

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-511095

(P2017-511095A)

(43) 公表日 平成29年4月13日(2017.4.13)

(51) Int.Cl.		F I		テーマコード (参考)
H04L 9/10	(2006.01)	H04L 9/00	621Z	5J104
H04L 9/32	(2006.01)	H04L 9/00	675B	

審査請求 未請求 予備審査請求 未請求 (全 21 頁)

(21) 出願番号 特願2017-505025 (P2017-505025)
 (86) (22) 出願日 平成27年4月9日 (2015.4.9)
 (85) 翻訳文提出日 平成28年12月9日 (2016.12.9)
 (86) 国際出願番号 PCT/KR2015/003576
 (87) 国際公開番号 W02015/156621
 (87) 国際公開日 平成27年10月15日 (2015.10.15)
 (31) 優先権主張番号 10-2014-0042360
 (32) 優先日 平成26年4月9日 (2014.4.9)
 (33) 優先権主張国 韓国 (KR)
 (31) 優先権主張番号 10-2015-0050155
 (32) 優先日 平成27年4月9日 (2015.4.9)
 (33) 優先権主張国 韓国 (KR)

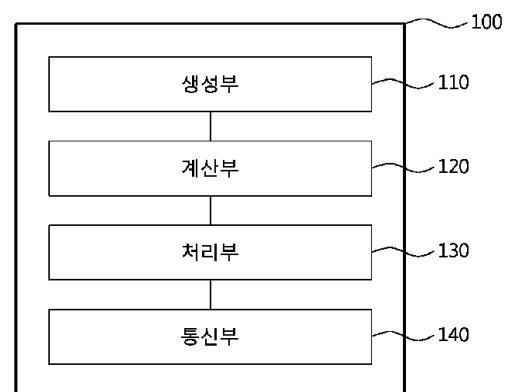
(71) 出願人 516196923
 アイシーティーケー カンパニー リミテ
 ッド
 大韓民国 463-400 キョンギ-ド
 ソンナム-シ ブンダン-ク パンギョ
 -ロ 323 3番 フロア

最終頁に続く

(54) 【発明の名称】 認証装置及び方法

(57) 【要約】

公開キー暗号化アルゴリズムを用いる認証装置を提示する。装置は、メッセージに対応する電子署名の生成リクエストに応答して、ランダムナンバーの生成過程で第1インスタント公開キーを生成する。そして、前記第1インスタント公開キーを用いて前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出する。



110 ... Generation unit

120 ... Calculation unit

130 ... Processing unit

140 ... Communication unit

【特許請求の範囲】

【請求項 1】

少なくとも 1 つのプロセッサを含み、公開キー基盤暗号化アルゴリズムによる認証手続を行う認証装置において、前記認証装置は、前記少なくとも 1 つのプロセッサによって少なくとも一時的に実現される、

前記アルゴリズムに対応する電子署名が必要な場合に応答して、第 1 インスタント公開キーを生成する生成部と、

前記第 1 インスタント公開キーを用いて、前記アルゴリズムで前記第 1 インスタント公開キーと対を成す第 1 インスタント個人キーを算出する算出部と、

前記第 1 インスタント個人キーを用いて前記アルゴリズムによる電子署名を生成する処理部と、

を含む、認証装置。

【請求項 2】

送信するメッセージを前記電子署名及び前記第 1 インスタント公開キーと共に相手機器に送信する通信部をさらに含む、請求項 1 に記載の認証装置。

【請求項 3】

前記相手機器から再送信リクエストが受信されることに応答して、通信 A c k が受信されて通信エラーがないものと判断される場合、前記生成部が前記第 1 インスタント公開キーと異なる第 2 インスタント公開キーを生成する、請求項 2 に記載の認証装置。

【請求項 4】

前記生成部は、ランダムナンバーの生成過程で前記第 1 インスタント公開キーを生成する、請求項 1 に記載の認証装置。

【請求項 5】

前記認証装置は、ランダムに発生する工程偏差を用いてハードウェアフィンガープリントを提供する P U F (P h y s i c a l l y U n c l o n a b l e F u n c t i o n) をさらに含み、

前記ランダムナンバーの生成過程は、前記ハードウェアフィンガープリントをオリジナル値として用いるランダムナンバー生成アルゴリズムを含む、請求項 4 に記載の認証装置。

【請求項 6】

前記算出の結果として、前記第 1 インスタント公開キーと対を成す前記第 1 インスタント個人キーが存在しないものと判断される場合、

前記生成部は、前記第 1 インスタント公開キーと異なる第 2 インスタント公開キーを生成し、前記算出部は、前記アルゴリズムで前記第 2 インスタント公開キーと対を成す第 2 インスタント個人キーを算出する、請求項 4 に記載の認証装置。

【請求項 7】

前記生成部は、前記第 2 インスタント公開キーを生成するために前記ランダムナンバーの生成過程を行う代わりに、前記第 1 インスタント公開キーに整数 2 を加えた数を前記第 2 インスタント公開キーとして決定して提供する、請求項 6 に記載の認証装置。

【請求項 8】

前記暗号化アルゴリズムが R S A - C R T (C h i n e s e R e m a i n d e r T h e o r e m) アルゴリズムである場合、前記算出部が算出する前記第 1 インスタント個人キーは第 1 d P 値及び第 1 d Q 値を含み、

前記算出の結果として、前記第 1 d P 値及び前記第 1 d Q 値のうちいずれか 1 つでも存在しないものと判断される場合、

前記生成部は、前記第 1 インスタント公開キーと異なる第 2 インスタント公開キーを生成し、前記算出部は、前記アルゴリズムで前記第 2 インスタント公開キーと対を成す第 2 d P 値及び第 2 d Q 値を算出する、請求項 6 に記載の認証装置。

【請求項 9】

少なくとも 1 つのプロセッサを含み、公開キー基盤暗号化アルゴリズムにより相手機器

10

20

30

40

50

が送信した電子署名を検証する認証装置において、前記認証装置は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現される、

保有していた前記相手機器の固定公開キー及び前記相手機器がインスタントに生成して前記電子署名と共に送信した第1インスタント公開キーを用いて、前記電子署名を検証する処理部を含む認証装置。

【請求項10】

前記第1インスタント公開キーが3以上の奇数でなければ、前記第1インスタント公開キーを有効でないものと判断する判断部をさらに含む、請求項9に記載の認証装置。

【請求項11】

前記第1インスタント公開キーが繰り返し生成されたものであれば、前記第1インスタント公開キーを有効でないものと判断する判断部をさらに含む、請求項9に記載の認証装置。

10

【請求項12】

少なくとも1つのプロセッサを含む認証装置において、前記認証装置は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現される、

相手機器から受信される第1インスタント公開キーが有効な値であるかを判断する判断部と、

前記第1インスタント公開キーが有効な値である場合、保有していた前記相手機器の固定公開キーと前記第1インスタント公開キーを用いて送信するデータを符号化する処理部と、

20

を含む認証装置。

【請求項13】

前記第1インスタント公開キーは、前記相手機器でランダムナンバーの生成過程で生成されたものである、請求項12に記載の認証装置。

【請求項14】

前記判断部は、前記第1インスタント公開キーが3以上の奇数でなければ、前記第1インスタント公開キーを有効でないものと判断する、請求項12に記載の認証装置。

【請求項15】

前記判断部は、前記第1インスタント公開キーが予め指定された再使用回数以上に繰り返し用いられる場合、前記第1インスタント公開キーを有効でないものと判断する、請求項12に記載の認証装置。

30

【請求項16】

少なくとも1つのプロセッサを含み、公開キー基盤暗号化アルゴリズムによる認証手続を行う認証装置において、前記認証装置は前記少なくとも1つのプロセッサによって少なくとも一時的に実現される、

前記認証手続の実行に応答して、ランダムナンバーの生成過程で第1インスタント公開キーを生成する生成部と、

前記第1インスタント公開キーを用いて、前記アルゴリズムで前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出する算出部と、

前記第1インスタント公開キーが送信された相手機器から、前記相手機器に予め保有している固定公開キーと前記第1インスタント公開キーを用いて符号化したメッセージが受信されれば、前記第1インスタント個人キーを用いて前記メッセージを復号化する処理部と、

40

を含む認証装置。

【請求項17】

前記認証装置は、ランダムに発生する工程偏差を用いてハードウェアフィンガープリントを提供するPUFをさらに含み、

前記ランダムナンバーの生成過程は、前記ハードウェアフィンガープリントをオリジナル値として用いるランダムナンバー生成アルゴリズムを含む、請求項16に記載の認証装置。

50

【請求項 18】

前記算出の結果として、前記第1インスタント公開キーと対を成す前記第1インスタント個人キーが存在しないものと判断される場合、

前記生成部は、前記第1インスタント公開キーと異なる第2インスタント公開キーを生成し、前記算出部は、前記アルゴリズムで前記第2インスタント公開キーと対を成す第2インスタント個人キーを算出する、請求項1に記載の認証装置。

【請求項 19】

コンピュータで読み出し可能な記録媒体に格納される非一時的なコンピュータプログラムにおいて、前記プログラムはプロセッサを含むコンピューティング装置で実行される場合に前記プロセッサが、

メッセージに対応する電子署名の生成リクエストに応答して、ランダムナンバーの生成過程で第1インスタント公開キーを生成させる命令語セットと、

前記第1インスタント公開キーを用いて、前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出させる命令語セットと、

前記第1インスタント個人キーを用いて公開キーアルゴリズムによる電子署名を生成させる命令語セットと、

を含むコンピュータで読み出し可能な記録媒体に格納されるプログラム。

【請求項 20】

コンピュータで読み出し可能な記録媒体に格納される非一時的なコンピュータプログラムにおいて、前記プログラムは、プロセッサを含むコンピューティング装置で実行される場合に前記プロセッサが、

相手機器からメッセージ及び電子署名と共に受信された第1インスタント公開キーが有効であるかを判断させる命令語セットと、

前記第1インスタント公開キーが有効である場合、前記コンピューティング装置に格納されていた前記相手機器の固定公開キー及び受信した前記第1インスタント公開キーを用いて前記電子署名を検証させる命令語セットと、

を含むコンピュータで読み出し可能な記録媒体に格納されるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は認証装置及び方法に関し、より詳細に、公開キー暗号アルゴリズム基盤認証装置のセキュリティー攻撃に強く向上された発明に関する。

【背景技術】

【0002】

機器認証やメッセージ電子署名で公開キー暗号アルゴリズムを用いた署名方式が用いられる。例えば、RSA (Rivest Shamir Adleman) アルゴリズムは、公開キーと個人キーをセットにして暗号化及び復号化を行うインターネット暗号化及び認証方法として、個人キーは機器に、公開キーは認証機関のような相手機器に伝えられて保管される。

【0003】

一方、RSAのような公開キーアルゴリズム基盤で個人キーが表示／流出される場合に署名を偽造することがあるため、個人キーはセキュリティー攻撃、例えば、副チャネル攻撃の目標となっている。副チャネル攻撃方法のうち、大量のデータを収集して統計的に分析するDPA (Differential Power Analysis) 攻撃は極めて強力なものとして知られている。

【0004】

一方、PUF (Physically Unclonable Function) は、予測不可能なデジタル値を提供し得る。個々のPUFは、正確な製造工程が与えられ、同じ工程で製造されても前記個々のPUFが提供しているデジタル値は異なる。PUFは複製できないPOWF (Physical One-Way Function pra

10

20

30

40

50

critically impossible to be duplicated) のように称される。

【0005】

このようなPUFの複製できない特性は、セキュリティー及び／又は認証のための機器の識別子を生成するために用いられる。例えば、デバイスを他のデバイスと区別するためのユニークキーを提供するためにPUFを用いてもよい。

【0006】

韓国登録特許10-1139630号（以下、'630特許）において、PUFを実現する方法が提示されている。'630特許では、半導体の工程偏差を用いて半導体の伝導性レイヤ間のインターレイヤコンタクト又はビア(via)生成の有無が確率的に決定されるようにした方法を提示している。

10

【発明の概要】

【課題を解決するための手段】

【0007】

実施形態によれば、副チャネルの攻撃に強い認証装置及び認証方法が提示される。例えば、公開キー基盤アルゴリズムを利用しながらもDPA攻撃を不可能にしたり、また、無意味にさせる認証装置及び方法が提示される。実施形態によれば、公開キー／個人キーの対が固定された値になることで、繰り返して使用されることなく、代わりに、認証が必要な場合にインスタントに生成して用いることができる。

【0008】

20

一側面によれば、少なくとも1つのプロセッサを含み、公開キー基盤暗号化アルゴリズム、例えば、非対称キー暗号化アルゴリズムのRSAによる認証手続を行う認証装置が提供される。装置には、すでに生成された固定個人キーp、qを有している。一態様によれば、装置は、前記アルゴリズムに対応する電子署名が必要な場合に応答して、第1インスタント公開キーを生成する生成部と、前記第1インスタント公開キーを用いて、前記アルゴリズムで前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出する算出部と、前記第1インスタント個人キーを用いて前記アルゴリズムによる電子署名を生成する処理部とを含む。前記生成部、前記算出部、及び前記処理部は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現され得る。一態様によれば、装置は、送信するメッセージを前記電子署名及び前記第1インスタント公開キーと共に相手機器に送信する通信部をさらに含み得る。

30

【0009】

一態様によれば、装置は、公開キーキー生成アルゴリズムによって前記固定個人キーを生成して保有している。前記固定個人キーは、前記第1インスタント公開キーを用いて前記第1インスタント個人キーを算出するときと、使用に前もって発給過程で他の機器に伝えられて今後署名の検証にともに用いられる固定公開キーを生成するとき用いられる。例示的で、しかし限定されないように、前記認証装置には、ランダムに発生する工程偏差を用いてハードウェアフィンガープリントを提供するPUFがさらに含まれる。一態様によれば、このPUFの値が前記固定個人キー値で直接又は間接的に用いることができる。この場合、メモリに前記固定個人キーを直接的に格納する必要がなく、物理的な攻撃から前記固定個人キーを保護できる。これは、前記固定個人キーが当該の機器内にのみ存在するという点が保障されるため、他の機器でインスタント公開キー個人キーの対を任意に作ることができず、また、保障される。また、他の実施形態では、前記PUFの値がインスタント公開キーを作るために直接又は間接的に用いることもできる。例えば、ランダムナンバーの生成過程におけるシード値又はオリジナル値として用いてもよい。この場合、PUFをランダムナンバー生成アルゴリズムのオリジナル値として用いることで、機器ごとに生成されるランダムナンバー生成結果が互いに独立的、また、値を互いに相違にするという効果を追加的に期待することができる。

40

【0010】

一方、前記相手機器から再送信リクエストの受信に応答して、下記のように対応するこ

50

とができる。単純通信エラーによる再送信リクエストの場合、生成したメッセージを再送信する。しかし、その他の場合は、例えば、誤った署名、又は、攻撃があるものと疑われる場合、第1インスタント公開キーを廃棄し、これとは異なる新しい第2インスタント公開キーを生成して再び電子署名を生成して送信する。

【0011】

一態様によれば、前記算出結果として、前記第1インスタント公開キーと対を成す前記第1インスタント個人キーが存在しないものと判断される場合、前記生成部は、前記第1インスタント公開キーと異なる第2インスタント公開キーを生成する。すると、前記算出部は前記アルゴリズムで前記第2インスタント公開キーと対を成す第2インスタント個人キーを算出する。一方、前記生成部は、前記第2インスタント公開キーを生成するために前記ランダムナンバーの生成過程を行う代わりに、前記第1インスタント公開キーに整数2を加えた数を前記第2インスタント公開キーとして決定して提供することもできる。第1インスタント公開キーに加えられる「2」という整数は例示的なものであるため、他の値に変更してもよい。もし、前記暗号化アルゴリズムがRSA-CRT (Chinese Remainder Theorem) アルゴリズムである場合、前記算出部が算出する前記第1インスタント個人キーは第1dP値及び第1dQ値を含む。このRSA-CRT実施形態において、前記算出結果による前記第1dP値及び前記第1dQ値のうちいずれか1つでも存在しないものと判断されれば、前記生成部は前記第1インスタント公開キーと異なる第2インスタント公開キーを生成する。そして、前記算出部は前記アルゴリズムで前記第2インスタント公開キーと対を成す第2dP値及び第2dQ値を算出する。

【0012】

他の一側面によれば、少なくとも1つのプロセッサを含み、公開キー基盤暗号化アルゴリズムにより相手機器が送信した電子署名を検証する認証装置、例えば、認証機関 (CA: Certification Authority) が提供される。装置は、保有していた前記相手機器の固定公開キー、及び前記相手機器がインスタントに生成して前記電子署名と共に送信した第1インスタント公開キーを用いて、前記電子署名を検証する処理部を含む。

【0013】

一態様によれば、装置は、前記第1インスタント公開キーが3以上の奇数でなければ、前記第1インスタント公開キーを有効でないものと判断する判断部をさらに含む。一方、前記処理部と前記判断部は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現され得る。

【0014】

更なる一側面によれば、少なくとも1つのプロセッサを含む認証装置において、相手機器から受信される第1インスタント公開キーが有効な値であるかを判断する判断部と、前記第1インスタント公開キーが有効な値である場合、保有していた前記相手機器の固定公開キーと前記第1インスタント公開キーを用いて、送信するデータを符号化する処理部とを含む認証装置が提供される。前記判断部と前記処理部は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現され得る。例示的に、しかし限定されないように、前記第1インスタント公開キーは、前記相手機器でランダムナンバーの生成過程により生成されたものであり得る。

【0015】

一態様によれば、前記第1インスタント公開キーが3以上の奇数でなければ、前記判断部が前記第1インスタント公開キーを有効でないものと判断する。更なる一側面によれば、少なくとも1つのプロセッサを含み、公開キー基盤暗号化アルゴリズムによる認証手続を行う認証装置が提供される。装置は、前記認証手続の実行に応答して、ランダムナンバーの生成過程で第1インスタント公開キーを生成する生成部と、前記第1インスタント公開キーを用いて、前記アルゴリズムで前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出する算出部と、前記第1インスタント公開キーが送信された相手機器から、前記相手機器に予め保有している固定公開キーと前記第1インスタント公開キ

ーを用いて符号化したメッセージが受信されれば、前記第1インスタント個人キーを用いて前記メッセージを復号化する処理部とを含む。前記生成部、前記算出部、前記処理部は、前記少なくとも1つのプロセッサによって少なくとも一時的に実現され得る。

【0016】

一態様によれば、前記認証装置には、ランダムに発生する工程偏差を用いてハードウェアフィンガープリントを提供するPUFをさらに含んでいる。この場合、前記ランダムナンバーの生成過程は、前記ハードウェアフィンガープリント値をオリジナル値として用いるランダムナンバー生成アルゴリズムを含む。

【0017】

一態様によれば、前記算出結果として前記第1インスタント公開キーと対を成す前記第1インスタント個人キーが存在しないものと判断される場合、前記生成部は前記第1インスタント公開キーと異なる第2インスタント公開キーを生成する。そして、前記算出部は前記アルゴリズムで前記第2インスタント公開キーと対を成す第2インスタント個人キーを算出する。

【0018】

更なる一側面によれば、コンピュータで読み出し可能な記録媒体に格納される非一時的なコンピュータプログラムが提供される。前記プログラムは、プロセッサを含むコンピューティング装置で実行される場合、前記プロセッサを動作させる以下の命令語セットを含む。命令語セットは、前記プロセッサがメッセージに対応する電子署名の生成リクエストにตอบสนองして、ランダムナンバーの生成過程で第1インスタント公開キーを生成するようにする命令語セットと、前記プロセッサが前記第1インスタント公開キーを用いて、前記第1インスタント公開キーと対を成す第1インスタント個人キーを算出するようにする命令語セットと、前記プロセッサが前記第1インスタント個人キーを用いて公開キーアルゴリズムによる電子署名を生成するようにする命令語セットを含む。

【0019】

更なる一側面によれば、コンピュータで読み出し可能な記録媒体に格納される非一時的なコンピュータプログラムが提供される。前記プログラムはプロセッサを含むコンピューティング装置で実行される場合、前記プロセッサを動作させる以下の命令語セットを含む。命令語セットは、前記プロセッサが相手機器からメッセージ及び電子署名と共に受信された第1インスタント公開キーが有効であるかを判断するようにする命令語セットと、前記プロセッサが前記第1インスタント公開キーが有効な場合、前記コンピューティング装置に格納されていた前記相手機器の固定公開キー、及び受信した前記第1インスタント公開キーを用いて前記電子署名を検証するようにする命令語セットを含む。

【図面の簡単な説明】

【0020】

【図1】一態様に係るインスタント公開キーとインスタント個人キーを提供する認証装置を示すブロック図である。

【図2】一態様に係る相手側が生成したインスタント公開キーが伝達されて使用する認証装置を示すブロック図である。

【図3】一態様に係る電子署名の検証過程を示すフローチャートである。

【図4】一態様に係る符号化及び復号化過程を示すフローチャートである。

【図5】一態様によりインスタント個人キーが存在しない場合の処理を示すフローチャートである。

【図6】一態様によりRSA-CRTアルゴリズム適用時個人キーが存在しない場合の処理を示すフローチャートである。

【発明を実施するための形態】

【0021】

以下で、実施形態を添付する図面を参照しながら詳細に説明する。しかし、権利範囲はこのような実施形態によって制限されたり限定されることはない。各図面に提示された同一の参照符号は同一の部材を示す。

10

20

30

40

50

【0022】

以下の説明で用いられる用語は、関連する技術分野で一般的かつ普遍的なものにより選択されたが、技術の発達及び／又は変化、慣例、技術者の選好などに応じて他の用語が存在し得る。したがって、下記の説明で用いられる用語は技術的な思想を限定するものとして理解されることなく、実施形態を説明するための例示的な用語として理解されなければならない。

【0023】

また、特定の場合は、出願人が任意に選定した用語もあり、この場合に該当する説明の部分で詳細な意味を記載すべきである。したがって下記の説明で用いられる用語は単純な用語の名称ではない、その用語が有する意味と明細書の全般にわたった内容に基づいて理解されなければならない。

10

【0024】

図1は、一態様によりインスタント公開キーとインスタント個人キーを提供する認証装置を示すブロック図である。装置100は、少なくとも1つのプロセッサを含むコンピューティング端末の少なくとも一部分である。このコンピューティング端末は例示的なものであり、これに限定されないように、スマートフォン、タブレット、ラップトップ、汎用コンピュータ、サーバ、又は、暗号化通信用専用端末などであってもよい。装置100は公開キー基盤暗号化アルゴリズム、例えば、RSAのような非対称キー暗号化アルゴリズムによる認証手続を行う。

【0025】

20

一態様によれば、装置100の生成部110は、RSAアルゴリズムに対応する電子署名が必要な場合に応答して、第1インスタント公開キー「E」を生成する。このような第1インスタント公開キーEの生成は、ランダムナンバー生成の過程で実行される。一方、生成されるEは3以上の奇数でなければならない。少数又は極めて大きい数である場合にも疑似少数でなければならないためである。生成部110は、生成されたEが奇数であるか、その値が1ではないかを確認する。

【0026】

一方、一態様によれば、装置100にはランダムに発生する半導体工程偏差を用いてハードウェアフィンガープリントを提供するPUF（図示せず）が含まれている。半導体工程偏差を用いてPUFを実現する例は様々である。例示的に、半導体の伝導性レイヤ間に配置されるビア又はインターレイヤコンタクトのランダム形成－形成失敗の結果を用いてPUFが実現され、これを詳細に公開した'630特許の明細書が参考としてこの明細書に引用される。

30

【0027】

一方、このような例示的な状況で、PUFが提供しているハードウェアフィンガープリントは前記固定個人キー生成アルゴリズムに用いられる。装置が基本的に有する301固定個人キーp、qは少数であり、これを生成するとき固定個人キーp、qの候補値としてハードウェアフィンガープリントを用いる。この場合、ハードウェアフィンガープリント値と実際に生成された固定個人キーp、q値との差のみをメモリに記録すればよい。記録される値は、32-bitとして充分であるため、その値のみをもって本来の固定個人キーp、qを推測することができない。また、必要に応じて、ハードウェアフィンガープリント値から固定個人キー値を早く再生産することも可能である。

40

【0028】

一方、このような例示的な状況で、PUFが提供するハードウェアフィンガープリントは、前記ランダムナンバー生成アルゴリズムに用いられてもよい。例えば、ソフトウェア及び／又はハードウェアに動作するランダムナンバーアルゴリズムで求められるオリジナル値、又は、シードキー（seed key）としてハードウェアフィンガープリントを使用することができる。

【0029】

【数 1】

$$E = \text{random}()$$

【0030】

上記の数式(1)によって第1インスタント公開キーEが生成されれば、算出部120は、RSA方式で規定された算出方式に基づいてアルゴリズムにより第1インスタント公開キーEを用いてEのRSA対である、言い換えれば、Eと対を成す第1インスタント個人キー「D」を算出する。

【0031】

【数 2】

$$D = E^{-1} \bmod (p-1)(q-1)$$

【0032】

このようにRSAアルゴリズムでキー発給過程の対象である、個人キー公開キーを直ちに生成及び算出することは次のような長所を有する。RSA方式で個人キーは{D、p、q}があり、相手側の機器に提供される公開キーは{E、N}がある。ここで、Nはpとqの積であり、DとEは $D \times E = 1 \bmod (p-1)(q-1)$ の関係が成立つ。他の機器や認証機関に伝えられるEやNとは異なって、認証装置の内部にのみ存在する（存在しなければならず）個人キー{D、p、q}はセキュリティ攻撃の対象となる。Dが第三者に露出されれば、直接的な電子署名の偽造が可能である。そして、Dを知らなくてもp及び／又はqの値を第三者が知ることになると、外部に公開されているEと共に用いてDを算出することもできるため、RSAの暗号化はこれ以上の価値がなくなる。

【0033】

前述したように、副チャネル攻撃、例えば、DPA(Differential Power Analysis、差分電力分析)は機器の消耗電力波形を分析するが、1つの電流消耗波形のみを観察するSPA(Simple Power Analysis)攻撃とは異なって、実際のキーが用いられた波形を複数収集した後に統計的な分析方法に基づいてD、p又はqを取得し得る。ノイズが激しい環境や電力消耗をシールドして観察し難い場合にSPA攻撃は成功的でない場合もあるが、依然として、DPA攻撃はアルゴリズムの安全に威嚇的である。複数の波形を通した統計的分析過程でノイズなどのその他のアウトライアーは相殺され、有意義なパターンが発見されるためである。

【0034】

従来におけるRSA暗号アルゴリズムでは認証装置の固定された個人キーである{D、p、q}を有し、相手側である認証機関が上記の認証装置の固定された公開キーである{E、N}を有する。したがって、攻撃子が機器に電子署名を繰り返してリクエストする形でDPAに必要な複数の波形を収集し得る可能であることから危険であった。

【0035】

しかし、前記実施形態によれば、この個人キーと公開キーのうち少なくともDとEが固定された値ではない動的に変化する値である。言い換えれば、電子署名のような暗号化アルゴリズムの実行が必要な場合、直ちにしばらくの間に使用するDとEを生成する。生成されたDとEは一回のみが使用されることから、攻撃子に電子署名が収集されても統計的に無意味なものである。実施形態はこのように固定されることなく動的に変更するEとDを生成して使用することによって、DPA攻撃などの副チャネル攻撃を基本的に防止することができる。

【0036】

さらに、前述したように、任意に第1インスタント公開キーEを生成するために用いられるPUFのハードウェアフィンガープリントは同一に設計されても、その値が異なるため物理的に複製することは不可能である。そして、PUF値や構造も外部で観察及び分析することがほとんど不可能である。したがって、このような実施形態によれば、PUF値

10

20

30

40

50

をシードにしてランダムな E を生成するアルゴリズムそのものを攻撃することも防止できる。

【0037】

このように第 1 インスタント公開キー E が生成され、これを用いて E の対である第 1 インスタント個人キー D が算出されるが、場合によって上記の数式 (2) を満足する D が存在しない場合もある。

【0038】

D が存在しなければ、有効な「インスタント D－インスタント E の対」が作られないため、生成部 110 が上記した第 1 インスタント公開キー E とは異なる第 2 インスタント公開キー E' を生成する。このような第 2 インスタント公開キー E' をもって算出部 120 が数式 (2) により第 2 インスタント個人キー D' を算出する。D' が存在すれば、E' と D' を使用し、そうでなければこの過程を繰り返す。

【0039】

ここで、生成部 110 が第 2 インスタント公開キー E' を作る過程について、第 1 インスタント公開キー E を作ったものと類似に、再度ランダムナンバーの生成過程を行う場合もある。しかし、このような過程よりも簡単な他の実施形態も可能である。例えば、生成部 110 は再度ランダムナンバーの生成過程を行う代わりに、生成されたものの対応する D が存在していない第 1 インスタント公開キー E に整数 2 を加えた数（言い換えれば、E の真上の奇数）を第 2 インスタント公開キー E' のように決定して提供することもできる。ここで、E' を生成するために E に加えられる「2」という整数は例示的なものであり、他の値に変更され得る。D の存在の有無に応じて E を再度生成することについては図 5 を参照して説明することにする。

【0040】

一方、前記暗号化アルゴリズムが CRT (Chinese Remainder Theorem) を用いるアルゴリズムであってもよいが、この場合、E をもって算出されなければならないインスタント個人キーは D 1 つでなく、数式 (3) と数式 (4) により算出される {dP、dQ} であってもよい。

【0041】

【数 3】

$$dP = E^{-1} \bmod (p-1)$$

【数 4】

$$dQ = E^{-1} \bmod (q-1)$$

【0042】

この RSA-CRT の実施形態において、算出部 120 の算出により E に対応する有効な dP 値及び有効な dQ 値のいずれか 1 つでも存在しないと判断されれば、同様に E を再び生成しなければならない。この場合も、ランダムナンバーの生成過程を再び行うが、E に 2 を加えて簡単に E' を決定し、該 E' に対応する dP' 値及び dQ' 値を算出することもできる。詳しい内容は図 6 を参照して再び説明する。

【0043】

以上の過程で有効なインスタント公開キー (E) とインスタント個人キー (D 又は {dP、dQ}) が決定されれば、これによって RSA 方式の暗号化アルゴリズムが実行され得る。メッセージ M を署名して電子署名 S を生成すれば、処理部 130 が次のような過程を行う。

【0044】

【数 5】

$S = \text{GenSign}(M, D, p, q)$

【0045】

GenSign() は電子署名の生成関数として、RSA アルゴリズムにより規定されている。通信部 140 は、生成された電子署名 S をメッセージ M と共に相手側の機器（例えば、認証機関）に送信するが、従来とは異なって上で生成したインスタント公開キー E も共に送信する。すると、相手側の機器はこのインスタント公開キー E をすでに保有していた装置 100 の固定公開キー N と共に用いて電子署名 S を検証する。以上の過程については図 3 を参照して再び説明することにする。

10

【0046】

一方、このように送信されたインスタント公開キー E を用いて相手側の機器がメッセージを符号化して送信されれば、装置 100 は持っているインスタント個人キー D （又は dP 、 dQ ）を p 、 q と共に用いてメッセージを復号化する。このような過程については図 4 を参照して後述することにする。

【0047】

このように実施形態によってセキュリティ攻撃の危険は極めて低下されるが、予想される数個の更なる攻撃が試みられる場合もあり、このような攻撃は次のような実施形態によって実現され得る。攻撃子が極めて短い時間にキーの再送信を数回要求することがある。一態様に係る装置 100 は、通信エラーの場合にインスタント個人キーを再使用して署名を再生成することなく、すでに生成された署名を再送信するだけである。そして、通信エラーではない場合、すでに生成されたインスタント公開キーを廃棄し、新しいインスタント公開キーを生成する。通信エラーであるか否かは送信メッセージに対する通信 Ack が受信されるか否かにより確認される。相手側の機器側から行う攻撃防止の代案については図 2 を参考してより詳細に説明する。

20

【0048】

図 2 は、一態様により相手側が生成したインスタント公開キーが伝達されて使用する認証装置を示すブロック図である。装置 200 は、例えば、認証機関（CA: Certification Authority）であり得る。そして、装置 200 は、少なくとも 1 つのプロセッサを含むコンピューティング端末の少なくとも一部分であってもよく、後述する判断部 210 と処理部 220 は前記プロセッサによって少なくとも一時的に実現され得る。

30

【0049】

一態様に係る装置 200 は、保有していた前記相手機器の固定公開キー N と、図 1 を参照して説明したように相手機器がインスタントに生成してメッセージ M 、電子署名 S と共に送信した第 1 インスタント公開キー E を用いて電子署名 S を検証する処理部 220 を含む。

【0050】

メッセージを符号化して相手機器に送らなければならない場合、処理部 220 は、保有していた相手機器の固定公開キー N と、すでに伝達された第 1 インスタント公開キー E を用いて送信するデータ M を符号化する。 M が正常に符号化された M' が相手機器に送信されれば、相手機器は自身の固定個人キー p 、 q とインスタント個人キー D （又は dP と dQ ）を用いて M' を M に復号化する。

40

【0051】

一方、一態様によれば、装置 200 は、相手機器から送信されたインスタント公開キー E が有効であるか否かを判断する判断部 210 をさらに含む。攻撃子が E と D を全て 1 にして電子署名を生成し、これを伝達する攻撃については予想することができる。この場合、電子署名の生成及び検証演算は実際に行われない。 E と D は、RSA 演算で指数値として用いられるため、値が 1 であれば、符号化／復号化のためにメッセージの「1」自乗することは演算しないものと同一である。ここで、認証機関 CA の立場から見れば、署名の

50

検証結果が有効として算出され得る。したがって、このような状況を防止するために判断部 210 は相手機器から伝達されたインスタント公開キー E が 3 以上の奇数であるかを確認する。これによって、E が偶数であるか E が 1 であれば、有効でない E として判断できる。

【0052】

さらに、他の一態様に係る判断部 210 は、E が指定された再使用回数以上に繰り返し使用される場合、これを非常な状況として認識してインスタント公開キー E を有効でないものと取り扱う。

【0053】

図 3 は、一態様に係る電子署名の検証過程を示すフローチャートである。上述したように、従来の RSA との差異点は、機器の固定された個人キー D を有することなく、相手認証機関もこの機器の固定された公開キー E を有しない点である。したがって、実施形態によれば、図 1 ～ 図 2 を参照して上述したように、認証が必要な場合にインスタント公開キー E と、これによって算出されるインスタント個人キー D が生成して活用される。

【0054】

図示した実施形態において、機器はリザーバ 301 に p と q のみを有している。そして、認証機関はこの機器の固定公開キーのうち N のみを有する。認証が必要な場合、ステップ S 310 が実行される。ステップ S 310 は、ランダムナンバーの生成過程でランダムなインスタント公開キー E が生成される過程であり、生成される E は 3 以上の奇数である。インスタント E の生成及びその有効性の検証については図 1 を参照して説明した通りである。

【0055】

ステップ S 320 において、インスタント公開キー E の RSA 対である D が算出される。RSA で規定された方式に基づくため、この分野の当業者によって D の算出は容易に理解されるのである。ステップ S 330 において、送信するメッセージ M に対する電子署名 S が生成される。そして、ステップ S 340 において、メッセージ M、電子署名 S と共に前記インスタント公開キー E が認証機関に送信される。すると、認証機関は、電子署名検証アルゴリズムを行うステップ S 350 において、すでに伝達された E を予め有する N と共に使用する。ステップ S 350 の実行に前もって、認証機関は、伝達された E が有効であるかを検証する過程を経てもよく、これについては図 2 を参照して詳細に説明した通りである。

【0056】

図 4 は、一態様に係る符号化及び復号化過程を示すフローチャートである。認証機関がメッセージ M を符号化して機器に送信する過程が示されている。認証機関は、ステップ S 410 において、予め保有している相手機器の固定公開キー N と、既に伝達されたインスタント公開キー E を用いて送信するデータ M を符号化する。そして、ステップ S 420 において、符号化されたメッセージ M' が機器に送信され、機器は、ステップ S 430 において自身の固定個人キー p、q とインスタント個人キー D（又は dP と dQ）を用いて M' を M に復号化し得る。

【0057】

図 5 は、一態様によりインスタント個人キーが存在しない場合の処理を示すフローチャートである。ステップ S 510 において、機器の生成部がランダムナンバーの生成過程でインスタント公開器 E を生成する。そして、ステップ S 520 において、機器の算出部が E を用いて数式 (2) により E の RSA 対であるインスタント個人キー D を算出する。ステップ S 530 において、この有効な D が存在する場合、図 1 ～ 図 4 を参照して説明したように、インスタント D とインスタント E を用いた認証過程が実行される。

【0058】

しかし、ステップ S 530 の判断として D が存在しない場合は、機器の生成部は、先のインスタント公開キー E と異なる第 2 インスタント公開キー E' を生成する。このような過程は再びランダムナンバーの生成過程を経たものであるが、図 5 に示す例では、より

10

20

30

40

50

簡単な実施形態を提示する。ステップ S 5 4 0 において、すでに生成されたが D が存在しなくて使用できないインスタント公開キー E に整数 2 を加える。このような過程が有効な $E - D$ の対が生じるまで繰り返す。

【0059】

図 6 は、一態様により RSA-CRT アルゴリズムの適用時に個人キーが存在しない場合の処理を示すフローチャートである。まず、CRT を使用しない上記の実施形態の場合に署名を生成するときと、CRT を使用する場合に署名を生成するときを比較すれば次の表の通りである。

【0060】

【表 1】

CRT を使用しない場合	CRT を使用する場合
$D = E^{-1} \bmod (p-1)(q-1)$	$dP = E^{-1} \bmod (p-1)$
$N = pq$	$dQ = E^{-1} \bmod (q-1)$
$S = M^D \bmod N$	$qInv = q^{-1} \bmod p$
	$s_1 = M^{dP} \bmod p$
	$s_2 = M^{dQ} \bmod q$
	$h = qInv \times (s_1 - s_2) \bmod p$
	$S = s_2 + h \times q$

【0061】

表 1 において、 M'' は RSA 署名フォーマットに適するようにメッセージ M のハッシュ値にパディングなどを追加した値である。表 1 から確認されるように CRT を用いる場合に式が複雑になるものの、RSA 演算で演算量の相当な部分を占める「modular exponentiation」の処理データ長が $1/2$ になるため、CRT を使用しない場合に比べてかえて演算速度が 4 倍～8 倍ほど速くなる。

【0062】

ランダムなインスタント公開キー E が生成された後、CRT が使用される場合 (S 6 1 0)、ステップ S 6 2 0 で dP が算出され、この dP が存在するかを判断する (S 6 3 0)。dQ の存在有無に関わらず dP が存在しなければ、E を使用することができない。したがって、ステップ S 6 3 1 において、E に 2 を加えた数を再び E に指定して dP を算出する過程を、dP が存在するまで繰り返す。もちろん、先に説明したように、ステップ S 6 3 1 は、選択的な実施形態であるため、ランダムナンバーの生成過程で完全に新しい E を再び生成することも可能である。

【0063】

dP が存在する場合、dQ に対しても同じ過程が繰り返される。dQ の算出 (S 6 4 0) 及び存在の有無判断 (S 6 5 0) 及び dQ が存在しないことによる E の再生成 (S 6 5 1) は、ステップ S 6 2 0、S 6 3 0、及び S 6 3 1 に説明した通りである。そして、有効な dP と dQ が全て存在する場合、ステップ S 6 6 0 において、CRT を用いる暗号化アルゴリズムが実行され得る。

【0064】

上述した実施形態に係る効果及び性能 이슈を説明することにする。実施形態のうち、PUF ハードウェアフィンガープリントをオリジナル値にするランダムナンバー生成の

10

20

30

40

50

場合、外部の攻撃が不可能である。EとDの対を常に再生成して用いてもEの値が極めて小さければ（例えば、16bit未満）、同一のE-Dの対が偶然に使用されることもあるが、これについてはEを僅かに増大することで防止される。Eの大きさが大きくなる場合、電子署名の検証に必要な演算量は増加するものの、このような演算を行う認証機関のハードウェアリソースを考慮すれば負担にならない程度である。したがって、E値の大きさは性能を低下しないレベルで十分に大きい値、例えば、128bit以上に決定される。

【0065】

一方、実施形態によりE-Dの対が持続的に再生成されることで発生する性能低下も大きくない。E-Dの対を生成する演算の時間複雑度はキーの長さ n に比例して（時間複雑度 $O(n)$ ）、署名生成演算は、実現の方式によってキーの長さ n の自乗又は三乗に比例する（時間複雑度 $O(n^2)$ 又は $O(n^3)$ ）。ところで、最近、用いられるRSAの最低キーの長さは1024、2048bit以上であるため、E-Dの対を生成する演算時間は署名生成時間の数千分の1に当該し、この程度の消耗時間は全体的に見ると、その比重を無視できるほどの小さい。したがって、実施形態によると、ハードウェア的な無理又は性能低下なしでDPAのような副チャンネル攻撃を基本的に防止することができる。

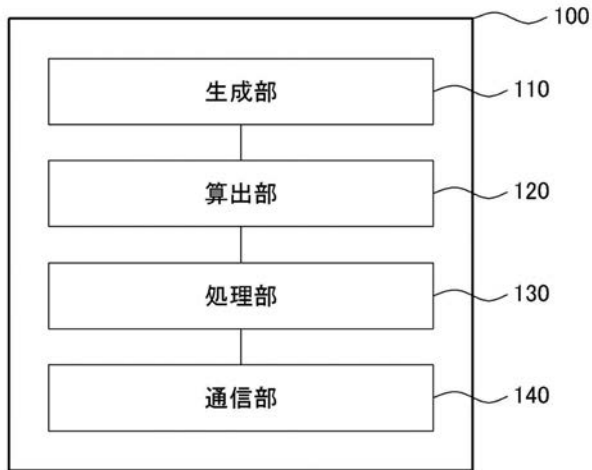
【0066】

本実施形態による方法は、多様なコンピュータ手段を介して実施されるプログラム命令の形態で具現され、コンピュータ読み取り可能な記録媒体に記録される。記録媒体は、プログラム命令、データファイル、データ構造などを単独又は組合せて含む。記録媒体及びプログラム命令は、本発明の目的のために特別に設計して構成されたものでもよく、コンピュータソフトウェア分野の技術を有する当業者にとって公知のものであり使用可能なものであってもよい。コンピュータ読み取り可能な記録媒体の例としては、ハードディスク、フロッピー（登録商標）ディスク及び磁気テープのような磁気媒体、CD-ROM、DVDのような光記録媒体、プロプティカルディスクのような磁気-光媒体、及びROM、RAM、フラッシュメモリなどのようなプログラム命令を格納して実行するように特別に構成されたハードウェア装置を含む。プログラム命令の例としては、コンパイラによって生成されるような機械語コードだけでなく、インタプリタなどを用いてコンピュータによって実行される高級言語コードを含む。ハードウェア装置は、本発明の動作を実行するために1つ以上のソフトウェアモジュールとして作動するように構成してもよく、その逆も同様である。

【0067】

以上、本発明の実施形態について図面を参照しながら詳細に説明したが、本発明は、上述の実施形態に限定されるものではなく、本発明の技術的範囲から逸脱しない範囲内で多様に変更実施することが可能である。

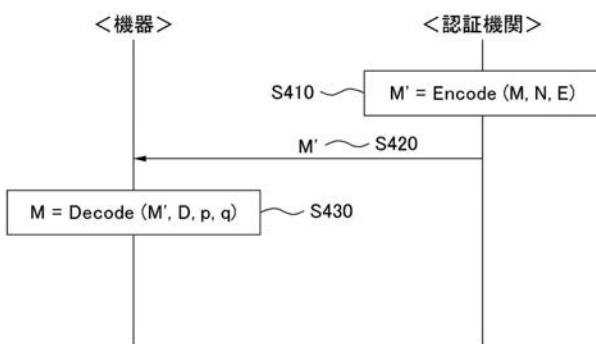
【図 1】



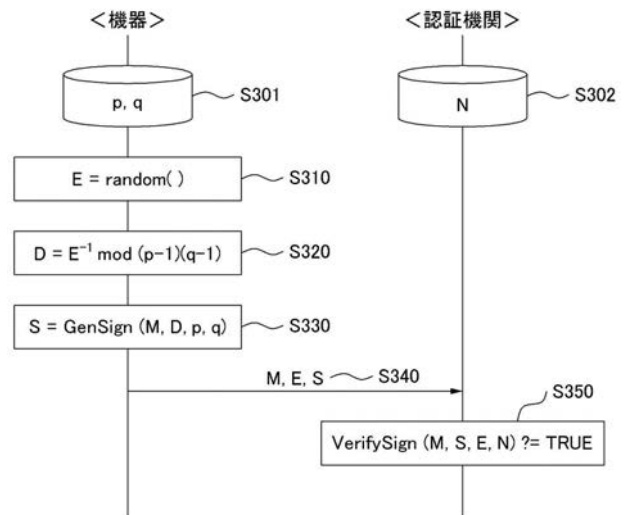
【図 2】



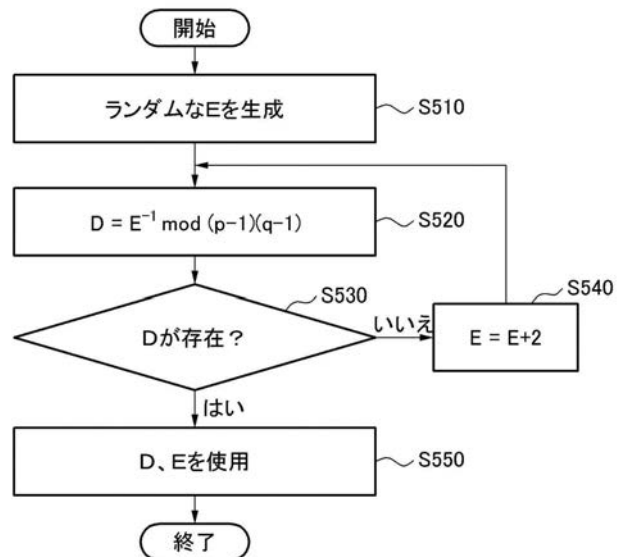
【図 4】



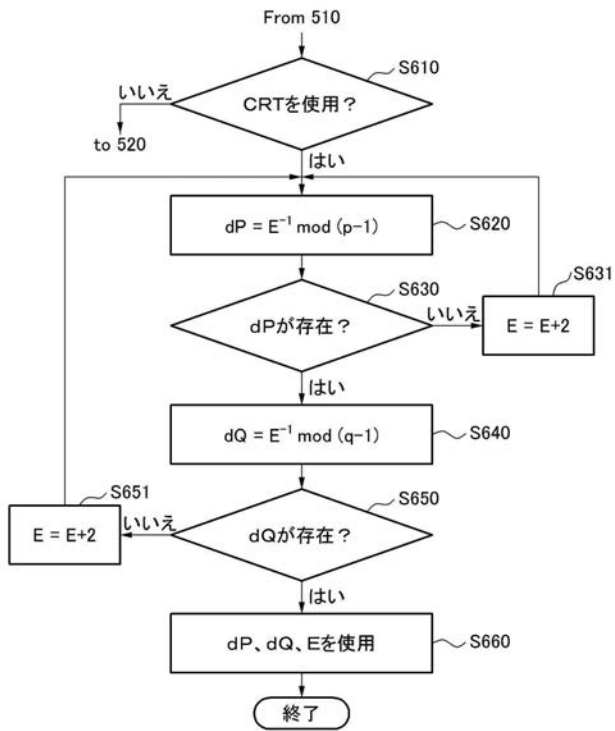
【図 3】



【図 5】



【図 6】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2015/003576

A. CLASSIFICATION OF SUBJECT MATTER H04L 9/32(2006.01)i, H04L 9/30(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L 9/32; H04L 9/08; G06F 11/30; G06F 21/20; H04L 9/00; H04L 9/30 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean Utility models and applications for Utility models: IPC as above Japanese Utility models and applications for Utility models: IPC as above Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS (KIPO internal) & Keywords: instant public key, instant private key, electronic signature, verification, encoding, decoding		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2009-0017538 A (INTERNATIONAL BUSINESS MACHINES CORPORATION.) 18 February 2009 See paragraphs [0060]-[0162]; and figures 2-5.	1,4,6-11,18-20
Y		2,3,5,12-17
Y	US 2011-0103589 A1 (TIE, Manxia et al.) 05 May 2011 See paragraphs [0073]-[0105]; and figures 5-7.	2,3,12-17
Y	US 2012-0321077 A1 (SHIOTA, Shigemasa et al.) 20 December 2012 See paragraphs [0185]-[0192]; and figure 18.	5,17
A	US 2005-0084114 A1 (JUNG, Bae - Eun et al.) 21 April 2005 See paragraphs [0018]-[0109]; and figures 1, 2.	1-20
A	US 2008-0008316 A1 (PILIPCHUK, Denis) 10 January 2008 See paragraphs [0020]-[0026]; and figures 1-5.	1-20
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 26 JUNE 2015 (26.06.2015)		Date of mailing of the international search report 29 JUNE 2015 (29.06.2015)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office Government Complex-Daejeon, 189 Seousa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2015/003576

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0017538 A	18/02/2009	CN 101411117 A	15/04/2009
		CN 101411117 B	14/12/2011
		EP 2030364 A2	04/03/2009
		JP 04731624 B2	27/07/2011
		JP 2009-538082 A	29/10/2009
		TW 200810485 A	16/02/2008
		US 2011-0013771 A1	20/01/2011
		US 8341416 B2	25/12/2012
		WO 2007-135580 A2	29/11/2007
		WO 2007-135580 A3	24/01/2008
US 2011-0103589 A1	05/05/2011	CN 101286840 A	15/10/2008
		CN 101286840 B	30/07/2014
		EP 2282442 A1	09/02/2011
		WO 2009-143765 A1	03/12/2009
US 2012-0321077 A1	20/12/2012	CN 102843231 A	26/12/2012
		EP 2544400 A2	09/01/2013
		EP 2544400 A3	17/07/2013
		JP 2013-031151 A	07/02/2013
		KR 10-2012-0140224 A	28/12/2012
US 2005-0084114 A1	21/04/2005	DE 602004004029 D1	15/02/2007
		DE 602004004029 T2	15/11/2007
		EP 1526676 A1	27/04/2005
		EP 1526676 B1	03/01/2007
		KR 10-0571820 B1	17/04/2006
		KR 10-2005-0037723 A	25/04/2005
		US 7716482 B2	11/05/2010
US 2008-0008316 A1	10/01/2008	US 8175269 B2	08/05/2012

국제조사보고서		국제출원번호 PCT/KR2015/003576
A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 9/32(2006.01)i, H04L 9/30(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 9/32; H04L 9/08; G06F 11/30; G06F 21/20; H04L 9/00; H04L 9/30 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 인스턴트 공개키, 인스턴트 개인키, 전자서명, 검증, 인코딩, 디코딩		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2009-0017538 A (인터내셔널 비지네스 머신즈 코포레이션) 2009.02.18 단락 [0060]-[0162]; 및 도면 2-5 참조.	1,4,6-11,18-20
Y		2,3,5,12-17
Y	US 2011-0103589 A1 (MANXIA TIE 등) 2011.05.05 단락 [0073]-[0105]; 및 도면 5-7 참조.	2,3,12-17
Y	US 2012-0321077 A1 (SHIGEMASA SHIOTA 등) 2012.12.20 단락 [0185]-[0192]; 및 도면 18 참조.	5,17
A	US 2005-0084114 A1 (BAE-EUN JUNG 등) 2005.04.21 단락 [0018]-[0109]; 및 도면 1, 2 참조.	1-20
A	US 2008-0008316 A1 (DENIS PILIPCHUK) 2008.01.10 단락 [0020]-[0026]; 및 도면 1-5 참조.	1-20
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “B” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2015년 06월 26일 (26.06.2015)		국제조사보고서 발송일 2015년 06월 29일 (29.06.2015)
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-472-7140		심사관 김도원 전화번호 +82-42-481-5560

서식 PCT/ISA/210 (두 번째 용지) (2015년 1월)

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/003576

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0017538 A	2009/02/18	CN 101411117 A CN 101411117 B EP 2030364 A2 JP 04731624 B2 JP 2009-538082 A TW 200810485 A US 2011-0013771 A1 US 8341416 B2 WO 2007-135580 A2 WO 2007-135580 A3	2009/04/15 2011/12/14 2009/03/04 2011/07/27 2009/10/29 2008/02/16 2011/01/20 2012/12/25 2007/11/29 2008/01/24
US 2011-0103589 A1	2011/05/05	CN 101286840 A CN 101286840 B EP 2282442 A1 WO 2009-143765 A1	2008/10/15 2014/07/30 2011/02/09 2009/12/03
US 2012-0321077 A1	2012/12/20	CN 102843231 A EP 2544400 A2 EP 2544400 A3 JP 2013-031151 A KR 10-2012-0140224 A	2012/12/26 2013/01/09 2013/07/17 2013/02/07 2012/12/28
US 2005-0084114 A1	2005/04/21	DE 602004004029 D1 DE 602004004029 T2 EP 1526676 A1 EP 1526676 B1 KR 10-0571820 B1 KR 10-2005-0037723 A US 7716482 B2	2007/02/15 2007/11/15 2005/04/27 2007/01/03 2006/04/17 2005/04/25 2010/05/11
US 2008-0008316 A1	2008/01/10	US 8175269 B2	2012/05/08

서식 PCT/ISA/210 (대응특허 추가용지) (2015년 1월)

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ

(71)出願人 515276668

アイユーシーエフエイチワイユー (インダストリーユニバーシティ コーオペレーション ファウンデーション ハンヤン ユニバーシティ)

IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY)

大韓民国 133-791 ソウル ソンドング ワンシムニーロ 222

(74)代理人 100079049

弁理士 中島 淳

(74)代理人 100084995

弁理士 加藤 和詳

(72)発明者 キム、ドン ケ

大韓民国 ソウル 130-718 トンデムング ジュハンロー 14-ギル 81 ナンバー 105-2103 (ジャンガンードン サムスン ラミヤン 1 チャ アパート)

(72)発明者 チョイ、ビョン デク

大韓民国 ソウル 134-840 カントング オリピックロー 62-ギル 9-24

(72)発明者 キム、ドン ヒュン

大韓民国 ギョンギード 448-522 ヨンインーシ スジグ サンヒョンロー 25 ナンバー 176-1201 (サンギョン マウル サンギョン アパート)

(72)発明者 パク、サン セン

大韓民国 ギョンギード 463-751 ソンナムーシ ブンダング ブルジョンロー 179 ナンバー 208-102 (ジョンジャードン ジョンデン マウル ドンガ アパート)

Fターム(参考) 5J104 AA09 AA16 EA15 KA21 LA03 LA06 MA02 NA02 NA37