

41 39 A

ESTADOS UNIDOS DE AMÉRICA

A TODOS A QUIENES LLEGUE EL PRESENTE:

DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS

Oficina de Marcas y Patentes

29 de marzo de 2000.

LA PRESENTE CERTIFICA QUE LA ADJUNTA ES UNA COPIA TOMADA DE LOS REGISTROS DE LA OFICINA DE MARCAS Y PATENTES DE LOS ESTADOS UNIDOS, DE LOS DOCUMENTOS DE LA SOLICITUD DE PATENTE ABAJO IDENTIFICADA Y LA CUAL CUMPLE CON LOS REQUISITOS PARA QUE LE SEA CONFERIDA UNA FECHA DE RADICACIÓN SEGÚN 35 USC 111.

NÚMERO DE SOLICITUD 60/130,944

FECHA DE RADICACIÓN: 26 de abril de 1999

Por Autoridad del

COMISIONADO DE MARCAS Y PATENTES

(FIRMA) N. WOODSON

Oficial de Certificaciones

(SELLO DORADO DE OBLEA)

* * * *

No. 0033250-3

Estados Unidos de América
DEPARTAMENTO DE ESTADO

A todos a Quienes Llegue el Presente, Os Saludo:

Certifico que el documento adjunto se encuentra bajo el sello de la Oficina de Marcas y Patentes del Departamento de Comercio de los Estados Unidos de América y que a dicho sello debe dársele plena fe y crédito.

En Testimonio de lo cual, Yo, Madeleine K. Albright, Secretaria de Estado, he ordenado al Oficial de Autenticaciones suscribir mi nombre y colocar el sello del Departamento de Estado en la Ciudad de Washington, Distrito de Columbia, hoy 5 de abril de 2000.

Madeleine K. Albright - Seecretaria de Estado
Patrick O. Harchett - Asistente del Oficial de
Autenticaciones. Departamento de Estado

EN ESPAÑOL: La legalización de la firma y cargo anterior por parte del Consulado de Colombia en Washington, D.C. de fecha 5 de abril de 2000, bajo el No. 857.

CUBIERTA DE SOLICITUD PROVISIONAL DE PATENTE

Esta es una solicitud de radicación de SOLICITUD PROVISIONAL DE PATENTE

Bajo 37 CFR 1.53(c)

Caso No.		040070-986	Escriba un signo (+) +	
INVENTOR(ES) SOLICITANTE(S)				
Apellidos	Nombre	Inicial	Dirección	
SMEETS	Ben			
HANSSON	Mattias			
TITULO DE LA INVENCION (máx 280 caracteres)				
METODO Y DISPOSITIVO PARA CONTROL EFECTIVO DE LONGITUD DE CLAVE.				
DIRECCION PARA CORRESPONDENCIA				
Ronald L. Grudziecki BURNS, DOANE, SWECKER & MATHIS, L.L.P P.O. Box 1404 Alexandria				
ESTADO	VIRGINIA	ZIP CODE	22313-1404	PAIS EE.UU.
PARTE(S) ADJUNTA(S) DE LA SOLICITUD (verifique que todas apliquen)				
☒	Especificación	455	No. de páginas	
☒	Dibujos	1	No. de hojas	
METODO DE PAGO (marcar uno)				
☐	Cheque u orden de dinero	No. de páginas		
☒	El Comisionado Asistente está autorizado Para cobrar comisión y crédito Cuenta No.	02-4800	COMISION PROVISIONAL	150.00

La invención fue hecha por una agencia del Gobierno de los Estados Unidos o bajo un contrato con una agencia del Gobierno de los Estados Unidos.

☒ NO

FIRMA STEVEN M. duBois

FECHA : 26 de abril de 1999

REGISTRO NO. 35,023

[X] Nombres de inventores adicionales en la página adjunta

90 44

[Handwritten signature]

INVENTOR(ES) ADICIONALES(S)			
Apellidos	Nombre	Inicial	Dirección
PERSSON	Joakim		



CONSULADO DE COLOMBIA
WASHINGTON, D.C.

46
41
WASHINGTON D.C.
[Signature]

No. 857

EL CONSULADO DE COLOMBIA

CERTIFICA:

Que es auténtica la firma de PATRICK O. HATCHETT.
quien el día 5 DE ABRIL DEL 2000.
desempeñaba las funciones de OFICIAL DE AUTENTICACIONES DEPARTAMENTO DE ESTADO.
la cual aparece al pie de los documentos anexos relacionados con APLICACION PARA PATENTE.

Dado en Washington, D.C. a los CINCO (5) días del mes de
ABRIL. del año dos mil (2000)

Pagado Impuesto de Timbre 7=

Pagado Derecho Consular 15=

Total 22=

[Signature]
JAQUELINE ESPITIA ARIAS
Vicecónsul

(El Consulado no asume ninguna
responsabilidad por el contenido de los
documentos anexos)

United States of America



DEPARTMENT OF STATE

To all to whom these presents shall come, Greetings:



I Certify That the document hereunto annexed is under the Seal of the Patent and Trademark Office, Department of Commerce, United States of America, and that such Seal is entitled to full faith and credit.*

In testimony whereof, I, Madeleine K. Albright, Secretary of State, have hereunto caused the seal of the Department of State to be affixed and my name subscribed by the Assistant Authentication Officer, of the said Department, at the city of Washington, in the District of Columbia, this fifth day of April, 2000.

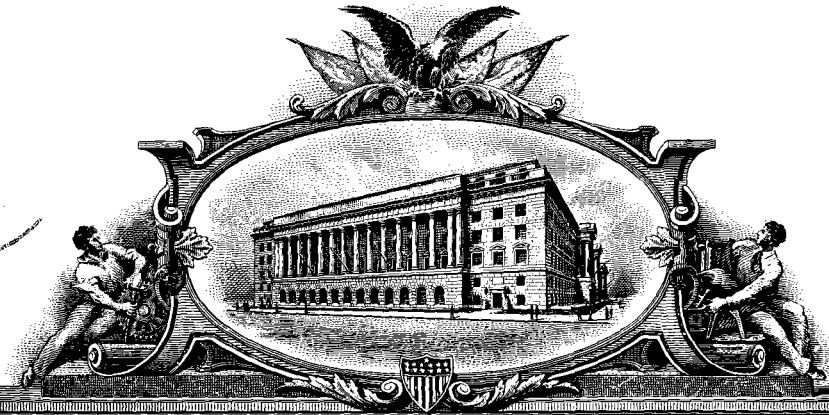
Madeleine K. Albright
Secretary of State
By Paul J. Hannon
Assistant Authentication Officer,
Department of State

*Issued pursuant to CHXIV, State of
Sept. 15, 1789, 1 Stat. 68-69; 22
USC 2657; 22USC 2651a; 5 USC
301; 28 USE 1733 et. seq.; 8 USC
1443(f); RULE 44 Federal Rules of
Civil Procedure.*

***For the contents of the annexed document, the Department assumes no responsibility**

This certificate is not valid if it is removed or altered in any way whatsoever

PA 224990



42
A
43

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 29, 2000

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 60/130,944

FILING DATE: April 26, 1999



**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**

N. WOODSON

Certifying Officer

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Docket Number		040070-986		Type a plus sign (+) inside this box		+	
INVENTOR(s)/APPLICANT(s)							
LAST NAME		FIRST NAME		MIDDLE INITIAL		RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)	
SMEETS		Ben					
HANSSON		Mattias					
TITLE OF THE INVENTION (280 characters max)							
METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL							
CORRESPONDENCE ADDRESS							
Ronald L. Grudziecki BURNS, DOANE, SWECKER & MATHIS, L.L.P. P.O. Box 1404 Alexandria,							
STATE		Virginia		ZIP CODE		22313-1404	
				COUNTRY		United States of America	
ENCLOSED APPLICATION PARTS (check all that apply)							
☒ Specification		Number of Pages		4		☐ Small Entity Statement	
☒ Drawing(s)		Number of Sheets		1		☐ Other (specify)	
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)							
☒ A check or money order is enclosed to cover the Provisional filing fees				PROVISIONAL FILING FEE AMOUNT(S)		\$ ☐ \$75.00	
☒ The Commissioner is hereby authorized to charge any deficiency in filing fees or credit any overpayment to Deposit Account Number 02-4800. This paper is submitted in triplicate.						\$ ☒ \$150.00	

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE

Date April 26, 1999

TYPED or PRINTED NAME Steven M. duBois

Registration No. 35,023
(if appropriate)

☒ Additional inventors are being named on separately numbered sheets attached hereto

ADDITIONAL INVENTOR(s)/APPLICANT(s)			
LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
PERSSON	Joakim		

659240"4460

SO. 46
X

Invention Disclosure:

Method and device for effective key length control

60130344.042659

ST 47 10

1 **NAME OF INVENTION**
Method and device for effective key length control

2 **INVENTOR(S)**
Ben Smeets
Mattias Hansson
Joakim Persson

3 **BACKGROUND**

Export regulations of encryption software and hardware differ among countries. On the other hand standardised systems should be able to support the best (longest) ciphering key that is possible. The proposed method provides an interface between the ciphering key generator in a communication system and the ciphering device that provides a controllable and secure way of limiting the effective key length. The proposed method has the additional benefit that the remaining randomness in the reduced key is spread evenly over all possible input combinations of the ciphering device. Furthermore, the method can be easily implemented in hardware as well as software. Fig 1 shows a shift register implementation that computes the desired output in 128 clock cycles after the register has been loaded with the (unreduced) ciphering key.

659210-11506709

Many communication systems are flexible when it comes to the key length of the encryption key. In principle, any key length between 1 and 16 bytes (8 to 128 bits) can be used. To facilitate a specific baseband implementation to restrict the maximum useable key length, a parameter L_{max} , $1 \leq L_{max} \leq 16$, has been defined. This parameter should be fixed to whatever key length restriction (in number of bytes) the baseband implementation is faced with. Such restrictions are most likely raised due to export regulations from the country where the silicon/module/accessory/... is manufactured. To prevent users from messing with this parameter it must be stored in a way that it cannot be changed easily. For instance, this can be achieved by storing it in ROM code on the same silicon that holds the E_0 implementation.

However, in a preferred embodiment, the encryption key K'_C is created from the 128 bit secret key K_C and a public 128 bit random number EN_RAND according to

$$K'_C[0...15] = \begin{cases} K_C[0...L-1] \cup EN_RAND[L...15], & L < 16, \\ K_C[0...15], & L = 16. \end{cases} \quad (BQ\ 1)$$

It is K'_C together with some other public parameters (master BD_ADDR and the master clock) that is used in the initialisation of the encryption algorithm E_0 . The idea behind (EQ 1) is to reduce the 128 secret bits of K_C into $8L$ secret bits, where L , $1 \leq L \leq \min\{L_{max}^{(A)}, L_{max}^{(B)}\}$ is a parameter agreed upon through LM signalling between the two involved units A and B. The part taken from EN_RAND is used to ensure that also the non-secret bits "look" random. This is an important property that was considered when the number of initial mixing (shuffle) rounds for the encryption engine was determined (i.e., the number of clock cycles that the engine is run before the output is used for encryption).

669240-4460E09

52 98

5 PROBLEM

The problem with the current method of generating K'_C is that it is difficult to ensure that the hardware implementing E_0 is not used with malicious software that overrides a pre-set value of L_{max} . For example, let's assume that (EQ 1) is performed in hardware. Now, EN_RAND is transmitted to the slave over air in an LM command. The baseband as such cannot extract this number—that will be the task of the LM, which in its turn is a piece of software. Clearly, this software can be changed to write K_C instead of EN_RAND into the hardware. Then, after executing (EQ 1) we will end up with $K'_C = K_C$ regardless of the value of L . Things do not improve if (EQ 1) is executed in software—any 128 bit string can be generated and used as K'_C .

6 SOLUTION

The trick is to reduce the encryption key space into $8L$ bits in hardware without the software being able to change this fact. A very simple hardware solution is to mask out $16-L$ bytes of K_C (replace by zeros or any other fixed string) and ignore EN_RAND . However, for small values of L this would have at least two negative consequences:

1. The initial shuffle period of E_0 registers would need to be run for a longer time due to the "non-randomness" of the fixed part in K'_C .
2. A ciphering attack needs to consider only the L first bytes of K'_C .

The first point is very important since this is something that is done for every (multi-)slot transmission. Increasing the number of iterations is not an option due to the strict timing requirements in Tx/Rx switching. Consequently, there is a risk of decreasing the strength of the cipher. The second is bad as well; a good solution should not give away information about which bits of K_C are important in creating K'_C .

To avoid the above-mentioned problems and solve the issue of overriding L_{max} , we propose the following way of generating the key (for notational convenience the bit strings are considered as binary polynomials):

$$K'_C(x) = g_2^{(L)}(x)(K_C(x) \bmod g_1^{(L)}(x)), \quad (\text{EQ 2})$$

60130944-042699

SB 19 J

SA 50

where $\deg(g_1^{(L)}(x)) = 8L$ and $\deg(g_2^{(L)}(x)) = 128 - 8L$. The modulo operation guarantees that the key space is $8L$ bits since the maximum degree of the remainder cannot exceed the denominator degree minus one. Moreover, it is not clear how changing one bit in K_C will affect the remainder. This means that point 2 above is of less concern. The multiplication will "spread" the $8L$ bits over the entire 128 bit area (note however, there are only 2^{8L} possible values of $K_C(x)$), thus eliminating the concern of point 1. Both the modulo operation and the polynomial multiplication are computations that rather easily can be implemented in hardware, especially if low weight polynomials are used.

The drawback with the above scheme is that we may need to store up to 30 polynomials in hardware (two for each possible value of $L \leq 15^1$). Therefore, we may consider implementations where only one (or a few) possible values of L can be used. One way of doing this is to bound the possible key lengths not only from above with L_{max} , but also from below with a parameter L_{min} . Clearly, letting $L_{min} = L_{max}$ results in only one possible key length. Already today we mention L_{min} in the specification, but we say that this parameter is determined by each application. This can be rephrased to letting the application or the baseband implementation decide.

1. For $L = 16$ we use $K'_C(x) = K_C(x)$.

7 MERITS OF INVENTION

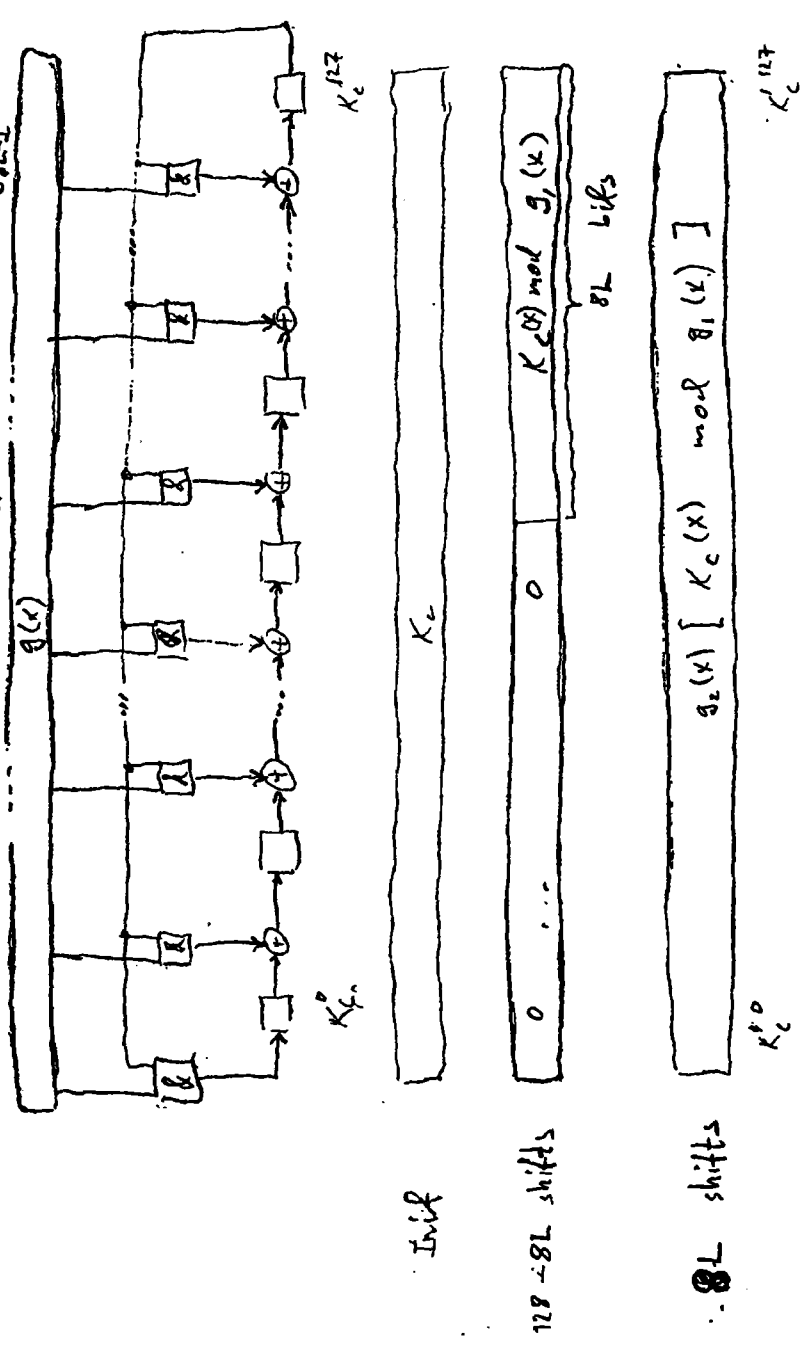
Only one shift register is needed, and the extra hardware for $g_2(x)$ is negligible, because the shift register is there anyway. The solution also ensures better Hamming distance between the initial states of the encryption engine.

669240-446699

Let $g_1(x) = \sum_{i=0}^{127} g_1^{(i)} x^i$
 $g_2(x) = \sum_{i=0}^{127} g_2^{(i)} x^i$

663210 "THEORETOS"

51



Note: $\deg(g_1(x)) + \deg(g_2(x)) \leq 128$ for all L

Fig. 1

85

~~85~~

57 52 8

ESTADOS UNIDOS DE AMÉRICA

A TODOS A QUIENES LLEGUE EL PRESENTE:

DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS

Oficina de Marcas y Patentes

29 de marzo de 2000..

LA PRESENTE CERTIFICA QUE LA ADJUNTA ES UNA COPIA TOMADA DE LOS REGISTROS DE LA OFICINA DE MARCAS Y PATENTES DE LOS ESTADOS UNIDOS, DE LOS DOCUMENTOS DE LA SOLICITUD DE PATENTE ABAJO IDENTIFICADA Y LA CUAL CUMPLE CON LOS REQUISITOS PARA QUE LE SEA CONFERIDA UNA FECHA DE RADICACIÓN SEGÚN 35 USC 111.

NÚMERO DE SOLICITUD 09/461,766

FECHA DE RADICACIÓN: 15 de diciembre de 1999

Por Autoridad del

COMISIONADO DE MARCAS Y PATENTES

(FIRMA) N. WOODSON

Oficial de Certificaciones

(SELLO DORADO DE OBLEA)

* * * *

58 53 91

No. 0033250-4

Estados Unidos de América
DEPARTAMENTO DE ESTADO

A todos a Quienes Llegue el Presente, Os Saludo:

Certifico que el documento adjunto se encuentra bajo el sello de la Oficina de Marcas y Patentes del Departamento de Comercio de los Estados Unidos de América y que a dicho sello debe dársele plena fe y crédito.

En Testimonio de lo cual, Yo, Madeleine K. Albright, Secretaria de Estado, he ordenado al Oficial de Autenticaciones suscribir mi nombre y colocar el sello del Departamento de Estado en la Ciudad de Washington, Distrito de Columbia, hoy 5 de abril de 2000.

Madeleine K. Albright - Seecretaria de Estado
Patrick O. Harchett - Asistente del Oficial de
Autenticaciones. Departamento de Estado

EN ESPAÑOL: La legalización de la firma y cargo anterior por parte del Consulado de Colombia en Washington, D.C. de fecha 5 de abril de 2000, bajo el No. 858.

59 54

inicializar dichas primeras entradas de dichas puertas AND a dichos coeficientes, de polinomio $g_1(x)$, e

inicializar dichas segundas entradas de dichas puertas AND en cero.

19. El método de la Reivindicación 17, donde dichos elementos de retardo son un registro de desplazamiento.

20. Un sistema para comunicar datos encriptados entre dos dispositivos de comunicación que constan de:

un primer dispositivo de comunicación con una longitud de clave de cifrado, L^A_{max} ; y

un segundo dispositivo de comunicación con una segunda longitud de clave de cifrado, L^B_{max} ; y

un medio para determinar la longitud de clave de cifrado máxima, L , donde $L = \min \{L^A_{max}, L^B_{max}\}$;

dicho primer dispositivo consta de:

un medio para obtener polinomios $g_1(x)$ y $g_2(x)$;

un medio para obtener una función de cifrado, $K_c(x)$; y

un medio para calcular una clave de encriptado, $K'_c(x)$,

donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

21. El sistema de la Reivindicación 20, donde dicho medio para calcular dicha clave de encriptado, $K'_c(x)$, consta de:

6055 AX1

2. El dispositivo de la Reivindicación 1, donde dichos elementos de conmutación son puertas AND.

3. El dispositivo de la Reivindicación 1, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado.

4. El dispositivo de la Reivindicación 3, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado y L_{max} es el número máximo de palabras utilizables en la clave de encriptado, K'_c .

5. El dispositivo de la Reivindicación 4, donde dichos elementos de retardo inicialmente se cargan con dicha clave de cifrado, $K'_c(x)$.

6. El dispositivo de la Reivindicación 5, donde dicho polinomio $g_1(x)$ tiene unos primeros coeficientes $w(L_{max}-L)$ iguales a una cadena fija.

61 50 22

7. El dispositivo de la Reivindicación 6, donde dicho polinomio $g_2(x)$ tiene unos últimos coeficientes wL iguales a una cadena fija.

8. El dispositivo de la Reivindicación 7, donde el último wL bits de dichos elementos de retardo almacenan un resultado de $K_c(x) \bmod g_1(x)$ después de desplazamientos $w(L_{max}-L)$.

9. El dispositivo de la Reivindicación 8, donde dichos elementos de retardo almacenan dicha clave de encriptado, K'_{c9} después de desplazamientos wL adicionales.

10. El dispositivo de la Reivindicación 1, donde dichos elementos de retardo son un registro de desplazamiento.

11. Un método para calcular una clave de encriptado, $K'_{c(x)}$, para encriptar datos que consta de los siguientes pasos:

obtener una clave de cifrado, K'_{c9} ;

determinar una longitud de clave de cifrado máxima, L ;

determinar una longitud de clave de encriptado utilizable máxima, L_{max}

obtener un polinomio $g_1(x)$;

obtener un polinomio $g_2(x)$, para extender los puntos de partida de dicha clave de encriptado, $K'_c(x)$; y

calcular dicha clave de encriptado, K'_{c9}

donde $K'_c(x) = g_2^{(L)}(x) [K_c(x) \bmod g_1^{(L)}(x)]$.

12. El método de la Reivindicación 11, además consta del paso de:

6257 M

seleccionar dicho polinomio $g_2(x)$ basado en L .

13. El método de la Reivindicación 12, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} = 0$$

y donde un grado alto de dicho polinomio $g_1(x)$ es igual a wL .

14. El método de la Reivindicación 13, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j.$$

15. El método de la Reivindicación 14, donde unos primeros coeficientes $w(L_{\max}-L)$ de $g_1(x)$ son iguales a una cadena fija.

16. El método de la Reivindicación 15, donde uno de los últimos coeficientes de $g_2(x)$ son iguales a una cadena fija.

17. El método de la Reivindicación 12, donde dicho paso de calcular se realiza utilizando una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, una pluralidad de elementos de retardo y una pluralidad de funciones de adición.

18. El método de la Reivindicación 17, donde dicho método además consta de los siguientes pasos:

63 50 29

una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, donde dichas primeras entradas de puerta están conectadas a dicho elemento de memoria;

una pluralidad de elementos de retardo, cada uno con una entrada y una salida, donde dicha salida de un elemento de retardo está conectado a dichas segundas entradas de puerta; y una pluralidad de funciones de adición, cada una con una primera entrada, una segunda entrada y una salida, donde dichas primeras entradas de funciones de adición están conectadas a todas excepto a una de dichas salidas del elemento de retardo, donde dichas segundas entradas de funciones de adición están conectadas a todas excepto a una de dichas salidas de puerta y donde dichas salidas de funciones de adición están conectadas a todas excepto a una de dichas entradas del elemento de retardo.

22. El sistema de la Reivindicación 21, donde dichos elementos de retardo están inicialmente cargados con dicha clave de cifrado, $K'_c(x)$.

23. El sistema de la Reivindicación 20, donde dichos medios para obtener polinomios $g_1(x)$ y $g_2(x)$ incluye recuperar dichos polinomios de un elemento de memoria contenido dentro de dicho primer dispositivo de comunicación.

24. El sistema de la Reivindicación 23, donde

$$g_1(x) = \sum_{l=0}^{wL} g_l^{(1)} x^l, \quad g_{wL} \neq 0.$$

25. El sistema de la Reivindicación 24, donde

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j.$$

64591

26. el sistema de la Reivindicación 25, donde el último wL bits de dichos elementos de retardo almacenan el resultado de $K_c(x) \bmod g_l(x)$ después de desplazamientos $w(L_{max}-L)$.

27. El sistema de la Reivindicación 26, donde dichos elementos de retardo almacenan dicha clave de encriptado, $K'_c(x)$, después de desplazamientos adicionales wL .

28. El sistema de la Reivindicación 21, donde dichos elementos de retardo son un registro de desplazamiento.

00033250-4

United States of America

66
61



DEPARTMENT OF STATE

To all to whom these



CONSULADO DE COLOMBIA
WASHINGTON, D.C.

656

No. 888

EL CONSULADO DE COLOMBIA

CERTIFICA:

Que es auténtica la firma de PATRICK O. HATCHETT.
quien el día 5 DE ABRIL DEL 2000
desempeñaba las funciones de OFICIAL DE AUTENTICACIONES DEPARTAMENTO DE ESTADO.
la cual aparece al pie de los documentos anexos relacionados con APLICACION PARA PATENTE.

Dado en Washington, D.C. a los CINCO (5) días del mes de
ABRIL. del año dos mil (2000)

Pagado Impuesto de Timbre 7=

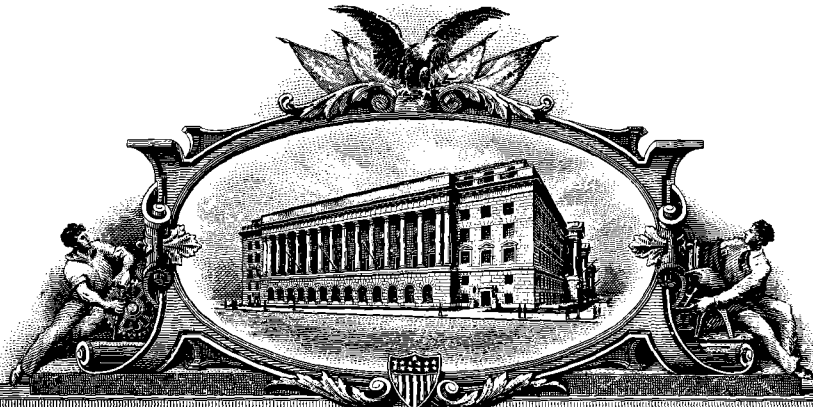
Pagado Derecho Consular 15=

Total 22=

JAQUELINE ESPITIA ARIAS
Vicecónsul

(El Consulado no asume ninguna
responsabilidad por el contenido de los
documentos anexos)

67 62 A



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 29, 2000

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 09/461,766

FILING DATE: December 15, 1999



**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**

N. Woodson

N. WOODSON

Certifying Officer

68 63 42

12/15/99
JCS03 U.S. PTO

Patent
Attorney's Docket No. 040070-986

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT
APPLICATION TRANSMITTAL LETTER

JCS03 U.S. PTO
09/461766
12/15/99

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Enclosed for filing is the utility patent application of Ben Smeets, Mattias Hansson, and Joakim Persson for METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL.

Also enclosed are:

- ☒ 4 (four) sheet(s) of ☐ formal ☒ informal drawing(s);
- ☐ a claim for foreign priority under 35 U.S.C. §§ 119 and/or 365 is ☐ hereby made to _
filed in _ on _;
☐ in the declaration;
- ☐ a certified copy of the priority document;
- ☐ a General Authorization for Petitions for Extensions of Time and Payment of Fees;
- ☐ _____ statement(s) claiming small entity status;
- ☐ an Assignment document;
- ☒ an Information Disclosure Statement; and
- ☐ Other: _____
- ☒ An ☐ executed ☒ unexecuted Declaration and Power of Attorney of the inventor(s)
☒ also is enclosed ☐ will follow.
- ☐ Please amend the specification by inserting before the first line the sentence --This application claims priority under 35 U.S.C. §§119 and/or 365 to _ filed in _ on _; the entire content of which is hereby incorporated by reference.--
- ☐ A bibliographic data entry sheet is enclosed.



21839

(10/99)

09461766.121599

[X] The filing fee has been calculated as follows [] and in accordance with the enclosed preliminary amendment:

FEE CALCULATION					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee					\$760.00 (101)
Total Claims	28	MINUS 20 =	8	x \$18.00 (103)	\$144.00
Independent Claims	3	MINUS 3 =	0	x \$78.00 (102)	-0-
If multiple dependent claims are presented, add \$260.00 (104)					-0-
Total Application Fee					\$904.00
If verified Statement claiming small entity status is enclosed, subtract 50% of Total Application Fee					—
Add Assignment Recording Fee of \$40.00 if Assignment document is enclosed					-0-
TOTAL APPLICATION FEE DUE					\$904.00

[] This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.

[X] A check in the amount of \$ 904.00 is enclosed for the fee due.

[] Charge \$ _____ to Deposit Account No. 02-4800 for the fee due.

[] The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Please address all correspondence concerning the present application to:

Ronald L. Grudziecki
Burns, Doane, Swecker & Mathis, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: December 15, 1999

By: Christine M. Szwerc
Christine M. Szwerc
Registration No. 43,177

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

7A 66 V
M

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL

by

**BEN SMEETS,
MATTIAS HANSSON
and
JOAKIM PERSSON**

**BURNS, DOANE, SWECKER & MATHIS, L.L.P.
POST OFFICE BOX 1404
ALEXANDRIA, VIRGINIA 22313-1404
(703) 836-6620
Attorney Docket No. 040070-986**

09461766-121599

7267
M

METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL

RELATED APPLICATION

5 This application is related to, and claims priority from, U.S. Provisional
Patent Application Serial No. 60/130,944, entitled "Method and Device for
Effective Key Length Control," filed on April 26, 1999, the disclosure of which is
incorporated here by reference.

BACKGROUND

10 The present invention relates to encryption, and in particular to a method
and device for providing a controllable and secure way of determining an
encryption key for use in an encryption algorithm.

15 In communication systems, data is often encrypted before transmission to
assure privacy and data integrity. The encryption of data takes place in an
encryption algorithm. The encryption algorithm manipulates or encodes the
transmission data using other data, mathematical operations and/or other means to
perform such encryption. For example, the encryption algorithm utilizes a data
parameter known as an encryption key, referred to herein by the variable K'_c , in
its initialization procedure. The encryption key is created in part from a ciphering
key or secret key, referred to herein as K_c , where K_c is known to both the
20 receiving device and the transmitting device for encrypting and decrypting the
data.

25 Governments regulate export communication parts and devices that are used
in the encryption and transmission of data, including but not limited to, encryption
software and hardware. Such export regulations differ among different countries.
Specifically, governments regulate the maximum allowable key length of ciphering
keys available to the export devices. The users who transmit and receive

73 68' 

encrypted data would prefer to use the best possible, that is, the longest possible, ciphering key, to maximize security; however, these users are limited by governmental regulations of the ciphering key.

Assume current technology provides for key lengths of the ciphering key, K_c , to be between 1 and 160 bytes (8 and 1280 bits). Governments typically limit the maximum allowable ciphering key length to, for example, 7 bytes (56 bits). To go beyond this ciphering key length, a manufacturer would have to apply for an export license. Communication devices, e.g., cellular phones, typically utilize the maximum ciphering key length permitted for the particular device under the applicable export regulations. The maximum ciphering key length should be stored in such a way to prevent users from easily manipulating the parameter to ensure compliance with governmental regulations. For example, this parameter could be stored in READ ONLY memory (ROM). However, from a manufacturing point of view, it is desirable to produce communication devices that are able to work in many different countries, thereby avoiding customization and permitting a user to use the same communication device in different geographic locations. The manufacturer would prefer to make a universal product with a standardized method of encryption that complies with the different regulations set by a variety of governments and also provides a high level of data security.

Currently, an encryption key, K'_c , together with other public parameters, such as a master clock, is used in the initialization of an encryption algorithm. Encryption key, K'_c , utilizes the ciphering key, K_c , and a public random number, designated $RAND$, in accordance with the following equation:

$$K'_c[0...15] = \begin{cases} K_c[0...L-1] \cup RAND[L...15], & L < 16, \\ K_c[0...15], & L = 16. \end{cases} \quad (EQ.1)$$

where L is $1 \leq L \leq \min \{L^A_{max}, L^B_{max}\}$ in bytes; and

where $RAND[L \dots 15]$ denotes the bytes L through 15 of $RAND$.

040070-986

7/4 69 ~~M~~

For exemplary purposes, the maximum usable encryption key length in bytes, L_{max} , is assumed to be 16 bytes, although different encryption key lengths could be used.

5 As disclosed by the above equation, the encryption key, K'_c , is created by affixing a random number to the end of the ciphering key, K_c , to complete the entire amount of available bytes for the encryption key length, i.e., 16 bytes in this case. The parameter L represents the smaller ciphering key length allowed between two ciphering key lengths, L^A_{max} and L^B_{max} of first communication device A and second communication device B which are manufactured under different governmental regulations. In other words, the ciphering key length used in computing the encryption key, K'_c , is the lesser of the two ciphering key lengths allowed to be used by the first and second communication devices A and B. Both devices can use encrypted communications with the smaller key length, but only one device can use encrypted communication with the larger key length.

10 One problem with the above equation for generating encryption key, K'_c , is that it is difficult to ensure that the hardware implementing the encryption algorithm is not altered by software that overrides the preset values of L_{max} . Furthermore, the *RAND* parameter, being public, can be misused to achieve an effective key length is not restricted at all, i.e., K'_c has a maximum number of effective key bits.

15 An alternative solution is to reduce the space provided for the encryption key, K'_c , to L bytes in the memory of the communication device to prevent the software from altering this length. This can be accomplished by "masking out" the entire amount of available bytes minus L bytes of the ciphering key, K'_c , and ignoring the *RAND*. For example, in this case, because the maximum encryption key length is assumed to be 16, 16 minus L bytes would be "masked out," or in other words, replaced with zeros or some other fixed string. The resulting encryption key, K'_c , would then consist of K_c for the first L bytes and zeros or

7/8 70 AK

some other fixed string for the next $16 - L$ bytes ($128 - 8L$ bits).

However, for small byte values of L , at least two undesirable consequences result from this solution. First, during the initialization of the encryption algorithm, the encryption algorithm shuffles the encryption key, K' , and determines a starting point of the encryption algorithm. To achieve a strong encryption, the shuffling period would need to be increased because of the "non-randomness" of the large fixed string in the 16 minus L bytes, where L is small. As the length of the "random" part of the encryption key decreases, the encryption algorithm would ideally increase the shuffling period, or number of iterations performed, in determining a starting point of the encryption key to compensate for the small length of "random" bits to achieve a better encryption. However, the number of the iterations able to be performed is limited by the strict timing requirements set in transmitting/receiving switching. Thus, this creates a risk of a weak encryption.

Second, an unauthorized person attempting to decrypt the encrypted data or performing a "ciphering attack," would only need to consider or analyze the first L bytes of the ciphering key, K' . In other words, the unauthorized person would only need to analyze the possible combinations of data in L bytes rather than the larger maximum usable encryption key length, in this case, 16 bytes, for small values of L . This creates a risk of unauthorized decryption.

In general, a good encryption algorithm receives as its input, one of, for example, 2^{8L} possible starting points in a binary system. Where L is 16 bytes, a good encryption algorithm would receive 2^{128} possible starting points in a binary system. Each of the possible combinations of the $8L$ K' bits would define one starting point out of the 2^{8L} starting points. An unauthorized person trying to decrypt encrypted data would have to try up to 2^{8L} possible combinations to do so. Fewer starting points are available where governmental regulations have restricted the key length. For example, if a government restricts a ciphering key length to a

76 71 21

maximum of 5 bytes (40 bits), an encryption algorithm would have a reduced number of starting points, that is 2^{40} starting points. Moreover, if one considers the space, or memory, available for storing all the possible 2^{8L} starting points, current technology typically restricts the total available memory to a specific area of the memory for storing the reduced number of starting points and does not use the remaining part of the memory. The remaining positions are constant. Thus, an unauthorized person trying to decrypt encrypted data would only have to analyze 2^{40} starting points and the unauthorized person would know where such starting points were located in memory.

SUMMARY

Accordingly, to overcome the above-mentioned problems, the present invention describes a method by which when an encryption key, K'_c , is generated, the total possible starting points are restricted to a subset of 2^{8L} starting points, where the subsets are different each time a new K'_c is generated over the total available memory or space. Thus, the starting points are no longer stored in the same location after every generation of a new encryption key, K'_c .

In addition, the present invention provides an interface between the generator of the ciphering key, K_c , in a communications system and the ciphering device that uses the ciphering key in encrypting data. The interface provides a controllable and secure way of limiting the key length to conform to the effective key length set by governmental regulations by including an addition or modulus function in the calculation of the encryption key, K'_c .

Moreover, the present invention provides for communication between two devices that are regulated by different governments setting different maximum ciphering key lengths.

Furthermore, the present invention provides for an encryption key, K'_c , where the "randomness" is spread over all the possible combinations of starting

05461766-121392

77 72 A

points for input into the encryption algorithm of the ciphering device.

The above and other advantages of the present invention are carried out in one form by a communication device for determining an encryption key for use in an encryption algorithm. The communication device comprises a memory element for storing one or more polynomials; a plurality of switching elements, each having a first input, a second input and an output, where the switching element first inputs are connected to the memory element; a plurality of delay elements, each having an input and an output, where the output of one delay element is connected to the switching element second inputs; and a plurality of addition or modulo functions, each having a first input, a second input and an output, where the modulo first inputs are connected to all but one of the delay element outputs, where the modulo second inputs are connected to all but one of the switching element outputs and where the modulo outputs are connected to all but one of the delay element inputs. The delay elements may be in the form of a shift register.

The above and other advantages of the present invention are also carried out in another form by a method for calculating an encryption key, $K'_c(x)$, for use in an encryption algorithm. The method comprises the steps of obtaining a ciphering key, $K_c(x)$; determining a maximum ciphering key length, L ; determining a maximum available encryption key length, L_{max} , obtaining a polynomial $g_1(x)$, wherein the highest degree is equal to L_{max} ; obtaining a polynomial $g_2(x)$, for spreading starting points of said encryption key, $K'_c(x)$; and calculating the encryption key, $K'_c(x)$, where $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the Figures where:

FIG. 1 shows two mobile communication devices transmitting and receiving

28 73

data in accordance with the present invention;

FIG. 2 shows a schematic for computing an encryption key, K'_c , in accordance with the present invention;

FIG. 3 shows a shift register in accordance with the schematic of FIG. 2 at different time intervals in accordance with the present invention; and

FIG. 4 shows a block diagram of a method for computing an encryption key, K'_c , in accordance with the present invention.

DETAILED DESCRIPTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular circuits, circuit components, techniques, etc. in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details. In other instances, detailed descriptions of well-known methods, devices, and circuits are omitted so as not to obscure the description of the present invention.

To ensure conformance to a regulated key length and improve the encryption of a data transmission between two or more devices, an encryption key, K'_c , is determined or calculated and input into an encryption algorithm in accordance with the present invention according to the following formula:

$$K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)] \quad (\text{Eq. 2})$$

where:

L is the maximum restricted ciphering key length in bytes and is $1 \leq L \leq \min \{L_{max}^A, L_{max}^B\}$, and $\deg(g_1(x)) + \deg(g_2(x)) \leq wL$ for all L bytes where w is a word length in bits.

79 74

The encryption key, K'_e , is written above in terms of a polynomial expression for exemplary purposes.

As disclosed in *Eq. 2*, the encryption key, K'_e , is based in part on the ciphering key, K_c . The ciphering key, K_c , can be obtained in any suitable way now known or later discovered. For example, the ciphering key, K_c , can be independently communicated to a Device A and a Device B from a third device to facilitate encryption and decryption. Alternatively, Device A can have ciphering key, K_c , stored and can communicate this to Device B. Assume current technology permits a ciphering key length to be between 1 and 160 bytes (8 and 1280 bits) in length. However, the governments from which Device A and Device B are exported have placed certain restrictions on the maximum length of the ciphering key. For example, assume Device A can communicate with a maximum key length of 5 bytes (40 bits) and Device B can communicate with a maximum key length of 7 bytes (56 bits). Once it is determined that Device A desires to transmit data to Device B, Device A and Device B "negotiate" an acceptable maximum key length, L , with which they can both communicate. Specifically, Device A and Device B will transmit and receive data to and from each other that specifies each devices' maximum key length. In this example, because L^A_{max} is 40 bits and L^B_{max} is 56 bits, the devices will "agree" to communicate with a maximum ciphering key length, L , of the lesser key length, or 40 bits.

Thus, in accordance with the present invention, the maximum possible key length is restricted to the minimum of the maximum key lengths between the Devices A and B. This key length restriction is implemented in the encryption through the addition or modulo function and the selection of the polynomial $g_1(x)$.

In an exemplary embodiment, $g_1(x)$ may be represented as the following polynomial:

8075

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0 \quad (Eq. 3)$$

where w equals a word length and L equals a number of words of ciphering key.

The polynomial $g_1(x)$ is created such that the highest degree of the polynomial will be that of the maximum allowable key length in bits. For example, if the word length is 8 bits and the number of words is 5, the highest degree of the $g_1(x)$ polynomial will be 40. Thus, the polynomial $g_1(x)$ could be, for example, as follows:

$$g_1(x) = Ax^{40} + Bx^{39} + Cx^{38} + \dots + Dx + E, \quad A \neq 0 \quad (Eq. 4)$$

The addition or modulo operation ensures that the key length is wL bits since the maximum degree of the remainder cannot exceed one less than the highest degree of the denominator. In this example, the computation of the operation $K_c(x) \bmod g_1^{(w)}(x)$ will yield a result where the highest degree possible is one less than 40, i.e., 39. The result has 40 bits which complies with the maximum allowable key length.

The polynomial $g_1(x)$ can be accessed from a table, for example, which identifies an appropriate $g_1(x)$ polynomial for a given L . This table is preferably located in the hardware so that the available $g_1(x)$ polynomials are secure. The $g_1(x)$ polynomials are thus protected from tampering to ensure compliance with governmental regulations. It will be recognized that a table is one way to store or obtain $g_1(x)$ polynomials but that other ways known in the art may also be used.

As discussed above, a good encryption algorithm receives as its input, one of 2^{8L} possible starting points in a binary system, L being the maximum ciphering key length possible in bytes. Each of the possible combinations of the $8L$ K'_c bits

8A 16 2/2

would define one starting point out of the 2^{8L} starting points. An unauthorized person trying to decrypt encrypted data would have to try up to 2^{8L} possible combinations to do so.

For example, if L equals 16 bytes, a good encryption algorithm receives as its input, one of 2^{128} possible starting points in a binary system. Each of the possible combinations of the 128 K'_c bits would define one starting point out of the 2^{128} starting points. An unauthorized person trying to decrypt encrypted data would have to try up to 2^{128} possible combinations to do so.

In the above example with Device A and Device B, an encryption algorithm would have a reduced number of starting points because of the smaller value of L , that is 2^{40} starting points. Current technology typically restricts the total available memory (in this case, 2^{40} possible starting points) to a specific area of the memory for storing the reduced number of starting points and does not use the remaining part of the memory. The remaining positions are constant. Thus, in this example under current technology, an unauthorized person trying to decrypt encrypted data would only have to analyze 2^{40} starting points and the unauthorized person would know where such starting points were located in memory.

In other words, if the encryption key, $K'_c(x)$, resulted solely from $K_c(x) \bmod g_1^{(L)}(x)$, $K'_c(x)$ would be stored in one specific part of memory according to current technology. The other bits would be zero or some other fixed string. The starting points would then be located in a specific subset of all the possible starting points. To increase the strength of the encryption, however, it is beneficial to have the starting points spread out over all the possible bits.

Hamming distance is a value that reflects the number of distinct bits in two data strings. The greater the Hamming distance among the possible starting points, the better the encryption. If the starting points are always located in a specific subset of positions, the Hamming distance, and thus the encryption, will be poor. The present invention provides a method and device by which the starting points

82 HJ

are spread out in a more effective way rather than being confined to a specific subset of bits so that the minimum distance between the starting points becomes larger.

This concept of increasing the distance or "spreading" is known in the art. For example, error correction coding uses this concept for a different application. Thus, to spread out the starting points over the possible bit range, the result of the $K_c(x) \bmod g_1^{(L)}(x)$ operation is multiplied by a polynomial $g_2(x)$, where an exemplary $g_2(x)$ polynomial is as follows:

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j \quad (Eq. 5)$$

where w equals a word length, L equals a number of words of the ciphering key and L_{max} equals a maximum number of words usable in the encryption key.

The multiplication of $g_2(x)$ with the result of $K_c(x) \bmod g_1^{(L)}(x)$ will "spread" the result of $K_c(x) \bmod g_1^{(L)}(x)$ over the entire bit area. The appropriate $g_2(x)$ polynomial will be selected based upon a given L as is currently known in the art. That is, for different key lengths, L , different coefficients of the $g_2(x)$ polynomial are selected to more effectively achieve desirable Hamming distances. For small values of L , one set of coefficients might achieve desirable Hamming distances while for large values of L , a different set of coefficients would be more appropriate to achieve desirable Hamming distances. In the binary case, $g_2(x)$ may be found as a generator polynomial of a BCH error-correcting code. The $g_2(x)$ polynomials can be stored either in a table which relates appropriate $g_2(x)$ polynomials for a given L . This table may be the same table in which $g_1(x)$ is stored or in another table. The $g_2(x)$ polynomials may be stored either in hardware or in software of the ciphering device. It will be recognized that a table is one way to store an retrieve $g_2(x)$ polynomials but that other ways known in the art may also be used. Alternatively, the $g_2(x)$ polynomials may be obtained from

83
10

memory at some other location, i.e., not located within the ciphering device.

$K'_c(x)$ results from this multiplication. $K'_c(x)$ is input into an encryption algorithm for use in encrypting data.

FIG. 1 shows mobile communication devices 100, 102 transmitting and receiving data from each other in accordance with the present invention. Devices 100, 102 can be any sort of hard wired or wireless device, including, without limitation, a cellular telephone or a computer.

FIG. 2 shows a more detailed view of a communication device 200. Communication device 200 includes a memory element 202, a plurality of switching elements, such as AND gates 204, a plurality of delay elements 206, and a plurality of addition or modulo functions 208.

Memory element 202 stores polynomial $g_1(x)$. Memory element 202 may be a look-up table or some other arrangement of stored information. Memory element 202 may also store polynomial $g_2(x)$. Alternatively, $g_2(x)$ may be stored in some other location within communication device 200 or may be obtained from some other location external to, but accessible to, communication device 200. For exemplary purposes, memory element 202 is described herein as storing both $g_1(x)$ and $g_2(x)$. The functions $g_1(x)$ and $g_2(x)$ are polynomials having specified coefficients, e.g., those described above.

Switching elements or AND gates 204 each have a first input, a second input and one output. Memory element 202 is connected to the first inputs of AND gates 204. Each delay element 206 has one input and one output. Delay elements 206 can be implemented as a shift register. The output of one of the AND gates 204a is connected to the input of a first delay element 206a. Modulo functions 208 each have a first input, a second input and one output. The outputs of the remaining AND gates 208 are connected to first inputs of modulo functions 208. The outputs of all delay elements 206, except for a last delay element 206b, are connected to the second inputs of modulo functions 208. The output of the last

delay element 206b is connected to the second input of AND gates 204. The outputs of modulo functions 208 are connected to the inputs of all delay elements 206 but first delay element 206a.

For exemplary purposes, assume a binary scheme for simplicity; however, those skilled in the art will appreciate that the present invention is equally applicable to other symbol representations.

Initially, communication devices 100, 102 as shown in FIG. 1 will "negotiate" or communicate between themselves to determine the maximum ciphering key length, L , that both devices 100, 102 can use to communicate, as discussed above. Devices 100, 102 might, for example, exchange each device's respective maximum ciphering key length. Devices 100, 102 then "agree" on a maximum ciphering key length, L , by selecting the smaller of the two ciphering key lengths required for each device, if the ciphering key lengths, L , differ.

Referring again to FIG. 2, the first input of AND gates 204 is the $g_1(x)$ binary polynomial from memory element 202. The first $w(L_{max}-L)$ coefficients are zero and the last wL coefficients can be non-zero numbers. In this case, w equals the word length, for all $w \geq 1$, L equals the "negotiated" number of words of the ciphering key, for all $L \geq 1$, L_{max} equals the maximum number of usable words in the encryption key, for all $L_{max} \geq 1$. The second input of AND gates 204 are initialized to zero. Thus, the output of AND gates 204 is zero for each gate corresponding to the first $w(L_{max}-L)$ bits. For the last wL bits, the output of AND gates 204 are a function of the coefficients of the $g_1(x)$ polynomial for each gate corresponding to the last wL coefficients. When the coefficient for $g_1(x)$ is 0, AND gate 204 will open. Conversely, when the coefficient for $g_1(x)$ is 1, AND gate 204 will close.

Delay elements 206 are initialized with the coefficients of the ciphering key, $K_c(x)$ (as shown in shift register 306a of FIG. 3.) These coefficients, as well as the outputs of AND gates 204, are input into exclusive-or functions 208. (This is

85 80 88

for the binary case. In cases other than binary, these coefficients are input into another appropriate addition function.) The initial inputs of AND gates 204 are a string of zeros and the $g_1(x)$ coefficients as described above. The outputs of exclusive-or functions 208 are input into all AND gates 206, except for first AND gate 206a. The output of last delay element 206b is fed back into the second inputs of all AND gates 204. This process is then repeated as the data is shifted, in accordance with available cycles, clock pulses or other timing mechanisms.

Ciphering key, $K_c(x)$, is initially located in delay elements 206 (or a shift register as shown in 306a in Figure 3). As the above described, computations are performed utilizing the ciphering key, $K_c(x)$. Ciphering key, $K_c(x)$, is shifted out of delay elements 206. The output of last delay element 206b is input into AND gates 204 at those positions where AND gates 204 are closed. After the completion of $w(L_{max}-L)$ shifts, delay elements 206 contain the result of the exclusive-or function, $K_c(x) \bmod g_1^{(L)}(x)$ in the last wL spaces (as shown in shift register 306b in Fig. 3). As stated above, this computation ensures that the maximum key length of the ciphering key, $K_c(x)$, does not exceed the governmental regulations of the maximum permitted key length.

After the completion of $w(L_{max}-L)$ shifts, $g_2(x)$ is input into AND gates 204. In contrast to $g_1(x)$, $g_2(x)$ is a polynomial where the first $w(L_{max}-L)$ coefficients can be non-zero numbers and the last wL coefficients are zeros. The above process continues for wL more shifts. The wL bits resulting from exclusive-or functions have now been "spread" over the area. The result in delay elements 206 (as shown in shift register 210c in Fig. 3) is encryption key, $K'_c(x)$, which can then be input into a suitable encryption algorithm for encrypting data.

For exemplary purposes, assume w equals 8, L equals 5, L_{max} equals 16. Assume again a binary scheme for simplicity.

Referring again to FIG. 2, the first input of AND gates 204 is the $g_1(x)$ binary polynomial from memory element 202. The first $w(L_{max}-L)$, or 88,

86 81 2

coefficients are zero and the last wL , or 40, coefficients can be non-zero numbers. The second input of AND gates 204 are initialized to zero. Thus, the output of AND gates 204 is zero for each gate corresponding to the first 88 bits. For the last 40 bits, the output of AND gates 204 are a function of the coefficients of the $g_1(x)$ polynomial for each gate corresponding to the last 40 bits. When the coefficient for $g_1(x)$ is 0, the AND gate will open. Conversely, when the coefficient for $g_1(x)$ is 1, the AND gate will close.

Delay elements 206 are initialized with the coefficients of the ciphering key, $K_c(x)$. These coefficients, as well as the outputs of AND gates 204, are input into exclusive-or functions 208. (The initial inputs of AND gates 204 are a string of zeros and the $g_1(x)$ coefficients as described above.) The outputs of exclusive-or functions 208 are input into all AND gates 206, except for first AND gate 206a. The output of last delay element 206b is input into AND gates 204 at those positions where AND gates 204 are closed. This process is then repeated as data is shifted.

Ciphering key, $K_c(x)$, is initially located in 128 delay elements 206 (or in a 128 bit shift register as shown in 306a in FIG. 3). As the above described computations are performed utilizing the ciphering key, $K_c(x)$. Ciphering key, $K_c(x)$, is shifted out of delay element 206. The output of last delay element 206b is input into AND gates 204. After the completion of 128-40, or 88 shifts, delay elements 206 contain the result of the exclusive-or function, $K_c(x) \bmod g_1^{(L)}(x)$ in the last 40 spaces.

The $g_2(x)$ coefficients are then input into AND gates 204. The above process continues for 40 more shifts, or a total of 128 shifts. The 40 bits resulting from exclusive-or function have now been "spread" over the area. The result in delay elements 206 (or in shift register 306c as shown in FIG. 3) is encryption key, $K'_c(x)$, which can then be input into a suitable encryption algorithm for encrypting data.

87 82 89

FIG. 4 shows a block diagram of a method 400 for computing the encryption key, K'_c , to encrypt data in accordance with the present invention. Method 400 includes the step of obtaining a ciphering key, $K_c(x)$ 402. As described above, ciphering key, $K_c(x)$ can be obtained in any number of ways known in the art. Next, the step of determining a maximum ciphering key length, L , 404 is performed. The maximum key length is typically a value in bytes. The devices that wish to communicate will exchange information or "negotiate" regarding the maximum ciphering key length with which each device can communicate. Typically, the maximum key length will be set to the largest negotiated available key length with which both devices can communicate. A polynomial $g_1(x)$ is then obtained according to step 406. Polynomial $g_1(x)$ is then mathematically manipulated with the ciphering key, $K_c(x)$ according to the function $K_c(x) \bmod g_1(x)$ to achieve a first result. A polynomial $g_2(x)$ is then obtained according to step 408. Step 408 spreads the starting points, or increases the Hamming distance, of encryption key, $K'_c(x)$. An appropriate polynomial $g_2(x)$ is selected based on the results of step 404. Finally, the encryption key, $K'_c(x)$, can be calculated according to step 410 where $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

The present invention has been described above with reference to preferred embodiments. However, those skilled in the art will recognize that changes and modifications may be made without departing from the scope of the present invention. For example, although the present invention describes a method and device where the maximum ciphering key length, L , is 5 bytes, and the maximum usable encryption key length, L_{max} , is 16 bytes, it will be appreciated that the present invention is not so limited to these lengths. In addition, it will also be appreciated that the data being transmitted and received is not limited to any particular type of data. It may constitute voice, written or other data. It may be binary, ASCII or any other form of data. In addition, the data may be transmitted over any media now known, such a wires or air waves, or later discovered.

88 82 82

CLAIMS

1. A communication device for calculating an encryption key, K'_c , by manipulating a ciphering key, K_c , for use in an encryption algorithm, said device comprising:

a memory element for storing one or more polynomials;

a plurality of switching elements, each having a first input, a second input and an output, wherein said switching elements first inputs are connected to said memory element;

a plurality of delay elements, each having an input and an output, where said output of one of said delay elements is connected to said switching elements second inputs; and

a plurality of addition functions, each having a first input, a second input and an output, wherein:

said addition functions first inputs are connected to all but one of said delay elements outputs,

said addition functions second inputs are connected to all but one of said switching elements outputs, and

said addition functions outputs are connected to all but one of said delay elements inputs.

2. The device of claim 1, where said switching elements are AND gates.

3. The device of claim 1, wherein the memory element stores a polynomial $g_1(x)$, wherein

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

and wherein w is a word length and L is a number of words of said ciphering key.

4. The device of claim 3, wherein the memory element stores a polynomial $g_2(x)$, wherein

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j$$

and wherein w is a word length, L is a number of words in said ciphering key, and L_{max} is the maximum number of usable words in the encryption key, K'_c .

5. The device of claim 4, wherein said delay elements are initially loaded with said ciphering key, $K_c(x)$.

6. The device of claim 5, wherein said polynomial $g_1(x)$ has a first $w(L_{max}-L)$ coefficients equal to a fixed string.

7. The device of claim 6, wherein said polynomial $g_2(x)$ has a last wL coefficients equal to a fixed string.

8. The device of claim 7, wherein the last wL bits of said delay elements store a result of $K_c(x) \bmod g_1(x)$ after $w(L_{max}-L)$ shifts.

9. The device of claim 8, wherein said delay elements store said encryption key, K'_c , after an additional wL shifts.

10. The device of claim 1, wherein said delay elements are a shift register.

90 85 ~~85~~

11. A method for calculating an encryption key, $K'_c(x)$, to encrypt data comprising the steps of:

obtaining a ciphering key, $K_c(x)$;

determining a maximum ciphering key length, L ;

determining a maximum usable encryption key length, L_{max}

obtaining a polynomial $g_1(x)$;

obtaining a polynomial $g_2(x)$, for spreading starting points of said encryption key, $K'_c(x)$; and

calculating said encryption key, $K'_c(x)$,

wherein $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

12. The method of claim 11, further comprising the step of:

selecting said polynomial $g_2(x)$ based on L .

13. The method of claim 12, wherein

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

and wherein a highest degree of said polynomial $g_1(x)$ is equal to wL .

14. The method of claim 13, wherein

$$g_2(x) = \sum_{j=0}^{w(L_{max}-L)} g_j^{(2)} x^j.$$

15. The method of claim 14, wherein a first $w(L_{max}-L)$ coefficients of $g_1(x)$ are equal to a fixed string.

09463766-121595

86
21

16. The method of claim 15, wherein a last wL coefficients of $g_2(x)$ are equal to a fixed string.

17. The method of claim 12, wherein said calculating step is performed using a plurality of AND gates, each having a first input, a second input and an output, a plurality of delay elements, and a plurality of addition functions.

18. The method of claim 17, said method further comprising the steps of:
initializing said delay elements with said ciphering key, $K_c(x)$;
initializing said first inputs of said AND gates to said $g_1(x)$ polynomial coefficients; and
initializing said second inputs of said AND gates to zero.

19. The method of claim 17, wherein said delay elements are a shift register.

20. A system for communicating encrypted data between two communication devices comprising:

a first communication device having a first ciphering key length, L_{max}^A ; and
a second communication device having a second ciphering key length, L_{max}^B ;
and

a means for determining a maximum ciphering key length, L ,
where $1 \leq L \leq \min \{L_{max}^A, L_{max}^B\}$;

said first device comprising:

a means for obtaining polynomials $g_1(x)$ and $g_2(x)$;
a means for obtaining ciphering function, $K_c(x)$; and
a means for calculating an encryption key, $K'_c(x)$,

where $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

92 8x [Signature]

21. The system of claim 20, wherein said means for calculating said encryption key, $K'_c(x)$, comprises:

a plurality of AND gates, each having a first input, a second input and an output, wherein said gate first inputs are connected to said memory element;

a plurality of delay elements, each having an input and an output, wherein said output of one delay element is connected to said gate second inputs; and

a plurality of addition functions, each having a first input, a second input and an output, wherein said addition functions first inputs are connected to all but one of said delay element outputs, wherein said addition functions second inputs are connected to all but one of said gate outputs and wherein said addition functions outputs are connected to all but one of said delay element inputs.

22. The system of claim 21, wherein said delay elements are initially loaded with said ciphering key, $K_c(x)$.

23. The system of claim 20, wherein said means for obtaining polynomials $g_1(x)$ and $g_2(x)$ includes retrieving said polynomials from a memory element contained within said first communication device.

24. The system of claim 23, wherein

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0.$$

25. The system of claim 24, wherein

$$g_2(x) = \sum_{j=0}^{w(L-\max)} g_j^{(2)} x^j.$$

93 88 ~~88~~

26. The system of claim 25, wherein the last wL bits of said delay elements store the result of $K_c(x) \bmod g_1(x)$ after $w(L_{max}-L)$ shifts.

27. The system of claim 26, wherein said delay elements store said encryption key, $K'_c(x)$, after an additional wL shifts.

28. The system of claim 21, wherein said delay elements are a shift register.

9/4 89 ~~18~~

10

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
(Includes Reference to Provisional and PCT International Applications)

Attorney's Docket No.

040070-986

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL

the specification of which (check only one item below):

☒ is attached hereto.

☐ was filed as United States application

Number _____

on _____

and was amended

on _____ (if applicable).

☐ was filed as PCT international application

Number _____

on _____

and was amended

on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

60/130,944

(Application Number)

April 26, 1999

(Filing Date)

(Application Number)

(Filing Date)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED)
(Includes Reference to Provisional and PCT International Applications)

Attorney's Docket No.

040070-986

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)		

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Michael J. Ure	33,089
Platon N. Mandros	22,124	James W. Peterson	26,057	Charles F. Wieland III	33,096
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Bruce T. Wieder	33,815
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Todd R. Walters	34,040
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Ronni S. Jillions	31,979
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunty	25,423	Harold R. Brown III	36,341
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Allen R. Baum	36,086
Regis E. Slutter	26,999	Bruce J. Boggs, Jr.	32,344	Steven M. du Bois	35,023
Samuel C. Miller, III	27,360	William H. Benz	25,952	Brian P. O'Shaughnessy	32,747
Robert G. Mukai	28,531	Peter K. Skiff	31,917		
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195		
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		



21839

and: Christine M. Szwerc, Reg. No. 43,177

Address all correspondence to:



21839

Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: Christine M. Szwerc at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

02 97 18

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONTINUED) (Includes Reference to Provisional and PCT International Applications)		Attorney's Docket No. 040070-986	
FULL NAME OF SOLE OR FIRST INVENTOR Ben SMEETS		SIGNATURE	
RESIDENCE Dalby, SWEDEN		CITIZENSHIP Dutch	
POST OFFICE ADDRESS Dalbackavägen 11, 240 10 Dalby, SWEDEN			
FULL NAME OF SECOND JOINT INVENTOR, IF ANY Mattias HANSSON		SIGNATURE	
RESIDENCE Lund, SWEDEN		CITIZENSHIP Swedish	
POST OFFICE ADDRESS Kännärsvägen 13 C, lägenhet 101, 226 46 Lund, SWEDEN			
FULL NAME OF THIRD JOINT INVENTOR, IF ANY Joakim PERSSON		SIGNATURE	
RESIDENCE Lund, SWEDEN		CITIZENSHIP Swedish	
POST OFFICE ADDRESS Iliongränden 197, 224 72 Lund, SWEDEN			
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			
FULL NAME OF NINTH JOINT INVENTOR, IF ANY		SIGNATURE	
RESIDENCE		CITIZENSHIP	
POST OFFICE ADDRESS			

98 98

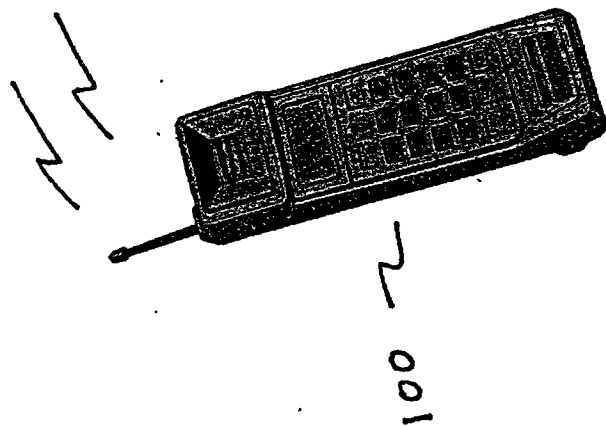
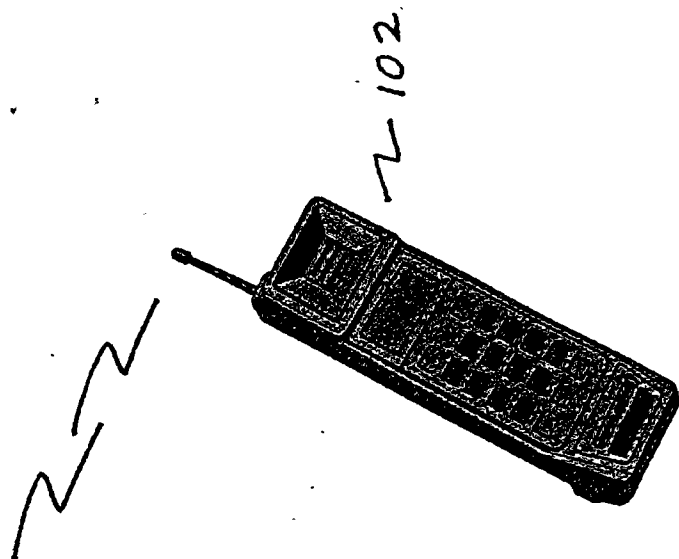


FIG. 1

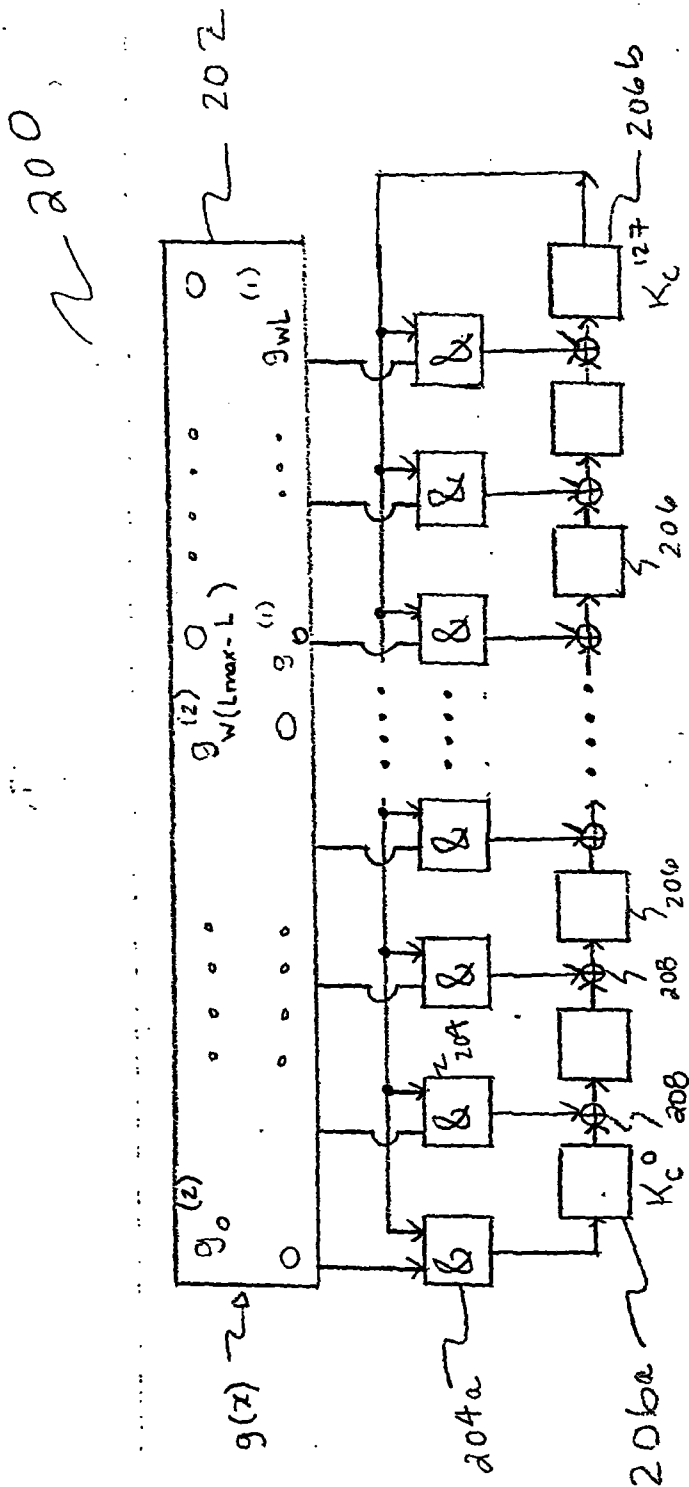


FIG. 2

99

99

306

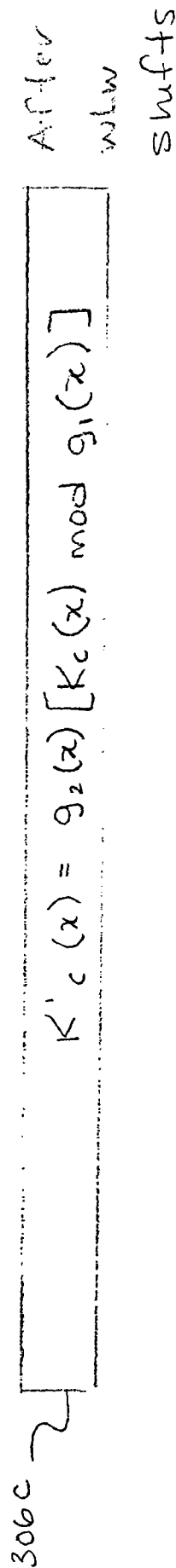
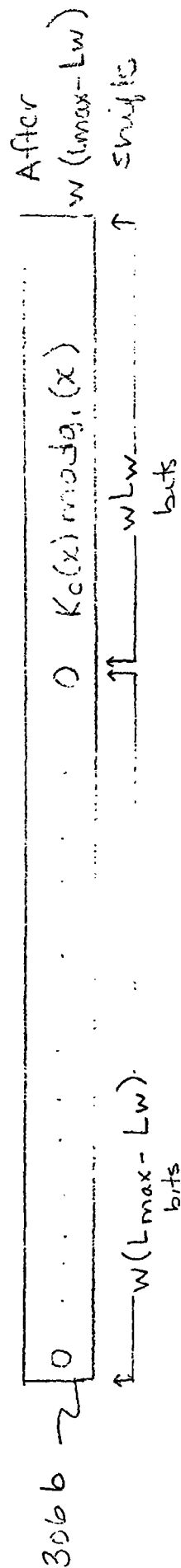
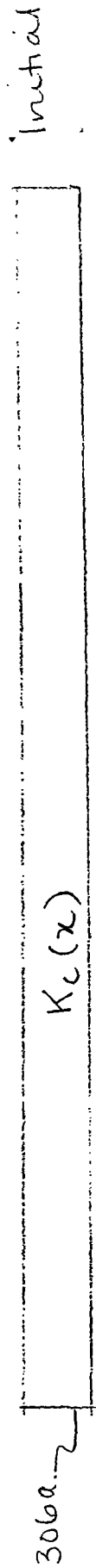


FIG. 3

~~SECRET~~

~~SECRET~~

96 ~~28~~
400
~~101~~

Obtaining a Cipherying Key, $K_c(x)$ ~ 402



Determining a Maximum Key Length, L ~ 404



Obtaining a Polynomial $g_1(x)$ ~ 406



Obtaining a Polynomial $g_2(x)$ ~ 408



Calculating Encryption Key, $K'_c(x)$
where $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$ ~ 410

FIG. 4

ciados 2
103 918

Señores

DIVISION DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Santafé de Bogotá, D.C.

02-01-08-

Re.: Expediente No. 00 - 29.649

Solicitud de Patente

En relación con la última providencia recaída en este expediente, le manifiesto lo siguiente:

- 1.- Debidamente traducidas, las copias oficiales de las solicitudes de patente básicas británicas No. 60/130.944 y 09/461.766 ya fueron acompañadas a mi escrito del 10 de Mayo del 2000.
- 2.- Se acompaña el arte final por triplicado.
- 3.- Se acompaña texto revisado de la descripción, reivindicaciones, resumen y dibujos.
- 4._ Por motivo de lo anterior, se acompaña nueva tarjeta de archivo temático.

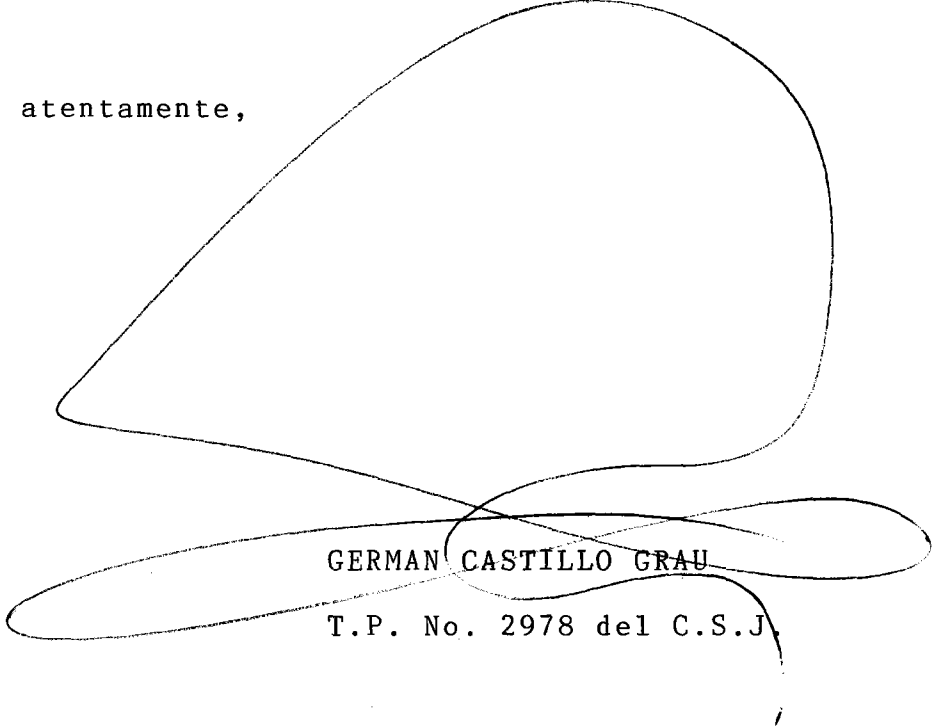
Renuncio al término faltante de traslado y le solicito ordenar la publicación del extracto.

104

Página No. 2

Expediente No. 00 - 29.649

De Ustedes atentamente,



GERMAN CASTILLO GRAU

T.P. No. 2978 del C.S.J.

99 M
105

SUPERINDUSTRIA Y COMERCIO

Radicacion : 00029649 00000001

Folios: 63

Fecha (AMD): 2008-05-18 10:02:09

Tramite : 002 PATENTES D 1 REGISTRO/ 329 COMPLEMEN

Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Señores

DIVISION DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Santafé de Bogotá, D.C.

Re.: Expediente No. 00 - 29.649

Solicitud de Patente

Debidamente traducidas, adjunto acompaño las solicitudes de patente básicas No. 60/130.944 y 09/461.766 las cuales le solicito agregar a este expediente para los efectos legales respectivos.

De Ustedes atentamente,

GERMAN CASTILLO GRAU

T.P. No. 2978 del C.S.J.

MÉTODO Y DISPOSITIVO PARA EL CONTROL EFECTIVO DE LA LONGITUD
DE CLAVE

Antecedentes

La presente invención se refiere al cifrado y en particular a un método y dispositivo para proporcionar una forma controlable y segura de determinar una clave de encriptado para utilizarse en un algoritmo de encriptado.

101
106

100

		FORMATO DE DIGITALIZACION RELACION DE ANEXOS		 Royal Technologies S.A. Integración Central Management & BPM
Expediente No		00029649	No de Folio	
		No de unidades	✓	
Item				
1	CD			
2	DVD			
3	REVISTA			
4	LIBRO			
5	PERIODICO			
6	DISQUETES			
7	SOBRE DE MANILA			
8	SOBRE BLANCO TAMAÑO CARTA	1		
9	SOBRE BLANCO TAMAÑO OFICIO			
10	OTROS:			
Observaciones: Acta Final				

... usuarios que transmiten y reciben datos encriptados preferirían utilizar la mejor clave posible, es decir, la clave de cifrado más larga posible para maximizar la seguridad; sin embargo, los usuarios están limitados por las regulaciones gubernamentales de la clave de cifrado.

Suponga que la tecnología actual proporciona longitudes de clave de la clave de cifrado, K_{cs} para que esté entre 1 y 160 bytes (8 y 1.280 bits). Los gobiernos típicamente limitan la longitud máxima de clave de cifrado permitida a por ejemplo 7 bytes (56 bits).

Para ir más allá de esta longitud de clave de cifrado, un fabricante tendría que aplicar para obtener una licencia de exportación. Los dispositivos para comunicaciones, por ejemplo, teléfonos celulares, típicamente utilizan el máximo

de longitud de clave permitida para un dispositivo en particular bajo las regulaciones de exportación aplicables. Por ejemplo, este parámetro podría almacenarse en la memoria de solo lectura (*READ ONLY memory* (ROM)). Sin embargo desde el punto de vista de fabricación, es conveniente producir dispositivos de comunicación que funcionen en diferentes países, evitando así la personalización y permitiéndole al usuario utilizar el mismo dispositivo en diferentes lugares geográficos. El fabricante preferiría producir un producto universal con un método estandarizado de encriptado que cumpla con las diferentes regulaciones establecidas por la variedad de gobiernos y también proporcionar una alto nivel de seguridad de datos.

Actualmente, una clave de encriptado K'_{c9} junto con otros parámetros públicos, como un reloj maestro, se utiliza para la inicialización de un algoritmo de encriptado. La clave de encriptado K'_{c9} utiliza la clave de cifrado, K_{c9} y un número aleatorio público, llamado *RAND*, de acuerdo con la siguiente ecuación:

$$K'_c[0...15] = \begin{cases} K_c[0...L-1] \cup \text{RAND}[L...15], & L < 16, \\ K_c[0...15], & L = 16. \end{cases} \quad (EQ.1)$$

donde L es $1 \leq L \leq \min \{L^A_{\max}, L^B_{\max}\}$ en bytes; y

donde $\text{RAND}[L...15]$ nota los L bytes hasta 15 de *RAND*.

Para fines de ilustración, la longitud de clave de encriptado utilizable máxima en bytes, $L_{\max9}$, se supone que es de 16 bytes, aunque se podrían utilizar diferentes longitudes de clave de encriptado.

Según lo revelado por la anterior ecuación, la clave de encriptado, K'_{c9} se crea añadiendo un número aleatorio al final de la clave de cifrado, K_{c9} para completar toda la cantidad de bytes disponibles para la longitud de clave de encriptado, es decir, 16 bytes en este caso. El parámetro L representa la longitud de clave de cifrado más pequeña permitida entre dos longitudes de clave de cifrado, $L^A_{\max}$ y $L^B_{\max}$ del primer dispositivo de comunicación A y el segundo dispositivo de comunicación B fabricados bajo diferentes regulaciones gubernamentales. En otras palabras, la longitud de clave de cifrado utilizada para computar la clave de encriptado, K'_{c9} es la menor de las dos longitudes de clave de cifrado permitidas para ser utilizadas por los dispositivos A y B primero y

109
123

segundo. Los dos dispositivos pueden utilizarse en comunicaciones de encriptado con la longitud más pequeña, pero solo un dispositivo puede utilizar comunicación encriptada con la longitud de clave más grande.

Uno de los problemas con la ecuación anterior para generar la clave de encriptado, K'_{cs} es que es difícil asegurar que el hardware que implemente el algoritmo encriptado no sea alterado por el software que cancele los valores preestablecidos de L_{max} . Además, el parámetro $RAND$, al ser público, puede dársele un mal uso para alcanzar una longitud de clave efectiva y no tiene restricción, es decir K'_c tiene un número máximo de bits de clave efectivos.

Una solución alterna es reducir el espacio proporcionado para la clave de encriptado, K'_{cs} a L bytes en la memoria del dispositivo de comunicación para prevenir que el software altere la longitud. Esto se puede llevar a cabo "enmascarando" toda la cantidad de bytes disponibles menos los K bytes de la clave de cifrado, K'_c e ignorando el $RAND$. Por ejemplo, en este caso, debido a que se supone que el máximo de longitud de clave de encriptado es 16, 16 menos los L bytes que serían "enmascarados" o en otras palabras, pueden ser remplazados con ceros o con otra cadena fija. La clave de encriptado resultante, K'_{cs} consistiría entonces de K_c para los primeros L bytes y de ceros o de cualquier otra cadena fija para los próximos $16 - L$ bytes ($128 - 8L$ bits).

Sin embargo, para los valores pequeños de bytes de L resultan, por lo menos, dos consecuencias no deseadas de esta solución. Primero, durante la inicialización del algoritmo de encriptado, el algoritmo de encriptado baraja la clave de encriptado, K'_{cs} y determina un punto de partida del algoritmo de encriptado. Para lograr un encriptado fuerte, el período de baraja necesitaría ser incrementado por la "falta de aleatoriedad" de la cadena fija grande en los 16 menos L bytes, donde L es pequeño. A medida que baja la longitud de la parte "aleatoria" de la clave de cifrado, el algoritmo de encriptado idealmente aumentaría el período de baraja, o el número de iteraciones realizadas, al determinar un punto de partida de la clave de encriptado para compensar la pequeña longitud de bits "aleatorios" y lograr así un mejor encriptado. Sin embargo, el número de iteraciones que se pueden realizar está limitado por los requerimientos estrictos de cronometraje establecidos en la conmutación de transmisión / recepción. Por lo tanto, esto crea el riesgo de un encriptado débil.

Segundo, una persona no autorizada que intente descifrar los datos encriptados o realizar un "ataque de cifrado" solo necesitaría considerar o analizar

los primeros L bytes de la clave de cifrado, K'_c . En otras palabras, la persona no autorizada solo tendría que analizar las posibles combinaciones de datos en los L bytes en lugar de analizar la longitud de clave de encriptado utilizable máxima más grande, en este caso, 16 bytes, para los valores pequeños de L . Esto crea el riesgo de desenscriptado no autorizado.

En general, un buen algoritmo de encriptado recibe como su entrada, uno de, por ejemplo, 2^{8L} posibles puntos de partida en un sistema binario. Donde L es 16 bytes, un buen algoritmo de encriptado recibiría 2^{128} posibles puntos de partida en un sistema binario. Cada una de las posibles combinaciones de los $8L$ K'_c bits definiría un punto de partida fuera de los puntos de partida 2^{8L} . Una persona no autorizada que intente desenscriptar los datos cifrados tendría que ensayar hasta 2^{8L} posibles combinaciones para lograrlo. Hay muy pocos puntos de partida disponibles donde las regulaciones gubernamentales tengan longitud de clave restringida. Por ejemplo, si un gobierno restringe una longitud de clave de cifrado a un máximo de 5 bytes (40 bits), un algoritmo de encriptado tendría un número reducido de puntos de partida, es decir 2^{40} puntos de partida. Es más, si se considera el espacio, o la memoria, disponible para almacenar todos los posibles 2^{8L} puntos de partida, la tecnología actual típicamente restringe la memoria total disponible a un área específica de la memoria para almacenar el número reducido de puntos de partida y no utiliza la parte restante de la memoria. Las posiciones restantes son constantes. Así, una persona no autorizada que intente desenscriptar los datos cifrados solo tendría que analizar 2^{40} puntos de partida y la persona no autorizada sabría donde estarían localizados en la memoria dichos puntos de partida.

RESUMEN

De conformidad, para vencer los problemas antes mencionados, la presente invención describe un método por el cual se genera una clave de encriptado, K'_c , el número total de posibles puntos de partida están restringidos a un subconjunto de 2^{8L} puntos de partida, donde los subconjuntos son diferentes cada vez que se genera un nuevo K'_c en el total de memoria o espacio disponible. Por consiguiente, los puntos de partida ya no están almacenados en el mismo lugar después de cada generación de una nueva clave de encriptado, K'_c .

Además, la presente invención proporciona una interfaz entre el generador de la clave de cifrado, K'_c en un sistema de comunicaciones y el dispositivo de cifrado que utiliza la clave de cifrado en los datos encriptados. La interfaz

247-8
105

proporciona una forma segura y controlable de limitar la longitud de clave para ajustarse a la longitud de clave efectiva establecida por las regulaciones gubernamentales al incluir una función de adición o de módulo en el cálculo de la clave de encriptado, K'_c .

Es más, la presente invención proporciona comunicaciones entre dos dispositivos que están regulados por diferentes gobiernos estableciendo distintos máximos de longitud de clave de cifrado.

Además, la presente invención proporciona una clave de encriptado, K'_{c9} , donde la "aleatoriedad" está extendida sobre todas las posibles combinaciones de puntos de partida para entrar en el algoritmo de encriptado del dispositivo de cifrado.

Las ventajas anteriores y otras de la presente invención se llevan a cabo en una forma por un dispositivo de comunicación para determinar una clave de encriptado para ser utilizada en un algoritmo de encriptado. El dispositivo de comunicación consta de un elemento de memoria para almacenar uno o más polinomios; una pluralidad de elementos de conmutación, cada uno con una primera entrada, una segunda entrada y una salida, donde las primeras entradas del elemento de conmutación están conectadas al elemento de memoria; una pluralidad de elementos de retardo, cada uno con entrada y salida, donde la salida de un elemento de retardo está conectado a las segundas entradas del elemento de conmutación; y una pluralidad de funciones de adición o de módulo, cada una con una primera entrada, una segunda entrada y salida, donde las primeras entradas de módulo están conectadas a todos excepto una de las salidas del elemento de retardo, donde las segundas entradas de módulo están conectadas a todas excepto a una de las salidas del elemento de conmutación y donde las salidas de módulo están todas conectadas excepto una de las entradas del elemento de retardo. Los elementos de retardo pueden ser un registro de desplazamiento.

Las ventajas anteriores y otras de la presente invención también pueden tener otra forma por medio de un método para calcular una clave de encriptado, $K'_c(x)$, para utilizarse en un algoritmo de cifrado. El método consta de pasos para obtener una clave de cifrado, $K'_c(x)$; para determinar una máxima longitud de clave de cifrado, L ; para determinar un máximo disponible de longitud de clave de encriptado, L_{max} , para obtener un polinomio $g_1(x)$, para extender los puntos de

AA2-106

partida de dicha clave de encriptación, $K'_c(x)$; y para calcular la clave de encriptado, $K'_c(x)$, donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se puede derivar una mejor comprensión de la presente invención al referirse a la descripción detallada y reivindicaciones cuando se consideran en conjunto con las figuras donde:

La Figura 1 muestra dos dispositivos de comunicación móvil transmitiendo y recibiendo datos de acuerdo con la presente invención;

La Figura 2 muestra un esquema para computar una clave de encriptado, K'_{c9} , de acuerdo con la presente invención;

La Figura 3 muestra un registro de desplazamiento de acuerdo con el esquema de la Figura 2 en diferentes intervalos de acuerdo con la presente invención; y

La Figura 4 muestra un diagrama de bloque de un método para computar una clave de encriptado, K'_{c9} , de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA

En la siguiente descripción, por razones de la explicación y no de limitaciones, se establecen los detalles específicos, tales como circuitos particulares, componentes de circuitos, técnicas, etc., para poder proporcionar una comprensión a fondo de la presente invención. Sin embargo, será evidente para alguien experimentado en la técnica que la presente invención puede ser practicada en otras realizaciones que partan de estos detalles específicos. En otros casos, las descripciones detalladas de los métodos bien conocidos, de los dispositivos y circuitos son omitidos como para no restarle importancia a la descripción de la presente invención.

Para asegurar conformidad con una longitud de clave regulada y para mejorar el encriptado de la transmisión de datos entre dos o más dispositivos, se determina o calcula una clave de encriptado, K'_{c9} y se entra en un algoritmo de encriptado de acuerdo con la presente invención según la siguiente fórmula:

$$K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)] \quad (\text{Eq. 2})$$

113
127

donde:

L es la longitud máxima de clave de cifrado restringida en bytes y es

$1 \leq L \leq \min \{L_{max}^A, L_{max}^B\}$, y $\deg(g_1(x)) + \deg(g_2(x)) \leq wL$ para todos los L bytes donde w es una longitud de palabra en bits.

La clave de encriptación, K'_{cg} está escrita encima en términos de una expresión de polinomio para fines de ilustración.

Como se reveló en la Ecuación 2, la clave de encriptación, K'_{cg} se basa en parte en la clave de cifrado, K_c . La clave de cifrado, K_c , se puede obtener en cualquier forma apropiada ahora conocida o descubierta más adelante. Por ejemplo, la clave de cifrado, K_c puede ser comunicada de manera independiente a un Dispositivo A y a un Dispositivo B desde un tercer dispositivo para facilitar la encriptación y la desencriptación. De manera alterna, el Dispositivo A puede tener una clave de cifrado, K_c almacenada y puede comunicar esto al Dispositivo B. Suponga que la tecnología actual permita una longitud de clave de cifrado que esté entre 1 y 160 bytes (8 y 1.280 bits) de longitud. Sin embargo, los gobiernos de los cuales se exportan el Dispositivo A y Dispositivo B han puesto ciertas restricciones a la longitud máxima de la clave de cifrado. Por ejemplo, suponga que el dispositivo A puede comunicarse con un máximo de longitud de clave de 5 bytes (40 bits) y que el Dispositivo B puede comunicarse con un máximo de longitud de clave de 7 bytes (56 bits). Una vez que se determina que el dispositivo A desea transmitir datos al Dispositivo B, el Dispositivo A y el Dispositivo B "negocian" una longitud de clave máxima aceptable, L en la cual los dos se pueden comunicar. Específicamente, el Dispositivo A y el Dispositivo B transmitirán y recibirán datos desde y hasta cada uno que especifique cada uno de las longitudes de clave máximas. En este ejemplo, debido a que L_{max}^A es 40 bits y L_{max}^B es 56 bits, los dispositivos "acordarán" comunicarse con un máximo de longitud de clave, L de la mínima longitud de clave, o 40 bits.

Así, de acuerdo con la presente invención, el máximo posible de longitud de clave está restringido al mínimo del máximo de las longitudes de clave entre los dispositivos A y B. Esta restricción de longitud de clave está implementada en la encriptación por medio de la función de adición o de módulo y la selección del polinomio $g_1(x)$.

En una realización ilustrada, $g_1(x)$ puede representarse como el siguiente polinomio:

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0 \quad (\text{Eq. 3})$$

donde w es igual a una longitud de palabra y L es igual al número de palabras en la clave de cifrado.

El polinomio $g_1(x)$ se crea de tal forma que el grado más alto del polinomio sea el del máximo permitido de longitud de clave en bits. Por ejemplo, si la longitud de la palabra es de 8 bits y el número de palabras es de 5, el grado más alto del polinomio $g_1(x)$ será 40. Así, el polinomio $g_1(x)$ puede ser, por ejemplo, de la siguiente manera:

$$g_1(x) = Ax^{40} + Bx^{39} + Cx^{38} + \dots + Dx + E, \quad A \neq 0 \quad (\text{Eq. 4})$$

La operación de adición o de módulo asegura que la longitud de clave sea de wL bits ya que el grado máximo de lo restante no puede exceder de uno menos que el grado más alto del dominador. En este ejemplo, la operación de computación $K_c(x) \bmod g_1^{(L)}(x)$ producirá un resultado donde el grado más alto posible es uno menos de 40, es decir 39. El resultado tiene 40 bits lo que está de conformidad con la longitud de clave máxima permitida.

El polinomio $g_1(x)$ puede accederse desde una tabla, por ejemplo, que identifica un polinomio $g_1(x)$ apropiado para un L dado. Esta tabla está preferiblemente localizada en el hardware de tal forma que los polinomios $g_1(x)$ disponibles estén seguros. Los polinomios $g_1(x)$ están protegidos de ser alterados para asegurar conformidad con las regulaciones gubernamentales. Se reconocerá que una tabla es una forma de almacenar o de obtener polinomios $g_1(x)$ pero que se pueden utilizar otras formas conocidas en la técnica.

Tal como se dijo anteriormente, un buen algoritmo de encriptado recibe como entrada, uno de los 2^{8L} posibles puntos de partida en un sistema binario, donde L es la longitud de clave máxima posible en bytes. Cada una de las

posibles combinaciones de $8L K'_c$ bits definirá uno de los puntos de partida fuera de los puntos de partida 2^{8L} . Una persona no autorizada que intente descryptar datos encriptados tendría que ensayar hasta las 2^{8L} posibles combinaciones para lograrlo.

Por ejemplo, si L es igual a 16 bytes, un buen algoritmo de encriptado recibe como entrada, uno de los posibles 2^{128} puntos de partida en un sistema binario. Cada una de las posibles combinaciones de los 128 K'_c bits definiría un punto de partida fuera de los 2^{128} puntos de partida. Una persona no autorizada que intente descryptar datos encriptados tendría que ensayar hasta 2^{128} posibles combinaciones para lograrlo.

En el ejemplo anterior con el Dispositivo A y el Dispositivo B un algoritmo de encriptado tendría un número reducido de puntos de partida debido al valor más pequeño de L que es 2^{40} puntos de partida. La tecnología actual típicamente restringe la memoria disponible total (en este caso, 2^{40} posibles puntos de partida) a un área específica de la memoria para almacenar el número reducido de puntos de partida y no utiliza la parte restante de memoria. Las posiciones restantes son constantes. Así, en este ejemplo en la tecnología actual, una persona no autorizada que intente descryptar datos encriptados solo tendría que analizar 2^{40} puntos de partida y dicha persona tendría que saber donde localizar los puntos de partida en la memoria.

En otras palabras, si la clave de encriptado, $K'_c(x)$ resulta solo de $K_c(x) \bmod g_1^{(L)}(x)$, $K'_c(x)$ sería almacenado en un lugar específico de la memoria de acuerdo con la tecnología actual. Los otros bits serían cero o cualquier otra cadena fija. Los puntos de partida estarían ubicados en un subconjunto específico de todos los posibles puntos de partida. Sin embargo, para incrementar la fuerza del encriptado, es beneficioso tener los puntos de partida extendidos de forma más efectiva en lugar de tenerlos confinados a un subconjunto específico de bits para que la distancia mínima entre los puntos de partida sea más grande.

Este concepto de incrementar la distancia o "extender" se conoce en la técnica. Por ejemplo, la codificación de corrección de error utiliza este concepto para una aplicación diferente. Por lo tanto, para extender los puntos de partida sobre el posible rango de bit, el resultado de la operación $K_c(x) \bmod g_1^{(L)}(x)$ se multiplica por un polinomio $g_2(x)$ donde se ilustra como sería un polinomio $g_2(x)$:

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j \quad (Eq. 5)$$

146 110

donde w es igual al largo de la palabra, L es igual al número de palabras de la clave de cifrado y L_{max} es igual al máximo número de palabras que se utilizan en la clave de encriptado.

La multiplicación de $g_2(x)$ más el resultado de $K_c(x) \bmod g_1^{(L)}(x)$ "extenderá" el resultado de $K_c(x) \bmod g_1^{(L)}(x)$ en toda el área bit. Se seleccionará el polinomio apropiado $g_2(x)$ con base en una L dada tal como actualmente se conoce en la técnica. Esto es, para diferentes longitudes de clave, L , se seleccionan diferentes coeficientes del polinomio $g_2(x)$ para alcanzar de manera más efectiva las distancias de Hamming deseadas. Para los valores pequeños de L , un conjunto de coeficientes puede alcanzar las distancias de Hamming deseadas, mientras que para los valores grandes de L , un conjunto diferente de coeficientes sería más apropiado para alcanzar las distancias de Hamming deseadas. En el caso binario $g_2(x)$ puede encontrarse como generador de polinomio de un código de corrección de error BCH. Los polinomios $g_2(x)$ pueden ser almacenados en una tabla que relaciona los polinomios $g_2(x)$ apropiados para una L dada. Esta tabla puede ser la misma tabla en la cual $g_1(x)$ está almacenado en otra tabla. Los polinomios $g_2(x)$ pueden almacenarse bien sea en el hardware o software del dispositivo de cifrado. Se reconocerá que una tabla sirve en una forma para almacenar y recuperar polinomios $g_2(x)$ pero que otras formas conocidas por la técnica también se pueden utilizar. Por otra parte, los polinomios $g_2(x)$ se pueden obtener de la memoria en otro lugar, es decir, que no estén localizados dentro del dispositivo de cifrado.

$K'_c(x)$ resulta de la siguiente multiplicación. $K'_c(x)$ es entrada al algoritmo de encriptado para ser utilizado en datos encriptados.

La Figura 1 muestra dispositivos de comunicación móvil (100), (102) transmitiendo y recibiendo datos entre sí de acuerdo con la presente invención. Los dispositivos (100), (102) pueden ser cualquier clase dispositivo alambrado o inalámbrico, incluyendo, sin limitarse, un teléfono celular o un computador.

La Figura 2 muestra una vista más detallada de un dispositivo de comunicación (200). El dispositivo de comunicaciones (200) incluye un elemento de memoria (202), una pluralidad de elementos de conmutación, tales como puertas AND (204), una pluralidad de elementos de retardo (206) y una pluralidad de funciones de adición o de módulo (208).

117-
111

El elemento de memoria (202) almacena polinomios $g_1(x)$. El elemento de memoria (202) puede ser una tabla de despliegue o cualquier otro arreglo para almacenar información. El elemento de memoria (202) también puede almacenar polinomios $g_2(x)$. Por otra parte, los $g_2(x)$ pueden almacenarse en otro lugar dentro del dispositivo de comunicaciones (200) o pueden obtenerse de un lugar externo al dispositivo de comunicación (200), pero que sea accesible. Para fines de ilustración, el elemento de memoria (202) se describe aquí como para almacenar tanto $g_1(x)$ como $g_2(x)$. Las funciones $g_1(x)$ y $g_2(x)$ son polinomios con coeficientes específicos, por ejemplo los descritos anteriormente.

Los elementos de conmutación o las puertas AND (204) cada una tiene una primera entrada, una segunda entrada y una salida. El elemento de memoria (202) está conectado a la primera entrada de las puertas AND (204). Cada elemento de retardo (206) tiene una entrada y una salida. Los elementos de retardo (206) pueden ser implementados como un registro de desplazamiento. La salida de una de las puertas AND (204a) está conectada a la entrada de un primer elemento de retardo (206a). Las funciones de módulo (208) cada una tiene una primera entrada, una segunda entrada y una salida. Las salidas de las puertas AND (208) restantes están conectadas a las primeras entradas de las funciones de módulo (208). Las salidas de todos los elementos de retardo (206), excepto el último elemento de retardo (206b), están conectadas a las segundas entradas de las funciones de módulo (208). La salida del último elemento de retardo (206b) está conectado a la segunda entrada de las puertas AND (204). Las salidas de las funciones de módulo (208) están conectadas a las entradas de todos los elementos de retardo (206) excepto al primer elemento de retardo (206a).

Para fines ilustrativos, imagínese un esquema binario para mayor facilidad; sin embargo, aquellos expertos en la técnica apreciarán que la presente invención sea igualmente aplicable a otras representaciones de símbolo.

Inicialmente, los dispositivos de comunicación (100), (102) como los muestra la Figura 1 van a "negociar" o a comunicarse entre sí para determinar la longitud de clave de cifrado, L , que utilizan los dos dispositivos (100) y (102) para comunicarse, como se vió anteriormente. Los dispositivos (100) (102) pueden, por ejemplo, intercambiar la longitud clave de cifrado máxima respectiva de cada dispositivo. Los dispositivos (100), (102) "acuerdan" un máximo de longitud de clave de cifrado, L , seleccionando la longitud más pequeña de los dos longitudes

118 110
112

de clave de cifrado requeridas para cada dispositivo, en caso de que las longitudes de clave de cifrado, L , sean diferentes.

Con referencia de nuevo a la Figura 2, la primera entrada de puertas AND (204) es el polinomio binario $g_1(x)$ del elemento de memoria (202). Los primeros coeficientes $w(L_{max}-L)$ son cero y los últimos coeficientes wL pueden ser números diferentes a cero. En este caso, w es igual a la longitud de la palabra, para todas las $w \geq 1$, L es igual al número "negociado" de palabras de la clave de cifrado, para todas las $L \geq 1$, L_{max} es igual al máximo número de palabras utilizables en la clave de cifrado, para todas las $L_{max} \geq 1$. La segunda entrada de las puertas AND (204) está inicializada en cero. Así, la salida de las puertas AND (204) es cero para cada puerta que corresponda a los primeros bits $w(L_{max}-L)$. Para el último bits wL , la salida de las puertas AND (204) son una función de los coeficientes del polinomio $g_1(x)$ para cada puerta que corresponda con los últimos coeficientes wL . Cuando el coeficiente para $g_1(x)$ es 0, la puerta AND (204) se abrirá. Inversamente, cuando el coeficiente para $g_1(x)$ es 1, la puerta AND (204) se cerrará.

Los elementos de retardo (206) se inicializan con los coeficientes de la clave de cifrado, $K_c(x)$ (tal como se muestra en el registro de desplazamiento (306a) de la Figura 3). Estos coeficientes, así como las salidas de las puertas AND (204), son entradas dentro de funciones/privativas $0-(208)$ (Esto para el caso binario. Para casos diferentes al binario, estos coeficientes son entradas a otra función de adición apropiada). Las entradas iniciales de las puertas AND (204) son una cadena de ceros y de coeficientes $g_1(x)$ según se describió anteriormente. Las salidas de las funciones privativas $0-(208)$ son entrada a todas las puertas AND (206), excepto a la primera puerta AND (206a). La salida del último elemento de retardo (206b) se vuelve a alimentar en las segundas entradas de todas las puertas AND (204). Este proceso se repite a medida que los datos se desplazan, de acuerdo con los ciclos disponibles, los pulsos de reloj u otros mecanismos de cronometraje.

La clave de cifrado, $K'_c(x)$, inicialmente se coloca en los elementos de retardo (206) (o como lo muestra un registro de desplazamiento (306a) en la Figura 3). Como se describió anteriormente, los cálculos se llevan a cabo utilizando la clave de cifrado, $K'_c(x)$. La clave de cifrado, $K'_c(x)$, se desplaza fuera de los elementos de retardo (206). La salida del último elemento de retardo (206b) es una entrada al interior de las puertas AND(204) en aquellas posiciones en donde las puertas AND -- -----

179 - 4
113

(204) están cerradas. Después de completar los desplazamientos $w(L_{max}-L)$, los elementos de retardo (206) contienen el resultado de la función derivada $-D$, $K'_c(x) \bmod g_1(L)(x)$ en el último espacio wL (como se muestra en el registro de desplazamiento (306b) en la Figura 3). Como se dijo anteriormente, este cómputo asegura que la longitud máxima de clave de cifrado, $K'_c(x)$, no excede las regulaciones gubernamentales de la longitud máxima de clave permitida.

Después de terminar los desplazamientos de $w(L_{max}-L)$, $g_2(x)$ es ingresado a las puertas AND (204). En contraposición a $g_1(x)$, $g_2(x)$ es un polinomio donde los primeros coeficientes $w(L_{max}-L)$ pueden ser números diferentes a cero y los últimos coeficientes wL son ceros. El anterior proceso continúa para otros desplazamientos wL . Los bits wL que resultan de la función derivada $-D$ han sido "extendidos" en el área. El resultado en los elementos de retardo (206) (como se muestran en el registro de retardo (210c) en la Figura 3) es una clave de encriptado, $K'_c(x)$ que entonces se puede ingresar a un algoritmo de encriptado adecuado para encriptar datos.

Para fines ilustrativos, suponga que w es igual a 8, L es igual a 5, L_{max} es igual a 16. Suponga de nuevo que es un esquema binario para mayor facilidad.

Con referencia de nuevo a la Figura 2, la primera entrada de las puertas AND (204) es el polinomio binario $g_1(x)$ desde el elemento de memoria (202). Los primeros coeficientes $w(L_{max}-L)$, u 88, son cero y el último coeficiente wL , o 40 pueden ser números diferentes a cero. La segunda entrada de las puertas AND (204) se inicializa en cero. Así, la salida de las puertas AND (204) es cero para cada puerta correspondiente a los primeros 88 bits. Para los últimos 40 bits, las salidas de las puertas AND (204) son una función de los coeficientes del polinomio $g_1(x)$ para cada puerta correspondiente a los últimos 40 bits. Cuando el coeficiente para $g_1(x)$ es 0, la puerta AND se abrirá. Inversamente, cuando el coeficiente para $g_1(x)$ es 1, la puerta AND se cerrará.

Los elementos de retardo (206) se inicializan con los coeficientes de la clave de cifrado $K_c(x)$.—Estos coeficientes, así como las salidas de las puertas AND(204) ingresan a las funciones derivadas $-D$ (208). (Las entradas iniciales de AND(204) son una cadena de ceros y los coeficientes $g_1(x)$ ya fueron mencionados). Las salidas de las funciones derivadas $-D$ (208) ingresan a todas las puertas AND(206), salvo la primera puerta AND(206a).— La salida del último elemento de retardo (206b) se ingresa a todas las puertas

120 ~~114~~

AND (204) en aquellas posiciones donde las puertas AND (204) están cerradas. Este proceso se repite a medida que los datos se desplazan.

La clave de cifrado, $K_c(x)$ se localiza inicialmente en 128 elementos de retardo (206) (o en un registro de desplazamiento de 128 bits como se muestra en (306a) en la Figura 3). De acuerdo con la anterior descripción el cómputo se lleva a cabo utilizando la clave de cifrado, $K_c(x)$. La clave de cifrado, $K_c(x)$, se desplaza fuera del elemento de retardo (206). La salida del último elemento de retardo (206b) se ingresa a las puertas AND (204). Después de completar 128-40 u 88 desplazamientos, los elementos de retardo (206) contienen el resultado de la función exclusiva-o, $K_c(x) \bmod g_1^{(L)}(x)$ en los últimos 40 espacios.

Los coeficientes $g_2(x)$ entran las puertas AND (204). Los anteriores procesos continúan durante 40 desplazamientos más o por un total de 128 desplazamientos. Los 40 bits resultantes de la función exclusiva-o han sido "extendidos" en el área. El resultado en los elementos de retardo (206) (o en el registro de desplazamiento (306c) como se muestra en la Figura 3) es la clave de encriptación, $K'_c(x)$, que se puede ingresar en un algoritmo de encriptado apropiado para encriptar datos.

La Figura 4 muestra un diagrama de bloque de un método (400) para computar la clave de encriptado, K'_{cs} , para encriptar datos de acuerdo con la presente invención. El método 400 incluye el paso para obtener una clave de cifrado, $K_c(x)$ (402). Tal como se describió anteriormente, la clave de cifrado, $K'_c(x)$ se puede obtener de varias formas conocidas en la técnica. Luego, se lleva a cabo el paso de determinar una longitud máxima de clave de cifrado, L (404). La longitud máxima de clave típicamente es un valor expresado en bytes. Los dispositivos que deseen comunicarse intercambiarán información o "negociarán" respecto a la longitud máxima de clave de cifrado con la cual cada dispositivo se puede comunicar. Típicamente, la longitud máxima de clave se establecerá a la longitud de clave más larga disponible negociada con la cual los dos dispositivos se pueden comunicar. Entonces se obtiene un polinomio $g_1(x)$ de acuerdo con el paso (406). Un polinomio $g_1(x)$ se manipula matemáticamente con la clave de cifrado, $K_c(x)$ de acuerdo con la función $K_c(x) \bmod g_1(x)$ para lograr un primer resultado. Un polinomio $g_2(x)$ se obtiene de acuerdo con el paso (408). El paso (408) extiende los puntos de partida, o incrementa la distancia de Hamming de la clave de encriptación, $K'_c(x)$. Se selecciona un polinomio apropiado $g_2(x)$ con base en los resultados del paso (404). Finalmente, se puede calcular la clave de

127 A
115
encripción, $K'_c(x)$ de acuerdo con el paso (410) donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

La presente invención ha sido descrita anteriormente con referencia a las realizaciones preferidas. Sin embargo, aquellos expertos en la técnica reconocerán que se puede hacer cambios y modificaciones sin alejarse del alcance de la presente invención. Por ejemplo, aunque la presente invención describe un método y un dispositivo donde la longitud máxima de clave de cifrado, L , es de 5 bytes, y la longitud máxima utilizable de clave de encriptado, L_{max9} , es de 16 bytes, se notará que la presente invención no está limitada a esas longitudes. Además, también se notará que los datos transmitidos y recibidos no están limitados a ningún tipo de dato en particular. Puede constituirse por voz, datos escritos u otros. Puede ser binario, ASCII o cualquier otra forma de datos. Además, los datos pueden ser transmitidos por cualquier medio conocido como por ejemplo alambre o alambres aéreos o según se descubra más adelante.

REIVINDICACIONES

1. Un dispositivo de comunicación para calcular una clave de cifrado, K'_{cg} manipulando una clave de cifrado, K'_{cg} para utilizarse en un algoritmo de encriptado; dicho dispositivo consta de:

un elemento de memoria para almacenar uno o más polinomios;

una pluralidad de elementos de conmutación, cada uno con una primera entrada, una segunda entrada y una salida, donde dichos elementos de conmutación de primera entrada están conectados a dicho elementos de memoria;

una pluralidad de elementos de retardo, cada uno con una entrada y una salida, donde dicha salida de uno de dichos elementos de retardo está conectado a dichos elementos de segundas entradas; y

una pluralidad de funciones de adición, cada una con una primera entrada, una segunda entrada y una salida, donde:

dichas primeras entradas de funciones de adición están conectadas a todas excepto a una salida de dichos elementos de retardo,

dichas segundas entradas de función de adición están conectadas a todas excepto a una de salidas de dichos elementos, y

dichas salidas de función de adición están conectadas a todas excepto a una de dichos entradas de elementos de retardo.

2. El dispositivo de la Reivindicación 1, donde dichos elementos de conmutación son puertas AND.

3. El dispositivo de la Reivindicación 1, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado.

123 A
118

4. El dispositivo de la Reivindicación 3, donde el elemento de memoria almacena un polinomio $g_1(x)$, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j$$

y donde w es una longitud de palabra y L es un número de palabras de dicha clave de cifrado y $L_{\max}$ es el número máximo de palabras utilizables en la clave de encriptado, K'_c .

5. El dispositivo de la Reivindicación 4, donde dichos elementos de retardo inicialmente se cargan con dicha clave de cifrado, $K'_c(x)$.

6. El dispositivo de la Reivindicación 5, donde dicho polinomio $g_1(x)$ tiene unos primeros coeficientes $w(L_{\max}-L)$ iguales a una cadena fija.

7. El dispositivo de la Reivindicación 6, donde dicho polinomio $g_2(x)$ tiene unos últimos coeficientes wL iguales a una cadena fija.

8. El dispositivo de la Reivindicación 7, donde el último wL bits de dichos elementos de retardo almacenan un resultado de $K_c(x) \bmod g_1(x)$ después de los desplazamientos $w(L_{\max}-L)$.

9. El dispositivo de la Reivindicación 8, donde dichos elementos de retardo almacenan dicha clave de encriptado, K'_{c9} después de desplazamientos wL adicionales.

10. El dispositivo de la Reivindicación 1, donde dichos elementos de retardo son un registro de desplazamiento.

11. Un método para calcular una clave de encriptado, $K'_{c(x)}$, para encriptar datos que constan de los siguientes pasos:

obtener una clave de cifrado, K'_{c9} ;

determinar una longitud de clave de cifrado máxima, L ;

determinar una longitud de clave de encriptado utilizable máxima, $L_{\max}$

124. 2
118

obtener un polinomio $g_1(x)$;

obtener un polinomio $g_2(x)$, para extender los puntos de partida de dicha clave de encriptado, $K'_c(x)$; y

calcular dicha clave de encriptado, K'_{c9}

donde $K'_c(x) = g_2^{(L)}(x) [K_c(x) \bmod g_1^{(L)}(x)]$.

12. El método de la Reivindicación 11, además consta del paso de:

seleccionar dicho polinomio $g_2(x)$ basado en L .

13. El método de la Reivindicación 12, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0$$

y donde un grado alto de dicho polinomio $g_1(x)$ es igual a wL .

14. El método de la Reivindicación 13, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j.$$

15. El método de la Reivindicación 14, donde unos primeros coeficientes $w(L_{\max}-L)$ de $g_1(x)$ son iguales a una cadena fija.

16. El método de la Reivindicación 15, donde uno de los últimos coeficientes de $g_2(x)$ son iguales a una cadena fija.

17. El método de la Reivindicación 12, donde dicho paso de calcular se realiza utilizando una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, una pluralidad de elementos de retardo y una pluralidad de funciones de adición.

18. El método de la Reivindicación 17, donde dicho método además consta de los siguientes pasos:

125.119-A

inicializar dichas primeras entradas de dichas puertas AND a dichos coeficientes de polinomio $g_1(x)$, e

inicializar dichas segundas entradas de dichas puertas AND en cero.

19. El método de la Reivindicación 17, donde dichos elementos de retardo son un registro de desplazamiento.

20. Un sistema para comunicar datos encriptados entre dos dispositivos de comunicación que constan de:

un primer dispositivo de comunicación con una longitud de clave de cifrado, L_{max}^A , y

un segundo dispositivo de comunicación con una segunda longitud de clave de cifrado, L_{max}^B , y

un medio para determinar la longitud de clave de cifrado máxima, L , donde $1 \leq L \leq \min \{L_{max}^A, L_{max}^B\}$;

dicho primer dispositivo consta de:

un medio para obtener polinomios $g_1(x)$ y $g_2(x)$;

un medio para obtener una función de cifrado, $K_c(x)$; y

un medio para calcular una clave de encriptado, $K'_c(x)$,

donde $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$.

21. El sistema de la Reivindicación 20, donde dicho medio para calcular dicha clave de encriptado, $K'_c(x)$, consta de:

una pluralidad de puertas AND, cada una con una primera entrada, una segunda entrada y una salida, donde dicha primeras entradas de puerta están conectadas a dicho elemento de memoria;

una pluralidad de elementos de retardo, cada uno con una entrada y una salida, donde dicha salida de un elemento de retardo está conectado a dichas segundas entradas de puerta; y una pluralidad de funciones de adición, cada una con una primera entrada, una segunda entrada y una salida, donde dichas primeras entradas de funciones de adición están conectadas a todas excepto a una de dichas salidas del elemento de retardo, donde dichas segundas entradas

126. ~~126~~ 120

de funciones de adición están conectadas a todas excepto a una de dichas salidas de puerta y donde dichas salidas de funciones de adición están conectadas a todas excepto a una de dichas entradas del elemento de retardo.

22. El sistema de la Reivindicación 21, donde dichos elementos de retardo están inicialmente cargados con dicha clave de cifrado, $K'_c(x)$.

23. El sistema de la Reivindicación 20, donde dichos medios para obtener polinomios $g_1(x)$ y $g_2(x)$ incluye recuperar dichos polinomios de un elemento de memoria contenido dentro de dicho primer dispositivo de comunicación.

24. El sistema de la Reivindicación 23, donde

$$g_1(x) = \sum_{i=0}^{wL} g_i^{(1)} x^i, \quad g_{wL} \neq 0.$$

25. El sistema de la Reivindicación 24, donde

$$g_2(x) = \sum_{j=0}^{w(L_{\max}-L)} g_j^{(2)} x^j.$$

26. el sistema de la Reivindicación 25, donde el último wL bits de dichos elementos de retardo almacenan el resultado de $K_c(x) \bmod g_1(x)$ después de desplazamientos $w(L_{\max}-L)$.

27. El sistema de la Reivindicación 26, donde dichos elementos de retardo almacenan dicha clave de encriptado, $K'_c(x)$, después de desplazamientos adicionales wL .

28. El sistema de la Reivindicación 21, donde dichos elementos de retardo son un registro de desplazamiento.

RESUMEN

La presente invención incluye un método y un dispositivo para calcular una clave de encriptado, K'_{c9} para utilizarse en la inicialización de un algoritmo de encriptado. La presente invención revela un método para calcular la clave de encriptado, $K'_c(x)$, obteniendo una clave de cifrado, $K_c(x)$, determinando una longitud máxima de clave de cifrado, L , basados en los requerimientos de los dos dispositivos que desean comunicarse y determinar una longitud de clave de encriptado máxima utilizable, L_{max} . La clave de cifrado, $K_c(x)$, luego se manipula por medio de una función de adición o por medio de una función exclusivamente de o con un polinomio $g_1(x)$. El resultado se multiplica con un polinomio $g_2(x)$, que extiende los puntos de partida de dicha clave de encriptado, $K'_c(x)$. La clave de encriptado se determina de acuerdo con $K'_c(x) = g_2^{(L)}(x) [K_c(x) \bmod g_1^{(L)}(x)]$. El método para calcular la clave de encriptado K'_{c9} asegura que no se excede una longitud máxima de clave de cifrado. Además, el método proporciona nuevos puntos de partida posibles cada vez que se genera una nueva clave de encriptado K'_{c9} .

122

122
128-Ab

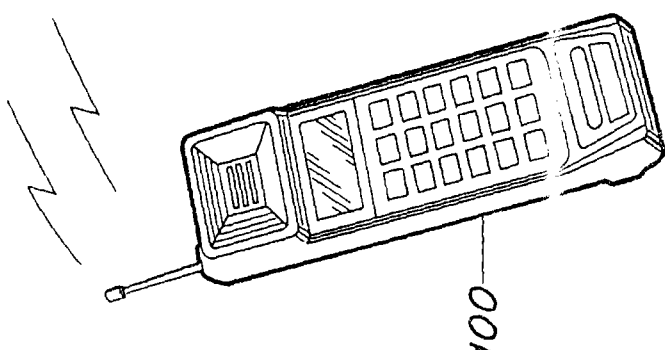
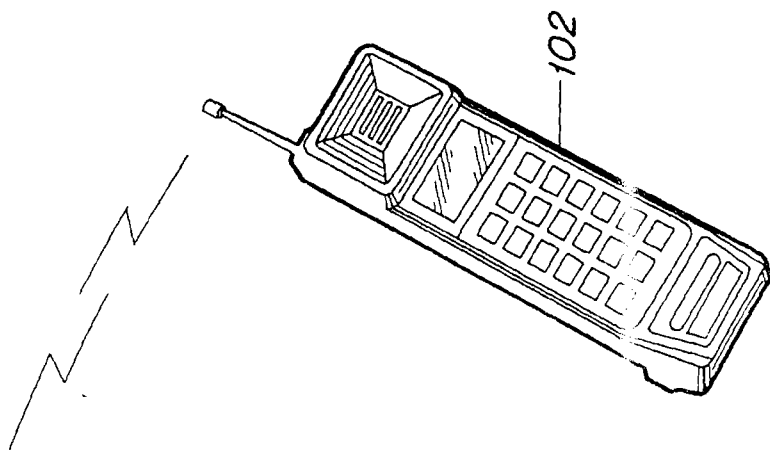
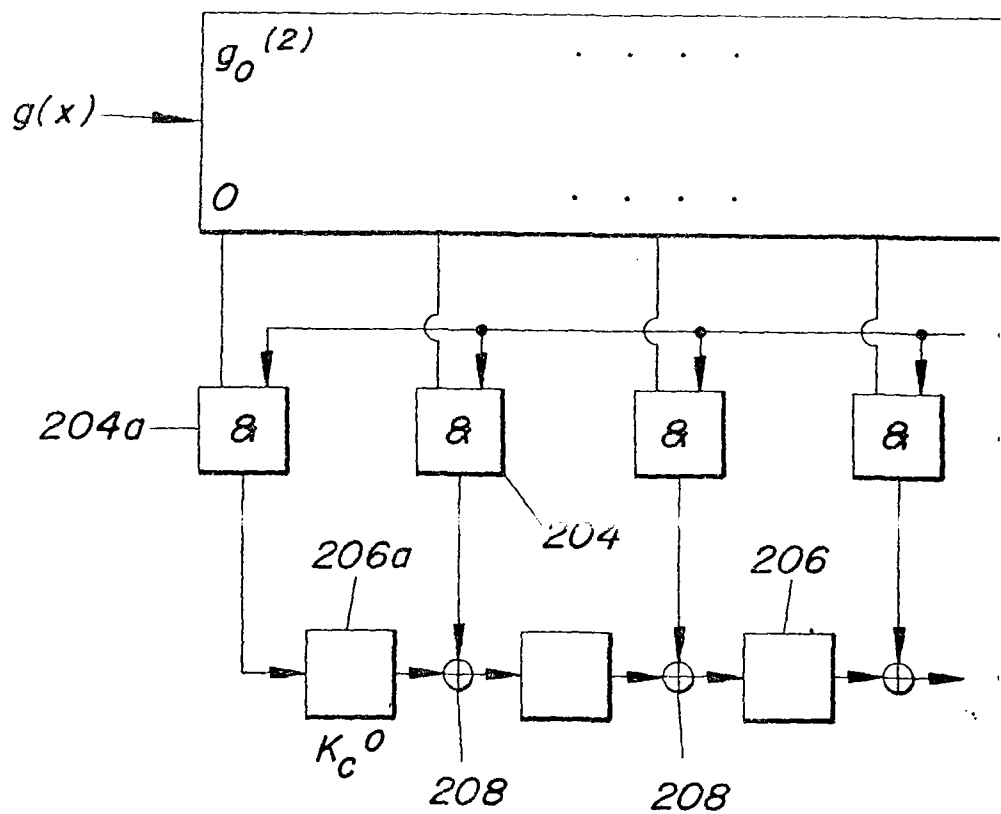


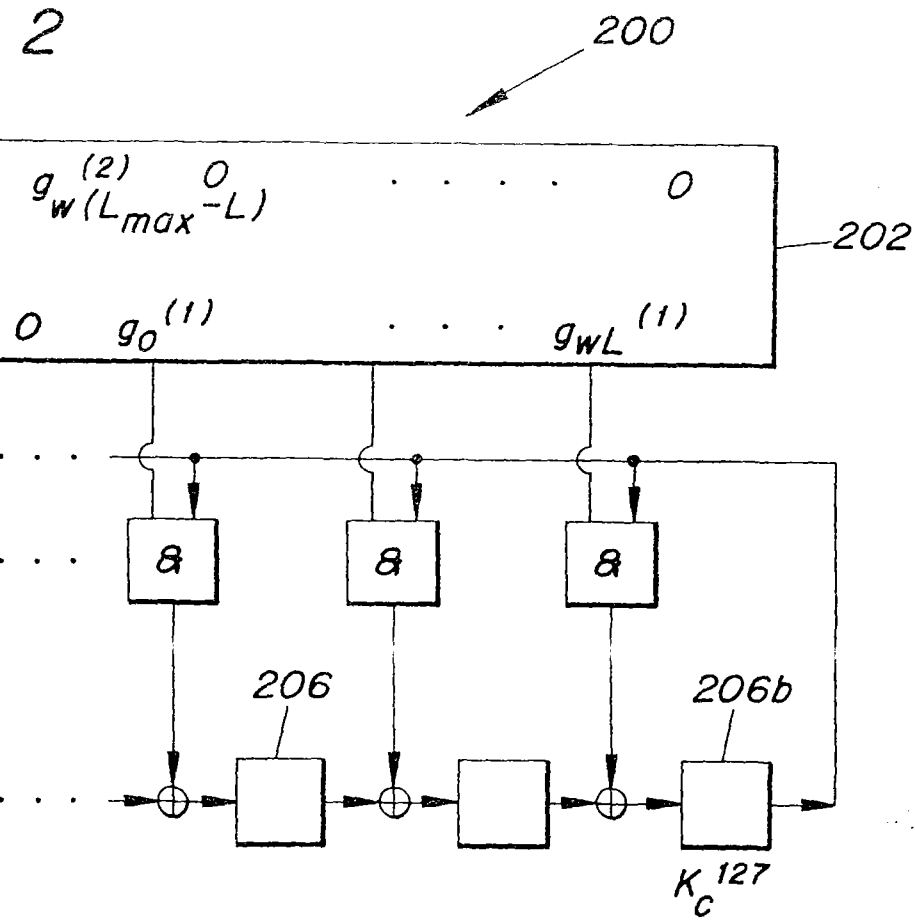
FIG. 1

FIG.



123

2

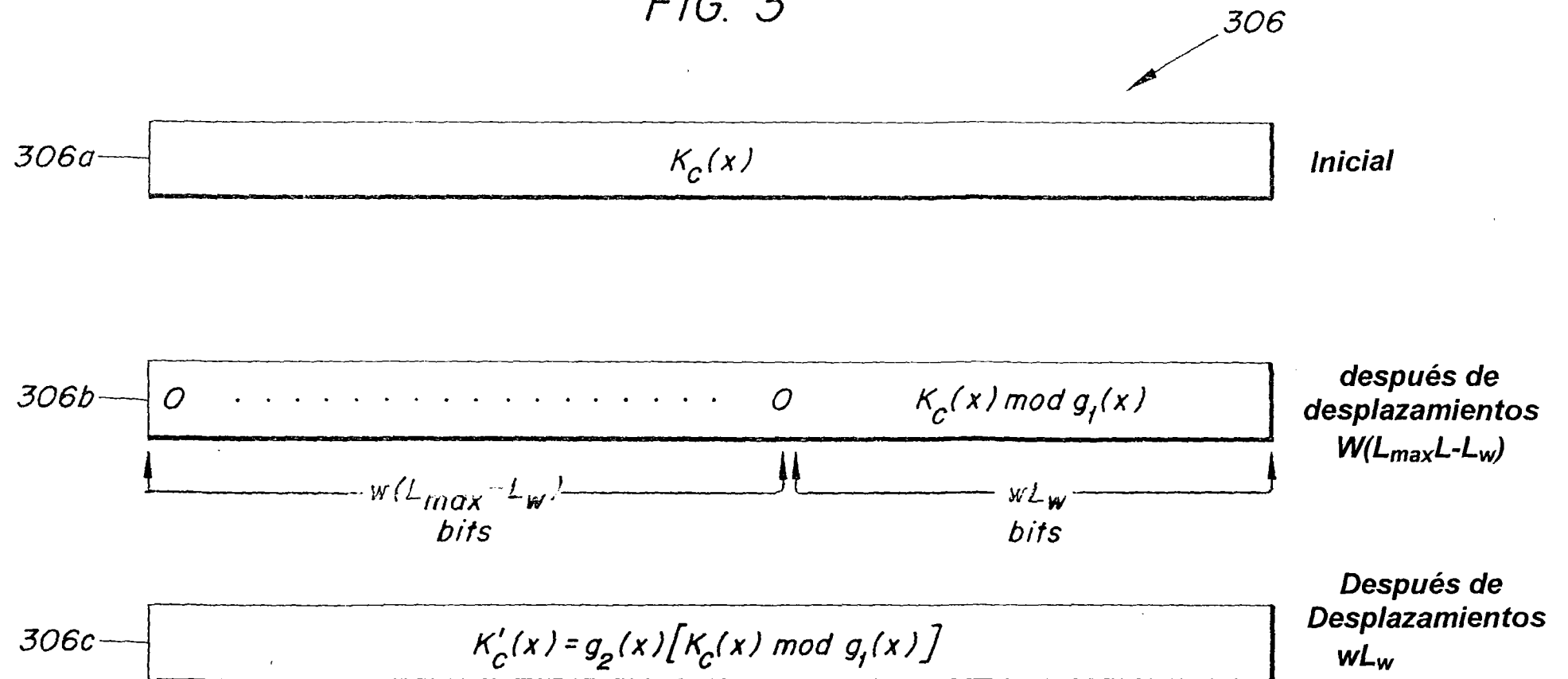


129

7

124

FIG. 3



120.

131.15 ~~10~~

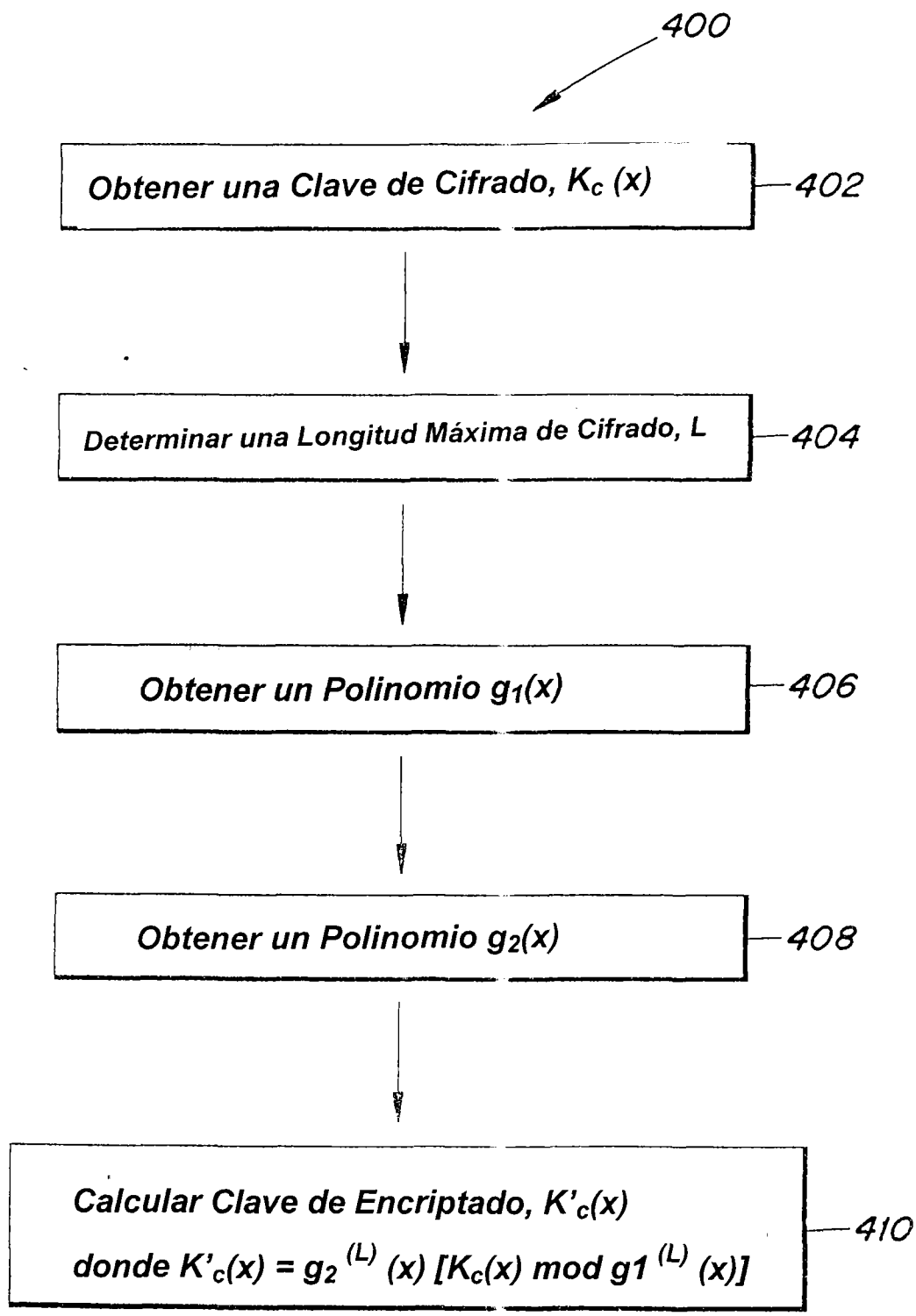


FIG. 4

folio 132 kayeto achiwo temar

febrero 17/03
uz



2do. EXAMEN DE FORMA PATENTE DE INVENCION

Folio 133

Radicación no 00-29649
Concepto Técnico no . 415
Clasificación Internacional de Patentes : H04L9/28//G09C1/00

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486 se determinó que esta solicitud de **Patente de Invención**:

- | | |
|--|---|
| SI ☒ NO ☐ | Contiene un resumen de la invención (Art.26-e). |
| SI ☒ NO ☐ | Contiene el título o nombre de la invención (Art.27-d). |
| SI ☒ NO ☐ | Contiene la descripción de la invención (Art.26-b). |
| SI ☒ NO ☐ | NO ES APLICABLE ☐ Contiene los dibujos necesarios para comprender la invención (Art.26-d) |
| SI ☒ NO ☐ | Contiene una o más reivindicaciones. (Art.26-c). |
| SI ☐ NO ☐ | NO ES APLICABLE ☒ Han sido desarrollados los productos y/o procedimientos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen. (Art. 26- h). |
| SI ☐ NO ☐ | NO ES APLICABLE ☒ Los productos y/o procedimientos han sido obtenidos o desarrollados a partir de los conocimientos tradicionales de las comunidades indígenas, afroamericanas, o locales de los países miembros, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes.(Art.26-i). |
| SI ☐ NO ☒ | La invención se refiere a un producto relativo a un material biológico. (Art.26-J). |
| SI ☒ NO ☐ | La prioridad coincide con la materia reivindicada. |
| SI ☒ NO ☐ | CUMPLE LOS REQUISITOS TÉCNICOS |

OBSERVACIONES Y OTROS: SI ☒ NO ☐ ver hoja(s) anexa(s)

EXAMINADOR TÉCNICO
202044

Bogotá D. C. Febrero 17 de 2003.



Folio 134

Concepto técnico no. 415

OBSERVACIONES

- ▣ Envía el documento mediante el cual reivindica la prioridad 60/130.944 Folios 45-56 y 09/461.766 Folios 65-102.
- ▣ Anexa la traducción del documento de prioridad 60/130.944 Folios 41-44 y 09/461.766 Folios 57-64.
- ▣ Anexa los dibujos alucivos a la invención. Folios 128-131.
- ▣ Anexa un nuevo capítulo descriptivo. Folios 106-121.
- ▣ anexa los artes finales. Folio 107.
- ▣ Anexa un nuevo capítulo reivindicatorio. Folios 122-126.

EXAMINADOR TECNICO

202044

Bogotá, Febrero 17 de 2003.

128



Industria y Comercio
SUPERINTENDENCIA

Folio 135

020
Bogotá DC

416
2003-02-18

Autor(a)
GERMAN CASTILLO GRAU
Acreditado(a)

REFERENCIA:	Radicación No.	00-29649
	Trámite	002
	Evento	001
	Actuación	416
	Oficio No.	373
	Folios	001

Se tiene en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial, conforme lo establece el artículo 40 de la misma Decisión.

los 18 FEB. 2003

E. VERGEL
Director General
20.

DIVISION DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No. 00-029649

EL EXTRACTO DE LA PRESENTE SOLICITUD DE **PATENTE DE INVENCION**
FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No **530**, DE
FECHA **31 DE JULIO DE 2003**, EL TERMINO HABIL SEÑALADO POR LA LEY
EXPIRA EL **28 DE OCTUBRE DE 2003**.

NOTA: Dentro del plazo de los seis (6) meses siguientes a partir de la fecha de publicación en la gaceta de Propiedad Industrial, deberá solicitar y cancelar el examen de patentabilidad so pena de que la solicitud caiga en abandono, de acuerdo con lo establecido en el Artículo 44 de la Decisión 486/2000.

SE PRESENTARON OPOSICIONES POR PARTE DE TERCEROS.

SI _____

NO ☒ _____

Bogotá D.C., Febrero de 2004

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RADICACIÓN: 0-29649

EDICTO No. 2524

LA SECRETARÍA GENERAL AD-HOC HACE SABER:

Que esta Superintendencia profirió **Resolución No. 2441 de 12-FEB-2004**. Que el contenido de la parte resolutive es como sigue: El Superintendente de Industria y Comercio.

RESUELVE

ARTICULO PRIMERO: Declarar abandonada la solicitud de privilegio de patente de invención contenida en el expediente de la referencia.

ARTICULO SEGUNDO: Notificar personalmente el contenido de la presente resolución al doctor Germán Castillo Grau, o a quien haga sus veces, en su calidad de apoderado de Telefonaktiebolaget LM Ericsson (publ)., entregándole copia de la misma, advirtiéndole que contra ella procede el recurso de reposición interpuesto ante el Superintendente de Industria y Comercio, al momento de la notificación o dentro de los 5 días hábiles siguientes a ella.

NOTIFÍQUESE Y CUMPLASE

Dada en Bogotá, D.C., a los 12 FEB. 2004

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,


JAIME RUBIO ESCOBAR

Para notificar a los interesados, se fija el presente EDICTO en lugar visible al público en la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, por el término de (10) diez días hábiles contados a partir de las 8:30 a.m. de hoy.

Secretaría General Ad-Hoc 04-MAR-2004
Secretaría General Ad-Hoc
EDICTO No. 2524

Este edicto se desfija hoy 17-MAR-2004 a las cinco (5:00 p.m.)