

(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2006-500814

(P2006-500814A)

(43) 公表日 平成18年1月5日(2006.1.5)

(51) Int. Cl.	F I	テーマコード (参考)
H04 L 9/08 (2006.01)	H04 L 9/00 G O I C	5 J 1 0 4
	H04 L 9/00 G O I E	

審査請求 未請求 予備審査請求 未請求 (全 11 頁)

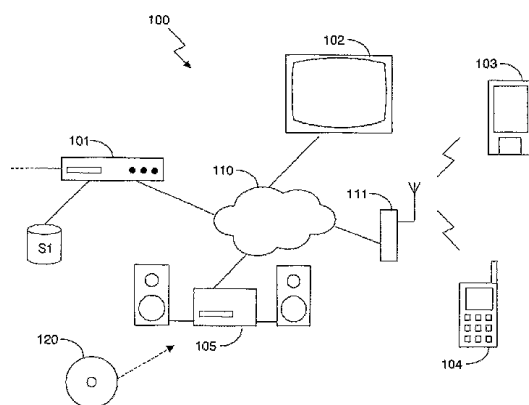
(21) 出願番号	特願2004-537385 (P2004-537385)	(71) 出願人	590000248
(86) (22) 出願日	平成15年8月11日 (2003. 8. 11)		コーニンクレッカ フィリップス エレク
(85) 翻訳文提出日	平成17年3月18日 (2005. 3. 18)		トロニクス エヌ ヴィ
(86) 国際出願番号	PCT/IB2003/003641		Koninklijke Philips
(87) 国際公開番号	W02004/028075		Electronics N. V.
(87) 国際公開日	平成16年4月1日 (2004. 4. 1)		オランダ国 5621 ペーアー アイン
(31) 優先権主張番号	02078952.5		ドーフエン フルーネヴァウツウェッハ
(32) 優先日	平成14年9月20日 (2002. 9. 20)		1
(33) 優先権主張国	欧州特許庁 (EP)		Groenewoudseweg 1, 5
			621 BA Eindhoven, T
			he Netherlands
		(74) 代理人	100070150
			弁理士 伊東 忠彦
		(74) 代理人	100091214
			弁理士 大貫 進介

最終頁に続く

(54) 【発明の名称】 共通の秘密鍵を生成する方法及びシステム

(57) 【要約】

第1のユーザ設備と第2のユーザ設備との間で共通の秘密データアイテムを生成する方法は、各ユーザ設備が、少なくとも部分的に秘密であるそれぞれ固有の量に基づくそれぞれ相補的なデータで相互に対称的な演算を実行することにより行われる。演算の結果は、前記共通の秘密データアイテムとして前記ユーザ設備の双方で使用される。特に、その方法は、Abelian Varietyに定められるGAP Diffie-Hellmann問題に属する前記相補的なデータを定めることに基づく。更に、Abelian Varietyは、楕円曲線を通じた1次元を有する



【特許請求の範囲】

【請求項 1】

各ユーザ設備により、少なくとも部分的に秘密であるそれぞれ固有の量に基づくそれぞれ相補的なデータで相互に対称的な演算を実行することを通じて、第 1 のユーザ設備 i と第 2 のユーザ設備 j との間で共通の秘密データアイテムを生成する方法であって、

前記演算の結果は、前記共通の秘密データアイテムとして前記ユーザ設備の双方で使用され、

前記方法は、Abelian Variety に定められる GAP Diffie-Hellmann 問題に属する前記相補的なデータを定めることに基づくことを特徴とする方法。

【請求項 2】

10

請求項 1 に記載の方法であって、

前記 Abelian Variety は、楕円曲線を通じた 1 次元を有する方法。

【請求項 3】

請求項 1 に記載の方法であって、

双一次特性と非縮退特性と計算可能特性とを特徴とするペア F を、前記 Abelian Variety の 2 つの線形独立のポイント P と D(P) に適用することを有する方法。

【請求項 4】

請求項 1 に記載の方法であって、

ユーザ設備 i の前記演算は、 $S_i = f_T(r_i)$ 及び $P_i = g(r_i)$ に従った一方向関数 f と g に基づき、パラメータ T は、信頼できるマスター設備から取得したマスター秘密であり、結果 S は秘密に保持され、共通の秘密データは、

$$K_{ij} = F(S_i, P_j) = F(S_j, P_i) = K_{ji}$$

に従って計算される方法。

【請求項 5】

請求項 4 に記載の方法であって、

前記演算は、データ S_i 及び P_i に基づき、

$$S_i : S_{i1} = T_{11} + r_i T_{12}; \quad (5')$$

$$S_{i2} = T_{21} + r_i T_{22}; \quad (6')$$

$$P_i : P_{i1} = r_i P; \quad (7')$$

$$P_{i2} = r_i^2 P; \quad (8')$$

30

である方法。

【請求項 6】

請求項 1 に記載の方法であって、

ユーザ設備 1 は、データ $r_1 D(P)$, $r_1^2 D(P)$ をユーザ設備 2 に送信し、

ユーザ設備 2 は、データ $r_2 D(P)$, $r_2^2 D(P)$ をユーザ設備 1 に送信し、

それに続いて、トリプル $r_2 D(P)$, $r_2 D(P)$, $r_2^2 D(P)$ が Diffie-Hellmann トリプルであるか否かをユーザ設備 1 が検査し、トリプル $r_1 D(P)$, $r_1 D(P)$, $r_1^2 D(P)$ が Diffie-Hellmann トリプルであるか否かをユーザ設備 2 が検査し、

肯定的な場合に、

$$\Pi_{k=1}^2 e((t_{k1} + r_1 t_{k2})P, v(r_2)_k D(P)) = e(P, D(P))^{<v(r_1), T v(r_2)>} \quad (40)$$

に従ってユーザ設備 1 による共有鍵を計算し、ここで、 $t_{12} = t_{21}$ であり、 $v(r_2)_k$ はベクトル $v(r_2)$ の第 k 成分を意味する方法。

【請求項 7】

請求項 1 に記載の方法であって、

固有のパラメータを各ユーザ設備に割り当てることを通じて、1 つ以上の選択されたユーザ設備を排除する標準的な機構の上に、取消機構を更に有する方法。

【請求項 8】

請求項 1 に記載の方法であって、

前記共有の秘密の生成が、識別又は認証手順の初期ステップとして使用される方法。

【請求項 9】

50

請求項 1 に記載の方法であって、
Weil Pairingは、真のプロトコルの実行の実質的に前にある時に求められる方法。

【請求項 1 0】

請求項 1 に記載の方法であって、
以前の秘密情報の漏洩に対して秘密情報を更新することを有する方法。

【請求項 1 1】

請求項 1 に記載の方法であって、
単一の統合した暗号化レベルのみを使用することを通じて実行される方法。

【請求項 1 2】

請求項 1 に記載の方法であって、
ランダム化機構が共通の秘密に適用される方法。

10

【請求項 1 3】

請求項 1 2 に記載の方法であって、
前記ランダム化機構は、チャレンジ・レスポンス型機構に基づく方法。

【請求項 1 4】

第 1 のユーザ設備と第 2 のユーザ設備とを有し、請求項 1 に記載の方法に従って通信するように構成されたシステム。

【請求項 1 5】

請求項 1 4 に記載のシステムの第 1 及び／又は第 2 のユーザ設備として動作するように構成された装置。

20

【請求項 1 6】

請求項 1 に記載の方法を実施するように 1 つ以上のデータ処理指向のハードウェアエンティティを制御する命令を有するコンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、各ユーザ設備により、少なくとも部分的に秘密であるそれぞれ固有の量に基づくそれぞれ相補的なデータで相互に対称的な演算を実行することを通じて、第 1 のユーザ設備と第 2 のユーザ設備との間で共通の秘密データアイテムを生成する方法に関するものであり、請求項 1 の preamble に更に記載されているように、前記演算の結果は、前記共通の秘密データアイテムとして前記ユーザ設備の双方で使用される。

30

【背景技術】

【0 0 0 2】

共有鍵の生成は、暗号化で重要な問題である。その問題は、家庭用電化製品の Pay TV システムや、多様な識別手順のような適用分野まで広がっている。秘密データアイテムは、ユーザ設備又はその他のものの間で相互の認証を実行する暗号鍵又は複号鍵として使用されることがある。従来技術は広く Diffie-Hellmann 機構を検討してきたが、不利なことに、その機構は計算された秘密データアイテムの信頼性を検査する制御機構を欠いている。代替として、共有秘密データアイテムの設定可能にする証明書に基づくシステムが、特に本発明の共同発明者の 1 人により本譲受人に譲渡された米国特許 5,218,637 (代理人管理番号 PHQ90.021) に提案されている。この技術は前記の問題を解決するが、他方で少なくとも 2 つのレベルの公開鍵の暗号化を利用する複雑な機構を必要とする。本発明の第 1 の目的は、単一の統合した暗号化レベルのみを使用することである。これは、確認動作を実行するために第 2 の秘密データアイテムが必要とされないことを意味する。

40

【0 0 0 3】

本発明の更なる目的は、本発明により実現される既存のシステムと同じレベルの秘密性を提供する特別のユーザ施設でシステムが拡張可能であるが、このような既存のシステムに更なる修正を必要としないことである。本発明の更にその他の目的は、ユーザ設備の任意の大量のサブセットに関する秘密データアイテムの認識が、システムに存在するその他のユーザ設備の各秘密データアイテムの簡単且つ実現可能な計算を可能にしないことであ

50

る。本発明の更なる目的は、使用される多様な量とデータアイテムのコンパクトな表示を可能にすることである。

【発明の開示】

【発明が解決しようとする課題】

【0004】

したがって、特に、前述の要件を満たしながら、2つのユーザ設備の間で共通の秘密データアイテムを生成する改善した方法を提供することが本発明の目的である。

【課題を解決するための手段】

【0005】

従って、その態様の1つによれば、本発明は、請求項1の特徴部分に従って特徴付けられる。特に、本発明の第1実施例は、Dan BonehとMatt Franklinによる“Identity Based Encryption from the Weil Pairing”という題のCRYPTO2001で提示された明確な論文に十分に説明されている、いわゆるWeil Pairingの使用に基づく。更に、本発明の第2実施例及び更に広い実施例は、いわゆるAbelian Varietiesの使用に基づき、Weil Pairingが実行される楕円曲線がサブクラスを構成する。しかし、前記の概念は、本発明と同じ動作方法と目的について検討されていない。Abelian Varietiesは、K.RubinとA.Silverbergによる“Supersingular Abelian Varieties in Cryptology”という題のCRYPTO2002で提示された明確な論文に十分に説明されている。本発明の更に有利な態様は、効果的に使用される簡単な数学手順のため、コンパクトな表示が可能になることである。

【0006】

本発明はまた、第1のユーザ設備と第2のユーザ設備とを有し、請求項1に記載の方法に従って通信するように構成されたシステムに関するものであり、請求項14に記載のシステムの第1及び／又は第2のユーザ設備として動作するように構成された装置に関するものであり、請求項1に記載の方法を実施するように1つ以上のデータ処理指向のハードウェアエンティティを制御するコンピュータ命令を有するコンピュータプログラム製品に関するものである。本発明の更に有利な態様が従属項に記載されている。

【発明を実施するための最良の形態】

【0007】

本発明の前記及び更なる態様と利点について、好ましい実施例の開示を参照して、特に添付図面を参照して以下に詳細に説明する。

【0008】

〔使用する手順の数学的な概略〕

本発明の基本的な実施例はWeil pairingに基づき、そのWeil pairingは楕円曲線から有限フィールドへの双一次マッピング(bilinear mapping)である。それは、楕円曲線のコンパクトな表示について有限フィールドでのDiscrete Log問題を表現するために使用される。この手順は、従来技術のものと同等又はそれより大きい計算の複雑性を備えた暗号解読を示し、そのような暗号解読を有効に実行不可能にする一方で、共有の秘密データアイテムと、200ビット未満の長さのビットを有することができる更なるパラメータとを使用することを可能にする。提案のシステムは、有限の数の関係者のデータの認識がシステムの秘密を明かさないという点で、更に非常に頑強である。そうでなければ、任意の従属のユーザで新しい共有鍵の生成が可能になる。

【0009】

更に、各ユーザ又は装置はその固有のパラメータを有し、その固有のパラメータにより、必要な場合に、選択された装置を排除する標準的な機構の上に、取消機構を設定することが可能になる。従って、そのシステムにより、従来のシステムよりかなり小さい記憶容量しか必要としない一方で、ユーザの如何なるペアの間で共有の秘密データアイテムを生成することが可能になる。

【0010】

次に、本実施例の提案プロトコルは、Diffie-Hellmann問題の拡張版に基づく。楕円曲

線Eについて、Computational Diffie-Hellmann(CDH)問題は以下のように見える。ポイント $P \in E$ と所定の aP と bP を仮定すると、多項式時間で abP を計算するアルゴリズムは存在しない。次に、本発明は、本発明に関しては以下のように定義付けられる拡張Diffie-Hellmann問題、すなわちEDHを適用する。

【0011】

$$P, aP, bP, a^2P, b^2P \rightarrow abP$$

明らかに、これは、計算について難解な問題を依然としてもたらす。ところで、楕円曲線のDecision Diffie Hellmann、すなわちDDH問題は、かなり簡単である。DDH問題は、 $P \in E$ であるつのポイント aP, bP, cP を仮定すると、 $cP = (a*b)P$ であるか否かを決定することにより定められる。この相対的な簡潔さは、Weil Pairingとして知られる効率的な計算可能双一次マッピングから得られる。そのWeil Pairingについては以下に詳細に説明する。更に、参照刊行物が追加情報を提供する。特に、DDHが相対的に簡単であるがCDHが難解であるようなグループは、GAP Diffie-Hellmanグループを示すと言われる。このようなグループはAbelian Varietiesに存在し、その特異な(supersingular)楕円曲線は、その1次元でのサブカテゴリである。Computational Diffie-Hellmann問題が難解であるがDDHが簡単であるような多様な実現可能な楕円曲線のうち、以下の例示的な実施例の曲線を使用する。

【0012】

$$E^+ : y^2 = x^3 + 2x + 1 \text{ over } F_3 l$$

$$E^- : y^2 = x^3 + 2x - 1 \text{ over } F_3 l$$

ここで、 $\langle P \rangle$ を、安全パラメータ α を備えたプライムオーダー(prime order) q の $E/F_p l$ のサブグループとする。このパラメータ α は、Computational Diffie-Hellmann問題CDHが十分に難解であるが、それと同時に、Decision Diffie-Hellmannの計算を非効率的に難解にしないように、十分に大きくなければならない。2つの例示的な曲線の上の安全パラメータは $\alpha=6$ である点に留意すべきである(Bonehを参照)。更に、ポイント $D(P) \in E/F_p l$ がポイント P と線形独立になるように、歪みマップ(distortion map) D 又はグループ同形(group isomorphism)の可用性を自由に仮定する。歪みマップは、主にE.Verheulによる刊行物“Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems”、EUROCRYPT2001に明確に説明されている。この歪みマップは、グループ $\langle P \rangle$ と $\langle D(P) \rangle$ とで効率的な計算可能同形(efficiently computable isomorphism)を構成する。この例の楕円曲線は、その多数の中から2つのみである点に留意すべきである。

【0013】

次に、2つの線形独立のポイント P と $D(P)$ で、ある問題を解決するためにWeil Pairingを使用することができる。 $E[q]$ を、 P と $D(P)$ により生成された $E/F_p l \alpha$ のサブグループを示すものとする。この場合、Weil Pairingは $e: E[q] \times E[q] \rightarrow F_p^*$ に従ったマップであり、以下の特性を満たす。

1. $P \in E[q]$ について、 $e(P, P) = 1$ を有する。
2. $P1, P2 \in E[q]$ と $r, s \in Z$ について、 $e(aP1, bP2) = e(P1, P2)^{a \cdot b}$ 、つまり、双一次特性を有する。
3. $P \in E[q]$ において、全ての $P' \in E[q]$ について $e(P, P') = 1$ を有する場合、 $P=0$ 、つまり、非縮退特性(non-degeneration property)である。
4. 全ての $P1, P2 \in E[q]$ について、Weil Pairing $e(P1, P2)$ が効率的に計算され得る。つまり、計算可能特性である。

【0014】

以下の機構が設定される。2つのユーザ設備のそれぞれは、信頼できる第三者機関から以下の秘密データアイテムを取得する。以下、そのアイテムがユーザ i について記載される(信頼できる機関は2つの共同動作するユーザ設備のうちの1つでもよい点に留意すべきである)。

【0015】

10

20

30

40

50

$$5. (t_{11} + r_i t_{12})P$$

$$6. (t_{12} + r_i t_{22})P$$

更に、以下の2つのデータアイテムも同様に提供される。

【0016】

$$7. r_i D(P)$$

$$8. r_i^2 D(P)$$

しかし、後者の2つのデータアイテムは必ずしも秘密に保持される必要はなく、そのため、後の参照のため、例えば公開ディレクトリに格納されてもよい。更に、以下の対称マトリクス $T(T_{12}=T_{21})$ が定められる。

【0017】

【数1】

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{12} & t_{22} \end{pmatrix} \in M_2(Z_q)$$

更に、 $v(r)=(1,r)$ のように、ポイント $r \in Z_q$ に関連付けられるベクトル $v(r)$ を導入する。その後、プロトコルは以下のように進む。

【0018】

最初に、ユーザ1がデータ $r_1 D(P), r_1^2 D(P)$ をユーザ2に送信し、更に、ユーザ2がデータ $r_2 D(P), r_2^2 D(P)$ をユーザ1に送信し、それに続いて、トリプル $r_2 D(P), r_2 D(P), r_2^2 D(P)$ が Diffie-Hellmann トリプルであるか否かをユーザ1が検査し、トリプル $r_1 D(P), r_1 D(P), r_1^2 D(P)$ が Diffie-Hellmann トリプルであるか否かをユーザ2が検査し、肯定的な場合に、双方が $\Pi_{i=1}^2 e((t_{i1} + r_1 t_{i2})P, v(r_2)_i D(P)) = e(P, D(P))^{\langle v(r_1), T v(r_2) \rangle}$ に従ってユーザ1による共有鍵、すなわち秘密の共通鍵を計算する。ここで、 $t_{12}=t_{21}$ であり、 $v(r_2)$ はベクトル $v(r_2)$ の第 i 成分を意味する。前記のプロトコルの安全性が高いことがわかる。実質的に、安全性は拡張 Diffie-Hellmann 問題が難解であることを見出すことにある。

【0019】

安全レベルを更に高める更なる措置は、タイムスタンプの適用と共に、生成した共有鍵のハッシュである。更に、共有の秘密を生成するプロトコルの生成は、この出願の同じ譲受人に割り当てられた欧州特許出願 02 075 983.3 (代理人管理番号 PHNL020192) に開示された識別手順の初期ステップとして使用され得る。

【0020】

更に、事前に Weil Pairing $e((t_{11} + r_1 t_{12})P, D(P))$ の計算を既に計算することにより、プロトコルがより効率的になり得る。これは、真のプロトコルの実行時にこの Weil Pairing の計算を行う必要性を回避するが、上昇する記憶装置の要件とのトレードオフになる。

【0021】

[好ましい実施例の詳細な説明]

図1は、ネットワークを介して相互接続され、本発明に従って動作するように構成されたシステム100を示している。一例として、このシステムはホームシステムであり、ラジオ受信機やテレビセット等のような装置を有してもよい。一般的に、特定の装置はシステムのマスターであり、他のものを制御する。一般的に、コンテンツは、ブロードバンドやインターネットや衛星のような外部ソースから、住宅用ゲートウェイ又はセットトップボックス101のような1つ以上の装置を通じて受信される。最終的に、コンテンツは、装置のうちの1つの適切な処理でネットワークを通じて転送される。

【0022】

一般的に、ホームネットワークの全ての装置は、実装の要件に従った安全のフレームワ

10

20

30

40

50

ークを実装する。このフレームワークを使用して、これらの装置は相互に認証し、安全な方法でコンテンツを配信する。真のコンテンツへのアクセスは、セキュリティシステムにより管理される。これにより、プロテクトされていないコンテンツが無許可の装置に漏れることを防止し、信頼のない装置から生じたデータがシステムに入ることを防止する。このようなプロテクションで、装置は、事前にうまく認証している他の装置にのみコンテンツを配信してもよい。このことにより、対抗者が不当な装置を通じて無許可のコピーを受信しないことを確保する。例えば、許可された製造者のみが認証の成功に必要な特定の秘密を認識しているため、装置は信頼できる第三者機関により発行された証明書を備えているため、ある装置は、許可された製造者により作られた場合にのみ、それ自体をうまく認証することができる。

10

【0023】

図2は、図1のシステムの一般化を示している。ここで、証明器Pと検証器Vと信頼できる第三者機関TTPが共同動作する。ここで、検証器Vは、信頼できる第三者機関TTPから受信した情報を使用して、証明器Pを認証しようとする。好ましくは、検証器Vが信頼できることを証明器Pが認識するように、認証は相互であるべきである。

【0024】

証明器Pに対して検証器Vを認証するために必要な情報は、TTPから関係者PとVに事前に配信されていると仮定する。これは、3つの関係者間の適切な通信設備で行われ得る。これはプロトコルを動的にし、対抗者が以前に配信された秘密に対して無許可のアクセスを取得しようとした場合に、情報の更新を可能にする。

20

【0025】

証明器Pと検証器Vは、必要な機能を備えるチップを備えた図1のキャリア120でもよく、更には音声再生装置105のような装置でもよい。このような場合、TTPから証明器Pと検証器Vへの通信チャネルが存在しない可能性が高い。そこで、秘密の配信は製造中のように事前に行われなければならない。

【0026】

証明器は、ネットワークモジュール301と、暗号化プロセッサ302と、記憶媒体303とを有する。ネットワークモジュール301を使用して、証明器Pは、検証器Vに対してデータを送受信することができる。ネットワークモジュール301は、図1のネットワーク110に接続されてもよく、また、検証器Vと無線のような直接接続を確立してもよい。

30

【0027】

暗号化プロセッサ302は、本発明による方法を実行するように構成される。通常は、このプロセッサ302はハードウェアとソフトウェアの組合せとして実現されるが、代替として、ソフトウェアモジュール又はオブジェクトの集合のように、完全にその一方で実現されてもよい。

【0028】

証明器Pは実行するアルゴリズムの多様なパラメータを記憶媒体に格納してもよいが、認証の成功の後に、検証器Vに配信するある程度のコンテンツを保持してもよい。記憶媒体303は、TTPから受信した情報を格納するために更に使用されてもよい。システムの安全性を高めるために、個々のパラメータのデータを格納するのではなく、その代わりに、又は代替として、1つ以上の中間計算結果が格納されてもよい。

40

【0029】

同様に、検証器Vは、証明器Pのものに対応する機能を備えたネットワークモジュール311と、暗号化プロセッサ312と、記憶設備313とを有する。検証器Vがディスク内チップ(Chip-in-Disc)を備えたキャリアとして具体化される場合、記憶設備313は、如何なる光ディスク又はその他のディスクに利用可能な記憶装置に対応してもよいが、ディスク内チップのROMに格納されることが好ましい。

【0030】

更に、証明器Pと検証器Vは、ハードウェア又はソフトウェアで実現され、暗号強度の強い擬似乱数を備えた擬似乱数生成器304,314を備えてもよい。この数は、本発明の多様な

50

好ましい用途で使用される。

【0031】

[補足の数学的説明]

前記では、共通の秘密鍵は、以下に従って行われている。

【0032】

$$K_{ij} = F(S_i, P_j) = F(S_j, P_i) K_{ji}$$

しかし、以下のデータが伝達される。

【0033】

$$S_i = f_T(r_i) \quad (5, 6)、及び$$

$$P_i = g(r_i) \quad (7, 8)$$

伝達されるデータアイテムのその他の表示は次に従う。

$$S_i \quad S_{i1} = T_{11} + r_i T_{12} \quad (5')$$

$$S_{i2} = T_{21} + r_i T_{22} \quad (6')$$

$$P_i \quad P_{i1} = r_i P \quad (7')$$

$$P_{i2} = r_i^2 P \quad (8')$$

ここで、 $T_{ij} = t_{ij} * P$ であり、数字は前の表示との対応を示す。

【図面の簡単な説明】

【0034】

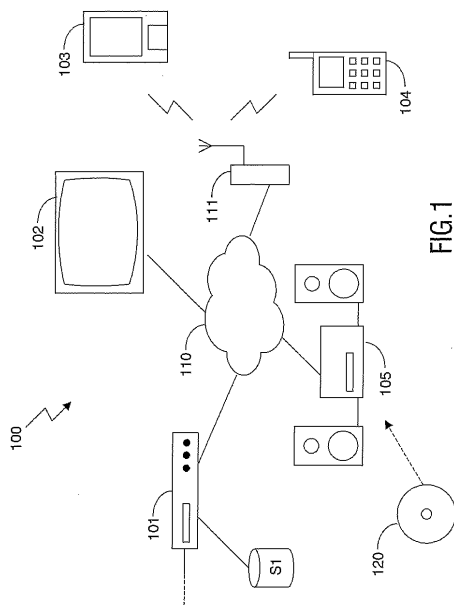
【図1】 ネットワークを介して相互接続され、本発明に従って動作するように構成された多様な装置を有するシステムである。

【図2】 図1のシステムの一般化である。

10

20

【図1】



【図2】

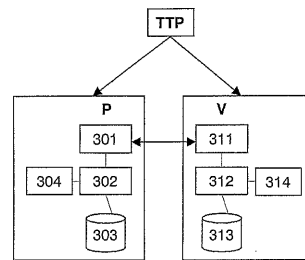


FIG.2

【国際調査報告】

INTERNATIONAL SEARCH REPORT		PCT/IB 03/03641
A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L9/30		
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) IPC 7 H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) INSPEC, WPI Data, PAJ, EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JOUX, A.: "A One Round Protocol for Tripartite Diffie-Hellman" LECTURE NOTES IN COMPUTER SCIENCE, vol. 1838, 2000, pages 385-393, XP008026749 page 387, line 1 - page 388, line 10 page 392, line 11 - line 25 --- -/--	1-3,7-16
☒ Further documents are listed in the continuation of box C. ☐ Patent family members are listed in 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 document 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		Date of mailing of the international search report
28 January 2004		13/02/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2250 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Liebhardt, I

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03641

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RUBIN K ET AL: "Supersingular abelian varieties in cryptology", ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2442), ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA , 2002, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 336 - 353 XP002268384 ISBN: 3-540-44050-X cited in the application page 336, line 1 -page 337, last line -----	1-16
A	VERHEUL E R: "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", ADVANCES IN CRYPTOLOGY - EUROCRYPT 2001. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2045), ADVANCES IN CRYPTOLOGY - EUROCRYPT 2001, INNSBRUCK, AUSTRIA, 6-10 M , 2001, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 195 - 210 XP002268385 ISBN: 3-540-42070-3 cited in the application the whole document -----	1-16

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA, GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ, EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,M W,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA ,ZM,ZW

(74)代理人 100107766

弁理士 伊東 忠重

(74)代理人 100135105

弁理士 渡邊 直満

(72)発明者 テュイルス, ピム テー

オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 ファン デイク, マールテン エー

オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 スフーンマケルス, ベリィ

オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

Fターム(参考) 5J104 EA23 EA29 NA16