【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17年11月10日(2005.11.10)

【公開番号】特開2003-188874(P2003-188874A)
【公開日】平成15年7月4日(2003.7.4)
【出願番号】特願2002-280384(P2002-280384)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/32
　Ｈ０４Ｌ　9/08
【ＦＩ】
　Ｈ０４Ｌ　9/00　６７５Ａ
　Ｈ０４Ｌ　9/00　６０１Ｃ
　Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成17年9月26日(2005.9.26)
【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】　安全にデータを伝送する方法であって、
　送信側においてキャラクタストリングを生成すること、
　前記キャラクタストリングおよび秘密鍵を使用してハッシュ鍵を生成すること、
　前記ハッシュ鍵を使用して前記データを暗号化すること、
　前記送信側に関連する識別鍵、前記キャラクタストリング、および前記暗号化データを前記送信側から受信側に伝送すること、を含む、方法。
　【請求項２】　前記ハッシュ鍵を生成することは、前記秘密鍵を使用して前記キャラクタストリングをハッシングすることを含む、請求項１記載の方法。
　【請求項３】　前記ハッシュ鍵および前記データを使用して署名を生成すること、前記署名を前記送信側から前記受信側に伝送すること、をさらに含む、請求項１記載の方法。
　【請求項４】　キャラクタストリングを生成することは、前記キャラクタストリングをランダムに生成することを含む、請求項１記載の方法。
　【請求項５】　前記識別鍵を使用して前記受信側において前記秘密鍵を決定すること、前記秘密鍵および前記キャラクタストリングを使用して、前記受信側において前記暗号化データを解読すること、をさらに含む、請求項１記載の方法。
　【請求項６】　前記秘密鍵を決定することは、前記識別鍵を前記秘密鍵に関連付ける関係データベースにアクセスすることを含む、請求項５記載の方法。
　【請求項７】　前記識別鍵を使用して前記受信側において前記秘密鍵を決定すること、前記秘密鍵および前記キャラクタストリングを使用して、前記受信側において前記ハッシュ鍵を決定すること、前記ハッシュ鍵を使用して前記暗号化データを解読すること、をさらに含む、請求項１記載の方法。
　【請求項８】　前記ハッシュ鍵を決定することは、前記キャラクタストリングを使用して前記秘密鍵をハッシングすることを含む、請求項７記載の方法。
　【請求項９】　前記送信側が前記ハッシュ鍵および前記データを使用して第１の署名を生成すること、前記第１の署名を前記受信側に伝送することであって、前記受信側は、前記ハッシュ鍵を決定して前記データを解読し、前記第１の署名を、前記ハッシュ鍵およ

び前記解読されたデータを使用して前記受信側が生成した第２の署名と比較するように構成される、該伝送すること、をさらに含む、請求項１記載の方法。

【請求項１０】　前記ハッシュ鍵および前記データを使用して署名を生成すること、前記署名を前記受信側に伝送すること、前記識別鍵を使用して前記受信側において前記秘密鍵を決定すること、前記秘密鍵および前記キャラクタストリングを使用して、前記受信側において前記ハッシュ鍵を決定すること、前記ハッシュ鍵を使用して前記受信側において前記暗号化データを解読すること、前記ハッシュ鍵および前記解読されたデータを使用して、前記受信側において前記署名を検証すること、をさらに含む、請求項１記載の方法。