行い、前記入出力データ形成手段は、前記最後のブロックを用いて前記復号処理手段への入力データを形成し、前記最後のブロックの復号処理後、前記復号処理手段で復号処理された前記最後のブロックを用いて前記認証処理手段への入力データを形成することを特徴とする。

【発明の効果】

【０００６】

本発明によれば、データの転送回数を従来より削減し、復号処理と認証処理との並列化処理の高速化が実現できる。

【図面の簡単な説明】

【０００７】

【図１】実施形態１における暗号処理装置の構成を示した図。

【図２】ＳＳＬ／ＴＬＳ処理において送受信されるデータフォーマットを示した図。

【図３】ＳＳＬ／ＴＬＳ処理において認証処理の対象となるデータグラムを示した図。

【図４】ＳＳＬ／ＴＬＳ受信処理において復号処理の対象となるデータグラムを示した図。

【図５】実施形態１におけるＳＳＬ／ＴＬＳ受信処理の先頭部分の処理フローを示した図。

【図６】実施形態１におけるＳＳＬ／ＴＬＳ受信処理の最後の部分の処理フローを示した図。

【発明を実施するための形態】

【０００８】

［実施形態１］

以下、本発明の実施形態についてＳＳＬ／ＴＬＳ受信処理を説明する。ここでは、ＳＳＬ／ＴＬＳ受信処理として、ＡＥＳ－１２８、ＳＨＡ－１の例を説明する。

【０００９】

図１は本発明の実施形態１における暗号処理装置の構成を示した図である。同図において１００は本発明に係る暗号処理装置である。暗号処理装置１００は中央演算処理装置１０１、外部記憶装置１０２、暗号処理アクセラレータ１０３から構成される。中央演算処理装置１０１は暗号処理アクセラレータ１０３にパラメータ設定し、外部記憶装置１０２と暗号処理アクセラレータ１０３間の入出力データ転送設定を制御する。外部記憶装置１０２には暗号処理アクセラレータ１０３との間で転送される入出力データ、暗号処理アクセラレータ１０３に設定されるパラメータが保持されている。

【００１０】

暗号処理アクセラレータ１０３はパラメータ保持・設定部１０４、入出力データ転送部１０５、入出力データ処理部１０６、暗号化・復号処理部１０７、認証処理部１０８から構成される。パラメータ保持・設定部１０４は中央演算処理装置１０１によって通信暗号処理に必要なパラメータを設定され、処理が終了するまで保持されるようになっている。入出力データ転送部１０５は中央演算処理装置１０１によって設定された入出力データ転送設定に従って外部記憶装置１０２、入出力データ処理部１０６間で入出力データを転送する。

【００１１】

入出力データ処理部１０６はパラメータ算出部１０６２、入出力データ成形部１０６３、中間データ保持部１０６４等から構成される。パラメータ算出部１０６２はパラメータ保持・設定部１０４で保持されるパラメータと入出力データ成形部１０６３で成形される入出力データから暗号化・復号処理、認証処理に必要なパラメータを算出する。そして算出されたパラメータを暗号化・復号処理部１０７、認証処理部１０８に設定する。また、一部の入力データを生成し、入出力データ成形部１０６３に出力する。

【００１２】

入出力データ成形部１０６３は暗号化・復号処理部１０７、認証処理部１０８への入力データを成形し、暗号化・復号処理部１０７、認証処理部１０８へ出力する。この入力データは入出力データ転送部１０５から転送される入力データ、中間データ保持部１０６４から転送される中間データ、パラメータ算出部１０６２の出力データから成形される。また入出力データ成形部１０６３は中間データ保持部１０６４から転送される中間データから出力データを成形し、入出力データ転送部１０５へ転送する。

【００１３】

中間データ保持部１０６４には暗号化・復号処理部１０７、認証処理部１０８からの出力データが入力し、一時保持され、入出力データ成形部へ転送される。

【００１４】

暗号化・復号処理部１０７にはパラメータ算出部１０６２から暗号化・復号処理に必要なパラメータが設定され、入出力データ成形部１０６３から成形処理された入力データが入力する。そして入力データを暗号化・復号処理したデータを中間データ保持部１０６４に出力する。

【００１５】

認証処理部１０８にはパラメータ算出部１０６２から認証処理に必要なパラメータが設定され、入出力データ成形部１０６３から成形処理された入力データが入力する。そして認証処理の中間データを内部で保持するとともに、出力データを入出力データ処理部１０６の中間データ保持部１０６４に出力する。出力データはここでは認証処理の１ブロック毎の処理終了信号であるが、前記中間データを出力してもよい。

【００１６】

暗号処理アクセラレータ１０３は設定に従って処理を行い、暗号化・復号処理されたデータおよび認証処理結果は外部記憶装置１０２に転送され、処理の終了を中央演算処理装置１０１へ通知する。

【００１７】

次にＳＳＬ／ＴＬＳ受信処理において暗号化・復号処理部１０７に入力するデータについて説明する。

【００１８】

図２は、ＳＳＬ／ＴＬＳ受信処理における受信データのフォーマットを示した図である。図２において、”Ｃｏｍｐｒｅｓｓｅｄ　ｆｒａｇｍｅｎｔ”、　”ＭＡＣ値”、”ｐａｄｄｉｎｇ　ｄａｔａ”、”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇｌｅｎｇｔｈ”の各フィールドのデータは送信側で連結され、ＡＥＳ－１２８で暗号化されている。この暗号化されたデータがＳＳＬ／ＴＬＳ受信処理において暗号化・復号処理部１０７で復号処理される。ここで、”Ｔｙｐｅ”、”Ｖｅｒｓｉｏｎ”、”　ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”は、ヘッダ部分に相当する。”Ｔｙｐｅ”はＳＳＬ／ＴＬＳのペイロード・データに格納されているデータの種類、”Ｖｅｒｓｉｏｎ”はＳＳＬ／ＴＬＳのバージョン、”　ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”は暗号化されているデータのデータ長である。”Ｃｏｍｐｒｅｓｓｅｄ　ｆｒａｇｍｅｎｔ”は、コンテンツデータ、“ＭＡＣ値”は、　改竄検知のための認証コードである。”ｐａｄｄｉｎｇ　ｄａｔａ”は暗号化対象データをＡＥＳ－１２８のブロックサイズの整数倍にするために付加されるデータである。”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇｌｅｎｇｔｈ”は”Ｃｉｐｈｅｒ＿Ｔｅｘｔ．ｐａｄｄｉｎｇｌｅｎｇｔｈ”フィールドを含めた”ｐａｄｄｉｎｇ　ｄａｔａ”のデータ長である。尚、図２のフォーマットに沿った暗号化データは、パケット、あるいは

データグラムの暗号化処理単位ごとに生成され、この暗号化処理単位ごとに、復号処理が実行される。

【００１９】

次にＳＳＬ／ＴＬＳ受信処理において認証処理部１０８に入力するデータについて説明する。

図３は本実施形態における認証処理部１０８の入力データを示した図である。

【００２０】

図３において、”Ｋ　ＸＯＲ　ｉｐａｄ”はＳＳＬ／ＴＬＳプロトコルで通信する双方で共有するＭＡＣ書き込みシークレットの後に０ｘ００を付加して６４バイトにしたものとｉｐａｄの排他的論理和である。”Ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ”は送信側ではデータの送出毎に、受信側ではデータの受信毎にデータのバイト数を加えて更新されるカウンタ値である。”Ｋ　ＸＯＲ　ｉｐａｄ”と”Ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ”については図２で示した受信データそのものに含まれていない。そのため、中央演算処理装置１０１が、Ｋと”Ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ”を、パラメータ保持・設定部１０４に設定し、そして、パラメータ算出部１０６２に送られる。パラメータ算出部１０６２は、Ｋと保持しているｉｐａｄから、”Ｋ　ＸＯＲ　ｉｐａｄ”を算出する。算出された”Ｋ　ＸＯＲ　ｉｐａｄ”と、”Ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ”を入出力データ成形部１０６３に送られる。そして、認証処理部１０８への入力データとして図２で示した受信データに先行して、”Ｋ　ＸＯＲ　ｉｐａｄ”と”Ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ”が連結される。これに続いて、受信データから暗号化されていない”Ｔｙｐｅ”、”Ｖｅｒｓｉｏｎ”の各データが入出力データ成形部１０６３で連結される。受信データではその後に　”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”が続くが認証処理においては、”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”を式（１）により算出された”Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ”に置き換える必要がある。

【００２１】

Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ

＝ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ－ＣｉｐｈｅｒＳｐｅｃ．ｍａｃ＿ｓｉｚｅ－（ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ＋１）　・・式（１）

ここで　”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”，　”ＣｉｐｈｅｒＳｐｅｃ．ｍａｃ＿ｓｉｚｅ”，　”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ＋１”はＲＦＣ２１０４に規定されており、図２に示されるような関係にある。”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”は、暗号化されているデータのデータ長、　”ＣｉｐｈｅｒＳｐｅｃ．ｍａｃ＿ｓｉｚｅ”は、ＭＡＣ値のデータ長、　”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ”は、パディングデータのデータ長である。

【００２２】

さらに復号処理により得られた”Ｃｏｍｐｒｅｓｓｅｄ　ｆｒａｇｍｅｎｔ”を入出力データ成形部１０６３で連結し、“ｐａｄｄｉｎｇ　ｄａｔａ”を入出力データ成形部１０６３で付加したものが、図３（Ａ）である。”Ｃｏｍｐｒｅｓｓｅｄ　ｆｒａｇｍｅｎｔ”と“ｐａｄｄｉｎｇ　ｄａｔａ”は、暗号化・復号処理部１０７における復号処理で得られる。そして、図３（Ａ）のデータから、ハッシュ値を認証処理部１０８で求める。次にＳＳＬ／ＴＬＳプロトコルで通信する双方で共有するＭＡＣ書き込みシークレットの後に０ｘ００を付加して６４バイトにしたものとｏｐａｄの排他的論理和である”Ｋ　ＸＯＲ　ｏｐａｄ”と上記算出されたハッシュ値を入出力データ成形部１０６３で連結する。算出されたハッシュ値は、図３（Ｂ）の”Ｈａｓｈ　Ｖａｌｕｅ”に相当する。尚、”Ｋ　ＸＯＲ　ｏｐａｄ”は、パラメータ算出部１０６２において、パラメータ保持・設定部１０４から受け取ったＫと保持しているｏｐａｄから、”Ｋ　ＸＯＲ　ｏｐａｄ”を算出し、その後、入出力データ成形部１０６３に送られる。復号処理された“Ｐａｄｄｉｎｇ　ｄａｔａ”を入出力データ成形部１０６３で付加したものが、図３（Ｂ）である。図３（Ｂ）のデータを認証処理部１０８に入力し、最終的なＭＡＣ値を認証処理部１０８で算出する。

【００２３】
図４は、ＳＳＬ／ＴＬＳ受信処理において復号処理の対象となるデータグラムを示した図である。図４（Ａ）は、図２と同じであり、ＳＳＬ／ＴＬＳ受信処理における受信データに相当する。図４（Ｂ）は、暗号処理アクセラレータ１０３への入力データであり、図４（Ａ）に示した受信データの先頭部分に、暗号化データの最終２ブロックを連結したデータである。復号処理は、暗号化・復号処理部１０７で、１６バイト単位で処理される。図４（Ｂ）に示した入力データの先頭に連結された暗号化データの最終２ブロックのうち、最後のブロック”ＣＥ”は復号処理の被処理データとして、最後から２番目のブロック”ＣＥ２”はブロック”ＣＥ”の復号処理のイニシャルベクタとして用いられる。
【００２４】
図５は実施形態１におけるＳＳＬ／ＴＬＳ受信処理の先頭部分の処理フローを示した図である。
【００２５】
ステップＳ４０１において中央演算処理装置１０１は暗号処理アクセラレータ１０３の動作に必要なパラメータをパラメータ保持・設定部１０４に設定する。ステップＳ４０２においてパラメータ保持・設定部１０４は設定されたパラメータを保持するとともにパラメータ算出部１０６２に転送する。ステップＳ４０３においてパラメータ算出部１０６２は転送されたパラメータのうち、”Ｋ　”を用いて、”Ｋ　ＸＯＲ　ｉｐａｄ”と”Ｋ　ＸＯＲ　ｏｐａｄ”を算出する。算出した”Ｋ　ＸＯＲ　ｉｐａｄ”と受け取った”Ｓｅｑｕｅｎｃｅ　Ｎｕｍｂｅｒ”　を入出力データ成形部１０６３に転送する。尚、ステップＳ４０１、ステップＳ４０２、ステップＳ４０３と、後述するステップＳ４２６のパラメータに関する処理は、暗号処理単位であるパケット、あるいはデータグラムごとに実行される。
【００２６】
ステップＳ４０４において、入出力データ成形部１０６３は、転送された”Ｋ　ＸＯＲ　ｉｐａｄ”と”Ｓｅｑｕｅｎｃｅ　Ｎｕｍｂｅｒ”から認証処理部１０８の入力データであるブロックＨ０を成形し、認証処理部１０８へ出力する。本実施形態では認証処理部１０８においてハッシュ関数ＳＨＡ－１の処理を行うので入力データは６４バイト単位となり、入力データであるブロックＨ０は、図３の”Ｋ　ＸＯＲ　ｉｐａｄ”となる。”Ｋ　ＸＯＲ　ｉｐａｄ”は送受信されるデータに先行して送信側・受信側双方で共有している情報から算出可能であるため、入力する受信データが６４バイトに達する前に認証処理部１０８での認証処理が開始できる。ステップＳ４０５において認証処理部１０８は図３に示した認証処理の対象となるデータの最初のブロックであるブロックＨ０に対してハッシュ値算出処理を行う。なお、認証処理部１０８は、ブロックＨ０に対する処理が終了すると中間値を内部に保持し、次のブロックであるブロックＨ１の処理における初期値として使用する。この中間値は１ブロックの処理が終了するたびに認証処理部１０８内部で保持され、対象となる全データに対する認証処理が終了するまで中間データ保持部１０６４に出力する必要はない。
【００２７】
ここで、ブロックＨｍは、図３（Ａ）のデータを、６４バイト単位で分割したブロックのうち、ｍ＋１番目のブロックである。また、ブロックＨＥは、図３（Ａ）のデータを、６４バイト単位で分割したブロックのうちの最後のブロックである。
【００２８】
一方、ステップＳ４０６において中央演算処理装置１０１は入出力データ転送部１０５と外部記憶装置１０２間の入出力データ転送設定を入出力データ転送部１０５に設定する。ステップＳ４０７において入出力データ転送部１０５は外部記憶装置１０２から入出力データ転送部１０５への図４（Ｂ）に示した入力データの転送を開始する。本実施例では暗号モードがＣＢＣモードであるのでイニシャルベクタがパラメータとして設定されるが、ＣＴＲモードであればカウンタ値がパラメータとして設定される。ステップＳ４２６において、パラメータ算出部１０６２は、入力データからブロック“ＣＥ２”を抽出し、イ

ニシャルベクタとして暗号処理部１０７に転送する。
【００２９】
ステップＳ４０８において入出力データ成形部１０６３は入力データからブロックＣＥを成形し、暗号化・復号処理部１０７に転送する。ここで、ブロックＣｎは、図２で、暗号化されているデータを、１６バイト単位で分割したブロックのうち、ｎ＋１番目のブロックである。また、ブロックＣＥは、図２で、暗号化されているデータを、１６バイト単位で分割したブロックのうちの最後のブロックである。ここで、図２、暗号化されているデータは、”Ｃｏｍｐｒｅｓｓｅｄ ｆｒａｇｍｅｎｔ”、” Ｐａｄｄｉｎｇ ｄａｔａ”、 ”ＭＡＣ値 ”、” ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇｌｅｎｇｔｈ”である。
【００３０】
上述したように図３で示した認証処理部１０８への入力データの成形にあたっては受信データの”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”を”Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ”に置き換える必要がある。この際、入出力データ成形部１０６３での成形処理に”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ＋１” が必要となる。そのため、受信データの暗号化された部分から先行して”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ＋１”を含むブロックの復号処理を行う。ＳＳＬ／ＴＬＳの規格上上記”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ＋１”を含むブロックは受信データの最後のブロックであるため、暗号化・復号処理部１０７で行う復号処理の最初のブロックは受信データの最後のブロックＣＥになる。
【００３１】
ステップＳ４０９において暗号化・復号処理部１０７はブロックＣＥに対する復号処理を行い、ブロックＣＥを平文化（復号処理）したブロックＰＥを中間データ保持部１０６４に出力する。ここで、ブロックＰｎは、ブロックＣｎを復号処理されたブロックである。ステップＳ４１０において中間データ保持部１０６４は入出力データ成形部１０６３にブロックＰＥを転送する。ステップＳ４２７において、入出力データ成形部１０６３はブロックＰＥから”ＣｉｐｈｅｒＴｅｘｔ．ｐａｄｄｉｎｇ＿ｌｅｎｇｔｈ”を抽出し、上述した式（１）によりパラメータである”Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ”を算出する。他のパラメータ”ＣｉｐｈｅｒＴｅｘｔ．ｌｅｎｇｔｈ”は受信データに平文として埋め込まれており、パラメータとしてパラメータ保持・設定部１０４に設定される。また、”ＣｉｐｈｅｒＳｐｅｃ．ｍａｃ＿ｓｉｚｅ”は認証処理部１０８で選択された認証アルゴリズムによって決まる固定値である。なお、ブロックＰＥはここでは上記”Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ”を算出するためにのみ使用しているので入出力データ転送部１０５を介して外部記憶装置１０２に転送していないが、暗号化されたデータの復号処理の最後にもう一度読み込む必要がある。ステップ４１０において外部記憶装置１０２に転送することにより再度最後のブロックの復号処理を省略することもできるが後述するようにトータルの処理時間は短縮できない。
【００３２】
ステップＳ４２８においてパラメータ算出部１０６２はパラメータ保持・設定部１０４から転送されたイニシャルベクタを暗号化・復号処理部１０７に転送する。ステップＳ４１１において入出力データ成形部１０６３は入力データからブロックＣ０を成形し、暗号処理部１０７に転送する。ここでブロックＣ０は、暗号化されているデータを、１６バイト単位で分割したブロックのうちの最初のブロックである。ステップＳ４１２において暗号化・復号処理部１０７はブロックＣ０に対する復号処理を行い、ブロックＣ０を平文化（復号処理）したブロックＰ０を中間データ保持部１０６４に出力する。また、ステップＳ４２８で設定されたイニシャルベクタをブロックＣ０に置き換え、内部で保持する。ステップＳ４１３において中間データ保持部１０６４は入出力データ成形部１０６３および入出力データ転送部１０５にブロックＰ０を転送する。ステップＳ４１４において入出力データ転送部１０５は外部記憶装置１０２にブロックＰ０を転送する。
【００３３】

ステップＳ４１５において入出力データ成形部１０６３は入力データからブロックＣ１を成形し、暗号処理部１０７に転送する。ここでブロックＣ１は、図２で、暗号化されているデータを、１６バイト単位で分割したブロックのうち、２番目のブロックである。ステップＳ４１６、ステップＳ４１７、ステップＳ４１８においてブロックＣ０と同様の手順で、ブロックＣ１を成形／転送、復号処理し、平文化（復号処理）したブロックＰ１を外部記憶装置１０２に転送する。ステップＳ４１９、ステップＳ４２０、ステップＳ４２１、ステップＳ４２２においても、ブロックＣ０と同様の手順で、ブロックＣ２を成形／転送、復号処理し、平文化（復号処理）したブロックＰ２を外部記憶装置１０２に転送する。

【００３４】

また、ブロックＣ３、Ｃ４、・・・についても同様の手順で復号処理を行ない、平文化（復号処理）したブロックＰ３、Ｐ４、・・・を外部記憶装置１０２に転送する。この間、ブロックＣ３、Ｃ４、・・・を含む入力データを外部記憶装置１０２から入出力データ転送部１０５に転送する必要があるが、図５においては省略し、明示していない。入出力データ転送部１０５、入出力データ成形部１０６３などが一時保持できればまとめてバースト転送してもよいし、平文化（復号処理）したブロックを外部記憶装置１０２に転送するたびに外部記憶装置１０２から転送してもよい。

【００３５】

一方、ステップＳ４０５において認証処理部１０８がブロックＨ０に対するハッシュ値算出処理を終えると中間データ保持部１０６４に対してブロックＨ０処理終了信号を出力する。ステップＳ４２３において中間データ保持部１０６４は入出力データ成形部１０６３に対してブロックＨ０処理終了信号を転送する。ステップＳ４２４において、入出力データ成形部１０６３は、ブロックＨ１を成形する。ブロックＨ１は、入出力データ転送部１０５から受け取った“Ｔｙｐｅ”と“Ｖｅｒｓｉｏｎ”と、ステップＳ４２７で算出した”Ｃｏｍｐｒｅｓｓｅｄ．ｌｅｎｇｔｈ”と、暗号化・復号処理部１０７で復号された“ｆｒａｇｍｅｎｔ”とから成形される。そして、成形したブロックＨ１を、認証処理部１０８に転送する。ステップＳ４２５において認証処理部１０８はブロックＨ０に対するハッシュ値算出処理を行った結果得られた中間値を初期値としてブロックＨ１に対してハッシュ値算出処理を行う。

【００３６】

そして、処理中のパケット、あるいはデータグラムのデータがなくなるまで、ブロックＣｎ成形／転送処理、ブロックＣｎ復号処理、ブロックＰｎ転送処理、ブロックＨｍ認証処理を繰り返す。

【００３７】

本実施形態では暗号化・復号処理アルゴリズムとしてＣＢＣモードのＡＥＳ－１２８、認証処理アルゴリズムとしてＨＭＡＣ－ＳＨＡ－１の組み合わせが選択された場合を想定している。ＡＥＳ－１２８は１２８ビットの入力データを１１ラウンド、ＳＨＡ－１は５１２ビットの入力データを８０ステップでそれぞれ処理するアルゴリズムである。ＳＳＬ／ＴＬＳでは送受信する被処理データに対し、暗号化・復号処理と認証処理の両方を行う必要がある。これらを並列処理する場合、ＳＨＡ－１が１ブロックの処理に要する時間が、ＡＥＳ－１２８が１ブロックの処理に要する時間の４倍より大きければ、ＳＨＡ－１の処理速度がＳＳＬ／ＴＬＳレコードプロトコル処理のスループットを決める支配要因になる。一方、ＳＨＡ－１が１ブロックの処理に要する時間が、ＡＥＳ－１２８が１ブロックの処理に要する時間の４倍より小さければ、ＡＥＳ－１２８の処理速度がＳＳＬ／ＴＬＳレコードプロトコル処理のスループットを決める支配要因になる。ここではハードウエアでＡＥＳ－１２８を１ラウンド／クロックサイクル、ＳＨＡ－１を２ステップ／クロックサイクルで処理すると想定し、ほぼ同等の処理速度を想定している。

【００３８】

図６は本実施形態におけるＳＳＬ／ＴＬＳ受信処理の最後の部分の処理フローを示した図である。

【００３９】
ステップＳ５１２において処理中のパケット、あるいはデータグラムの入力データがなくなると、入出力データ転送部１０５は外部記憶装置１０２から入出力データ転送部１０５への入力データの転送を終了する。
【００４０】
ステップＳ５１３のブロックＣＥ復号処理は、図４のステップ４０９と同様の処理である。ステップＳ５１４のブロックＰＥ転送処理は、図４のステップ４１０と同様の処理である。
【００４１】
ステップＳ５０１において入出力データ転送部１０５は復号処理した最後のブロックＰＥを外部記憶装置１０２に転送する。
【００４２】
ステップＳ５０２において認証処理部１０８は最後のブロックであるブロックＨＥに対するハッシュ値算出処理を行ない、算出したハッシュ値を中間データ保持部１０６４へ転送する。ステップＳ５０３において中間データ保持部１０６４はハッシュ値を入出力データ成形部１０６３に転送し、入出力データ成形部１０６３はハッシュ値を保持しておく。ここで、ハッシュ値は、図３（Ｂ）における“Ｈａｓｈ　Ｖａｌｕｅ”に相当する。
【００４３】
ステップＳ５０４において入出力データ成形部１０６３はブロックＭ０を成形し、認証処理部１０８に転送する。ここで、ブロックＭ０は、図３（Ｂ）における”Ｋ　ＸＯＲ　ｏｐａｄ”の部分である。
【００４４】
ステップＳ５０５において認証処理部１０８はブロックＭ０に対するハッシュ値算出処理を行ない、中間データ保持部１０６４に対してブロックＭ０処理終了信号を出力する。ステップＳ５０６において中間データ保持部１０６４は入出力データ成形部１０６３に対してブロックＭ０処理終了信号を転送する。
【００４５】
ステップＳ５０７において入出力データ成形部１０６３は、認証処理部１０８で算出したハッシュ値と、暗号化・復号処理部１０７で復号されたＰａｄｄｉｎｇ　ｄａｔａとから、ブロックＭ１を成形し、認証処理部１０８に転送する。ここで、ブロックＭ１は、図３（Ｂ）における“Ｈａｓｈ　Ｖａｌｕｅ”および”Ｐａｄｄｉｎｇ　ｄａｔａ”の部分である。ステップＳ５０８において認証処理部１０８はブロックＭ１に対するハッシュ値算出処理を行ない、算出したＭＡＣ値を中間データ保持部１０６４へ転送する。ステップＳ５０９において中間データ保持部１０６４はＭＡＣ値を入出力データ成形部１０６３に転送する。ステップＳ５１０において、入出力データ成形部１０６３は、認証処理部１０８で算出されたＭＡＣ値が復号処理して得られたＭＡＣ値と一致するか比較を行う。また、算出したＭＡＣ値およびＭＡＣ値の比較結果を入出力データ転送部１０５に転送する。ステップＳ５１１において、入出力データ転送部１０５はＭＡＣ値およびＭＡＣ値の比較結果を外部記憶装置１０２に転送する。
【００４６】
図５と図６のフローチャートは、ある１つの暗号化処理単位のデータについての処理であり、受信した暗号化データを復号処理・認証処理する場合は、図５と図６のフローチャートを、暗号化処理単位ごとに処理される。
【００４７】
以上説明したようにＳＳＬ／ＴＬＳ受信処理の設定に従って、暗号化・復号処理および認証処理に必要なパラメータの算出、設定と入力データの成形を行う入出力データ処理をハードウエアで行っている。そのため、ハードウエア、ソフトウエア間の切替が不要な一括処理が可能になった。また、復号処理、認証処理を並列化し、データ転送回数も削減することができたため、ＳＳＬ／ＴＬＳ受信処理の処理速度を向上させることができた。
【００４８】

本実施形態によれば、通信暗号処理に必要な設定を行い、その後、入力データを一度入力することでハードウエアが一連の通信暗号処理に必要なパラメータの算出、入出力データの成形を行っている。このためハードウエア処理、ソフトウエア処理の切替によるオーバーヘッドがなくなり、データの転送回数が従来より削減される。また、暗号化・復号処理と認証処理を並列化するだけでなく暗号、認証アルゴリズムに応じて最適な順序で処理でき、通信暗号処理全体のスループットを向上させることができる。

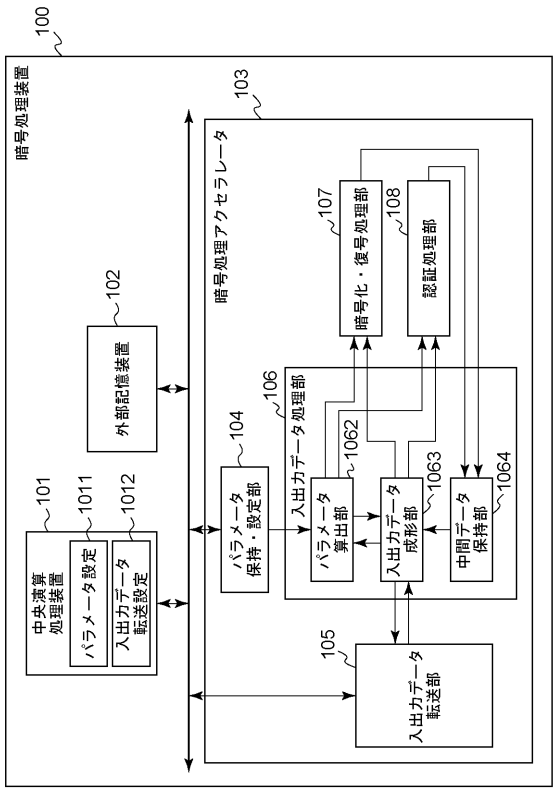
【００４９】

また、本実施形態によれば、処理中の暗号化処理単位の通信暗号処理を行う際に、一度だけ必要な設定を行い、入力データを入力すれば良いので従来必要であった復号されたデータを保持する記憶容量が必要なくなる。結果として、メモリコストを削減出来る。

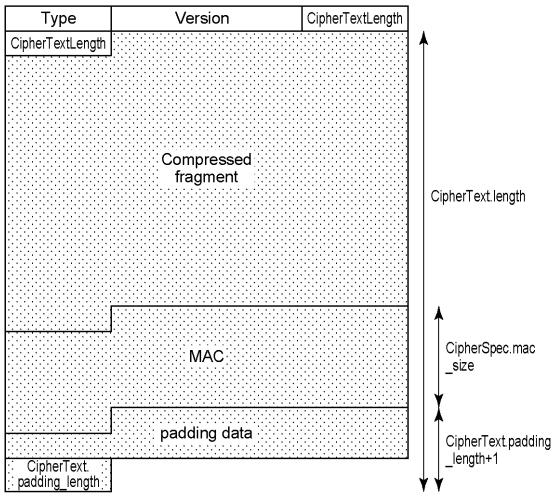
【００５０】

なお、本実施形態においては暗号アルゴリズムとしてＣＢＣモードのＡＥＳ－１２８を例にしたが、ＣＴＲモードにおいてもＩＶの代わりにＣＴＲ初期値をパラメータとして設定して同様の動作が実現できる。また認証アルゴリズムとしてＨＭＡＣ－ＳＨＡ－１を例にしたが、ＳＨＡ－１の代わりにＭＤ５、ＳＨＡ－２５６などを使った場合でも適用可能である。ＭＤ５、ＳＨＡ－２５６などを使った場合に得られるハッシュ値のデータサイズがそれぞれ１６バイト、３２バイトとなる点が異なるが、入力データのブロックサイズはＳＨＡ－１の場合と同様に６４バイトであるので本実施例と同様の処理が実現できる。

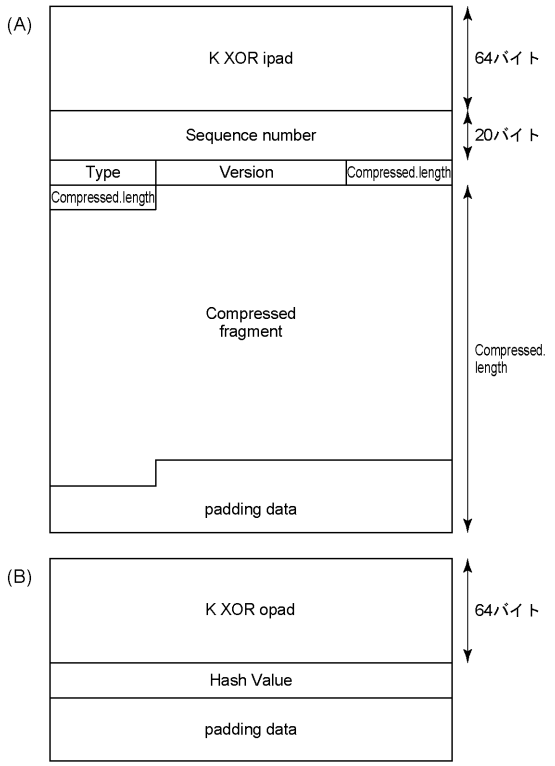
【図１】



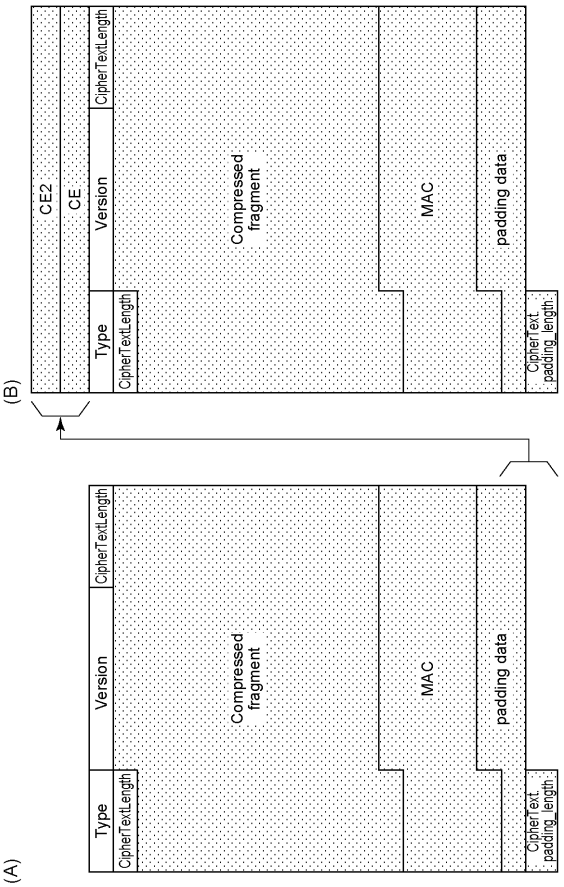
【図２】



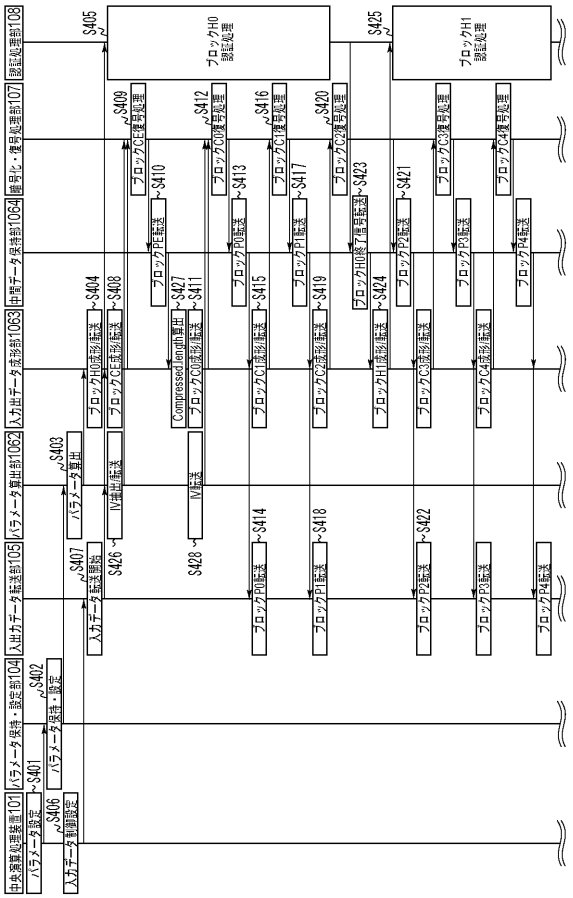
【図３】


(A)
K XOR ipad
64バイト
Sequence number
20バイト
Type
Version
Compressed.length
Compressed.length
Compressed fragment
Compressed. length
padding data
(B)
K XOR opad
64バイト
Hash Value
padding data

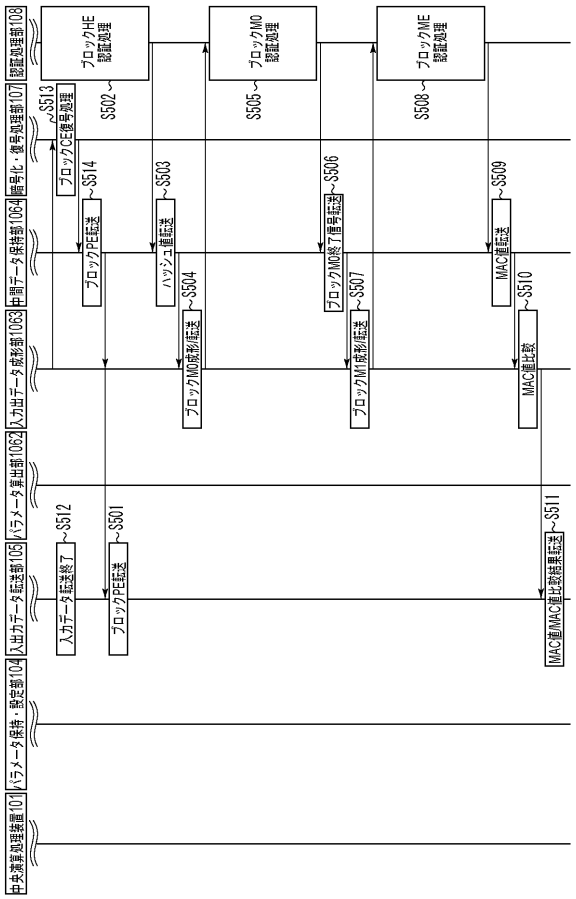
【図４】


(B)
CE2
CE
Version
CipherTextLength
Type
CipherTextLength
Compressed fragment
MAC
padding data
CipherText padding_length
(A)
Type
CipherTextLength
Version
CipherTextLength
Compressed fragment
MAC
padding data
CipherText padding_length

【図５】


中央演算処理装置101
パラメータ保持・設定部104
入出力データ転送部105
パラメータ算出部1062
入出力データ疎務部1063
申請データ保持部1064
暗号化・復号処理部107
認証処理部108
パラメータ設定
入力データ制御設定
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411
S412
S413
S414
S415
S416
S417
S418
S419
S420
S421
S422
S423
S424
S425
S426
S427
S428
パラメータ算出
入力データ転送開始
IV値生成転送
IV転送
Compressed.length算出
ブロックH0認証処理
ブロックH0疎務転送
ブロックCE疎務転送
ブロックCE復号処理
ブロックPE転送
ブロックC0疎務転送
ブロックC0復号処理
ブロックP0転送
ブロックC1疎務転送
ブロックC1復号処理
ブロックP1転送
ブロックC2疎務転送
ブロックC2復号処理
ブロックH0終了情報転送
ブロックH1疎務転送
ブロックH1認証処理
ブロックP2転送
ブロックC3疎務転送
ブロックC3復号処理
ブロックP3転送
ブロックC4疎務転送
ブロックC4復号処理
ブロックP4転送

【図６】


中央演算処理装置101
パラメータ保持・設定部104
入出力データ転送部105
パラメータ算出部1062
入出力データ疎務部1063
申請データ保持部1064
暗号化・復号処理部107
認証処理部108
S501
S502
S503
S504
S505
S506
S507
S508
S509
S510
S511
S512
S513
S514
入力データ転送終了
ブロックPE転送
ブロックHE認証処理
ハッシュ値転送
ブロックM0疎務転送
ブロックM0認証処理
ブロックM0終了情報転送
ブロックM1疎務転送
ブロックM1認証処理
MAC値転送
MAC値比較
MAC値MAC値比較結果転送

フロントページの続き

(56)参考文献 米国特許出願公開第２００３／０２３１７６５（ＵＳ，Ａ１）
特開２００４－３４３７３１（ＪＰ，Ａ）
特開２００４－３６４０２２（ＪＰ，Ａ）
特表２００６－５１１１２６（ＪＰ，Ａ）
特開２０１０－０５７１２３（ＪＰ，Ａ）
米国特許出願公開第２００２／０１９１７９０（ＵＳ，Ａ１）
舟津 泰史，“ＳＳＬ／ＴＬＳ受信時の高速処理方法及びその装置”，ソニー公開技報集，日本，ソニー（株），２００４年１１月１０日，Ｖｏｌ．１３、Ｎｏ．１３，ｐ．１－７
磯部 隆史、堤 聡、瀬戸 康一郎、青島 健次、苅谷 和俊，“ＦＰＧＡを用いた１０ＧｂｐｓＴＬＳ／ＳＳＬアクセラレータの開発”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１０年 2月２５日，Ｖｏｌ．１０９、Ｎｏ．４４８，ｐ．５４９－５５４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／３６