【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成18年10月19日(2006.10.19)

【公表番号】特表2002-529779(P2002-529779A)
【公表日】平成14年9月10日(2002.9.10)
【出願番号】特願2000-580354(P2000-580354)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　12/22　(2006.01)
Ｈ０４Ｌ　12/56　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６１０Ａ
Ｈ０４Ｌ　12/22
Ｈ０４Ｌ　12/56　１００Ｚ
Ｈ０４Ｌ　9/00　６０１Ｚ

【手続補正書】
【提出日】平成18年8月29日(2006.8.29)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　下記の段階を含む、特定の順序に配置された複数のデータ・バイトを含むデータを第1のコンピュータから第2のコンピュータに送信する方法：
（1）複数のデータ・パケットにデータを無作為に分配するにはどうすべきかを決定する共通のアルゴリズムを第1のコンピュータおよび第2のコンピュータにおいて確立する段階、
（2）第1のコンピュータにおいて、共通のアルゴリズムに従って複数のデータ・パケットに複数のデータ・バイトを無作為に分配する段階、
（3）複数のデータ・パケットを第1のコンピュータから第2のコンピュータに送信する段階、および
（4）第2のコンピュータにおいて、無作為に分配された複数のデータ・バイトを、複数のデータ・パケットから抽出し、共通のアルゴリズムに従って特定の順序に並べ直す段階。
【請求項２】　段階（3）が、複数のデータ・パケットのそれぞれをコンピュータ・ネットワーク内の異なるパスを介して送信する段階を含む、請求項1記載の方法。
【請求項３】　複数のデータ・パケットにデータを割り付けるための無作為分配パターンを確立するアルゴリズムを含み、データ供給源からのデータ・バイトを無作為分配パターンに従って複数のデータ・パケットに無作為に分配し、複数のデータ・パケットをネットワークを介して送信する第1のコンピュータと、
ネットワークを介して第1のコンピュータに結合されており、第1のコンピュータから複数のデータ・パケットを受信し、無作為に分配されたデータ・バイトを抽出し、該データ・バイトをアルゴリズムに従って最初の順序に並べ直す第2のコンピュータとを備えるシステム。
【請求項４】　第1のコンピュータが、複数のデータ・パケットのそれぞれをネットワーク内のそれぞれの異なるパスを介して送信する、請求項3記載のシステム。

【請求項５】　下記の段階を含む、送信側コンピュータと受信側コンピュータとの間でデータ・パケットを安全に送信する方法：
（1）送信側コンピュータおよび受信側コンピュータに知られているが、送信側コンピュータと受信側コンピュータとの間の中間コンピュータには知られていないセッション鍵を使用してデータ・パケットを暗号化する段階、
（2）段階（1）で暗号化されたデータ・パケットに、該データ・パケットを識別するパケット・ヘッダを付加する段階、
（3）段階（2）で作成された組み合わされたパケット・ヘッダと暗号化データ・パケットを、第1のコンピュータと第2のコンピュータとの間に配置された複数の各中間コンピュータに知られているリンク鍵を使用して暗号化する段階、
（4）段階（3）で暗号化されたパケットをルーティングするために平文パケット・ヘッダを付加する段階、および
（5）段階（4）で作成されたパケットを送信する段階。
【請求項６】　（5）各中間コンピュータにおいて、前のコンピュータから受信されたパケットを復号し、かつリンク鍵を使用して復号する段階と、
（6）ネットワーク内の次の中間コンピュータに知られている異なるリンク鍵を使用してパケットを再暗号化する段階と、
（7）段階（6）で再暗号化されたパケットをルーティングするために平文パケット・ヘッダを付加する段階と、
（8）段階（7）で作成されたパケットを次の中間コンピュータに送信する段階とをさらに含む、請求項5記載の方法。
【請求項７】　受信側コンピュータにおいて、セッション鍵を使用してパケットを復号する段階をさらに含む、請求項6記載の方法。
【請求項８】　下記の段階を含む、コンピュータ・ネットワークを介してデータを送信する方法：
コンピュータ・ネットワークに接続された発信側端末において、データ・ストリームを受信し、該データ・ストリームから第1レベル・データ・パケット・ペイロードを形成する段階、
データ・ストリーム用のネットワーク着信先アドレスを識別し、ネットワーク着信先アドレスを表すデータを含む第1レベル・ヘッダを各データ・パケットに付加して第1レベル・パケットを形成する段階、
各第1レベル・パケットを暗号化して第2レベル・パケット・ペイロードを形成する段階、
発信側端末を着信先に接続する少なくとも1つの中間ルータのアドレスを着信先アドレスとして含むペイロード・ヘッダを第2のレベル・パケットに付加して第2レベル・パケットを形成する段階、
第2レベル・パケットを該少なくとも1つの中間ルータに送信する段階、および
該少なくとも1つの中間ルータにおいて、少なくとも1つの第2レベル・ペイロードを復号し、第1レベル・ヘッダから着信先アドレスを判定し、少なくとも第1レベル・パケット・ペイロードを含む新しいパケットを形成し、着信先アドレスを含むヘッダを新しいパケットに付加し、それによって、データ・ストリームの真の着信先が、ネットワークを介して送信される少なくとも一部の時間の間、暗号化層に隠される段階。
【請求項９】　付加段階が、一群の中間ルータから無作為に選択することによって少なくとも1つの中間ルータを決定することを含む、請求項8記載の方法。
【請求項１０】　第1レベル・ヘッダから着信先アドレスを判定する段階が、中間ルータ上に記憶されている相関データによって、ネットワーク着信先アドレスを表すデータをネットワーク着信先アドレスに変換することを含む、請求項8記載の方法。

【請求項１１】　第1レベル・パケットがネットワーク着信先に到着する前に行うホップの数のインディケータを第1層ヘッダと第2層ヘッダの一方に含める段階をさらに含み

、少なくとも1つの中間ルータが、ホップの数のインディケータを減分させ、ホップの数のインディケータの値に応じてそれぞれ別の中間ルータに第1レベル・パケットを送信する、請求項8記載の方法。

【請求項１２】　下記の段階を含む、パケット・ネットワーク上でパケットをルーティングする方法：

セッション鍵を用いてメッセージ・データをブロック暗号化してペイロードを形成する段階、

ブロック暗号化によって暗号化されたブロックを、ブロック暗号化段階によるデータのインタリーブ部分が少なくとも2つのデータ・ペイロードの間に入るように少なくとも2つのデータ・ペイロードに分割する段階、

少なくとも2つのデータ・ペイロードのそれぞれを、パケットの最終的な着信先を識別する着信先データと共に、リンク鍵を用いて暗号化する段階、

第1の中間着信先アドレスを示す第1のホップ・アドレスを最後の暗号化段階の結果として得られた第1のペイロードと組み合わせ、結果として得られた第1のパケットを第1の中間着信先アドレスに送信する段階、および

第2の中間着信先アドレスを示す第2のホップ・アドレスを最後の暗号化段階の結果として得られた第2のペイロードと組み合わせ、結果として得られた第2のパケットを第2の中間着信先アドレスに送信する段階。

【請求項１３】　第1のパケットに第1のホップ・カウンタを組み合わせる段階と、

第1の中間着信先アドレスに一致する端末において、第1のホップ・カウンタに応じて、第1のパケットを最終的な着信先アドレスに送信するよう判定する段階と、

第1の中間着信先アドレスに一致する端末において、リンク鍵を用いて第1のペイロードを復号して最終的な着信先アドレスを明らかにし、判定段階に応じて第1のパケットを最終的な着信先アドレスに送信する段階とをさらに含む、請求項12記載の方法。

【請求項１４】　第2のパケットに第2のホップ・カウンタを組み合わせる段階と、

第2の中間着信先アドレスに一致する端末において、第2のホップ・カウンタに応じて、第1のパケットを最終的な着信先アドレスに送信するよう判定する段階と、

第2の中間着信先アドレスに一致する端末において、リンク鍵を用いて第2のペイロードを復号して最終的な着信先アドレスを明らかにし、最後の判定段階に応じて第2のパケットを最終的な着信先アドレスに送信する段階とをさらに含む、請求項12記載の方法。