【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19年11月22日(2007.11.22)

【公開番号】特開2006-109107(P2006-109107A)
【公開日】平成18年4月20日(2006.4.20)
【年通号数】公開・登録公報2006-016
【出願番号】特願2004-293075(P2004-293075)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成19年10月5日(2007.10.5)
【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】
署名対象のメッセージを入力する入力工程と、
前記メッセージに付加情報を付加する付加工程と、
ハッシュ関数及び公開鍵暗号を用いて前記付加情報を付加したメッセージの署名データを生成する生成工程と、
前記署名データを付加情報として、前記付加工程及び前記生成工程を規定回数繰り返す工程と、
繰り返し生成された署名データ及び付加情報を前記メッセージと共に出力する出力工程とを有することを特徴とする署名生成方法。
【請求項２】
前記繰り返す工程では、前記ハッシュ関数に異なるアルゴリズムを利用することを特徴とする請求項１に記載の署名生成方法。
【請求項３】
前記繰り返す工程では、前記公開鍵暗号に異なるアルゴリズムを利用することを特徴とする請求項１に記載の署名生成方法。
【請求項４】
前記繰り返す工程では、前記公開鍵暗号で用いる鍵長を順に短くすることを特徴とする請求項１に記載の署名生成方法。
【請求項５】
署名対象のメッセージ、署名データ、及び付加情報を入力する入力工程と、
前記メッセージに前記付加情報を付加する付加工程と、
ハッシュ関数及び前記署名データを用いて前記付加情報が付加されたメッセージを検証する署名検証工程と、
前記検証の結果を出力する出力工程と、
前記入力工程では検証のために必要な付加情報を複数個入力し、前記付加工程及び前記署名検証工程を規定回数繰り返す工程とを有することを特徴とする署名検証方法。
【請求項６】

前記繰り返す工程では、前記署名検証工程で用いられる鍵長を順に短くすることを特徴とする請求項５に記載の署名検証方法。
【請求項７】
署名対象のメッセージを入力する入力手段と、
前記メッセージに付加情報を付加する付加手段と、
ハッシュ関数及び公開鍵暗号を用いて前記付加情報を付加したメッセージの署名データを生成する生成手段と、
前記署名データを付加情報として、前記付加手段及び前記生成手段を規定回数繰り返すよう制御する制御手段と、
繰り返し生成された署名データ及び付加情報を前記メッセージと共に出力する出力手段とを有することを特徴とする情報処理装置。
【請求項８】
署名対象のメッセージ、署名データ、及び付加情報を入力する入力手段と、
前記メッセージに前記付加情報を付加する付加手段と、
ハッシュ関数及び前記署名データを用いて前記付加情報が付加されたメッセージを検証する署名検証手段と、
前記検証の結果を出力する出力手段と、
前記入力手段にて検証のために必要な付加情報を複数個入力し、前記付加手段及び前記署名検証手段を規定回数繰り返すよう制御する制御手段とを有することを特徴とする情報処理装置。
【請求項９】
請求項１に記載の署名生成方法又は請求項５に記載の署名検証方法をコンピュータに実行させるためのプログラム。
【請求項１０】
請求項９に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】署名生成方法、署名検証方法、及び情報処理装置
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
また、本発明は、署名検証方法であって、署名対象のメッセージ、署名データ、及び付加情報を入力する入力工程と、前記メッセージに前記付加情報を付加する付加工程と、ハッシュ関数及び前記署名データを用いて前記付加情報が付加されたメッセージを検証する署名検証工程と、前記検証の結果を出力する出力工程と、前記入力工程では検証のために必要な付加情報を複数個入力し、前記付加工程及び前記署名検証工程を規定回数繰り返す工程とを有することを特徴とする。