

(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2005-287024

(P2005-287024A)

(43) 公開日 平成17年10月13日(2005. 10. 13)

(51) Int.Cl.⁷
H04L 9/10F I
H04L 9/00 621Zテーマコード (参考)
5J104

審査請求 有 請求項の数 10 O L 外国語出願 (全 63 頁)

(21) 出願番号 特願2005-82797 (P2005-82797)
 (22) 出願日 平成17年3月22日 (2005. 3. 22)
 (31) 優先権主張番号 10/806, 668
 (32) 優先日 平成16年3月23日 (2004. 3. 23)
 (33) 優先権主張国 米国 (US)

(特許庁注：以下のものは登録商標)

1. Macintosh
 2. マッキントッシュ
 3. Linux
 4. リナックス

(71) 出願人 594071675
 ハリス コーポレーション
 Harris Corporation
 アメリカ合衆国 フロリダ 32919
 メルバーン、ウエスト・ナサ・ブルバード
 1025
 (74) 代理人 100070150
 弁理士 伊東 忠彦
 (74) 代理人 100091214
 弁理士 大貫 進介
 (74) 代理人 100107766
 弁理士 伊東 忠重

最終頁に続く

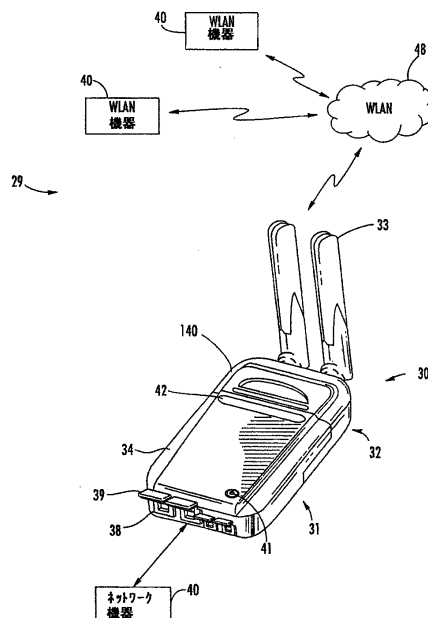
(54) 【発明の名称】 マルチモード無線LAN動作機能を備えるモジュール型暗号機器及び関連する方法

(57) 【要約】 (修正有)

【課題】 高レベルセキュリティ、多対応暗号機器の提供

。【解決手段】 暗号機器 (30) は、暗号モジュール (31) と、それに取り外し可能に結合される通信モジュール (32) とを含み得る。暗号モジュール (31) は、第1ハウジング (34)、第1ハウジングによって収容されるユーザ・ローカル・エリア・ネットワーク (LAN) インタフェース、及び第1ハウジングによって収容され、ユーザLANインタフェースに結合される暗号プロセッサを含み得る。通信モジュール (32) は、第2ハウジング、及び第2ハウジングによって収容されるネットワーク無線LANインタフェースを含み得る。ネットワーク無線LANインタフェースは、暗号プロセッサに結合される場合があり、無線LANモード間で切り替え可能であり得る。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

暗号機器であって：
暗号モジュール；及び
該暗号モジュールに結合される通信モジュール；
を備え；
該暗号モジュールは：
第 1 ハウジング；
該第 1 ハウジングによって収容されるユーザ・ローカル・エリア・ネットワーク（LAN）；及び
該第 1 ハウジングによって収容され、該ユーザ LAN インタフェースに結合される暗号プロセッサ；
を備え；
該通信モジュールは：
第 2 ハウジング；及び
該第 2 ハウジングによって収容され、該暗号プロセッサに結合され、かつ無線 LAN モード間で切り替え可能なネットワーク無線 LAN インタフェース；
を備えることを特徴とする暗号機器。

【請求項 2】

請求項 1 記載の暗号機器であって、該ネットワーク無線 LAN インタフェース回路が：
アクセス・ポイント（AP）モードと、インフラストラクチャ・モードと、アドホック・モードとのうちの 1 つに切り替え可能であることを特徴とする暗号機器。

【請求項 3】

請求項 1 記載の暗号機器であって、該暗号モジュールが更に：
該第 1 ハウジングによって収容され、該暗号プロセッサに結合される第 1 コネクタ；
を備え；
該通信モジュールが更に：
該第 2 ハウジングによって収容され、該ネットワーク無線 LAN インタフェースに接続される第 2 コネクタ；
を備え；
該第 2 コネクタが、該暗号モジュールの該第 1 コネクタと取り外し可能につがわせることが可能であることを特徴とする暗号機器。

【請求項 4】

請求項 1 記載の暗号機器であって、該ユーザ LAN インタフェースが：
イーサネット（登録商標）インタフェース；
を備えることを特徴とする暗号機器。

【請求項 5】

請求項 1 記載の暗号機器であって、該暗号プロセッサが：
該ユーザ LAN インタフェースに結合されるホスト・ネットワーク・プロセッサ；及び
該ホスト・ネットワーク・プロセッサに結合される暗号回路；
を備えることを特徴とする暗号機器。

【請求項 6】

請求項 1 記載の暗号機器であって、該暗号モジュールが更に：
該暗号プロセッサを、該第 1 ハウジングによるタンパリングに基づいて動作不能にするタンパ回路；
を備えることを特徴とする暗号機器。

【請求項 7】

通信する方法であって：
暗号モジュールをローカル・エリア・ネットワーク（LAN）機器に結合する工程；
を備え；

10

20

30

40

50

該暗号モジュールが：

第 1 ハウジング；

該第 1 ハウジングによって収容されるユーザ LAN インタフェース；

該第 1 ハウジングによって収容され、該ユーザ LAN インタフェースに結合される暗号プロセッサ；

を備え；

更に、通信モジュールを備える工程；

を備え；

該通信モジュールが：

第 2 ハウジング；及び

該第 2 ハウジングに収容され、該暗号モジュールに取り外し可能に結合されるネットワーク無線 LAN インタフェース；

を備え；

更に、無線 LAN モード間で該ネットワーク無線 LAN インタフェースを切り替える工程；及び

該ネットワーク無線 LAN を用いて無線 LAN と通信する工程；

を備えることを特徴とする通信する方法。

【請求項 8】

請求項 7 記載の方法であって、該切り替える工程が：

アクセス・ポイント（AP）モードと、インフラストラクチャ・モードと、アドホック・モードとのうちの 1 つに切り替える工程；

を備えることを特徴とする方法。

【請求項 9】

請求項 7 記載の方法であって、該暗号モジュールが更に：

該第 1 ハウジングによって収容され、該暗号プロセッサによって結合される第 1 コネクタ；

を備え；

該通信モジュールが更に：

該第 2 ハウジングによって収容され、該ネットワーク無線 LAN インタフェースに結合される第 2 コネクタ；

を備え；

該取り外し可能に結合させる工程が：

該第 2 コネクタを該第 1 コネクタに取り外し可能につがわせる工程；

を備えることを特徴とする方法。

【請求項 10】

請求項 7 記載の方法であって、該ユーザ LAN インタフェースが：

イーサネット（登録商標）インタフェース；

を備えることを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、マルチモード無線 LAN 動作機能を備えるモジュール型暗号機器及び関連する方法に関する。

【背景技術】

【0002】

セキュリティは、ネットワーク通信において極めて重要な考慮事項である。インターネット利用の一層の増大によって、大半のネットワークは今日では、それらのネットワークを自称ハッカによる外部攻撃に開放するインターネット・ゲートウェイを有する。更に、無線ネットワークの人気も、技術によって無線通信の高速化と高信頼化とが可能になるにつれて劇的に高まってきている。それにもかかわらず、無線通信は、本来は有線通信より

10

20

30

40

50

も安全性が低いものであるが、それは無線通信信号が、多くの場合にアクセスが困難なケーブル上の信号よりも傍受することがずっと簡単であるからである。

【0003】

その結果、暗号が、多くの場合、私的通信すなわち秘密通信を暗号化するように用いられて、その通信が悪意のある個人又は組織体によって解読され、用いられることになる可能性を低減する。例として、無線ローカル・エリア・ネットワーク（WLAN）やWLAN機器は、ケーブルを通すことが困難であるか、そうでなくても非実用的な場合にネットワーク通信を実施するうえで、広く用いられ、費用効果の高い手法を備える。WLAN内部での通信を規制するうえで策定されてきた重要な標準の1つとして、米国電気電子技術者協会（IEEE）802 LAN/MAN標準委員会によって公表されている、802.11標準がある。無線通信プロトコルを備えることに加えて、802.11標準は、無線信号が盗聴されることから保護するよう用いられるウェッパ（WEP：有線と同等のプライバシ）暗号アルゴリズムも規定する。

10

【0004】

WEPは、無線局とアクセス・ポイントとの間で共有される秘密鍵に依拠する。秘密鍵は、データ・パケットを送信前に暗号化するのに用いられ、パッケージが送信中に修正されないよう完全性チェックが用いられる。それにもかかわらず、WEPアルゴリズムは、以前考えられていたほどは外部攻撃に強いものでないことが最近判明している。例えば、Borisovなどは、「Intercepting mobile communications: The insecurity of 802.11, MOBICOM, Rome, Italy」と題する西暦2001年7月公表の論文において、WEPにおけるいくつかの脆弱性を表している。特に、2つのメッセージが同じ初期化ベクトル（IV）と秘密鍵とを用いて暗号化される場合に重大なセキュリティ違反が起こり、このことは両方のメッセージに関する情報を明らかにし得るからであるということが記載されている。

20

【0005】

更に、WEPメッセージ暗号文が排他的OR演算を用いて生成される。同じIVを用いて生成される2つのメッセージからの暗号文の排他的ORをとることによって、キー・ストリームは相殺され、その場合には、平文を復元することが可能である。そういうものとして、このようにキー・ストリームを再使用することは、同じIVによって生成される複数のメッセージを探すよういくつかのメッセージが記憶され、比較される、復号辞書攻撃を受けやすいものである。

30

【0006】

その結果、更に頑強なネットワーク・セキュリティが多くの場合、多くのネットワーク・アプリケーションに必要である。保護クライアントとネットワークとの間で接続される対象のネットワーク・セキュリティ機器の一例を開示するものがある（Friedmanなどによる米国特許記載の特許出願1参照。）。このネットワーク・セキュリティ機器では、何れかの別の保護クライアントとセッション鍵が取り決められる。その場合、その2つのクライアント間の通信は全て、暗号化される。この機器は自己構成され、この機器自体をそのクライアントのIPアドレスにロックさせる。よって、クライアントはそのIPアドレスを一度設定すると変えることが可能でなく、したがって、別のクライアントのIPアドレスのエミュレーションを行うことが可能でない。パケットが保護ホストから送信される場合、セキュリティ機器はクライアントのMACアドレスをそれ自身のMACアドレスにパケットをネットワークに送信する前に変換する。ホストに対してアドレス指定されるパケットは、セキュリティ機器のMACアドレスを含む。セキュリティ機器はそのMACアドレスをクライアントのMACアドレスに、パケットをクライアントに送信する前に変換する。

40

【0007】

更に頑健な暗号機器が、注意を要する通信又は機密通信を保護するのに要し得る。特に、米国では、注意を要する（が非機密の）情報を含む、政府機関の通信は、「Secur

50

ity Requirements For Cryptographic Modules」と題する、Federal Information Processing Standards Publication (FIPS) publication 140-2を遵守しなければならない。通常、タイプ1通信と呼ばれる機密通信は、更に厳格な標準を遵守しなければならない。

【0008】

タイプ1通信に認定されている暗号化機器の一例として、ジェネラル・ダイナミクス社 (General Dynamics Corp.) によるタックレーン (TACLANE) 暗号化装置KG-175がある。TACLANE暗号化装置の「クラシック」バージョンはインターネット・プロトコル (IP) インタフェース及び非同期転送モード (ATM) インタフェースを有し、E100バージョンは高速イーサネット (登録商標) ・インタフェースを有する。クラシック・バージョンは更に、高速インターネットに、その中にあるIP/ATMネットワーク・インタフェース・カードを2枚の新しいE100のインタフェース・カードと置き換えることによってアップグレードさせ得る。

10

【0009】

そのような機器によって備えられるセキュリティ上の恩恵にもかかわらず、これらの暗号化装置の多くは、かなりかさばり、相当の電力量を消費する場合がある。空間と電力とを節減する特徴を備える1つの特に効果的な暗号機器として、本願の譲受人である、ハリス社 (Harris Corp.) によるシエラ (Sierra) モジュールがある。シエラ・モジュールは、ハイグレード・セキュリティ (例えば、タイプ1) の効果を、再プログラム可能で、商用生産されている、FIPS 140-2レベル3又は4の暗号化モジュールのコスト効率と組み合わせた、組み込み可能な暗号化機器である。シエラ・モジュールは、暗号化/復号機能、ディジタル音声処理 (ボコーディング) 機能及び暗号鍵管理支援機能を備えて、複数の暗号化の性質を特定のアプリケーションによって持ち得る。シエラ・モジュールは更に、タイプ1の機能を取り除く機能をユーザに備え、それによって、当該機器を非機密機器に格下げすることが可能になる。更に、その特性が相対的に、小型で、低電力で、高データ・レートであることから、この機器はバッテリー依存アプリケーションによく適している。

20

【0010】

例として、シエラ・モジュールは、セクネット (SecNet) 11と呼ぶ、これもハリス社によって生産されているセキュアなWLAN (SWLAN) パーソナル・コンピュータ (PC) カードにおいて実施されている。セクネット11カードによって、マルチメディア情報 (データ、音声、及びビデオ) の高速通信をセキュアな環境において可能にする。セクネット11カードは、例えば、WLAN「局」用、無線ブリッジ用、及びアクセス・ポイント (AP) 用の、無線ネットワーク・インタフェースとして用い得る。更に、セクネット11機器を詳細に記載するものがあり (特許文献2及び3参照。)、該文献は何れも全体を、本明細書及び特許請求の範囲に援用することとする。

30

【0011】

よって、セクネット11カードは、サイズ、所要電力、及びWLAN環境における柔軟性の点で数多くの効果を備える。しかし、そのような効果を別のネットワーク環境においても備えることが望ましい場合がある。

40

【特許文献1】米国特許第6240513号明細書

【特許文献2】米国特許出願公開第2002/0094087号明細書

【特許文献3】米国特許出願公開第2002/0095594号明細書

【発明の開示】

【発明が解決しようとする課題】

【0012】

上記背景に鑑みると、よって、本発明の目的は、高レベルのセキュリティを備え、数多くのネットワーク環境及び関連する方法に比較的容易に形成可能な暗号機器を備えることにある。

50

【課題を解決するための手段】

【0013】

本発明による、これら及びその他の、目的、特徴、及び効果は、暗号モジュールと、それに取り外し可能に結合される通信モジュールとを含み得る暗号機器によって備えられる。特に、暗号モジュールは、第1ハウジング、第1ハウジングによって収容されるユーザ・ローカル・エリア・ネットワーク（LAN）・インタフェース、及び第1ハウジングによって収容され、ユーザLANインタフェースに結合される暗号プロセッサを含み得る。更に、通信モジュールは、第2ハウジング、及び第2ハウジングによって収容されるネットワーク無線LANインタフェースを含み得る。ネットワーク無線LANインタフェースは、暗号プロセッサに結合される場合があり、無線LANモード間で切り替え可能であり得る。 10

【0014】

特に、ネットワーク無線LANインタフェース回路は、アクセス・ポイント（AP）モード、インフラストラクチャ・モード、及びアドホック・モードのうちの1つに切り替え可能であり得る。よって、暗号機器は、WLANにおける何れかの各種機器と相互交換可能に用いられる場合があり、よって複数の種類のWLAN暗号化機器に対する必要性がなくなる。

【0015】

それに加えて、暗号モジュールは更に、第1ハウジングによって収容され、暗号プロセッサに結合される第1コネクタを含む場合があり、通信モジュールは更に、第2ハウジングによって収容され、ネットワーク無線LANインタフェースに接続される第2コネクタを含み得る。更に、第2コネクタは、暗号モジュールの第1コネクタと取り外し可能につながせることが可能であり得る。よって、本発明の別の特徴によれば、通信モジュールは、複数の相互交換可能な通信モジュールからの所定のものである場合があり、相互交換可能な通信モジュールのネットワーク無線LANインタフェースの各々は、別々の無線LANモード（すなわち、AP、インフラストラクチャ、又はアドホック）において動作する。よって、同じ暗号モジュールを効果的に、何れかのWLAN機器とともに、その特定の機器に適切な通信モジュールを暗号モジュールに単に結合させることによって用い得る。 20

【0016】

ユーザLANインタフェースは、例えば、イーサネット（登録商標）インタフェースであり得る。更に、暗号機器は、第1ハウジングによって収容され、暗号プロセッサ、ユーザLANインタフェース、及びネットワークLANインタフェースに電源を供給する電源回路を含む場合もある。暗号プロセッサは、例えば、タイプ1のセキュリティ・レベル以下の所定のセキュリティ・レベルを備えるよう暗号化アルゴリズムを実施し得る。 30

【0017】

特に、暗号プロセッサは、ユーザLANインタフェースに結合されるホスト・ネットワーク・プロセッサ、及びホスト・ネットワーク・プロセッサに結合される暗号回路を含み得る。更に、暗号プロセッサは、ユーザLANインタフェースと暗号回路との間で結合される非暗号化データ・バッファ回路、及び暗号回路とネットワークLANインタフェースとの間を結合される暗号化データ・バッファ回路を含む場合もある。 40

【0018】

暗号モジュールは更に効果的には、第1ハウジングによるタンパリングに基づいて暗号プロセッサを動作不能にするタンパ回路を含み得る。例として、タンパ回路は、暗号プロセッサを実質的に取り囲む1つ又は複数の導体を含む場合があり、暗号プロセッサは導体における開路に基づいて動作不能にし得る。

【0019】

本発明の通信方法の特徴は、上記に簡単に説明したものなどの暗号モジュールをLAN機器に結合させる工程を含む場合があり、通信モジュールは暗号モジュールに取り外し可能に結合される。上記のように、通信モジュールは、第2ハウジング及び、第2ハウジングによって収容され、暗号プロセッサに結合されるネットワーク無線LANインタフェー 50

スを含み得る。更に、該方法はそれに加えて、無線LANモード間でネットワーク無線LANインタフェースを切り替える工程を含み得る。通信モジュールはその場合、LANと通信するのに用い得る。

【0020】

本発明の別の方法の特徴は、それに複数の暗号モジュールのうちの1つを取り外し可能に結合させたその暗号モジュールを備える工程及び暗号モジュールをLAN機器に結合させる工程を含む。特に、通信モジュールは、第2ハウジング及び、第2ハウジングによって収容されるネットワーク無線LANインタフェースを含む場合があり、複数の相互交換可能な通信モジュールのネットワーク無線LANインタフェースは各々、別々の無線LANモードにおいて動作し得る。通信モジュールはその場合、無線LANと通信するのに用い得る。

10

【0021】

本発明による通信システムは、無線LANを規定するようお互いに結合される複数のLAN機器及び、該LAN機器のうちの少なくとも1つに結合される、上記に簡単に説明したものなどの暗号機器を含み得る。

【発明を実施するための最良の形態】

【0022】

本発明は次に、添付図面を参照しながら以下に更に全面的に説明することとし、添付図面においては本発明の好適実施例を表す。しかし、本発明は、多くの種々の形態において実施し得るものであり、本明細書及び特許請求の範囲記載の実施例に限定されるものとして解すべきでない。むしろ、これらの実施例は、本開示が徹底的で完全なものになり、本発明の範囲を当業者に十分伝達することになるように備えられている。同じ数字は全般的に同じ構成要素を表し、プライム符号は別々の実施例における同様な構成要素又は工程を示すのに用いられる。

20

【実施例】

【0023】

まず、図1乃至図9を参照すれば、本発明による通信システム29は図では、暗号機器30、複数のネットワーク機器40、及び無線ローカル・エリア・ネットワーク(WLAN)48などのネットワークを含む。暗号機器30は図では、機器40のうちの1つと通信モジュール32とに結合される暗号モジュール31を含む。図2に表すように、通信モジュール32は、以下に更に記載するように、暗号モジュール31に取り外し可能に結合される。一般的に言えば、本発明によって、複数の交換可能な通信モジュール32を暗号モジュール31に接続して種々の通信媒体上を通信し得る。図示した実施例では通信モジュール32が、デュアル・トライバンド・アンテナ33を含むWLANモジュールであるが、暗号機器30を数多くの種類の、有線ネットワーク及び無線ネットワークとともに用いることが可能であることは以下の記載に基づいて分かるものである。

30

【0024】

適切なチップ・セット／インタフェース回路を種々の通信モジュール32に含めることによって、これらのモジュールの各々は別々のネットワーク媒体(例えば、WLAN、有線媒体、光ファイバ媒体など)とインタフェースし得るが、全て同じ暗号モジュール31とインタフェースする。すなわち、同じ暗号モジュール31を数多くのネットワーク・アプリケーションに、単に、所望のアプリケーションに適切な通信モジュール32をそこに結合させることによって用い得る。用い得る各種通信モジュール32の例としては、WLANモジュール、既存電話サービス(POTS)モジュール、軍事用機器モジュール、E1/T1モジュール、インライン・ネットワーク暗号化装置(INE)モジュール、バーサ・モジュール・ユーロカード(VersaModule Eurocard)(VME)バス・モジュールなどが含まれる。

40

【0025】

モジュール型デザインと、容易に交換可能であることは、暗号モジュール31を種々のアプリケーション用にすばやく構成するうえでの好都合な方法を備えるのみならず、タイ

50

プ 1、FIPS 140-2 レベル 4 などの高レベル・セキュリティ・アプリケーションに特に有用であり得る。これは、暗号機器をこれらのレベルでの、注意を要する通信又は機密通信に用いるために認定させるうえでの評価プロセスは時間が非常に多くかかり、非常に広い範囲に及び、よって費用が非常に多くかかり得る。よって、種々のネットワーク・アプリケーション用にめいめいの暗号機器を製造することは、費用が法外なものとなり得るが、それは各々のものが厳しくかつ費用のかかる認定を個々に経なければならないことになるからである。

【0026】

しかし、本発明によって暗号モジュール 31 は好ましくは、注意を要する暗号回路及び関連する暗号アルゴリズム／鍵の全てを含んでいるので、種々の通信モジュール 32 は単 10
に、各種ネットワーク用インタフェースを備える。すなわち、それらは、「赤」（すなわち、非暗号化）守秘／機密データを処理も送信もしないものであり、よって、認定されるうえで、暗号モジュール 31 との同様な精査を必要としないと思われることになる。よって、通信モジュール 32 は、所望のアプリケーション毎に異なるネットワーク・インタフェースを備えている全く新しい暗号機器を購入するよりもかなりの費用節減を備え得る。

【0027】

特に、暗号モジュール 31 は図では、第 1 ハウジング 34、第 1 ハウジングによって収容されるユーザ・ネットワーク 35、第 1 ハウジングによって収容され、ユーザ・ネットワーク・インタフェースに結合される暗号プロセッサ 36、及び第 1 ハウジングによって 20
収容され、暗号プロセッサに結合される第 1 のモジュール間コネクタ 37 を含む。ユーザ・ネットワーク・インタフェース 35 は、例えば、当業者が分かるように、IEEE 802.3 標準互換のイーサネット（登録商標）物理層（PHY）インタフェースであり得る。種々のコネクタ 38 は、更に、第 1 ハウジング 34 によって収容されて、暗号モジュール 31 を種々のネットワーク機器 40（例えば、パーソナル・コンピュータ（PC）、サーバ、携帯型通信機器など）に結合させる。

【0028】

例として、コネクタ 38 は、RJ 45 コネクタ 85（図 8）などの有線コネクタ、又は LC 光ファイバ・コネクタ 86 などの光ファイバ・コネクタであり得る。コネクタ 38 を保護するのにキャップ 39 も含み得る。電源スイッチ 41 及び LED ステータス表示器 4 30
2（すなわち、電源、リンク・ステート、フィル、アラーム）も第 1 ハウジング 34 によって収容される。

【0029】

なお、本明細書及び特許請求の範囲の原文記載の「user」の語は、ユーザ・ネットワーク・インタフェース 35 に関して用いていて、このインタフェースが、暗号機器 30 の、ユーザ・ネットワーク機器側用であり、通信ネットワーク側用でないことを単に示している。すなわち、「user」は、インタフェース 35 が PC などの個々のユーザ機器 40
用のみであるということを表すものでない。その代わりに、ユーザ・ネットワーク・インタフェースは、上記のように、各種の LAN 機器（例えば、サーバ、ブリッジ、アクセス・ポイントなど）に接続し得る。

【0030】

通信モジュール 32 は図では、第 2 ハウジング 45、第 2 ハウジングによって収容され、暗号モジュール 31 の第 1 コネクタ 37 と取り外し可能につがわせることが可能である 40
第 2 のモジュール間コネクタ 46、及び第 2 ハウジング 45 によって収容され、第 2 コネクタに結合されるネットワーク通信インタフェース 47 を含む。本例では、ネットワーク通信インタフェース 47 は、WLAN 通信回路（例えば、802.11 チップ・セット）を含んでいて、以下に記載するように、アンテナ 33 と協調してネットワーク（例えば、LAN）48 と無線通信する。しかし、上記のように、ネットワーク通信インタフェース 47 は、例えば、有線 LAN 通信回路、光 LAN 通信回路などであり得る。

【0031】

暗号モジュール 31 の種々の回路構成部分は、当業者が分かるように、例えば、暗号化 50

回路カード（C C A）50において実施し得る。通信モジュール32の回路は同様にC C A 51において実施し得る。通信モジュール31は更に、第1ハウジング34によって収容され、暗号プロセッサ36、ユーザ・ネットワーク・インタフェース35、及び通信モジュール32に電源を供給する電源／フィルタ化回路53を含む電源C C A 52を含み得る。

【0032】

暗号プロセッサ36は、ユーザ・ネットワーク・インタフェース35に接続されるホスト・ネットワーク・プロセッサ54及び、ホスト・ネットワーク・プロセッサに接続される暗号回路55を含み得る。特に、暗号回路55は図では、ホスト・ネットワーク・プロセッサ54に接続される、非暗号化（すなわち、「赤」）データ・バッファ56、非暗号化データ・バッファに接続される暗号回路57、及び暗号回路と第1コネクタ37との間に接続される暗号化（すなわち、「黒」）データ・バッファ58を含む。

10

【0033】

例として、非暗号化データ・バッファ及び暗号化データ・バッファは、フィールドでプログラム可能なゲート・アレイ（FPGA）を用いて実施される先入れ先出し（FIFO）バッファである場合があり、暗号回路57は特定用途向集積回路（ASIC）において実施し得る。本発明に用いるのに特によく適した暗号ASICの1つに、ハリス社による上記シエラ（及びシエラII）素子がある。当然、別の適切な回路も用い得ることは当業者によって分かるものである。

【0034】

ホスト・ネットワーク・プロセッサ54は図では、当業者には分かるように、ハードウェア及び／又はソフトウェアを用いて実施し得る複数のモジュールを含む。一般的に言えば、ホスト・ネットワーク・プロセッサ54は、ユーザ・ネットワーク・インタフェース35をインタフェースする第1の802.3媒体アクセス（MAC）・コントローラ60、以下に更に記載するように、暗号プロセッサ36及びネットワーク通信インタフェース47をインタフェースする第2の802.3MACアクセス・コントローラ61、及び上記MACコントローラ間を結合するプロセッサ62を含む。ホスト・ネットワーク・プロセッサ54及びユーザ・ネットワーク・インタフェース35は、以下に記載するように、媒体独立インタフェース（MII）通信用専用線、及び、例えば、管理データ入出力バス（図6及び図8）を介して通信し得る。

20

30

【0035】

特に、プロセッサ62は、ハイパテキスト転送プロトコル（HTTP）サーバ・モジュール73、簡易型ネットワーク管理プロトコル・エージェント63、ファイヤウォール／ルーティング・モジュール64、オーバ・ザ・エアでの鍵の再交換／オーバ・ザ・ネットワークでの鍵の再交換（OTAR／OTNR）のモジュール65、及びオーバ・ザ・エアでのゼロ化／オーバ・ザ・ネットワークでのゼロ化（OTAR／OTNR）のモジュール66を含み得る。更に、プロセッサ54は、図では、それによって暗号モジュール31が動作する対象のその特定のモード又は媒体（例えば、WLANアクセス・ポイント（AP）モード、アドホック・モード、インフラストラクチャ・モードなど）に基づいて適切な構成を備えるモード・コントローラ67も含む。モード・コントローラ67は更に、当業者が分かるように、暗号モジュール31が用いられる対象の特定のアプリケーションによって、サービス・セット識別子（SSID）、チャンネル、送信レベル、データ・レート、802.11バンド選択（すなわち、a、b、g）などについての、別の構成／監視機能を実行し得る。インターネット・プロトコル（IP）セキュリティ・プロトコル（IPSec）／高度保証レベルIP暗号化（HAIPe）モジュール68、鍵管理モジュール69、及び／又は機器発見モジュール70などの別のモジュールも、この場合もまた当業者が分かるように、当該実施形態によって含み得る。暗号モジュールは好ましくは、ホスト・ネットワーク・プロセッサ54と暗号回路57との各々用のメモリ素子71、72も含む。

40

【0036】

50

電源回路 53 は図では、D C（直流）源（例えば、バッテリー）、壁いぼ A C アダプタ、イーサネット（登録商標）電源などに接続し得る外部電源インタフェース（I / F）回路 75 を含む。当然、別の電源を種々の実施形態において用い得ることが分かるものである。電源回路 53 は更に図では、外部電源 I / F 回路 75 に結合される暗号／通信モジュール電源アイソレーション／フィルタリング回路 76 を含む。暗号モジュール電源回路 77 及び通信モジュール電源回路 78 は、電源アイソレーション／フィルタ化回路 76 に結合されて、各々、暗号モジュール 31 と通信モジュール 32 とに供給する。更に、当業者が分かるように、暗号モジュール 31 と通信モジュール 32 との間で通信される信号をフィルタリングするデータ・フィルタ／静電気放電（E S D）保護回路 79 が含まれる。

【0037】

10

機密通信及び／又は秘密通信について高レベルの認定（例えば、レベル 4、F I P S 140-2、タイプ 1）を受けよう、暗号機器は通常、悪意のある個人又は組織体が該機器を物理的に危殆化させ、使用されている秘密鍵又はアルゴリズムを発見することを妨げるよう、ある程度の物理的なタンパ保護を含んでいる必要がある。本発明によれば、暗号モジュール 31 は更に、図では、第 1 ハウジング 34 によるタンパリングに基づいて暗号回路 57 を動作不能にするタンパ回路 80 を含む。例として、タンパ回路 80 は好ましくは、暗号プロセッサが、導体のうちの何れか 1 つにおける開路に基づいて動作不能にされるように暗号回路 57 を実質的に取り囲む 1 つ又は複数の導体を含む。

【0038】

特に、導体は、第 1 ハウジング 34 の内側に印刷され、暗号プロセッサ 36 に接続される比較的薄いプリント回路トレースであり得る。導体は暗号プロセッサ 36（又はその一部分）を実質的に取り囲むので、誰かが第 1 ハウジング 34 を突き通して暗号プロセッサをアクセスしようとする場合、1 つ又は複数のプリント・トレースは壊されることになる。同じことは、だれかが第 1 ハウジングを開けた場合に当てはまるが、それはトレースが暗号プロセッサ 36 から引き離されることになり、それによってその中に開路がもたらされるからである。

20

【0039】

いずれの場合でも、開路導体から生じる開回路状態によって、暗号電源インタフェース回路 81 に対する電源が中断されて中止されることになる。すなわち、専用暗号化アルゴリズム／秘密鍵バッテリー 82 からの電源は、暗号電源インタフェース回路 81 に暗号モジュール電源回路 77 を介して流入することが禁止される。その結果、揮発性メモリに好ましくは記憶される、アルゴリズム及び秘密鍵は、永久的にかつ即座に消去されるので、悪意のある個人又は組織体によって発見されることは可能でない。タンパ回路 80 はよって、所望の場合、全ての角度からのタンパ保護を備え得る。

30

【0040】

上記のように、暗号回路 57 は、所定のセキュリティ・レベル（例えば、タイプ 1、F I P S 140-2 レベル 1 乃至 4 など）を備えるよう所望の暗号化アルゴリズムを実施する。例として、A E S（次世代暗号化標準）、ベートン（B a t o n）、やメドレイ（M e d l e y）の、暗号化アルゴリズムを用いてそのような高レベルのセキュリティを備え得る。当然、当業者に分かる別の高レベル・セキュリティ・アルゴリズムも用い得る。更に、上記よりもセキュアでないと考えられる別の暗号アルゴリズムも本発明によって、暗号機器 30 が、より注意を要しない環境（例えば、一般の、商用又は企業向のアプリケーション）において用いる対象である場合に用い得る。

40

【0041】

暗号回路 55 は図では、ハードウェア及び／又はソフトウェアを用いて実施し得る複数のモジュールも含む。図 8 を特に参照すれば、非暗号化データ・バッファ（すなわち、赤の F P G A）56 は図では、ホスト・ネットワーク・プロセッサ 54 と M I I プロトコルを介して通信するホスト・インタフェース／F I F O 制御モジュール 90 及びホスト・インタフェース／F I F O 制御モジュールの出力を受信するトラフィック及びコマンド（C M D）F I F O 91、92 を含む。なお、図 8 における種々のデータ・パスは、非暗号化

50

データと暗号化データとの各々又は両方を伝達するか否かを示すよう「赤」及び／又は「黒」として印して本発明がよりよく分かるようにしている。

【0042】

トラフィックFIFO91の出力はバッファ93に接続され、該バッファは暗号回路57の第1の高速並列インタフェース94に接続される。コマンドFIFO92の出力は暗号回路57の第1の外部バス・インタフェース装置(EBIU)106に接続される。このEBIU106は更に、制御レジスタ95とマルチプレクサ96とに接続される。マルチプレクサ96の別の入力は、暗号回路57の第2の高速並列インタフェース97の出力に接続される。マルチプレクサ96の出力は巡回冗長度検査モジュール98に転送され、該モジュールの出力は出力FIFO100を通過してもう一度、ホスト・インタフェース／FIFO制御モジュール90に転送される。

【0043】

暗号回路57の第1高速並列インタフェース94は、それと関連する当該ワード・カウンタ101を有する。暗号回路57の暗号処理モジュール102は、第1と第2の高速並列インタフェース94、97及び1つ又は複数の暗号エンジン・モジュールをバス・コントローラ104を介してインタフェースする。暗号処理モジュール102は更に、暗号鍵をロードするフィル回路105と通信する。EBIU106は更に、暗号処理モジュール102をメモリ72とインタフェースする。第2EBIU107は暗号処理モジュール102を、暗号化データ・バッファ(すなわち、黒のFPGA)58の、制御レジスタ110及びマルチプレクサ111とインタフェースする。第2EBIU107とマルチプレクサ111との間の信号バスはコマンド信号バスを備える。

【0044】

ホスト・ネットワーク・プロセッサ54、赤のFPGA56、暗号回路57、及び黒のFPGA58も、当業者が分かるように、図の1つ又は複数の汎用入出力(GPIO)バスを介して通信する。別の回路112も、これも又、当業者が分かるように、特定の実施例において暗号回路57に結合させて、特定の実施形態について必要な、過大／過小電圧検知、温度検知、及び／又はパニック・ゼロ化を行い得る。

【0045】

第2の高速並列インタフェース97の出力はバッファ113を介して、赤データが黒FPGA58に入るのを禁止する保護ゲーティングを含む入力インタフェース114に転送される。入力インタフェース114の出力は、そこへのトラフィック(すなわち、データ)・バスを規定するマルチプレクサ111の第2の入力に接続される。マルチプレクサ111の出力は、巡回冗長度検査モジュール115に備えられ、該モジュールの出力は出力FIFO117に備えられる。MACインタフェース／FIFO制御モジュール118の出力はトラフィックFIFO116の入力に備えられる。トラフィックFIFO116の出力はバッファ120を介して暗号回路57の第1の高速並列インタフェース94の入力にもう一度転送され、出力FIFO117の出力はMACインタフェース／FIFO制御モジュール118に接続され、以下に更に記載するように、該モジュールは通信モジュール32と通信する。

【0046】

通信モジュール32の種々の回路は次に、更に詳細に、図5乃至図7を特に参照しながら説明することとする。上記のように、通信モジュール32の種々の回路は通信CCA51において実施される。特に、通信のCCA51(又はこのWLANの例においては無線のCCA51)は図では、通信電源回路78と連動して種々の通信回路構成部分に電源を供給する電源インタフェース126を含む。所望される場合、暗号モジュール31からの信号バスにおいて、別のフィルタ／ESD回路127も含み得る。

【0047】

特に、暗号モジュール31と通信モジュール32との間の信号バスは、図6に見られるように、MII通信用の複数のライン、更には3線直列インタフェース(3WSI)を含む。一般的に言えば、MIIラインは、暗号化データを暗号モジュール31と通信モジュール32と

ール 3 2 との間で転送するためのものであり、3 線直列インタフェースは、以下に更に記載するように、通信モジュールのステータス／構成動作である。

【0048】

特に、M I I ラインはフィルタ／E S D 回路 1 2 7 を通過してネットワーク通信インタフェース 4 7 まで延びている。本 W L A N 例では、ネットワーク通信インタフェース 4 7 は、M I I ラインに接続される 8 0 2 . 1 1 a / b / g A P / M A C チップ・セット 1 2 8 を含み、更に、8 0 2 . 1 1 a / b / g A P / M A C チップ・セットに接続される関連 8 0 2 . 1 1 a / b / g 無線部 1 2 9 を含んで、W L A N と無線通信する。1 つ又は複数のメモリ 1 3 0 を 8 0 2 . 1 1 a / b / g A P / M A C チップ・セット 1 2 8 に備え得る。8 0 2 . 1 1 a / b / g A P / M A C チップ・セット 1 2 8 は図では、処理モジュール 1 4 1、暗号モジュール 3 1 と通信するイーサネット（登録商標）M A C モジュール 1 4 2、及び、当業者が分かるように、適切な 8 0 2 . 1 1 W L A N インタフェース動作及び処理動作を行う W L A N M A C モジュール 1 4 3 を含む。

10

【0049】

通信 C C A 5 1 は更に、上記 3 線直列インタフェースに接続される複雑なプログラム可能論理素子（C P L D）などの論理素子 1 3 1 を含む。一般的に言えば、C P L D 1 3 1 は暗号プロセッサ 3 6 と協調して、各種の通信モジュール 3 2 のステータス及び構成を検知する。特に、ホスト・ネットワーク・プロセッサ 5 4 は、当業者が分かるように、C P L D 1 3 1 をポーリングして、どの種類の通信モジュール 3 2 が暗号モジュール 3 1（例えば、W L A N、有線、光ファイバなど）に接続されているか、更には、その動作ステータスを判定する。C P L D 1 3 1 は更に、これも又当業者が分かるように、ホスト・ネットワーク・プロセッサ 5 4 が、特定のアプリケーションにおける動作にネットワーク通信インタフェース 4 7 を構成することを可能にする。

20

【0050】

更に、図 9 及び図 1 0 を参照すれば、3 線直列インタフェースの 3 線は各々、暗号モジュールと通信モジュール 3 1、3 2 との間でクロック信号、データ信号及びイネーブル信号を伝達する。クロック信号は、（別のサイズも用い得るが）1 6 ビットのシリアル・パラレル・データ・コンバータ 1 3 5、出力レジスタ 1 3 6、1 6 ビットのパラレル・シリアル・データ・コンバータ 1 3 7、及び制御ロジック 1 3 8 に備えられる。特に、データ・ラインを介した暗号プロセッサ 3 6 からの制御データは、出力レジスタ 1 3 6 によって出力されるよう、シリアル・パラレル・データ・コンバータ 1 3 5 に書き込まれる。

30

【0051】

特に、通信モジュール 3 2 は更に、動作モード、バンド、又は別の適切なステータスの、情報を示す、第 2 ハウジング 4 5 によって収容される 1 つ又は複数のステータス表示器 1 4 0（例えば、発光ダイオード（L E D））を更に含み得る。L E D 1 4 0 は複数ビット（例えば、8 ビット）を出力レジスタ 1 3 6 から受信する。レジスタ 1 3 6 からの別のビット群（例えば、7 ビット）は、通信モジュール伝送回路（例えば、無線電力増幅器（P A））を動作可能／不能にし、1 6 ビット出力の残りのビットは、通信モジュール 3 2 用リセット信号を備える。

【0052】

入力バッファ 1 3 9 は、複数ビット（例えば、8 ビット）のステータス（例えば、W L A N 実施形態についての無線ステータス）情報及び、8 0 2 . 1 1 チップ・セット 1 2 8（又は別の実施例における別のネットワーク通信インタフェース）からの複数ビット（例えば、8 ビット）のハードウェア情報を受信して、暗号プロセッサ 3 6 に、パラレル・シリアル・データ・コンバータ 1 3 7 及び 3 線シリアル・バスのデータ・ラインを介して転送する。読み取り及び書き込みデータ・バッファ 1 5 0、1 5 1 は更に、所望の場合、データ・ラインに接続し得る。それに加えて、制御回路 1 3 8 は、更に、イネーブル信号を受信し、出力レジスタ 1 3 6 及び入力バッファ 1 3 9 を動作可能にする。

40

【0053】

読み取り動作又は書き込み動作は、イネーブル信号が、図 1 0 から分かるように、高に

50

なる場合に行われる。暗号プロセッサ 36 から C P L D 1 3 1 まで送出されるコマンド・パケットのフォーマットは以下の通りである。パケットの第 1 の 4 アドレス・ビット (A 1 5 - A 1 2) は C P L D 1 3 1 に、それは、データを暗号プロセッサ 36 から受信する対象か否か、又はそれに対して要求データを供給する対象か否かを命令する。残りのアドレス・ビット (A 1 1 - A 0) は、要求されている適切な構成部分又は動作のアドレスを備える一方、データ・ビット (D 1 5 - D 0) はデータ用にとっておく。そういうものとして、32 ビットのシリアル・ワードが暗号プロセッサ 36 と C P L D 1 3 1 との間で交換される。

【0054】

例示的な読み取り／書き込みアドレス指定手法は、図示するように、書き込み動作についてはビット A 1 5 乃至 A 1 2 に対して 0 1 1 0 を用い、読み取り動作については 1 0 1 1 を用いるものであるが、別のアドレス指定手法も用い得る。暗号モジュール 3 1 及び通信モジュール 3 2 は好ましくは、クロック信号の立下りエッジでクロック・データ出力が行われ、立上がりエッジでクロック・データ入力が行われるが、別のタイミングの手順を種々の実施例で用い得る。

【0055】

次に、暗号プロセッサ 36 から通信モジュール 3 2 までコマンド・パケットを転送する特に効果的な手法を説明することとする。ホスト・ネットワーク・プロセッサ 5 4 は暗号プロセッサ 36 用暗号プロセッサ・コマンド・パケットを生成する。このパケットは各々、暗号回路 5 7 をアドレス指定するイーサネット (登録商標) ・アドレス部分と暗号コマンドをカプセル化する I P パケットとを含む。本発明によれば、ホスト・ネットワーク・プロセッサ 5 4 は、図 1 1 に表すように、通信モジュール 3 2 によって操作される対象のコマンド・パケットを暗号コマンドにおいてカプセル化する。例えば、第 2 E B I U 1 0 7 を用いることによって、通信モジュール・コマンド・パケットは処理 (すなわち、暗号化) なしで通信モジュール 3 2 に転送し得る。これによって、セキュリティを潜在的に危殆化させることなく赤／黒データ境界 (図 6) を超える便利な方法を備える。

【0056】

特に、暗号プロセッサ・コマンド・パケットのフォーマットは以下の通りである。パケットのイーサネット (登録商標) ・アドレス部分は暗号回路 5 7 にアドレス指定される。特に、アドレス部分は、当業者が分かるように、イーサネット (登録商標) ・ヘッダ・アドレス、I P ヘッダ、及び暗号コマンド情報を含み得る。通信モジュール宛ての通信モジュール・コマンド・パケットは I P パケットのデータ部分においてカプセル化される。よって、暗号回路 5 7 は、そのような暗号プロセッサ・コマンド・パケットを受信する場合、パケットを暗号コマンドとして認識することになる。そういうものとして、暗号回路 5 7 はそれ自身のアドレス情報をパケットから取り除いて、残りの部分 (すなわち、カプセル化された通信モジュール・コマンド・パケット) を通信モジュール 3 2 に転送することになる。好ましくは、ホスト・ネットワーク・プロセッサ 5 4 は I P パケットのデータ部分 (、更には、通信モジュール 3 2 用コマンド・パケット) を簡易型ネットワーク管理プロトコル (S N M P) に基づいてフォーマット化するが、別のプロトコルも用い得る。

【0057】

当業者が分かるように、通信モジュール・コマンド・データを M I I ライン又は B W S I を介して送出するのに上記手法を用い得るものであり、この手法はホスト・ネットワーク・プロセッサ 5 4 に情報を逆方向に返信するよう用い得る。通常の従来の暗号機器は、同じハウジング内に暗号回路と通信回路との全てを含むので、通信回路用ステータス／構成コマンドのフォーマット化は通常、問題でない。しかし、当業者が分かるように、上記手法は、暗号モジュール 3 1 と通信モジュール 3 2 が分離されているにもかかわらず、そのようなコマンド／制御動作を行ううえでの好都合でかつセキュアな方法を備える。当然、当業者が分かるように、そのようなコマンド・パケットのフォーマット化及び／又はカプセル化を行う別の手法も用い得る。

【0058】

通信モジュール 32 の上記交換可能性と、コマンドが赤／黒境界を通過することができることは、同じ、所定のインタフェース・プロトコル、すなわち M I I プロトコルを、ユーザ・ネットワーク・インタフェース 35 とネットワーク通信インタフェース 47 との間の信号経路全体に沿って用いることによって促進される。すなわち、暗号プロセッサ 36 は、M I I ベースのプロトコルを用いてユーザ・ネットワーク・インタフェース 35 と通信するのみならず、ネットワーク通信インタフェース 47 と、同じ M I I ベースのプロトコルを用いて通信する。M I I プロトコルは、I E E E 802.3 標準に表されている元の M I I 標準に基づくものであってよく、例えば、リデュースド M I I (R M M I) 又はギガビット M I I (G M I I) などの、その変形であってもよいが、別のプロトコルも用い得る。

10

【0059】

ユーザ・ネットワーク・インタフェース 35 からネットワーク通信インタフェース 47 までの一連の回路を通して M I I のプロトコルを一貫して用いることを維持することによって、暗号モジュール 31 と通信モジュール 32 との両方が、一意の外部 M A C アドレスを用いると同時に、固定内部 M A C アドレスを用いて動作することが可能である。特に、イーサネット（登録商標）M A C モジュール 60 及び 143 は各々、個々の暗号モジュール 31 及び通信モジュール毎に一意の外部 M A C アドレスを用いて動作する一方、イーサネット（登録商標）M A C モジュール 61 及び 142 は、暗号機器 30 毎に同じ固定 M A C アドレスを用いる。

【0060】

20

よって、暗号回路 55 は、イーサネット（登録商標）M A C モジュール 61 に直結されているようにその通信モジュールには見えるので、その通信モジュールに対して実質的に透過的なものとなる。更に、モジュール 61 及び 142 におけるイーサネット（登録商標）M A C によって用いられる「ハード・コード」M A C アドレスは、当業者が分かるように、上記コマンド・パケットを転送できるようにするとともに暗号化データ・パケットの制御伝送ができるようにする。

【0061】

本発明の別の特に効果的な特徴としては、種々の通信モジュール 32 が、単一の暗号モジュール 31 を複数の媒体種類（例えば、無線、有線、光ファイバなど）とともに用いることを可能にするよう使い得るのみならず、通信モジュールも、W L A N の場合のように、特定の媒体について複数モードの動作を備えるよう使い得る。特に、W L A N 通信モジュール 32 は効果的には、例えば、上記コマンド・パケットを用いて暗号モジュール 31 によって無線 L A N モード（すなわち、アクセス・ポイント（A P）・モード、インフラストラクチャ・モード、及びアドホック・モード）間で切り替え可能な、802.11 a / b / g チップ・セット 128 を効果的に使い得る。

30

【0062】

よって、本発明による同じ W L A N 通信モジュール 32 は効果的には、当業者が分かるように、個々の局の動作、有線ネットワークへのブリッジ、ピア・ツー・ピア通信などの所望の機能を W L A N において備えるうえでの何れかのアドバイスとともに使い得る。更に、モード変更はコマンド・パケットを用いて所望のように「その場で」実現し得る。よって、そのような W L A N 通信モジュール 32 によって、暗号機器 30 は、単一ユニットにおいて 802.11 の機能全部を、セキュアなネットワークをアクセスするのに使い得る無線ブリッジを備える一方で備える。暗号モジュール 30 は効果的には、例えば、標準ウェブ・ブラウザを介して 802.11 動作モジュールの選択と構成とを可能にするよう構成し得る。

40

【0063】

あるいは、W L A N 動作モジュール間で切り替えることは、別々の W L A N 通信モジュールにおける各々の W L A N 動作モードについて各種の 802.11 のチップ・セット 128 を用いることによっても実現し得る。すなわち、別々の W L A N 通信モジュール 32 を、A P モード、インフラストラクチャ・モード、又はアドホック・モードが特定の L A

50

N機器40について所望されるかによって用いられることになる。

【0064】

図12乃至14に移れば、暗号モジュール31と通信モジュール32との結合構造を次に、更に説明することとする。特に、暗号モジュール31の第1ハウジング34は第1ボディー180と、そこから外に伸びる第1エクステンション181とを含んでよく、第2ハウジング45は第2ボディー182と、そこから外に伸びる第2エクステンション183とを含んでよい。そういうものとして、第1エクステンション181と第2エクステンション183は、第1コネクタ37と第2コネクタ46とを、取り外し可能にお互いにつながせる場合に、重なり合う関係で位置合せし得る。

【0065】

第1コネクタ37は、図では、第1エクステンション181に隣接する第1ボディー180によって収容され、第2コネクタ46は第2エクステンション186によって収容される。別の配置も本発明によって用い得るが、この配置は、第1エクステンション181の追加の長さ（更には、したがって、追加の表面積）を利用するよう、電源CCA52よりも回路を多く有する暗号CCA50を位置決めすることを可能にするという点で特に効果的である。同様に、通信CCA51は、第2エクステンション183の追加の長さを利用するよう位置決めされる。

【0066】

第1エクステンション181と第2エクステンション183との各々は更に、その対向する表面上に表面特徴を有して、暗号モジュール31と通信モジュール32とをお互いにつながせる関係で、摺動可能に係合させかつ案内させ得る。例として、表面特徴は、その間の（その2つを例示的实施形態において表す）その1つ又は複数の摺動可能な噛み合い（例えば、蟻継ぎ）接合部の範囲を定める、レール185と、相当するチャンネル186とを含み得る。相当するネジ穴188とつながせるキャプティブ・スクリュー187などの1つ又は複数のファスナーも好ましくは、暗号モジュール31と通信モジュール32とをお互いに取り外し可能に締めるよう含まれる。

【0067】

図の例に表すように、第1コネクタ37と第2コネクタ46はマルチピン電気コネクタであるが、当業者が分かる種々の電気コネクタを用い得る。更に、1つ又は複数のシール190を暗号モジュール31と通信モジュール32との間に配置させ得る。したがって、上記電氣的／機械的構造は、所望のEMIシールドと環境シールドとを備えることができる、頑健ではあるが単純な相互接続を備えることが分かるものである。この場合も又、当業者が分かるように、種々の材料（例えば、金属、プラスチックなど）を第1ハウジング37及び第2ハウジング45に用い得る。

【0068】

上記記載に基づいて、本発明の数多くの効果が当業者に明らかとなる。例えば、暗号機器30は標準の商用の802.11ネットワークング機器及び802.3ネットワークング機器と相互運用可能である。特に、暗号機器30はイーサネット（登録商標）・インタフェースを備えている何れかのコンピュータ・プラットフォーム（例えば、リナックス／ユニックス（LINUX／UNIX（登録商標））、ブイエックスワークス（VxWorks）、ウィンドウズ（登録商標）（Windows（登録商標））、マッキントッシュ（Macintosh）など）とともに用い得る。そういうものとして、独立系開発者は効果的には、ユーザ・ネットワーク・インタフェース35と通信する特殊なドライバを記述する必要なくアプリケーションを開発することができる場合がある。同様に、独立系開発者は、明確に定義され、制御された電氣的／機械的インタフェースを介して暗号モジュール31とインタフェースすることになるので、効果的には、種々の通信アプリケーション及び／又は専門通信アプリケーション用通信モジュール32を開発することができる場合がある。更に、結合構造は、種々の通信モジュール32を、単一の暗号モジュールによって容易に相互交換する可能性を備えるのみならず、ハウジングとコネクタとの頑強な設計によって、広い範囲の環境と条件にわたる動作が可能となる。

10

20

30

40

50

【0069】

更に図15に移れば、本発明の通信方法の第1の特徴を次に説明することとする。ブロック250から始まって、暗号モジュール31のユーザ・ネットワーク・インタフェース35は、ブロック251で、LAN機器40に結合される。更に、暗号モジュール31に接続されると、通信モジュール32は更に、種々のネットワーク（すなわち、LAN）48と通信するよう利用可能であり、よって、ブロック254で図の方法を終了する。

【0070】

図16を参照すれば、本発明の第1の通信方法の特徴が（ブロック260で）始まり、ブロック261では、暗号モジュール31がネットワーク機器40に結合され、上記通信モジュール32が暗号モジュールに結合される。該方法は更に、上記のように、ブロック263で、同じ所定のプロトコル（例えば、MII）を用いて、ユーザ・ネットワーク・インタフェース35及びネットワーク通信インタフェース47と通信するよう暗号プロセッサ36を用いる工程、及び、ブロック264で、ネットワーク（すなわち、LAN）48と通信する工程を含み、よって、（ブロック265で）図の方法を終了する。

【0071】

WLAN動作についての2つの別の方法の特徴を次に、図17及び図18を参照しながら説明する。ブロック270から始まって、ブロック271では、暗号モジュール31はネットワーク機器40に結合され、上記のように、通信モジュール32は暗号モジュール31に取り外し可能に結合される。ブロック273で、動作の過程の間に、別のWLAN動作モードが必要であるということが判定された際に、マルチモードのネットワーク無線ネットワーク・インタフェース274がWLAN通信モジュール32に含まれる場合には、ブロック274で、インタフェースは所望の無線LANモードに切り替え得る。その後、又は新たなWLANモードが必要でない場合、ブロック275で、ネットワーク（すなわち、LAN）48との無線通信を行い得るものであり、よって（ブロック276で）図の方法を終了する。種々の802.11モードが、上記のように、各々のWLAN通信モジュール32において実施される場合、ブロック274で図示する工程は、ブロック280'での、所望のWLAN動作モードを暗号モジュール31に備える新たな通信モジュールを取り外し可能に結合させる工程によって置き換え得る。

【0072】

本発明の更に別の通信方法の特徴を次に、図19を参照しながら説明する。方法は（ブロック290から）開始され、ブロック291では、暗号モジュール31がネットワーク機器40に結合され、通信モジュール32は、暗号モジュールに取り外し可能に結合され、更に、ブロック293で、上記のように、通信モジュールを用いてネットワーク（すなわち、LAN）48と通信する。該方法は更に、ブロック294で、論理CPUD131を暗号プロセッサ36と協調して用いて通信モジュール32のステータスを判定する工程も含み、よってブロック295で、図の方法を終了する。当然、ネットワーク（すなわち、LAN）48との通信を開始する前にステータスが取得される（及び／又は構成が行われる）場合があり、かつ繰り返されるステータス更新が通信処理によって取得され続ける場合があることが分かるものである。

【0073】

本発明の別の通信方法の特徴を次に、図20を参照しながら説明することとする。該方法は（ブロック300で）開始され、ブロック301で、上記のように、暗号モジュール31がネットワーク機器40に結合され、通信モジュール32は暗号モジュールに取り外し可能に結合される。該方法は更に、上記のように、ブロック302で、ホスト・ネットワーク・プロセッサに、その各々がアドレス部分とデータ部分とを含む、暗号回路についてのその暗号パケットを生成させ、暗号パケットのデータ部分においてネットワーク通信インタフェース47についてのコマンド・パケットをカプセル化させる工程を含み得る。よって、暗号回路57は、コマンド・パケットが暗号パケットにおいてカプセル化されているということを判定した場合、この場合も又上記のように、ブロック304で、その上で暗号処理を行うことなく、暗号回路はそのコマンド・パケットを通信モジュール32に

転送する。さもなければ、暗号処理は、ブロック 305 で、暗号パケットにおけるデータに対して行われ、よって（ブロック 306 で）図の方法が終了する。

【図面の簡単な説明】

【0074】

【図1】本発明による暗号機器の斜視図である。

【図2】その種々のモジュールを示す、図1のその暗号機器の組み立て分解図である。

【図3】図1の暗号機器の平面図である。

【図4】図1の暗号機器の種々の構成部分を示す概略構成図である。

【図5】図1の暗号機器の種々の構成部分を示す別の概略構成図である。

【図6】図1の暗号機器の種々の構成部分を示す更に別の概略構成図である。

10

【図7】図1の暗号機器の種々の構成部分を示す更に別の概略構成図である。

【図8】図1の暗号機器の種々の構成部分を示す更に別の概略構成図である。

【図9】図1の暗号機器の種々の構成部分を示す更に別の概略構成図である。

【図10】図1の暗号機器の通信モジュールについてのステータス動作と構成動作とを示すタイミング図である。

【図11】本発明によって生成される暗号パケットの構成図である。

【図12】図1の暗号機器の通信モジュールのコネクタ構成を示す斜視図である。

【図13】図1の暗号機器の暗号モジュールのコネクタ構成を示す斜視図である。

【図14】図1の暗号機器の下面を表し、更に、その種々のモジュールの結合を示す別の組み立て分解斜視図である。

20

【図15】本発明による種々の通信方法の特徴を示す流れ図である。

【図16】本発明による種々の通信方法の特徴を示す別の流れ図である。

【図17】本発明による種々の通信方法の特徴を示す更に別の流れ図である。

【図18】本発明による種々の通信方法の特徴を示す更に別の流れ図である。

【図19】本発明による種々の通信方法の特徴を示す更に別の流れ図である。

【図20】本発明による種々の通信方法の特徴を示す更に別の流れ図である。

【符号の説明】

【0075】

0-3 クロック

15-16 クロック

30

29-31 クロック

29 通信システム

30 暗号機器

31 暗号モジュール

32 通信モジュール

33 アンテナ

34 第1ハウジング

35 ユーザ・ネットワーク・インタフェース

35 イーサネット（登録商標）PHY

35 802.3 イーサネット（登録商標）PHY

40

35 デュアル・イーサネット（登録商標）PHY

36 暗号プロセッサ

37 第1コネクタ

38 コネクタ

39 キャップ

40 ネットワーク機器

40 WLAN機器

41 電源スイッチ

42 LEDステータス表示器

45 第2ハウジング

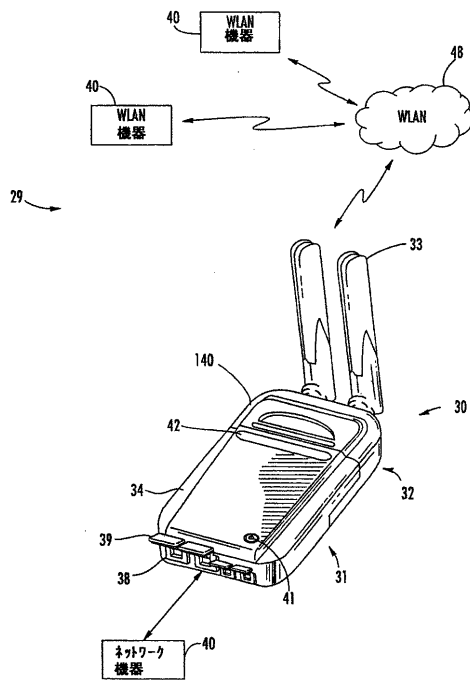
50

4 6	第 2 コネクタ	
4 7	ネットワーク通信インタフェース	
4 8	ネットワーク	
5 0	暗号化回路カード (C C A)、赤／黒境界	
5 1	通信 C C A	
5 2	電源 C C A	
5 3	電源／フィルタ化回路	
5 4	暗号モジュール	
5 4	ホスト・ネットワーク・プロセッサ	
5 5	暗号回路	10
5 6	データ・バッファ、赤 F P G A	
5 7	暗号回路 (シエラ I I)	
5 8	データ・バッファ、黒 F P G A	
6 0	第 1 8 0 2 . 3 媒体アクセス・コントローラ (M A C)	
6 0	イーサネット (登録商標) M A C モジュール	
6 1	第 2 8 0 2 . 3 媒体アクセス・コントローラ (M A C)	
6 1	イーサネット (登録商標) M A C モジュール	
6 2	プロセッサ	
6 3	S N M P エージェント	
6 4	ファイヤウォール／ルーティング・モジュール	20
6 5	O T A R / O T N R モジュール	
6 6	O T A Z / O T N Z モジュール	
6 7	モード・コントローラ	
6 8	I P S e c / H A I P E モジュール	
6 9	鍵管理モジュール	
7 0	機器発見モジュール	
7 1	メモリ素子	
7 2	メモリ素子	
7 3	H T T P サーバ	
7 5	外部電源インタフェース回路	30
7 6	暗号／通信．電源アイソレーション及びフィルタリング回路	
7 7	暗号モジュール電源回路	
7 8	通信モジュール電源回路	
7 9	データ・フィルタ／E S D 保護回路	
8 0	タンパ回路	
8 1	暗号電源インタフェース回路	
8 2	専用暗号化アルゴリズム／秘密鍵バッテリー	
8 5	R J 4 5 コネクタ	
8 6	L C 光ファイバ・コネクタ	
9 0	ホスト・インタフェース／F I F O 制御モジュール	40
9 1	トラフィック F I F O	
9 2	コマンド F I F O	
9 3	バッファ	
9 4	第 1 の高速並列インタフェース	
9 5	制御レジスタ、赤 F P G A	
9 6	マルチプレクサ	
9 7	第 2 の高速並列インタフェース	
9 8	巡回冗長度検査モジュール	
1 0 0	出力 F I F O	
1 0 1	ワード・カウンタ	50

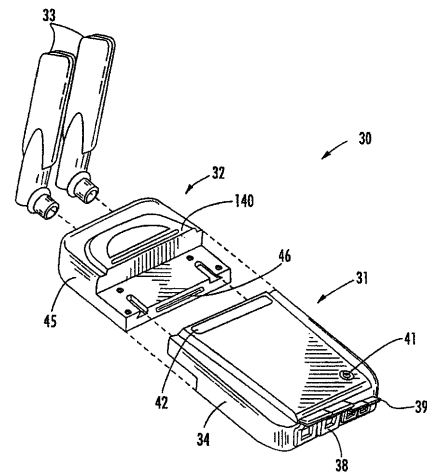
1 0 2	暗号 A S I C	
1 0 2	暗号処理モジュール	
1 0 3	暗号エンジン・モジュール	
1 0 4	バス・コントローラ	
1 0 5	フィル回路	
1 0 6	第 1 の外部バス・インタフェース装置 (E B I U)	
1 0 7	第 2 E B I U	
1 1 0	制御レジスタ	
1 1 1	マルチプレクサ	
1 1 2	過大／過小電圧検知、温度検知、パニック・ゼロ化回路	10
1 1 3	バッファ	
1 1 4	入力インタフェース	
1 1 5	巡回冗長度検査モジュール	
1 1 6	トラフィック F I F O	
1 1 7	出力 F I F O	
1 1 8	M A C インタフェース／F I F O 制御モジュール	
1 2 0	バッファ	
1 2 6	電源 I F	
1 2 7	フィルタ／E S D 保護回路	
1 2 8	無線モジュール	20
1 2 8	8 0 2 . 1 1 a / b / g A P / M A C チップ・セット	
1 2 9	8 0 2 . 1 1 a / b / g 無線部	
1 2 9	無線 C C A	
1 3 0	メモリ	
1 3 1	論理素子 (C P L D)	
1 3 5	1 6 ビット・シリアル・パラレル・データ・コンバータ	
1 3 6	出力レジスタ	
1 3 7	1 6 ビット・パラレル・シリアル・データ・コンバータ	
1 3 8	制御ロジック	
1 3 9	入力バッファ	30
1 4 0	ステータス表示器 (L E D)	
1 4 1	処理モジュール	
1 4 2	イーサネット (登録商標) M A C モジュール	
1 4 3	イーサネット (登録商標) M A C モジュール	
1 4 3	W L A N M A C モジュール	
1 5 0	読み取り及び書き込みデータ・バッファ	
1 5 1	読み取り及び書き込みデータ・バッファ	
1 8 0	第 1 ボディー	
1 8 1	第 1 エクステンション	
1 8 2	第 2 ボディー	40
1 8 3	第 2 エクステンション	
1 8 5	レール	
1 8 6	チャンネル	
1 8 7	キャプティブ・スクリュー	
1 8 8	ネジ穴	
1 9 0	シール	
2 5 0	ブロック	
2 5 1	ブロック	
2 5 3	ブロック	
2 5 4	ブロック	50

2 6 0	ブロック	
2 6 1	ブロック	
2 6 3	ブロック	
2 6 4	ブロック	
2 6 5	ブロック	
2 7 0	ブロック	
2 7 1	ブロック	
2 7 3	ブロック	
2 7 4	ブロック	
2 7 5	ブロック	10
2 7 6	ブロック	
2 7 0 '	ブロック	
2 7 1 '	ブロック	
2 7 3 '	ブロック	
2 8 0 '	ブロック	
2 7 5 '	ブロック	
2 7 6 '	ブロック	
2 9 0	ブロック	
2 9 1	ブロック	
2 9 3	ブロック	20
2 9 4	ブロック	
2 9 5	ブロック	
3 0 0	ブロック	
3 0 1	ブロック	
3 0 2	ブロック	
3 0 3	ブロック	
3 0 4	ブロック	
3 0 5	ブロック	
3 0 6	ブロック	
A 0 - A 1 5	アドレス・ビット	30
D 0 - D 1 5	データ・ビット	

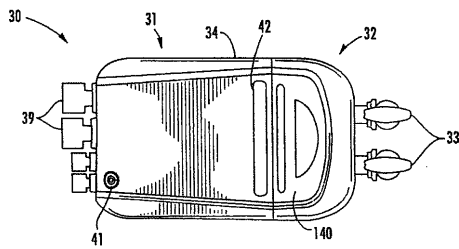
【図 1】



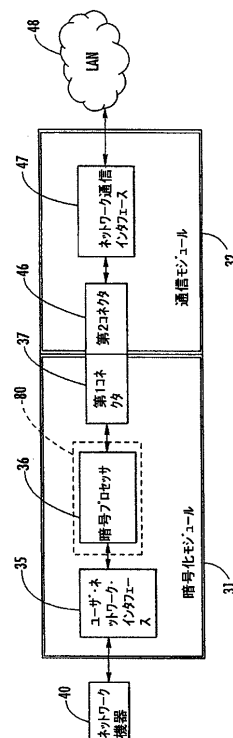
【図 2】



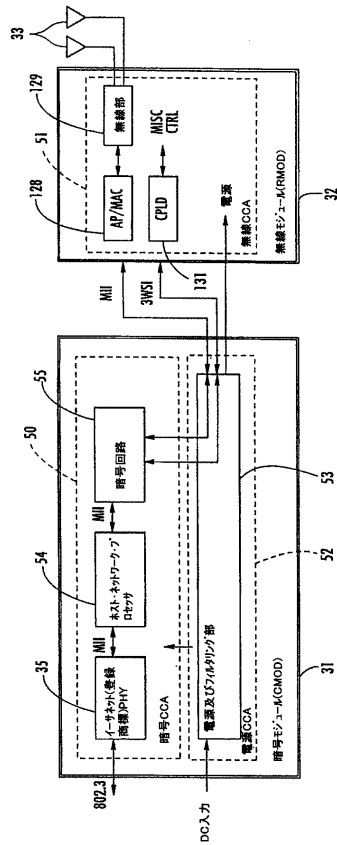
【図 3】



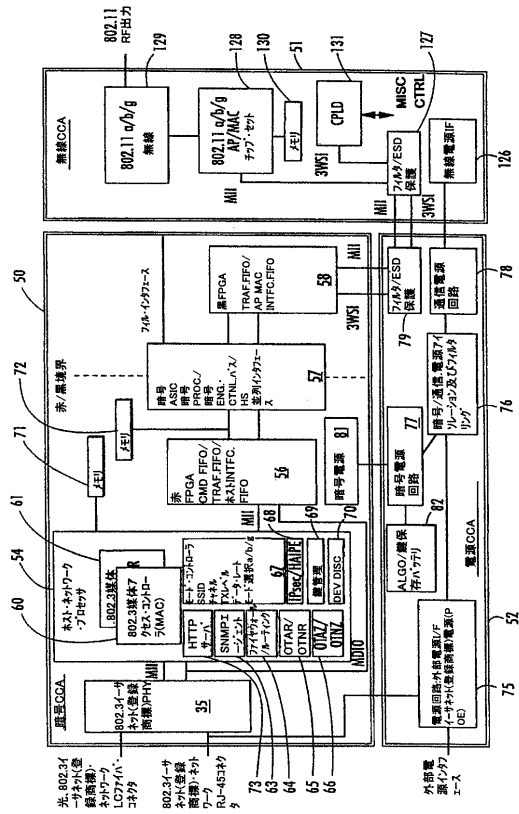
【図 4】



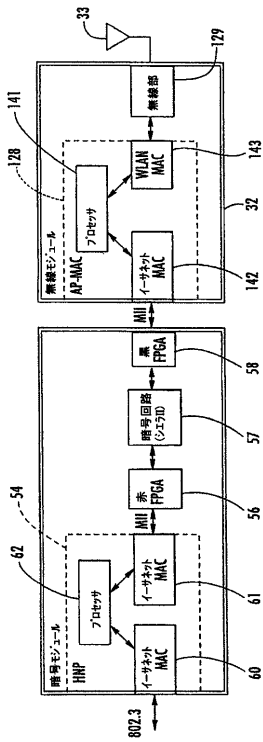
【図 5】



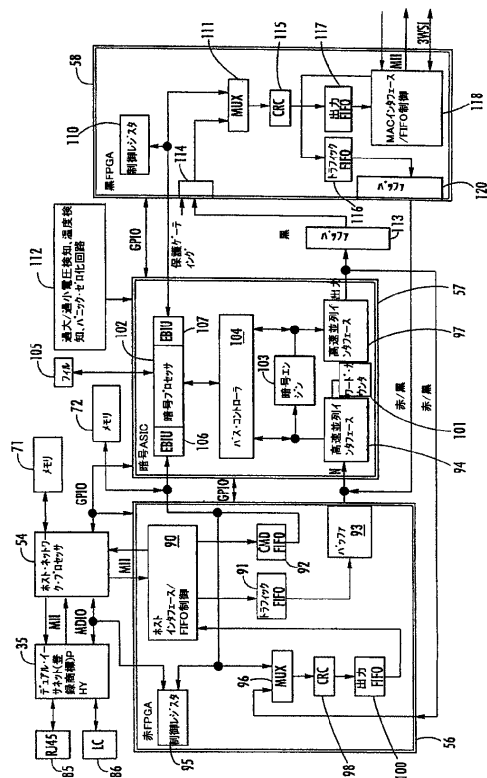
【図 6】



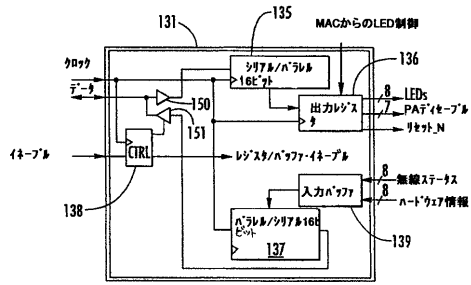
【図 7】



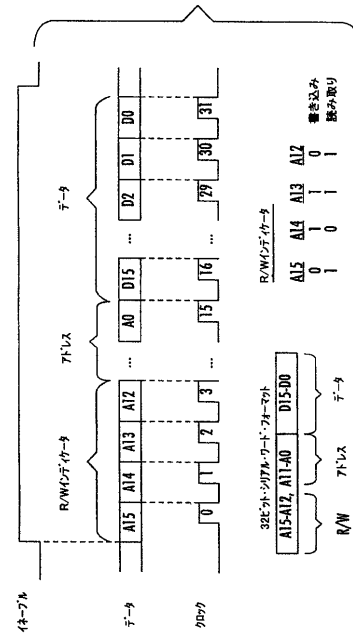
【図 8】



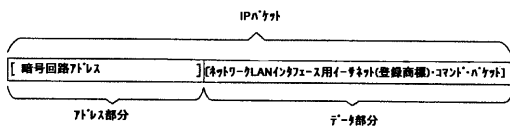
【 図 9 】



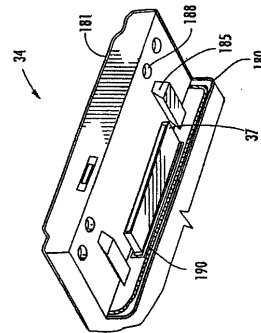
【 図 1 0 】



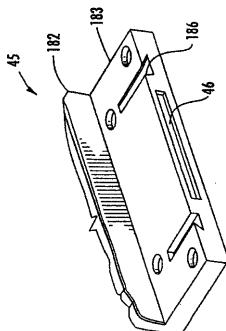
【 図 1 1 】



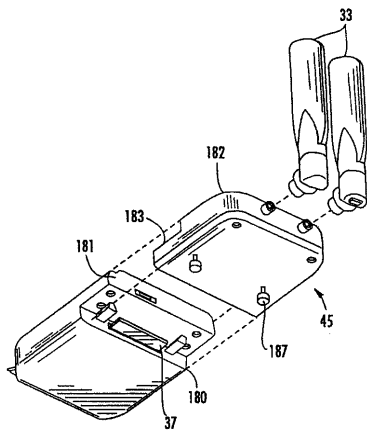
【 図 1 3 】



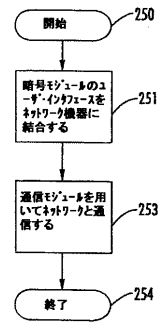
【图 1 2】



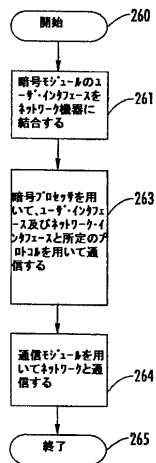
【図 14】



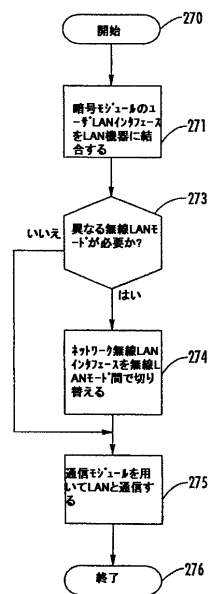
【図 15】



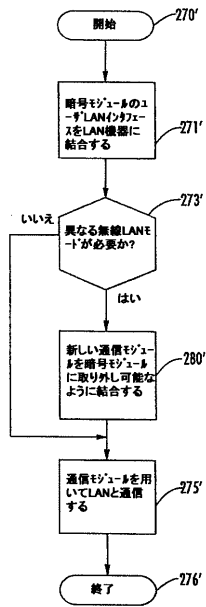
【図 16】



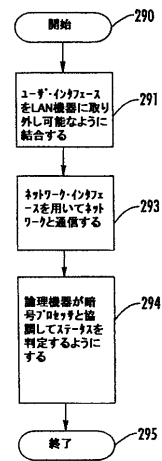
【図 17】



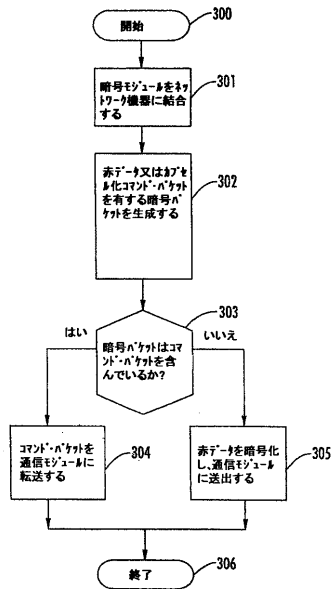
【図 18】



【図 19】



【図 20】



フロントページの続き

(72)発明者 ラッセル ウェイン デルモ
アメリカ合衆国 フロリダ 32907 パーム・ベイ ランプライター・ドライブ・ノースウェ
スト 1209

(72)発明者 エリック エドモンド ペトカス
アメリカ合衆国 フロリダ 32907 パーム・ベイ ネヴァダ・ドライブ・ノースイースト
897

(72)発明者 ブルース ウェイン ヤンシー
アメリカ合衆国 フロリダ 32905 パーム・ベイ シトラス・アヴェニュー・ノースイース
ト 1083

Fターム(参考) 5J104 AA01 NA39 NA41 NA42 NA43 PA07

【外国語明細書】

1. Title of Invention

5 MODULAR CRYPTOGRAPHIC DEVICE PROVIDING MULTI-MODE WIRELESS LAN
OPERATION FEATURES AND RELATED METHODS

2. Detailed Description of Invention

10 Background of the Invention

Security is an extremely important consideration in network communications. With the ever-increasing utilization of the Internet, most networks now have Internet gateways which open them up to external attacks by would-be hackers. 15 Further, the popularity of wireless networks has also increased dramatically as technology has enabled faster and more reliable wireless communications. Yet, wireless communications are inherently less secure than wired communications, since wireless communication signals are 20 typically much easier to intercept than signals on cables which are often difficult to access.

As a result, cryptography is often used to encrypt private or secret communications to reduce the likelihood that they will be deciphered and used by malicious individuals or 25 organizations. By way of example, wireless local area networks (WLANs) and WLAN devices are widely used and provide a convenient and cost-effective approach for implementing network communications where it may be difficult or otherwise impractical to run cables. One of the more prominent standards 30 which has been developed for regulating communications within WLANs is promulgated by the Institute of Electrical and Electronic Engineers' (IEEE) 802 LAN/MAN Standards Committee, which is the 802.11 standard. In addition to providing wireless communications protocols, the 802.11 standard also 35 defines a wireless equivalent privacy (WEP) cryptographic

algorithm which is used to protect wireless signals from eavesdropping.

WEP relies on a secret key that is shared between wireless stations and an access point. The secret key is used
5 to encrypt data packets prior to transmission, and an integrity check is used to ensure that packages are not modified during the transmission. Nonetheless, it has recently been discovered that the WEP algorithm is not as immune to external attacks as once believed. For example, in an article
10 entitled "Intercepting mobile communications: The Insecurity of 802.11" by Borisov et al., MOBICOM, Rome, Italy, July 2001, the authors set forth a number of vulnerabilities in WEP. In particular, it was noted that a significant breach of security occurs when two messages are encrypted using a same
15 initialization vector (IV) and secret key, as this can reveal information about both messages.

Moreover, WEP message ciphertext is generated using an exclusive OR operation. By exclusive ORing ciphertext from two messages generated using the same IV, the key streams
20 cancel out and it is then possible to recover the plain text. As such, this key stream re-use is susceptible to a decryption dictionary attack in which a number of messages are stored and compared to find multiple messages generated with a same IV.

As a result, more robust network security is often
25 required for many network applications. One example of a network security device to be connected between a protected client and a network is disclosed in U.S. Patent No. 6,240,513 to Friedman et al. The network security device negotiates a session key with any other protected client. Then, all
30 communications between the two clients are encrypted. The device is self-configuring and locks itself to the IP address of its client. Thus, the client cannot change its IP address once set and therefore cannot emulate the IP address of another client. When a packet is transmitted from the
35 protected host, the security device translates the MAC address

of the client to its own MAC address before transmitting the packet into the network. Packets addressed to the host contain the MAC address of the security device. The security device translates its MAC address to the client's MAC address before
5 transmitting the packet to the client.

Even more robust cryptographic devices may be required to secure sensitive or classified communications. More particularly, in the U.S. the communications of government entities that include sensitive (but unclassified)
10 information must comply with the Federal Information Processing Standards Publication (FIPS) publication 140-2 entitled "Security Requirements For Cryptographic Modules." Classified communications, which are typically referred to as Type 1 communications, must comply with even stricter
15 standards.

One example of an encryptor which is certified for Type 1 communications is the TACLANE Encryptor KG-175 from General Dynamics Corp. The "classic" version of the TACLANE encryptor has Internet Protocol (IP) and Asynchronous Transfer
20 Mode (ATM) interfaces, and an E100 version has a fast Ethernet interface. The classic version may also be upgraded to fast Internet by replacing the IP/ATM network interface cards therein with two new E100 interface cards.

Despite the security benefits provided by such
25 devices, many of these encryptors are fairly bulky and may consume significant amounts of power. One particularly advantageous cryptographic device which provides both space and power saving features is the Sierra module from Harris Corp., Assignee of the present application. The Sierra module
30 is an embeddable encryption device that combines the advantages of high-grade security (e.g., Type 1) with the cost efficiency of a reprogrammable, commercially produced, FIPS 140-2 level 3 or 4 encryption module. The Sierra module can take on multiple encryption personalities depending on the
35 particular application, providing encryption/decryption

functionality, digital voice processing (vocoding) and cryptographic key management support functions. The Sierra module also provides the user with the capability to remove the Type 1 functionality, allowing the device to be downgraded
5 to an unclassified device. Also, because of its relatively small size, low power and high data rates, this device is well-suited for battery sensitive applications.

By way of example, the Sierra module has been implemented in a Secure WLAN (SWLAN) personal computer (PC) card called SecNet 11, which is also produced by Harris Corp.
10 The SecNet 11 card allows rapid communication of multimedia information (data, voice, and video) in a secure environment. The SecNet 11 card may be used as a wireless network interface card for WLAN "stations," for wireless bridges, and for access
15 point (APs), for example. The SecNet 11 device is more fully described in U.S. published application nos. 2002/0094087 and 2002/0095594, both of which are hereby incorporated herein in their entireties by reference.

Accordingly, the SecNet 11 card provides numerous
20 advantages in terms of size, power requirements, and flexibility in WLAN environments. However, it may be desirable to provide such benefits in other network environments as well.

Summary of the Invention

25 In view of the foregoing background, it is therefore an object of the present invention to provide a cryptographic device that provides high level security and is relatively easily adaptable to numerous network environments and related methods.

30 This and other objects, features, and advantages in accordance with the present invention are provided by a cryptographic device which may include a cryptographic module and a communications module removably coupled thereto. More particularly, the cryptographic module may include a first
35 housing, a user Local Area Network (LAN) interface carried by

the first housing, and a cryptographic processor carried by the first housing and coupled to the user LAN interface. Furthermore, the communications module may include a second housing, and a network wireless LAN interface carried by the second housing. The network wireless LAN interface may be coupled to the cryptographic processor, and it may be switchable between wireless LAN modes.

More particularly, the network wireless LAN interface circuit may be switchable to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode. Accordingly, the cryptographic device may be used interchangeably with any of the various types of devices in a WLAN, thus avoiding the need for multiple types of WLAN encryption devices.

In addition, the cryptographic module may further include a first connector carried by the first housing and coupled to the cryptographic processor, and the communications module may further include a second connector carried by the second housing and connected to the network wireless LAN interface. Moreover, the second connector may be removably mateable with the first connector of the cryptographic module. Thus, in accordance with another aspect of the invention, the communications module may be a predetermined one from among a plurality of interchangeable communications modules, where the network wireless LAN interfaces of the interchangeable communications modules each operates in a different wireless LAN mode (i.e., AP, infrastructure, or ad-hoc). Accordingly, the same cryptographic module may advantageously be used with any WLAN device by simply coupling the appropriate communications module for that particular device to the cryptographic module.

The user LAN interface may be an Ethernet interface, for example. Furthermore, the cryptographic device may also include a power circuit carried by the first housing and powering the cryptographic processor, the user LAN interface,

and the network LAN interface. The cryptographic processor may implement an encryption algorithm to provide a predetermined security level, up to and including Type 1 security, for example.

5 More particularly, the cryptographic processor may include a host network processor coupled to the user LAN interface, and a cryptographic circuit coupled to the host network processor. Further, the cryptographic processor may also include an unencrypted data buffer circuit coupled
10 between the user LAN interface and the cryptography circuit, and an encrypted data buffer circuit coupled between the cryptography circuit and the network LAN interface.

 The cryptographic module may also advantageously include a tamper circuit for disabling the cryptographic
15 processor based upon tampering with the first housing. By way of example, the tamper circuit may include one or more conductors substantially surrounding the cryptographic processor, and the cryptographic processor may be disabled based upon a break in the conductor(s).

20 A communications method aspect of the invention may include coupling a cryptographic module, such as the one described briefly above, to a LAN device, a communications module being removably coupled to the cryptographic module. As noted above, the communications module may include a second
25 housing and a network wireless LAN interface carried by the second housing and coupled to the cryptographic processor. Furthermore, the method may additionally include switching the network wireless LAN interface between wireless LAN modes. The communications module may then be used for communicating
30 with a LAN.

 Another method aspect of the invention includes providing a cryptographic module, such as the one described briefly above, having one of a plurality of cryptographic modules removably coupled thereto, and coupling the
35 cryptographic module to a LAN device. More particularly, the

communications module may include a second housing and a network wireless LAN interface carried by the second housing, and the network wireless LAN interfaces of the plurality of interchangeable communications modules may each operate in a different wireless LAN mode. The communications module may then be used for communicating with a wireless LAN.

A communications system in accordance with the invention may include a plurality of LAN devices coupled together to define a wireless LAN, and a cryptographic device, such as the one described briefly above, coupled to at least one of the LAN devices.

Detailed Description of the Preferred Embodiments

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime notation is used to indicate similar elements or steps in different embodiments.

Referring initially to FIGS. 1 through 9, a communication system **29** in accordance with the present invention illustratively includes a cryptographic device **30**, a plurality of network devices **40**, and a network such as a wireless Local Area Network (WLAN) **48**. The cryptographic device **30** illustratively includes a cryptographic module **31** coupled to one of the devices **40** and a communications module **32**. As shown in FIG. 2, the communications module **32** is removably coupled to the cryptographic module **31**, as will be discussed further below. Generally speaking, in accordance with the present invention, a plurality of interchangeable

communications modules **32** may be connected to the cryptographic module **31** for communicating over different communications media. While in the illustrated embodiment the communications module **32** is a WLAN module which includes dual tri-band antennas **33**, it will be appreciated based upon the following discussion that the cryptographic device **30** can be used with numerous types of wired and wireless networks.

By including the appropriate chip sets/ interface circuitry in different communications modules **32**, each of these modules may interface with a different network medium (e.g., WLAN, wireline medium, fiber optic medium, etc.), yet all interface with the same cryptographic module **31**. That is, the same cryptographic module **31** may be used for numerous network applications simply by coupling the appropriate communications module **32** thereto for the desired application. Examples of various types of communications modules **32** that may be used include WLAN modules, plain old telephone service (POTS) modules, tactical radio modules, E1/T1 modules, in-line network encryptor (INE) modules, a VersaModule Eurocard (VME) bus module, etc.

The modular design and ease of interchangeability not only provides a convenient way to quickly configure the cryptographic module **31** for different applications, but it may also be particularly useful for high level security applications such as a Type 1, FIPS 140-2 level 4, etc. This is because the evaluation process to have a cryptographic device certified for use with sensitive or classified communications at these levels can be quite lengthy and extensive, and consequently costly. Thus, to manufacture respective cryptographic devices for different network applications can be cost prohibitive since each one will have to individually undergo the rigorous and costly certification.

Yet, since in accordance with the present invention the cryptographic module **31** preferably includes all of the sensitive cryptographic circuitry and associated cryptographic

algorithms/keys, the various communications modules **32** merely provide interfaces for different types of networks. That is, they do not process or transmit "red" (i.e., unencrypted) confidential/classified data, and thus they will likely not require the same certification scrutiny as the cryptographic module **31**. Accordingly, the communications modules **32** may provide significant cost savings over having to purchase an entirely new cryptographic device with a different network interface for each desired application.

In particular, the cryptographic module **31** illustratively includes a first housing **34**, a user network interface **35** carried by the first housing, a cryptographic processor **36** carried by the first housing and coupled to the user network interface, and a first inter-module connector **37** carried by the first housing and coupled to the cryptographic processor. The user network interface **35** may be an Ethernet physical layer (PHY) interface compatible with the IEEE 802.3 standard, for example, as will be appreciated by those skilled in the art. Various connectors **38** are also carried by the first housing **34** for coupling the cryptographic module **31** to different network devices **40** (e.g., personal computers (PCs), servers, portable communications devices, etc.).

By way of example, the connectors **38** may be wireline connectors, such as an RJ45 connector **85** (FIG. 8), or fiber optic connectors, such as an LC fiber optic connector **86**. Caps **39** may also be included for protecting the connectors **34**. A power switch **41** and LED status indicators **42** (i.e., power, link state, fill, and alarm) are also carried by the first housing **34**.

It should be noted that the term "user" is used with relation to the user network interface **35** simply to indicate that this interface is for the user network device side and not the communications network side of the cryptographic device **30**. That is, "user" does not mean that the interface **35** is only for individual user devices such as PCs. Instead, the

user network interface may be connected to a variety of different LAN devices (e.g., servers, bridges, access points, etc.), as noted above.

The communications module **32** illustratively includes
5 a second housing **45**, a second inter-module connector **46**
carried by the second housing and removably mateable with the
first connector **37** of the cryptographic module **31**, and a
network communications interface **47** carried by the second
housing **45** and coupled to the second connector. In the present
10 example, the network communications interface **47** includes a
WLAN communication circuit (e.g., an 802.11 chip set) for
cooperating with the antennas **33** to wirelessly communicate
with a network (e.g., LAN) **48**, as will be discussed further
below. Yet, as noted above, the network communications
15 interface **47** may be a wireline LAN communication circuit, a
fiber optic LAN communication circuit, etc., for example.

The various circuit components of the cryptographic
module **31** may be implemented in a cryptographic circuit card
(CCA) **50**, for example, as will be appreciated by those skilled
20 in the art. The circuitry of the communications module **32** may
similarly be implemented in a CCA **51**. The cryptographic module
31 may also include a power CCA **52** carried by the first
housing **34** and including power supply/filtering circuitry **53**
for powering the cryptographic processor **36**, the user network
25 interface **35**, and the communications module **32**.

The cryptographic processor **36** may include a host
network processor **54** connected to the user network interface
35, and cryptography circuitry **55** connected to the host
network processor. More particularly, the cryptography
30 circuitry **55** illustratively includes an unencrypted (i.e.,
"red") data buffer **56** connected to the host network processor
54, a cryptography circuit **57** connected to the unencrypted
data buffer, and an encrypted (i.e., "black") data buffer **58**
connected between the cryptography circuit and the first
35 connector **37**.

By way of example, the unencrypted and encrypted data buffers may be first-in, first-out (FIFO) buffers implemented using field-programmable gate arrays (FPGAs), and the cryptography circuit 57 may be implemented in an application specific integrated circuit (ASIC). One cryptography ASIC that is particularly well suited for use with the present invention is the above-noted Sierra (and Sierra II) device from Harris Corp. Of course, it will be appreciated by those skilled in the art that other suitable circuitry may be used as well.

The host network processor 54 illustratively includes a plurality of modules which may be implemented using hardware and/or software, as will be appreciated by those skilled in the art. Generally speaking, the host network processor 54 includes a first 802.3 medium access controller (MAC) controller 60 for interfacing the user network interface 35, a second 802.3 MAC controller 61 for interfacing the cryptographic processor 36 and network communications interface 47, as will be described further below, and a processor 62 coupled between the MAC controllers. The host network processor 54 and user network interface 35 may communicate via dedicated lines for Media Independent Interface (MII) communications, as will be discussed further below, and a management data input/output bus (FIGS. 6 and 8), for example.

More specifically, the processor 62 may include a hypertext transfer protocol (HTTP) server module 73, a simple network management protocol agent 63, a firewall/routing module 64, an over the air re-keying/over the network re-keying (OTAR/OTNR) module 65, and an over the air zeroization/over the network zeroization (OTAZ/OTNZ) module 66. Moreover, the processor 54 also illustratively includes a mode controller 67 for providing proper configuration based upon the particular mode or media with which the cryptographic module 31 is to operate (e.g., WLAN access point (AP) mode,

ad-hoc mode, infrastructure mode, etc.). The mode controller 67 may also perform other configuration/monitoring functions, such as for service set identifiers (SSIDs), channel, transmission level, data rate, 802.11 band selection (i.e., a, b, g) depending upon the particular application the cryptographic module 31 is to be used for, as will be appreciated by those skilled in the art. Additional modules such as an Internet protocol (IP) security protocol (IPSec)/high-assurance IP encryption (HAIPE) module 68, a key management module 69, and/or a device discovery module 70 may also be included depending upon the given implementation, as will also be appreciated by those skilled in the art. The cryptographic module also preferably includes respective memory devices 71, 72 for the host network processor 54 and cryptography circuit 57.

The power circuitry 53 illustratively includes external power interface (I/F) circuitry 75, which may be connected to a DC source (e.g., battery), a wall wart AC adapter, an Ethernet power source, etc. Of course, it will be appreciated that other power sources may be used in different implementations. The power circuitry 53 further illustratively includes cryptographic/communications module power isolation/filtering circuitry 76 coupled to the external power I/F circuitry 75. A cryptographic module power circuit 77 and a communications module power circuit 78 are coupled to the power isolation/filtering circuitry 76 for respectively supplying the cryptographic and communications modules 31, 32. Further, a data filter/electrostatic discharge (ESD) protection circuit 79 is included for filtering signals communicated between the cryptographic module 31 and communications module 32, as will be appreciated by those skilled in the art.

To receive high level certification (e.g., level 4 FIPS 140-2, Type 1) for classified and/or secret communications, cryptographic devices typically have to

include some degree of physical tamper protection to prevent malicious individuals or organizations from physically compromising the device and discovering the secret key or algorithm being used. In accordance with the present invention, the cryptographic module 31 also illustratively includes a tamper circuit 80 for disabling the cryptography circuit 57 based upon tampering with the first housing 34. By way of example, the tamper circuit 80 preferably includes one or more conductors substantially surrounding the cryptography circuit 57 so that the cryptographic processor is disabled based upon a break in any one of the conductors.

More particularly, the conductors may be relatively thin printed circuit traces printed on the inside of the first housing 34 and attached to the cryptographic processor 36. Since the conductors substantially surround the cryptographic processor 36 (or some portion thereof), if someone attempts to drill through the first housing 34 to access the cryptographic processor then one or more of the printed traces will be broken. The same holds true if someone opens the first housing, as the traces will be pulled away from the cryptographic processor 36 also causing breaks therein.

In either event, the open circuit condition resulting from the broken conductor(s) causes power to a cryptographic power interface circuit 81 to be disrupted to be discontinued. That is, power from a dedicated encryption algorithm/secret key battery 82 is prohibited from flowing to the cryptographic power interface circuit 81 via the cryptographic module power circuitry 77. As a result, the algorithm and secret key, which are preferably stored in a volatile memory, are permanently and instantly erased so that they cannot be discovered by malicious individuals or organizations. The tamper circuit 80 may thus provide tamper protection from all angles, if desired.

As noted above, the cryptography circuit 57 implements a desired encryption algorithm to provide a

predetermined security level (e.g., Type 1, FIPS 140-2 levels 1 through 4, etc.). By way of example, Advanced Encryption Standard (AES), Baton, or Medley encryption algorithms may be used to provide such high level security. Of course, other
5 high level security algorithms known to those skilled in the art may be used as well. Additionally, other cryptographic algorithms which are considered to be less secure than those noted above may also be used in accordance with the present invention when the cryptographic device 30 is to be used in
10 less sensitive environments (e.g., general commercial or corporate applications).

The cryptography circuitry 55 also illustratively includes a plurality of modules which may be implemented using hardware and/or software. Referring particularly to FIG. 8,
15 the unencrypted data buffer (i.e., red FPGA) 56 illustratively includes a host interface/FIFO control module 90 for communicating with the host network processor 54 via the MII protocol, and traffic and command (CMD) FIFOs 91, 92 receiving outputs of the host interface/FIFO control module. It should
20 be noted that various data paths in FIG. 8 are labeled as "red" and/or "black" to indicate whether they convey unencrypted or encrypted data, respectively, or both, to aid in understanding of the present invention.

The output of the traffic FIFO 91 is connected to a
25 buffer 93, which is connected to a first high speed parallel interface 94 of the cryptographic circuit 57. The output of the command FIFO 92 is connected to a first external bus interface unit (EBIU) 106 of the cryptographic circuit 57. This EBIU 106 is also connected to control registers 95 and a
30 multiplexer 96. Another input of the multiplexer 96 is connected to the output of a second high speed parallel interface 97 of the cryptographic circuit 57. The output of the multiplexer 96 is passed to a cyclic redundancy check module 98, the output of which is passed through an output
35 FIFO 100 back to the host interface/FIFO control module 90.

The first high speed parallel interface **94** of the cryptography circuit **57** has a respective word counter **101** associated therewith. A cryptographic processing module **102** of the cryptography circuit **57** interfaces the first and second
5 high speed parallel interfaces **94**, **97** and one or more cryptographic engine modules **103** via a bus controller **104**. The cryptographic processing module **102** also communicates with a fill circuit **105** for the loading of cryptographic keys. The EBIU **106** also interfaces the cryptographic processing module
10 **102** with the memory **72**. A second EBIU **107** interfaces the cryptographic processing module **102** with control registers **110** and a multiplexer **111** of the encrypted data buffer (i.e., black FPGA) **58**. The signal path between the second EBIU **107** and the multiplexer **111** provides a command signal path.

15 Various components of the host network processor **54**, red FPGA **56**, cryptographic circuit **57**, and black FPGA **58** also communicate via one or more general purpose input/output (GPIO) busses as shown, as will be appreciated by those skilled in the art. Additional circuitry **112** may also be
20 coupled to the cryptography circuit **57** in certain embodiments for over/undervoltage detection, temperature detection, and/or panic zeroizing as required for a particular implementation, as will also be appreciated by those skilled in the art.

An output of the second high speed parallel
25 interface **97** is passed via a buffer **113** to an input interface **114** which includes protection gating to prohibit red data from entering the black FPGA **58**. The output of the input interface **114** is connected to a second input of the multiplexer **111** defining a traffic (i.e., data) path thereto. The output of
30 the multiplexer **111** is provided to a cyclic redundancy check module **115**, the output of which is provided to an output FIFO **117**. An output of the MAC interface/FIFO control module **118** is provided to the input of the traffic FIFO **116**. The output of the traffic FIFO **116** is passed via a buffer **120** back to the
35 input of the first high speed parallel interface **94** of the

cryptographic circuit **57**, and the output of the output FIFO **117** is connected to the MAC interface/FIFO control module **118**, which communicates with the communications module **32**, as will be discussed further below.

5 The various circuitry of the communication module **32** will now be described in further detail with particular reference to FIGS. 5 through 7. As noted above, the various circuitry of the communications module **32** is implemented in the communications CCA **51**. In particular, the communications
10 (or radio in the present WLAN example) CCA **51** illustratively includes a power interface **126** for cooperating with the communications power circuit **78** to supply the various communications circuitry components. Additional filter/ESD circuitry **127** may also be included in the signal path from the
15 cryptographic module **31**, if desired.

 More particularly, the signal path between the cryptographic module **31** and communications module **32** includes a plurality of lines for MII communications, as well as a three-wire serial interface (3WSI), as seen in FIG. 6.
20 Generally speaking, the MII lines are for transferring encrypted data between the cryptographic module **31** and the communications module **32**, and the three wire serial interface is for status/configuration operations of the communications module, as will be discussed further below.

25 More particularly, the MII lines pass through the filter/ESD circuitry **127** to the network communications interface **47**. In the present WLAN example, the network communications interface **47** includes an 802.11 a/b/g AP/MAC chip set **128** connected to the MII lines, and an associated
30 802.11 a/b/g radio **129** connected to the 802.11 a/b/g AP/MAC chip set for wirelessly communicating with a WLAN. One or more memories **130** may be provided for the 802.11 a/b/g AP/MAC chip set **128**. The 802.11 a/b/g AP/MAC chip set **128** illustratively includes a processing module **141**, an Ethernet MAC module **142**
35 for communicating with the cryptographic module **31**, and a WLAN

MAC module **143** for performing the appropriate 802.11 WLAN interface and processing operations, as will be appreciated by those skilled in the art.

The communications CCA **51** also illustratively includes a logic device **131**, such as a complex programmable logic device (CPLD), which is connected to the above-noted three wire serial interface. Generally speaking, the CPLD **131** cooperates with the cryptographic processor **36** to detect, status, and configure different types of communications modules **32**. More particularly, the host network processor **54** polls the CPLD **131** to determine what type of communications module **32** is connected to the cryptographic module **31** (i.e., WLAN, wireline, fiber optic, etc.), as well as its operational status, as will be appreciated by those skilled in the art.

The CPLD **131** also permits the host network processor **54** to configure the network communications interface **47** for operation in a given application, as will also be appreciated by those skilled in the art.

Referring additionally to FIGS. 9 and 10, the three lines of the three wire serial interface respectively carry clock signals, data signals, and enable signals between the cryptographic and communications modules **31**, **32**. The clock signal is provided to a sixteen bit (although other sizes may also be used) serial to parallel data converter **135**, an output register **136**, a sixteen bit parallel to serial data converter **137**, and control logic **138**. More particularly, control data coming from the cryptographic processor **36** via the data line is written to the serial to parallel data converter **135** to be output by the output register **136**.

More particularly, the communications module **32** may further include one or more status indicators **140** (e.g., light emitting diodes (LEDs)) carried by the second housing **45** for indicating operational mode, band, or other appropriate status information. The LEDs **140** receive multiple bits (e.g., eight) from the output register **136**. Another set of bits (e.g., seven

bits) from the register **136** are for enabling/disabling the communication module transmission circuitry (e.g., radio power amplifiers (PA)), and the remaining bits of the sixteen bit output is for providing a reset signal for the communications module **32**.

The input buffer **139** receives multiple bits (e.g., eight) of status (e.g., radio status for a WLAN implementation) information and multiple bits (e.g., eight) of hardware information from the 802.11 chip set **128** (or other network communications interfaces in other embodiments) to pass along to the cryptographic processor **36** via the parallel to serial data converter **137** and the data line of the three wire serial bus. Read and write data buffers **150**, **151** may also be connected to the data line, if desired. Furthermore, the control circuitry **138** also receives the enable signal and enables the output register **136** and input buffer **139**.

A read or write operation occurs when the enable signal goes high, as seen in FIG. 10. The format of the command packets sent from the cryptographic processor **36** to the CPLD **131** are as follows. The first four address bits (A15-A12) of a packet instruct the CPLD **131** whether it is to receive data from the cryptographic processor **36**, or whether it is to supply requested data thereto. The remaining address bits (A11-A0) provide the address for the appropriate component or operation being requested, while the data bits (D15-D0) are reserved for data. As such, thirty-two bit serial words are exchanged between the cryptographic processor **36** and CPLD **131**.

An exemplary read/write addressing scheme is to use 0110 for the bits A15-A12 for a write operation, and 1011 for a read operation as shown, although other addressing schemes may also be used. Both the cryptographic module **31** and communications module **32** preferably clock data out on falling edges of the clock signal and clock data in on the leading

edges, although other timing arrangements may be used in different embodiments.

A particularly advantageous approach for transferring the command packets from the cryptographic processor 36 to the communications module 32 will now be described. The host network processor 54 generates cryptographic processor command packets for the cryptographic processor 36. These packets each include an Ethernet address portion for addressing the cryptography circuit 57 and an IP packet that encapsulates a cryptographic command. In accordance with the present invention, the host network processor 54 encapsulates a command packet to be operated upon by the communications module 32 within the cryptographic command, as shown in FIG. 11. By using the second EBIU 107, for example, the communications module command packets may be passed to the communications module 32 without processing (i.e., encrypting). This provides a convenient way to transcend the red/black data boundary (FIG. 6) without potentially compromising security.

More particularly, the format of a cryptographic processor command packet is as follows. The Ethernet address portion of the packet is addressed to the cryptography circuit 57. More particularly, the address portion may include Ethernet header addresses, an IP header, and cryptographic command information, as will be appreciated by those skilled in the art. The communications module command packet destined for the communications module is encapsulated in the data portion of the IP packet. Accordingly, when the cryptography circuit 57 receives such a cryptographic processor command packet, it will recognize the packet as a cryptographic command. As such, the cryptography circuit 57 will strip its own address information from the packet and transfer the remaining portion (i.e., the encapsulated communications module command packet) to the communications module 32. Preferably, the host network processor 54 formats the data

portions of the IP packets (and, thus, the command packets for the communications module **32**) based upon the simple network management protocol (SNMP), although other protocols may also be used.

5 The above-described approach may be used for sending communications module command data via the MII lines or the BWSI, and this approach may be used in reverse to communicate information back to the host network processor **54**, as will be appreciated by those skilled in the art. Since typical prior
10 art cryptographic devices include all of the cryptography and communications circuitry within the same housing, the formatting of status/configuration commands for the communications circuitry is typically not an issue. However, as will be appreciated by those of skill in the art, the
15 above-described approach provides a convenient and secure way to perform such command/control operations despite the separation between the cryptographic and communications modules **31**, **32**. Of course, it will be appreciated that other approaches for formatting and/or encapsulating such command
20 packets may also be used, as will be appreciated by those skilled in the art.

 The above-described interchangeability of the communications modules **32** and the ability to pass the command packets through the red/black boundary is facilitated by using
25 a same, predetermined interface protocol, i.e., an MII protocol, along the entire signal path between the user network interface **35** and the network communications interface **47**. That is, the cryptographic processor **36** not only communicates with the user network interface **35** using an MII-
30 based protocol, it also communicates with the network communications interface **47** using the same MII-based protocol. The MII protocol may be based upon the original MII standard set forth in the IEEE 802.3 standard, or it may be a variant thereof such as reduced MII (RMMI) or gigabit MII (GMII), for
35 example, although other protocols may be used as well.

Maintaining the consistent use of the MII protocol through the chain of circuitry from the user network interface 35 to the network communications interface 47 allows the cryptographic module 31 and the communications module 32 both to operate using a unique external MAC addresses, while at the same time using fixed internal MAC addresses. More particularly, the Ethernet MAC modules 60 and 143 operate using a unique external MAC addresses for each individual cryptographic module 31 and communications module respectively, while the Ethernet MAC modules 61 and 142 use fixed MAC addresses which are the same for every cryptographic device 30.

Thus, the cryptographic circuitry 55 essentially becomes transparent to the communications module 32, as it appears to the communications module that it is connected directly to the Ethernet MAC module 61. Moreover, the "hard-coded" MAC addresses used by the Ethernet MAC's in both modules 61 and 142 provide for the transfer of command packets as described above, as well as a controlled transmission of encrypted data packets, as will be appreciated by those skilled in the art.

Another particularly advantageous feature of the invention is that different communications modules 32 may not only be used to allow a single cryptographic module 31 to be used with multiple media types (e.g., wireless, wireline, fiber optic, etc.), but the communications modules may also be used to provide multi-mode operation for a given media, such as in the case of a WLAN. More particularly, a WLAN communications module 32 may advantageously use an 802.11 a/b/g chip set 128 that is switchable between wireless LAN modes (i.e., access point (AP) mode, infrastructure mode, and ad-hoc mode) by the cryptographic module 31 using the above-described command packets, for example.

Thus, a same WLAN communications module 32 in accordance with the present invention may advantageously be used with any advice in a WLAN to provide desired

functionality, such as individual station operation, bridging to a wired network, peer-to-peer communications, etc., as will be appreciated by those skilled in the art. Moreover, mode changes can be accomplished "on the fly" as desired using
5 command packets. It will therefore be appreciated that with such a WLAN communications module **32**, the cryptographic device **30** provides complete 802.11 functionality in a single unit while also providing a wireless bridge that can be used to access a secure network. The cryptographic module **30** may
10 advantageously be configured to allow selection and configuration of 802.11 modules of operation via a standard Web browser, for example.

Alternately, switching between WLAN operational modules may also be accomplished by using different types of
15 802.11 chip sets **128** for respective WLAN operational modes in different WLAN communications modules. That is, a different WLAN communications module **32** would be used depending upon whether an AP, infrastructure, or ad-hoc mode was desired for a given LAN device **40**.

20 Turning to FIGS. 12-14, the coupling structure of the cryptographic and communications modules **31**, **32** will now be further described. More particularly, the first housing **34** of the cryptographic module **31** may include a first body **180** and a first extension **181** extending outwardly therefrom, and
25 the second housing **45** may include a second body **182** and a second extension **183** extending outwardly therefrom. As such, the first and second extensions **181**, **183** may be aligned in overlapping relation when the first and second connectors **37**, **46** are removably mated together.

30 The first connector **37** is illustratively carried by the first body **180** adjacent the first extension **181**, and the second connector **46** is carried by the second extension **186**. Although other arrangements may be used in accordance with the present invention, this arrangement is particularly
35 advantageous in that it allows the cryptographic CCA **50**, which

has more circuitry than the power supply CCA 52, to be positioned to take advantage of the extra length (and, therefore, surface area) of the first extension 181. Similarly, the communications CCA 51 is positioned to take advantage of the additional length of the second extension 183.

Each of the first and second extensions 181, 183 may also have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules 31, 32 together in mating relation. By way of example, the surface features may include rails 185 and corresponding channels 186 which define one or more slidable interlocking (e.g., dovetail) joints therebetween (two are shown in the exemplary implementation). One or more fasteners, such as captive screws 187 which mate with corresponding threaded holes 188, are also preferably included for removably fastening the cryptographic and communications modules 31, 32 together.

As shown in the illustrated example, the first and second connectors 37, 46 are multi-pin electrical connectors, although various electrical connector styles known to those skilled in the art may be used. Also, one or more seals 190 may be positioned between the cryptographic module 31 and the communications module 32. It will therefore be appreciated that the above-described electrical/mechanical structure provides a robust yet simple interconnection that is capable of providing desired EMI shielding and environmental sealing. Various materials (e.g., metal, plastic, etc.) may be used for the first and second housings 37, 45, as will also be appreciated by those skilled in the art.

Based upon the foregoing description, numerous advantages of the present invention will be apparent to those skilled in the art. For example, the cryptographic device 30 is interoperable with standard commercial 802.11 and 802.3 networking equipment. More particularly, it may be used with any computing platform with an Ethernet interface (e.g.,

LINUX/UNIX, VxWorks, Windows, Macintosh, etc.). As such, independent developers may advantageously be able to develop applications without the need to write special drivers to communicate with the user network interface **35**. Likewise,
5 independent developers may advantageously be able to develop communications modules **32** for various and/or specialized communications applications since they will interface with the cryptographic module **31** via a well-defined, controlled electrical/mechanical interface. Furthermore, the coupling
10 structure not only provides for easy interchangeability of different communications modules **32** with a single cryptographic module **31**, the rugged housing and connector design allows for operation over a wide range of climates and conditions.

15 Turning additionally to FIG. 15, a first communications method aspect of the invention will now be described. Beginning at Block **250**, the user network interface **35** of the cryptographic module **31** is coupled to a LAN device **40**, at Block **251**. Further, the communications module **32**, once
20 attached to the cryptographic module **31**, may then be used to communicate with various networks (i.e., LAN) **48**, thus concluding the illustrated method, at Block **254**.

Referring to FIG. 16, another communications method aspect of the invention begins (Block **260**) with coupling the
25 cryptographic module **31** to the network device **40**, at Block **261**, with the communications module **32** being coupled to the cryptographic module as described above. The method further includes using the cryptographic processor **36** to communicate with the user network interface **35** and the network
30 communications interface **47** using a same predetermined protocol (e.g., MII), at Block **263**, as discussed above, and also communicating with the network (i.e., LAN) **48**, at Block **264**, thus concluding the illustrated method (Block **265**).

Two additional method aspects for WLAN operation are
35 now described with reference to FIGS. 17 and 18. Beginning at

Block 270, the cryptographic module 31 is coupled to the network device 40, at Block 271, with the communications module 32 being removably coupled to the cryptographic module 31, as described above. If during the course of operation it
5 is determined that a different WLAN mode of operation is required, at Block 273, if a multi-mode network wireless network interface 274 is included in the WLAN communications module 32, as discussed above, the interface may be switched to the desired wireless LAN mode, at Block 274. Thereafter, or
10 if a new WLAN mode is not required, wireless communications with the network (i.e., LAN) 48 may be conducted, at Block 275, thus concluding the illustrated method (Block 276). If different 802.11 modes are implemented in respective WLAN communications modules 32, as discussed above, the step
15 illustrated at Block 274 may be replaced with the step of removably coupling a new communications module providing the desired WLAN operational mode to the cryptographic module 31, at Block 280'.

Still another communications method aspect of the
20 invention is now described with reference to FIG. 19. The method beings (Block 290) with coupling the cryptographic module 31 to the network device 40, at Block 291, with the communications module 32 being removably coupled to the cryptographic module, and using the communications module to
25 communicate with the network (i.e., LAN) 48, at Block 293, as described above. The method also includes using the logic CPLD 131 in cooperation with the cryptographic processor 36 to determine a status of the communications module 32, at Block 294, thus concluding the illustrated method, at Block 295. Of
30 course, it will be appreciated that status may be obtained (and/or configuration performed) prior to commencing communications with the network (i.e., LAN) 48, and that repeated status updates may continue to be obtained through the communications process.

Another communications method aspect of the invention will now be described with reference to FIG. 20. The method begins (Block 300) with coupling the cryptographic module 31 to the network device 40, as described above, at Block 301, with a communications module 32 being removably coupled to the cryptographic module. The method may further include causing the host network processor 54 to generate cryptographic packets for the cryptographic circuit 57 each including an address portion and a data portion, and to encapsulate command packets for the network communications interface 47 in the data portions of the cryptographic packets, at Block 302, as previously described above. Thus, if the cryptographic circuit 57 determines that a command packet is encapsulated in the cryptographic packet, the cryptographic circuit passes the command packet to the communications module 32 without performing cryptographic processing thereon, at Block 304, as also discussed above. Otherwise, cryptographic processing is performed on the data in the cryptographic packet, at Block 305, thus concluding the illustrated method (Block 306).

3. Brief Description of the Drawings

Brief Description of the Drawings

FIG. 1 is perspective view of a cryptographic device in accordance with the present invention.

FIG. 2 is an exploded view of the cryptographic device of FIG. 1 illustrating the various modules thereof.

FIG. 3 is top plan view of the cryptographic device of FIG. 1.

FIGS. 4 through 9 are schematic block diagrams illustrating the various components of the cryptographic device of FIG. 1 in greater detail.

FIG. 10 is a timing diagram illustrating status and configuration operations for the communications module of the cryptographic device of FIG. 1.

5 FIG. 11 is a block diagram of a cryptographic packet generated in accordance with the present invention.

FIGS. 12 and 13 are perspective views illustrating the connector configurations of the communications module and cryptographic module, respectively, of the cryptographic device of FIG. 1.

10 FIG. 14 is another exploded perspective view showing the bottom of the cryptographic device of FIG. 1 and further illustrating coupling of the various modules thereof.

FIGS. 15 through 20 are flow diagrams illustrating various communications method aspects in accordance with the
15 present invention.

1. Claims

CLAIMS

- 5 1. A cryptographic device comprising:
 a cryptographic module and a communications module
removably coupled thereto;
 said cryptographic module comprising
 a first housing,
10 a user Local Area Network (LAN) interface
carried by said first housing, and
 a cryptographic processor carried by said
first housing and coupled to said user LAN
interface;
15 said communications module comprising
 a second housing, and
 a network wireless LAN interface carried by
said second housing, coupled to said cryptographic
processor and switchable between wireless LAN modes.
20
2. The cryptographic device of Claim 1 wherein
said network wireless LAN interface circuit is switchable to
one of an access point (AP) mode, an infrastructure mode, and
an ad-hoc mode.
25
3. The cryptographic device of Claim 1 wherein
said cryptographic module further comprises a first connector
carried by said first housing and coupled to said
cryptographic processor; wherein said communications module
30 further comprises a second connector carried by said second
housing and connected to said network wireless LAN interface,
said second connector being removably mateable with said first
connector of said cryptographic module.

4. The cryptographic device of Claim 1 wherein said user LAN interface comprises an Ethernet interface.

5. The cryptographic device of Claim 1 wherein
5 said cryptographic processor comprises:
a host network processor coupled to said user LAN interface; and
a cryptography circuit coupled to said host network processor.

10

6. The cryptographic device of Claim 1 wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing.

15

7. A communications method comprising:
coupling a cryptographic module to a Local Area Network (LAN) device, the cryptographic module comprising a first housing, a user LAN interface carried by the first
20 housing, a cryptographic processor carried by the first housing and coupled to the user LAN interface;
providing a communications module comprising a second housing and a network wireless LAN interface carried by the second housing and removably coupled to the cryptographic
25 module; and
switching the network wireless LAN interface between wireless LAN modes, and using the network wireless LAN to communicate with a wireless LAN.

8. The method of Claim 7 wherein switching
30 comprises switching the network wireless LAN interface circuit to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

9. The method of Claim 7 wherein the cryptographic module further comprises a first connector carried by the first housing and coupled to the cryptographic processor; wherein the communications
5 module further comprises a second connector carried by the second housing and connected to the network wireless LAN interface; and wherein removably coupling comprises removably mating the second connector to the first connector.

10

10. The method of Claim 7 wherein the user LAN interface comprises an Ethernet interface.

1. Abstract

ABSTRACT

5 A cryptographic device (30) may include a
cryptographic module (31) and a communications module (32)
removably coupled thereto. The cryptographic module (31) may
include a first housing (34), a user Local Area Network (LAN)
interface (35) carried by the first housing, and a
10 cryptographic processor (36) carried by the first housing and
coupled to the user LAN interface. The communications module
(32) may include a second housing (45) and a network wireless
LAN interface (47) carried by the second housing. The network
wireless LAN interface (47) may be coupled to the
15 cryptographic processor (36), and it may be switchable between
wireless LAN modes.

2. Representative Drawing

Fig. 1

20

【図 1】

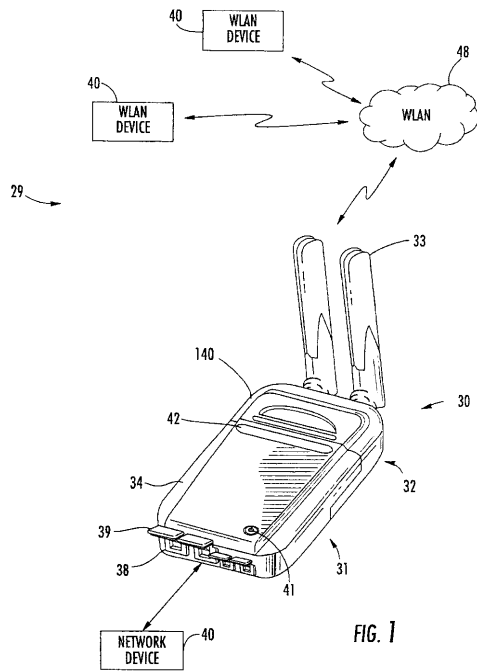


FIG. 1

【図 2】

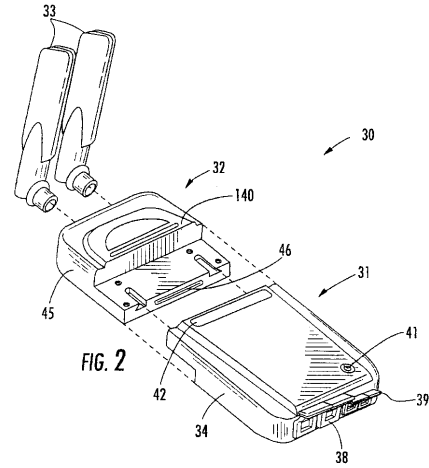


FIG. 2

【図 3】

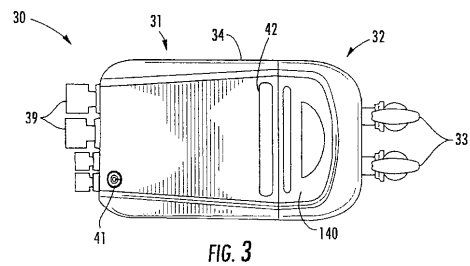


FIG. 3

【図 4】

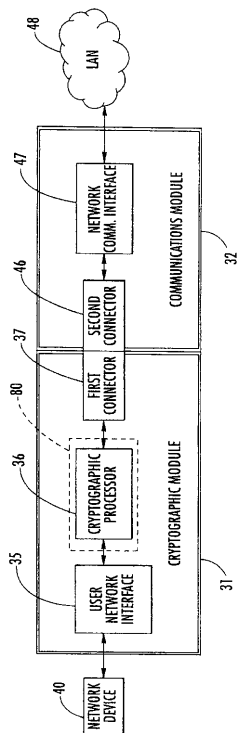


FIG. 4

【図 5】

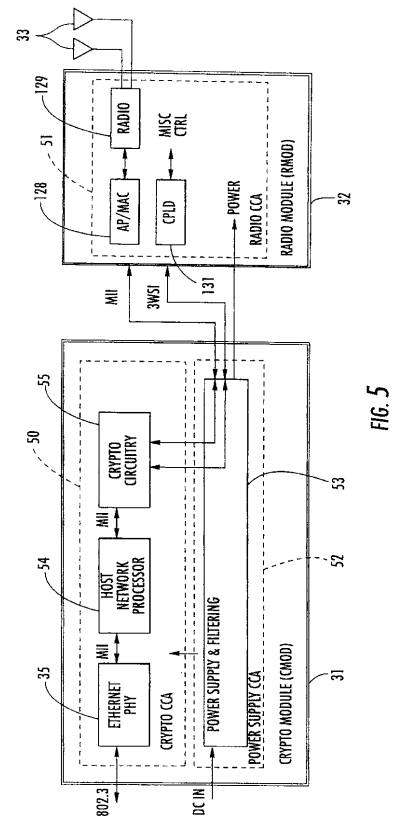
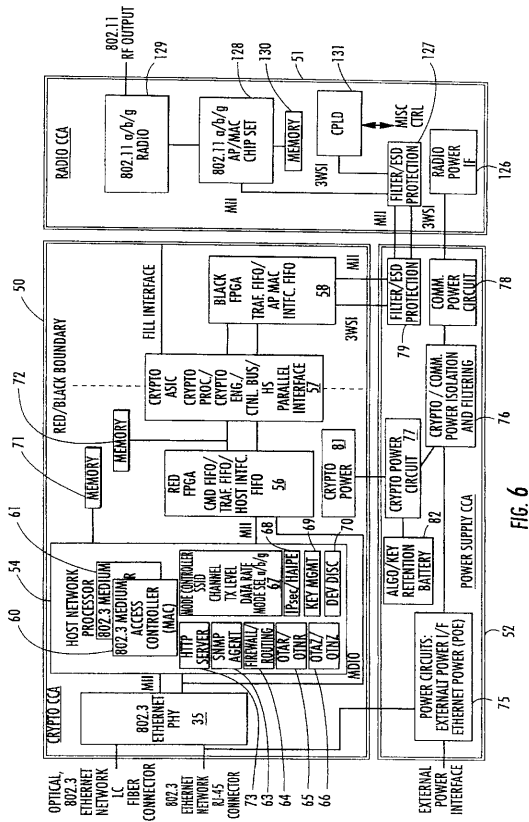
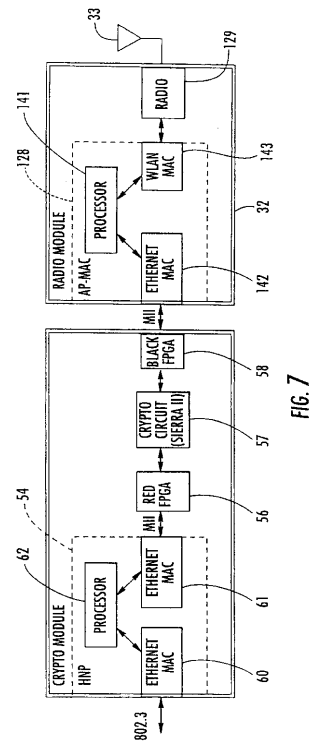


FIG. 5

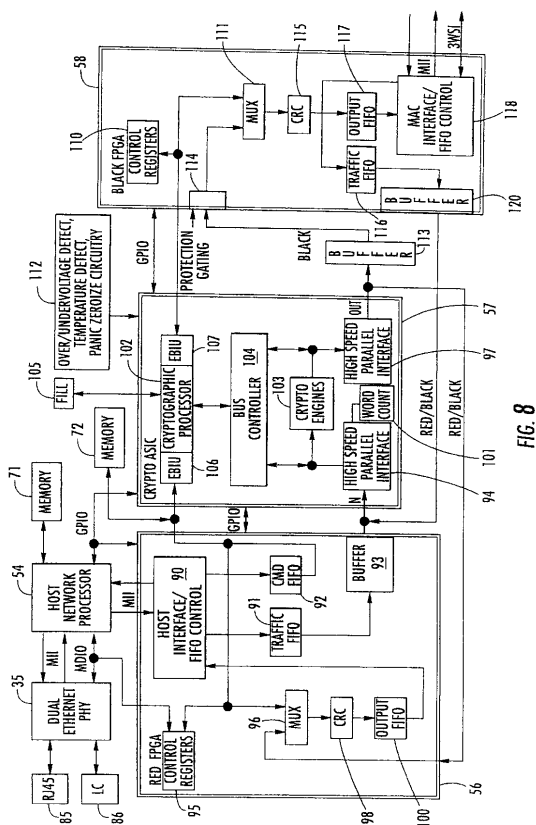
【図 6】



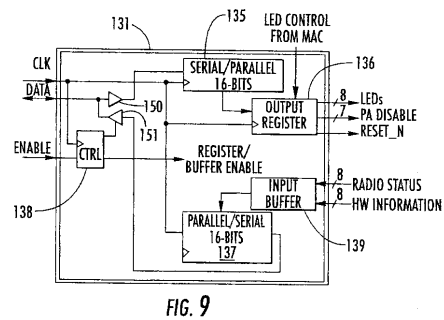
【圖 7】



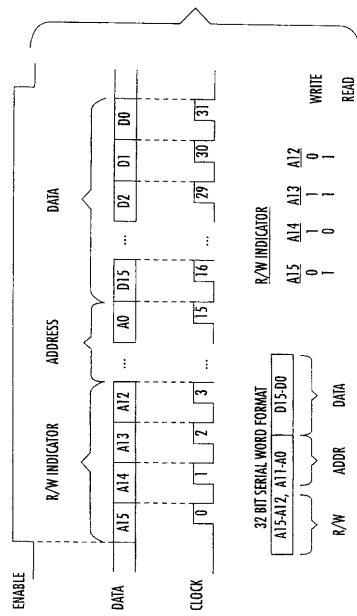
【図 8】



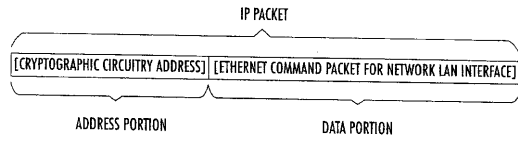
【图 9】



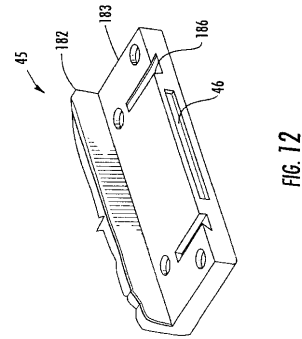
【図 10】



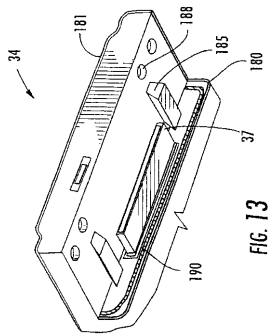
【図 11】



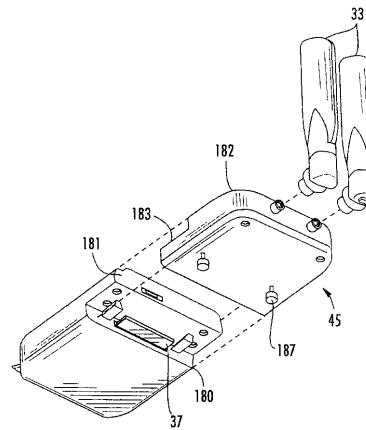
【図 12】



【図 13】



【図 14】



【図 15】

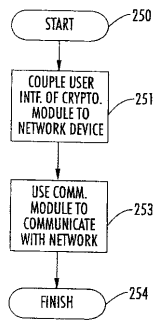


FIG. 15

【図 16】

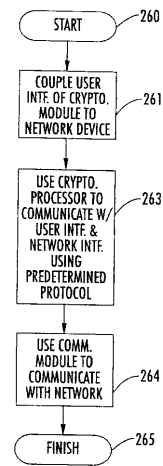


FIG. 16

【図 17】

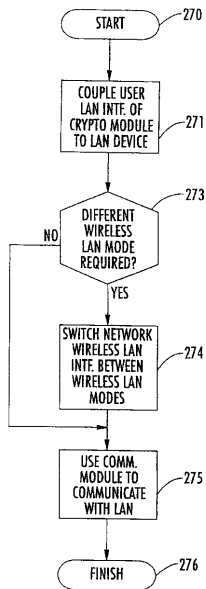


FIG. 17

【図 18】

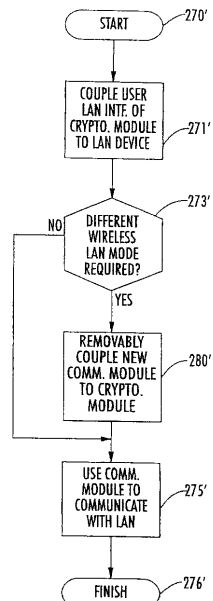


FIG. 18

【図 19】

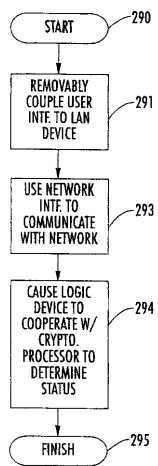


FIG. 19

【図 20】

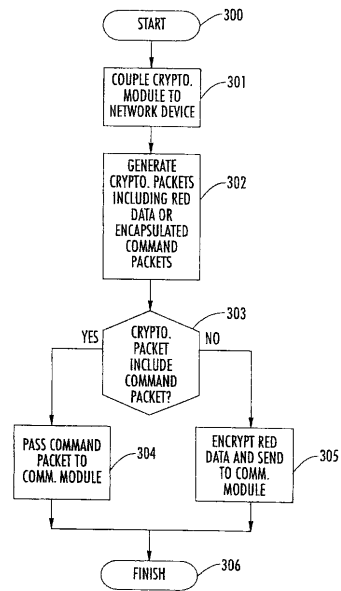


FIG. 20