Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2341689 C 2010/05/25

(11)(21) 2 341 689

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2000/07/06
(87) Date publication PCT/PCT Publication Date: 2001/02/01
(45) Date de délivrance/Issue Date: 2010/05/25
(85) Entrée phase nationale/National Entry: 2001/02/26
(86) N° demande PCT/PCT Application No.: EP 2000/006388
(87) N° publication PCT/PCT Publication No.: 2001/008349
(30) Priorité/Priority: 1999/07/27 (DE199 35 286.0)

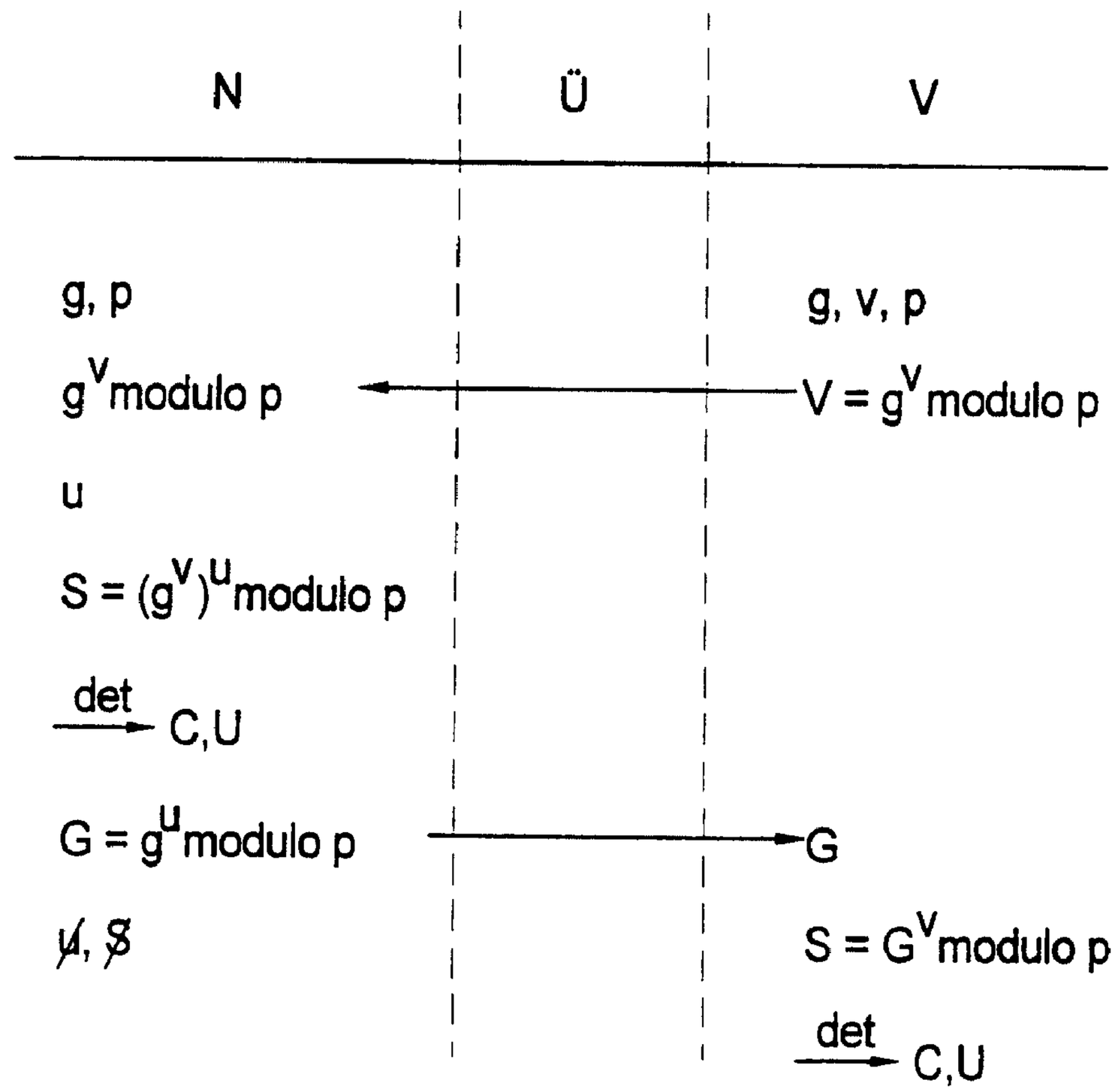
(51) Cl.Int./Int.Cl. *H04L 9/30* (2006.01),
H04L 9/08 (2006.01)

(72) Inventeur/Inventor:
SCHWENK, JORG, DE

(73) Propriétaire/Owner:
DEUTSCHE TELEKOM AG, DE

(74) Agent: FETHERSTONHAUGH & CO.

(54) Titre : PROCEDE DE GENERATION REPARTIE SECURITAIRE D'UNE CLE DE CODAGE
(54) Title: METHOD FOR THE SECURE, DISTRIBUTED GENERATION OF AN ENCRYPTION KEY



(57) Abrégé/Abstract:
In a method for the secure, distributed generation of an encryption key for a cryptographic method, where the encryption key, as well as a public key are generated using deterministic methods from a large random number (seed), the seed (S) is generated on

CA 2341689 C 2010/05/25

(11)(21) 2 341 689

(13) C

(57) Abrégé(suite)/Abstract(continued):
the user side by consulting variables known only to the user, and a public key (V) that is transmitted in advance from the trust center. Generation information suitable for generating the seed and, on the basis of which, the seed is able to be derived deterministically from the trust center, by consulting information known only to the center, is produced on the user side, and transmitted to the trust center to create the seed in parallel.

Abstract

In a method for the secure, distributed generation of an encryption key for a cryptographic method, where the encryption key, as well as a public key are generated using deterministic methods from a large random number (seed), the seed (S) is generated on the user side by consulting variables known only to the user, and a public key (V) that is transmitted in advance from the trust center. Generation information suitable for generating the seed and, on the basis of which, the seed is able to be derived deterministically from the trust center, by consulting information known only to the center, is produced on the user side, and transmitted to the trust center to create the seed in parallel.

28030-79

METHOD FOR THE SECURE, DISTRIBUTED GENERATION OF AN ENCRYPTION KEY

Field of the Invention

The present invention is directed to a method for the secure, distributed generation of an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using deterministic methods from a large random number (seed).

Background Information

To secure communications data and stored data, it is becoming increasingly prevalent to use the cryptographic technique of encryption. In this context, the data are enciphered under the control of a cryptographic key. The data can also be deciphered again using the same key. Marketable products and software libraries are available for this purpose.

In encryption operations, a so-called hybrid method is mostly used. In this method, the actual message is encrypted using a randomly selected symmetric key (session key) and a preselected symmetric encryption method (e.g., Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA)). The session key is then encrypted, in turn, in each case using the public key of the receiver (a plurality of receivers is possible) and using a predefined asymmetric or public key method (e.g., Rivest, Shamir, Aldeman Code(RSA), EIGamal (a public key encryption algorithm)). The session key encrypted using this process is included with the encrypted message for each receiver. A description of this procedure and of the algorithms

employed is found, for example, in William Stallings: "Cryptography and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998.

To decode a message, the receiver must first decipher the session key using his private key, which belongs to his public key, and a preselected public key algorithm, to then decrypt the message using this session key.

Besides encrypting messages, cryptographic methods are also used to encrypt stored data, e.g., on one's own personal computer. Here as well, one typically employs a hybrid method, where the user first encrypts the data using a randomly selected symmetric key (session key) and a predefined symmetric encryption method (e.g., DES, IDEA). The session key is then encrypted, in turn, using the user's public key and a preselected asymmetric or public key method (e.g., RSA, EIGamal).

Using his or her private key, which belongs to his or her public key, and a predefined public key algorithm, the user first encrypts the session key and then, a using this session key, the stored data.

In the following, the term "encryption key" is used in each case to refer to the private key of the user, i.e., of the receiver.

The encryption key is either stored on a smart card, access to the smart card being protected by a personal identification number (PIN) known only to the user, or it is stored on another storage medium (for example a hard disk or diskette), in which case it is protected preferably by a long password.

It can happen that the encryption key is lost. For

example, if the storage medium where it was located is destroyed, or if the user forgets the PIN number or the password which he or she used to secure the encryption key, then it is no longer possible to use it to access the encrypted data.

To be able to make encrypted data accessible again in the event the encryption key is lost, mechanisms are needed to enable the encryption key to be regenerated in a secure manner. For this purpose, the encryptior key is typically generated nowadays at a trust center or a confidential central location and securely stored. As a rule, the encryption key is produced by initially generating a large random number (seed) using a statistically valid random process. From this random number, the key pair made up of the public key/private key is then generated with the aid of a deterministic method. This seed is subsequently deleted. If necessary, a copy of his or her encryption key is then delivered to the user for use.

In the process, the user does not have any influence on how his or her encryption key is generated and further handled by the generator. It is expensive to securely transport the copy of the encryption key to the user. As a transport medium, the smart card mentioned above can be used, for example, which is sent to the user.

28030-79

Summary of the Invention

Some embodiments of the present invention provide a method of the type mentioned at the outset which can solve one or more of the aforementioned problems.

Some embodiments of the present invention provide a method eliminating the need to provide an expensive, secure transport of the encryption key to the user.

In accordance with one aspect of the present invention, there is provided a method for the secure, distributed generation of an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using deterministic methods from a large random number (seed), the method comprising: generating the seed (S) on a user side by consulting variables known only to a user, and a public key (V) that is transmitted in advance from a trust center; and producing generation information on the user side (G) which is suitable for generating the seed and, on the basis of which, the seed is able to be derived deterministically from the trust center by consulting information known only to the center, and transmitting the generation information to the trust center to create the seed in parallel.

In this manner, the seed can be created in parallel, both by involving the user, as well as the trust center, without third parties being able to reconstruct the seed from possibly eavesdropped information. The user's private encryption key and his public key U can be derived from this seed using deterministic, generally known methods. Thus, the user is able to create his key himself from this seed, thereby eliminating the need for transporting the encryption key.

In some embodiments, the method as recited herein, wherein said variables known only to a user comprise a random number u and said information known only to the center comprises a secret key v, the method further comprising: employing a key agreement mapping k: k(x,y)=z, where x, y are parameters of the mapping k and z is the result of the key agreement mapping for which it holds that: a) k (k (u, v) , w) = k (k (u, w) , v) for all u, v, w; b) from the

knowledge of u and k(u,v), in practice, one cannot infer v; c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v); that a public parameter g known to the trust center and the secret key v available at the trust center are linked to the public key V=k(g,v) of the trust center; that the public key V and the random number u selected on the user side are linked on the user side to the seed S=k(V,u); that a key pair made up of encryption key C and public user key U is derived from seed S on the user side using a predefined deterministic method; that to enable seed S to be created, generation information G=k(g,u) is generated on the user side and transmitted to the trust center; and that seed S is generated in parallel on the part of the trust center by S=k(G,v).

Once information G is generated, the user should again destroy random number u and seed S for security reasons. Information G is generated on the user side under tap-proof conditions, for example within the user-side computer terminal, so that there is no chance of random number u or of seed S falling into the hands of the public. Without knowledge of secret key v, generation information G, by itself, may not be suitable for creating the seed and, therefore, does not need to be kept secret.

For that reason, generation information G can be sent over any tappable route (e-mail, WWW, ftp, ...) to the trust center.

Due to the property of the mapping k used, it holds that $k(G,v) = k(k(g,u),v) = k(k(g,v),u) = k(V,u) = S$, which effectively corresponds again to original seed S. Since the deterministic method, v and p, are known to the trust center, encryption key C can be readily reproduced by the trust center with the aid of generation information G, without knowledge of random number u. Encryption key C generated in parallel at the trust center can be stored there so as to be secure against tapping.

Examples of suitable key agreement mappings k are known from the theory of numbers. Provision can be made, for example, for key agreement mapping k to be a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and for public parameter g to be an

element of a mathematical field GF(p) of a high multiplicative power, or for key agreement mapping k to be the multiplication on an elliptic curve. In practice, one should select the order of magnitude of the numbers used such that, even by summoning up modern technical means, it is impossible to calculate value y from values x and k(x,y), which, presupposing today's deciphering technology, is ensured at orders of magnitude of the prime numbers used of between 500 and 1000 bits.

One can find a description of such functions in William Stallings: "Cryptography and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998. The present invention makes use of the Diffie-Hellman key exchange principle, which is likewise described in the mentioned work. The method of the present invention presupposes a trust center, which, if needed, can regenerate the encryption key with the aid of regeneration information R.

A further refinement of the method according to the present invention provides that the trust center selects a specific secret key vu for each user, that on the part of the trust center, instead of the general public key V, a user-specific key Vu=k(g,vu) is generated and transmitted to the user to enable him to generate his key pair C and U. The user-specific secret key vu can, as can the general secret key v as well, be a statistically valid random number.

To ensure the functional reliability of the method, a next further refinement of the method of the present invention provides that the trust center does not transmit the information Vu needed by the user to create seed (S) until it has received generation information G. This ensures that the trust center receives the generation information.

In yet another embodiment of the method, it is provided for there to be a plurality of trust centers which use key agreement mapping k and public parameter g. The user selects one or more of these trust centers, and with each of these, implements the method of the present invention, recovering each time a different portion Sv of seed S. To generate encryption key C, partial values Sv of seed S calculated by the trust centers are linked on the user side to the entire seed S. To create the entire seed S in parallel on the part of the trust centers, the selected trust centers must cooperate. Only by acting jointly can they generate seed S and, thus, encryption key C. This procedure can prevent encryption key C from being misused by an individual trust center or can prevent secret information from becoming known due to possible malfunctions at a trust center.

Another embodiment of the method provides for the various trust centers to use different functions kv and different public parameters gv. In this case, the user must carry out the method in accordance with the present invention for each trust center, and a different generation information Gv must be generated for each trust center.

Brief Description of the Drawing

The Figure shows an embodiment of the present invention.

Detailed Description

The Figure shows a diagram of the operations necessary for generating a reconstructible, user-specific seed S in parallel, as well as a key pair made up of encryption key C and public user key U in accordance with the method of the present invention. The user-side data occurring in succession are listed from top to bottom in the column designated by N. Ü denotes the data transmission link to

a trust center V. Trust center V and user N have at their disposal public parameter g and large prime number p. Public key $V = g^v$ modulo p is generated by trust center V and transmitted by simple channels to user N. Using a random number u that he selects, the user then generates a seed S and generation information G, and deletes random number u again for security reasons. Generation information G is transmitted to trust center V. By applying a predefined deterministic method known equally to the user and the trust center, a public user key U, as well as a private, likewise user-specific encryption key C are generated from seed S. Here, encryption key C is used to decrypt messages or user data.

28030-79

CLAIMS:

1. A method for the secure, distributed generation of an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using deterministic methods from a large random number (seed), the method comprising:

generating the seed (S) on a user side by consulting variables known only to a user, and a public key (V) that is transmitted in advance from a trust center; and

producing generation information on the user side (G) which is suitable for generating the seed and, on the basis of which, the seed is able to be derived deterministically from the trust center by consulting information known only to the center, and transmitting the generation information to the trust center to create the seed in parallel.

2. The method as recited in claim 1, wherein said variables known only to a user comprise a random number u and said information known only to the center comprises a secret key v, the method further comprising:

employing a key agreement mapping k: k(x,y)=z, where x, y are parameters of the mapping k and z is the result of the key agreement mapping for which it holds that:

a) k (k (u, v) , w) = k (k (u, w) , v) for all u, v, w;

b) from the knowledge of u and k(u,v), in practice, one cannot infer v;

c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v);

that a public parameter g known to the trust center and the secret key v available at the trust center are linked to the public key V=k(g,v) of the trust center;

that the public key V and the random number u selected on the user side are linked on the user side to the seed S=k(V,u);

that a key pair made up of encryption key C and public user key U is derived from seed S on the user side using a predefined deterministic method;

that to enable seed S to be created, generation information G=k(g,u) is generated on the user side and transmitted to the trust center; and that seed S is generated in parallel on the part of the trust center by S=k(G,v).

3. The method as recited in claim 2 wherein key agreement mapping k is a discrete exponential function modulo a large prime number p: $k(x,y) := x^Y$ modulo p, and that the public parameter g is an element of a mathematical field GF(p) of a high multiplicative power.

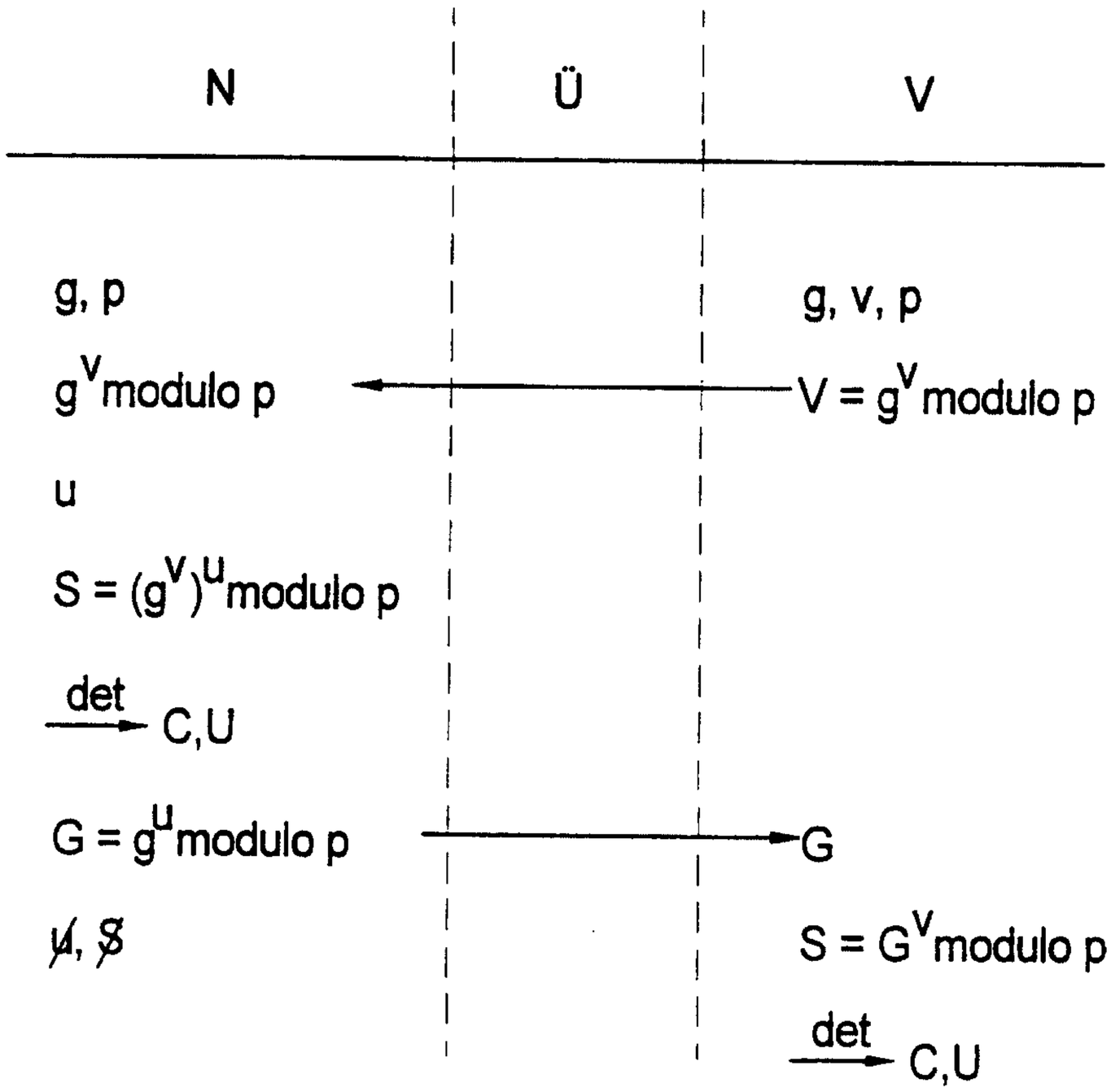
4. The method as recited in claim 2 wherein the key agreement mapping k is a multiplication on an elliptic curve.

5. The method as recited in one of the claims 2 to 4 further comprising the trust center selecting a specific secret key vu for each user, that on the part of the trust center, instead of a general public key V, a user-specific key Vu=k(g,vu) is generated and transmitted to the user to enable him to generate his key pair C and U.

6. The method as recited in claim 5, characterized in that the trust center does not transmit the information Vu needed by the user to create seed (S) until it has received generation information G.

7. The method as recited in one of the claims 2 to 6, characterized in that there is a plurality of trust centers which use the key agreement mapping k and the public parameter g, the user selects one or more of these trust centers, and with each of these, implements the method of the present invention, recovering each time a different portion Sv of seed S, to generate encryption key C, partial values Sv of seed S calculated by the trust centers are linked on the user side to the entire seed S.

8. The method as recited in claim 7, characterized in that the various trust centers use different functions kv and different public parameters gv.


N
Ü
V
g, p
g, v, p
g^v modulo p
V = g^v modulo p
u
S = (g^v)^u modulo p
det
C,U
G = g^u modulo p
G
S = G^v modulo p
det
C,U

N | Ü | V

g, p

g^v modulo p

u

$S = (g^v)^u$ modulo p

det → C, U

$G = g^u$ modulo p

μ, σ

g, v, p

$V = g^v$ modulo p

G

$S = G^v$ modulo p

det → C, U