【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７部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2005-503714(P2005-503714A)
【公表日】平成17年2月3日(2005.2.3)
【年通号数】公開・登録公報2005-005
【出願番号】特願2003-529673(P2003-529673)
【国際特許分類】
Ｈ０４Ｌ　9/16　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４３

【手続補正書】
【提出日】平成17年9月2日(2005.9.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
情報ストリングをソースエンティティから宛て先エンティティに送信する方法であって、このような情報を各々が前記ストリング中の所定の関連した時間間隔でのみ有効である暗号化キーの時間シーケンスを通じて暗号化し、暗号化キーの前記時間シーケンスに基づいて前記宛て先エンティティが前記情報を解読するのを可能にし、前記宛て先エンティティに2つの特定の暗号化キー間の転換瞬間に関する制御情報を示す方法において、
－前記情報ストリング中で、前記宛て先エンティティに知られている、前記転換に関連する前記ストリングの所定のローカライゼーションでデータブロックを選出し、前記データブロックを実際に有効な暗号化キーで暗号化するステップと、
－前記暗号化されたデータブロックのフィンガープリントを形成するステップと、
－前記暗号化されたデータブロックの代わりに前記所定のローカライゼーションの前記フィンガープリントを送信するステップと、
－更新が起こったことを示すために帯域外制御メッセージを送信するステップと、
を有する方法。
【請求項２】
請求項1に記載の方法において、前記制御メッセージは、暗号化の後であって前記フィンガープリントの形成の前の前記データブロックを含む、方法。
【請求項３】
請求項1に記載の方法において、前記制御メッセージの送信は、前記転換を含む前記セキュリティ保護されたコンテンツに関する可変遅延期間の対象となる、方法。
【請求項４】
請求項1に記載の方法において、前記ストリングのどのローカライゼーションにおいても1つのキーのみがアクティブである方法。
【請求項５】
請求項1に記載の方法において、前記所定のローカライゼーションは、前に存在していた暗号化キーを用いる前記ストリング内の最後のブロック位置である、方法。
【請求項６】
請求項1に記載の方法において、暗号化／解読のために用いられるブロック暗号アルゴリズムに基づくセキュリティ保護されたリンクに適用される方法。

【請求項７】
請求項2に記載の方法を実行することにより生じる暗号化された情報ストリングを受信するための方法において、前記制御メッセージのペイロードをフィンガープリントするステップと、前記暗号化されたデータストリームとのマッチを検索するステップと、このようなマッチが見つかったら前記転換の指示を生じるステップと、暗号化キーの前記シーケンスに関連する次の解読キーに変更するステップとを有する方法。
【請求項８】
情報ストリングをソースエンティティから宛て先エンティティに送信設備上で送信するための請求項1に記載の方法を実行するように構成された装置であって、このような情報を各々が前記ストリング中の所定の関連した時間間隔でのみ有効である暗号化キーの時間シーケンスを通じて暗号化する暗号化手段を有し、更に、前記宛て先エンティティに2つの特定の暗号化キー間の転換瞬間に関する制御情報を示す表示手段を有する装置において、
－前記情報ストリング中で、前記宛て先に知られている、前記転換に関連する前記ストリングの所定のローカライゼーションでデータブロックを選出し、前記データブロックを前記符号化手段に示す選択手段と、
－前記暗号化されたデータブロックのフィンガープリントを形成して、前記暗号化されたデータブロックの代わりに前記所定のローカライゼーションの前記フィンガープリントを前記送信設備上で送信するための、前記暗号化手段によって供給されるフィンガープリント手段と、
－更新が起こったことを示すために帯域外制御メッセージを送信するための制御メッセージ手段と、
を有する装置。
【請求項９】
請求項8に記載の装置において、前記制御メッセージは、暗号化の後であって前記フィンガープリントの形成の前の前記データブロックを含む、装置。
【請求項１０】
請求項7に記載の方法を実行するように構成された装置において、請求項1に記載の方法を実行することにより生じる暗号化された情報ストリングを受信するための受信手段と、前記制御メッセージのペイロードをフィンガープリントするための2次フィンガープリント手段と、前記暗号化されたデータストリームとのマッチを検索するための、前記受信手段及び前記2次フィンガープリント手段によって供給される比較検索手段とを有する装置。
【請求項１１】
請求項8に記載の装置において、ストリーム暗号に基づいた暗号化手順に用いられると共に、前記データブロックを収容するための追加のビットバッファを備えている装置。
【請求項１２】
請求項8に記載の装置及び請求項10に記載の装置の互いにインタフェースされた対を含む送信システム。