世界知的所有権機関
国際事務局

PCT 特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 H04L 9/08	A1	(11) 国際公開番号	WO97/31449
		(43) 国際公開日	1997年8月28日(28.08.97)

(21) 国際出願番号 PCT/JP97/00433

(22) 国際出願日 1997年2月19日(19.02.97)

(30) 優先権データ

特願平8/70832	1996年2月21日(21.02.96)	JP
特願平8/70835	1996年2月21日(21.02.96)	JP
特願平8/210376	1996年7月8日(08.07.96)	JP

(81) 指定国 AU, BG, BR, CA, CN, CU, CZ, HU, IL, KR, LT, MX, NO, NZ, PL, RO, RU, SG, SK, TR, UA, VN.

添付公開書類
国際調査報告書

(71) 出願人
カード・コール・サービス株式会社
(CARD CALL SERVICE CO., LTD.)[JP/JP]
〒150 東京都渋谷区道玄坂1丁目22番7号 Tokyo, (JP)
(72) 発明者
馬場芳美(BABA, Yoshimi)
〒273 千葉県船橋市宮本8丁目10番3号 Chiba, (JP)
(74) 代理人
弁理士 佐藤辰彦, 外(SATO, Tatsuhiko et al.)
〒151 東京都渋谷区代々木2丁目1番1号
新宿マインズタワー16階 Tokyo, (JP)

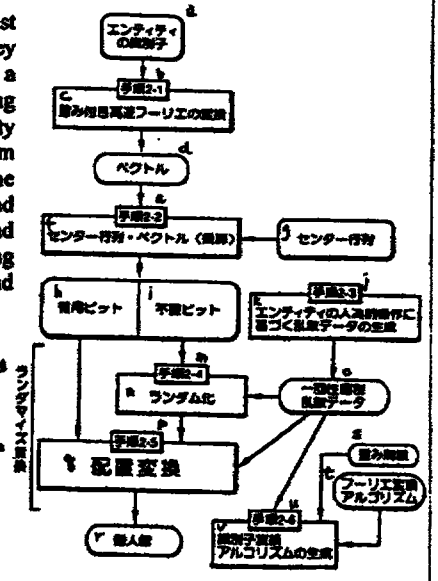
(54)Title: COMMUNICATION METHOD USING COMMON CRYPTOGRAPHIC KEY

(54)発明の名称 暗号鍵共有方法

(57) Abstract

A communication method using a common cryptographic key by which security against various kinds of attacks can be improved while the preparation of a common cryptographic key prepared at the time of performing communication or a cryptographic communication system on a network is simplified. At a center, a personal key peculiar to each entity is prepared by applying Fourier transformation with weight function and center matrix to the identifier of each entity (procedures 2-1 and 2-2) and performing randomized transformation based on one-time random number data prepared by artificial processing of the entities (procedures 2-3 to 2-5) and, at the same time, an identifier converting algorithm is prepared based on the random number data and Fourier transformation with weight function (procedure 2-6) and distributes the algorithm and personal keys to the entities. Each entity prepares a common key used for performing cryptographic communication with a partner by applying the identifier converting algorithm and personal key to the identifier of the partner.

a ... identifier of entity
b ... procedure 2-1
c ... weighted fast Fourier transformation
d ... vector
e ... procedure 2-2
f ... center matrix and vector (multiplication)
g ... center matrix
h ... significant bit
i ... unnecessary bit
j ... procedure 2-3
k ... preparation of random number data based on artificial operation of entity
l ... randomizing conversion
m ... procedure 2-4
n ... randomization
o ... individual one-time random number data
p ... procedure 2-5
q ... rearrangement
r ... personal key
s ... weight function
t ... Fourier transformation algorithm
u ... procedure 2-6
v ... preparation of identifier converting algorithm



（５７）要約

通信に際しての共通の暗号鍵の生成やネットワーク上の暗号通信システムの簡素化を図りつつ、種々の攻撃に対する安全性を高めることができる暗号鍵共有方法を提供する。センターにおいて、各エンティティの識別子に、重み関数付きフーリエ変換及びセンター行列を作用させ（手順２－１，２－２）、さらにそのエンティティの人為的操作により生成した一回性の乱数データに基づくランダマイズ変換を施すことによって、各エンティティに固有の個人鍵を生成する（手順２－３～５）と共に、上記乱数データ及び重み関数付きフーリエ変換に基づき識別子変換アルゴリムを生成し（手順２－６）、このアルゴリズム及び個人鍵をエンティティに配付する。各エンティティは通信相手側の識別子に識別子変換アルゴリム及び個人鍵を作用させることで通信相手側との暗号通信のための共通鍵を生成する。

情報としての用途のみ
ＰＣＴに基づいて公開される国際出願をパンフレット第一頁にＰＣＴ加盟国を同定するために使用されるコード

AL	アルバニア	ES	エストニア	LR	リベリア	RU	ロシア連邦
AM	アルメニア	FI	フィンランド	LS	レソト	SD	スーダン
AT	オーストリア	FR	フランス	LT	リトアニア	SE	スウェーデン
AU	オーストラリア	GA	ガボン	LU	ルクセンブルグ	SG	シンガポール
AZ	アゼルバイジャン	GB	英国	LV	ラトヴィア	SI	スロヴェニア
BB	バルバドス	GE	グルジア	MC	モナコ	SK	スロヴァキア共和国
BE	ベルギー	GH	ガーナ	MD	モルドバ	SL	シエラレオネ
BF	ブルキナ・ファソ	GN	ギニア	MG	マダガスカル	SN	セネガル
BG	ブルガリア	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	SZ	スワジランド
BJ	ベナン	HU	ハンガリー	ML	マリ	TD	チャード
BR	ブラジル	IE	アイルランド	MN	モンゴル	TG	トーゴ
BY	ベラルーシ	IL	イスラエル	MR	モーリタニア	TJ	タジキスタン
CA	カナダ	IS	アイスランド	MW	マラウイ	TM	トルクメニスタン
CF	中央アフリカ共和国	IT	イタリー	MX	メキシコ	TT	トリニダード・トバゴ
CG	コンゴー	JP	日本	NE	ニジェール	UA	ウクライナ
CH	スイス	KE	ケニア	NL	オランダ	UG	ウガンダ
CI	コート・ジボアール	KG	キルギスタン	NO	ノルウェー	US	米国
CM	カメルーン	KP	朝鮮民主主義人民共和国	NZ	ニュージーランド	UZ	ウズベキスタン共和国
CN	中国	KR	大韓民国	PL	ポーランド	VN	ヴィエトナム
CS	チェッコ共和国	KZ	カザフスタン	PT	ポルトガル	YU	ユーゴスラビア
CZ	チェッコ	LC	セントルシア	RO	ルーマニア		
DE	ドイツ	LI	リヒテンシュタイン				
DK	デンマーク	LK	スリランカ				