(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 177 536 B9

(12) **KORRIGIERTE EUROPÄISCHE PATENTSCHRIFT**
Hinweis: Bibliographie entspricht dem neuesten Stand

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 B1)
Korrekturen, siehe Seite(n) 2,3,7

(48) Corrigendum ausgegeben am:
24.05.2006 Patentblatt 2006/21

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
31.08.2005 Patentblatt 2005/35

(21) Anmeldenummer: **00926744.4**

(22) Anmeldetag: **21.03.2000**

(51) Int Cl.:
G07F 7/10 *(1974.07)* ***G07C 9/00*** *(1968.09)*

(86) Internationale Anmeldenummer:
PCT/EP2000/002481

(87) Internationale Veröffentlichungsnummer:
WO 2000/060551 (12.10.2000 Gazette 2000/41)

(54) VERFAHREN ZUR ABLEITUNG VON IDENTIFIKATIONSNUMMERN

METHOD OF DERIVING AN IDENTIFICATION NUMBER

PROCEDE POUR DERIVER DES NUMEROS D'IDENTIFICATION

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priorität: **30.03.1999 DE 19914407**

(43) Veröffentlichungstag der Anmeldung:
06.02.2002 Patentblatt 2002/06

(73) Patentinhaber: **Deutsche Telekom AG**
53113 Bonn (DE)

(72) Erfinder:
- **SCHWENK, Jörg**
  D-64807 Dieburg (DE)
- **MARTIN, Tobias**
  D-35466 Rabenau-Ruddinghausen (DE)

(74) Vertreter: **Gornott, Dietmar**
Zilleweg 29
64291 Darmstadt (DE)

(56) Entgegenhaltungen:
EP-A- 0 798 891
FR-A- 2 577 704
US-A- 3 846 622
US-A- 4 605 820

EP 1 177 536 B9

Beschreibung

[0001] Die Erfindung betrifft ein **Verfahren zur maschinellen Ableitung von Personen-Identifikations-Nummern (PINs)** für eine große Anzahl von Geldkarten oder anderen sicherheitsbedürftigen Einrichtungen, wobei die PINs aus einer Anzahl N dezimaler Ziffern bestehen, die jeweils einer Geldkarte oder einer sicherheitsbedürftigen Einrichtung zugeordnet sind, aus einer auf der Geldkarte oder Einrichtung gespeicherten binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode.

[0002] Bei der Verwendung automatischer Geldausgabesysteme oder ähnlicher mit einer Plastikkarte zu benutzenden Einrichtungen muß sich der Benutzer häufig mittels einer nur ihm bekannten vierstelligen Nummer (PIN) authorisieren. Es gibt jedoch bei weitem nicht soviele verschiedene PINs wie Benutzer, weshalb jede PIN mehrfach existiert.

[0003] Die PINs dürfen nur dezimale Ziffern enthalten, damit sie mit numerischen Tastaturen eingegeben werden können. Ferner sollen sie nicht mit einer Null beginnen. Daraus ergibt sich bei vier Stellen ein Bereich von 9000 unterschiedlichen PINs. Die theoretisch geringstmögliche Wahrscheinlichkeit, eine PIN zu erraten, beträgt somit 1/9000.

[0004] Aufgabe der vorliegenden Erfindung ist es, ein Verfahren anzugeben, welches die Wahrscheinlichkeit möglichst gering hält, daß eine PIN erraten werden kann. In FR 2 577 704 A1 wurde diese Aufgabe bereits erwähnt, jedoch nicht gelöst.

[0005] Wenn die PINs so erzeugt werden, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind, ist die Wahrscheinlichkeit, eine PIN zu erraten, minimal. Dies wird anhand des folgenden Beispiels erläutert.

[0006] Aus persönlichen Daten des Benutzers kann mit einem geheimen Schlüssel unter Zuhilfenahme eines Verschlüsselungsalgorithmus ein Binärcode erzeugt werden. Bei Verwendung des beispielsweise zur Erzeugung von PINs für Geldkarten vorgesehenen DES- oder Triple-DES-Algorithmus' wird mit Hilfe eines bankeigenen Schlüssels aus den Daten eines Kunden ein 64-stelliger Binärcode generiert. Aus einem Abschnitt von 16 Stellen dieses Binärcodes kann die PIN beispielsweise auf folgende Weise erzeugt werden:

[0007] Es werden vier Teile zu jeweils vier Stellen dieser binären Zahl zu vier Dezimalzahlen zusammengefaßt. Die vier Ziffern der PIN ergeben sich als Rest einer Division dieser vier Dezimalzahlen durch 10 (Modulo-Funktion). Falls die erste Ziffer eine Null ist, wird sie gegen eine Eins ausgetauscht. Die daraus resultierenden PINs sind jedoch in hohem Maße ungleichmäßig über den zur Verfügung stehenden Zahlenbereich von 1 bis 9000 verteilt. Die Wahrscheinlichkeit, eine derartig erzeugte PIN zu erraten, ist gar höher als 1/150, falls sie mit einer 1 beginnt.

[0008] Verteilt man die PINs dagegen gleichmäßig über den Zahlenbereich, so ist die Auftretenshäufigkeit einer jeden PIN konstant 1/9000 und daher ist auch die Wahrscheinlichkeit minimal, daß sie erraten wird.

[0009] Die Erfindung sieht vor, daß eine statistisch gleichmäßige Verteilung der PINs auf den zur Verfügung stehenden Zahlenbereich dadurch erzielt wird, daß zur Erstellung der Ziffern der PIN folgende Schritte ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus 210 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen Abbildungen hexadezimaler Ziffern in dezimale Ziffern in eine dezimale Ziffer umgesetzt,

  werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.

[0010] Für der Fall daß die erste Ziffer der PIN keine Null sein soll, wird in einer Weiterbildung der Erfindung vorgeschlagen, daß zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus 36 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
- die 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der

[0011] Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt.

[0012] Bei dem erfindungsgemäßen Verfahren wird aus N Gruppen von jeweils 4 bit Länge je eine Hexadezimalzahl gebildet. Diese soll nun in eine Dezimalziffer umgesetzt werden. Für diese Umsetzung stehen insgesamt (10 über 6) = (10 über 4) = 210 unterschiedliche Abbildungen der hexadezimalen Ziffern in die Menge der dezimalen Ziffern zur Verfügung. Eine mögliche Abbildung ist die Bildung des Rests bei der Division durch 10: (0 -> 0, 1 - > 1, 2 -> 2, 3 -> 3,

4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Nach dieser Abbildung treten die Ziffern 0 bis 5 jeweils mit der Häufigkeit von 1/8 und die Ziffern von 6 bis 9 mit der Häufigkeit 1/16 auf. Um nun Ziffern zu erhalten, deren Auftretenswahrscheinlichkeit nicht oder unmerklich von 1/10 abweicht, wird vorgeschlagen, die 210 Hexadezimalziffern, die beispielsweise durch 14-maliges Anwenden des o.g. DES-Algorithmus auf die 64-stellige binäre Ausgangszahl erzeugt wurden (daher Pseudo-Zufallszahl, da die erzeugte Zahl mitnichten zufällig entstanden ist), mit je einer anderen der 210 möglichen Abbildungen in eine Dezimalziffer umzusetzen und anschließend alle 210 Dezimalziffern mit einer Gruppenoperation einer mathematischen Gruppe mit zehn Elementen zu einer einzigen Ziffer zu verknüpfen. Die Auftretenswahrscheinlichkeit jeder so erzeugten dezimalen Ziffer liegt nahe bei 1/10.

[0013] Es ist bei einer nächsten Weiterbildung der Erfindung vorgesehen, daß die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der 210 Ziffern verwendet wird. Es werden dabei jeweils 210 Dezimalziffern zu einer einzigen Ziffer verknüpft, indem man alle Ziffern addiert und den Rest einer Division der Summe durch 10 als Ergebnis nimmt. Die dabei auftretenden zehn möglichen Ergebnisse sind die Elemente der additiven Gruppe $Z_{10,+}$.

[0014] Bei einer anderen Weiterbildung der Erfindung ist vorgesehen , daß die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der 210 Ziffern verwendet wird. Diese Gruppe $Z_{11}^{\bullet}$ weist ebenfalls zehn Elemente auf und eignet sich daher zur Verknüpfung der Zahlen zu einer Dezimalziffer. In $Z_{11}^{\bullet}$ rechnet man, indem man zwei Elemente multipliziert und das Ergebnis durch 11 dividiert. Der dabei bleibende Rest bildet das Ergebnis der Operation. Die Null ist aus der Gruppe ausgenommen. Die in den Ziffern auftretende 0 indiziert das Element Nr. 10 der Gruppe $Z_{11}^{\bullet}$.

[0015] Eine andere Weiterbildung der Erfindung sieht vor, daß die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen dieser Gruppe eine andere dezimale Ziffer zugeordnet wird. Dazu kann ferner vorgesehen sein, daß der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den fünf Spiegelungen um die fünf Symmetrieachsen des Fünfecks die Ziffern 5 bis 9 zugeordnet werden. Führt man zwei Symmetrieabbildungen hintereinander aus, so entsteht wieder eine Symmetrieabbildung. Es läßt sich mit diesen Zuordnungen die folgende Multiplikationstabelle aufstellen:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	5	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

[0016] Die 210 Ziffern werden mit Hilfe dieser Tabelle zu einer einzigen Ziffer verknüpft, indem sukzessiv mit dem Ergebnis der letzten Operation als Zeilenindikator und mit der nächsten Ziffer als Spaltenindikator das nächste Ergebnis in der Tabelle abgelesen wird, bis alle Ziffern berücksichtigt wurden. Das letze Ergebnis bildet die gesuchte Ziffer der PIN.

[0017] Ein Ausführungsbeispiel der Erfindung ist in der Zeichnung dargestellt und in der nachfolgenden Beschreibung näher erläutert. Die Figur zeigt ein Diagramm zur Erzeugung einer PIN durch Reduktion von Hexadezimalzahlen mit Hilfe mathematischer Gruppen.

[0018] Aus den persönlichen Daten Dc eines Kunden werden, wie in der Figur gezeigt, mit Hilfe eines geheimen Schlüssels und eines Zufallszahlen-Generators eine Folge von 210 Hexadezimalziffern erzeugt, indem beispielsweise ein Verschlüsselungsergebnis des DES-Algorithmus aus Fig. 1 wiederum mit dem Algorithmus verschlüsselt wird und so fort. Die daraus resultierenden 14 64-stelligen Binärcodes werden in 14 Hexadezimalzahlen Hi mit je 16 Stellen gewandelt. Aneinandergehängt gibt das 224 Hexadezimalziffern, wovon 210 in die Erzeugung der PIN eingehen.

[0019] Es gibt 210 unterschiedliche Möglichkeiten fi, die Menge der 16 Hexadezimalziffern in die Menge der 10 Dezimalziffern abzubilden. Jede der 210 Hexadezimalziffern wird daher mit einer anderen dieser Abbildungen in eine Dezimalziffer di umgesetzt. Um aus den 210 Dezimalziffern eine Ziffer Zi einer PIN zu erzeugen, werden diese mit Hilfe der Gruppenoperation F einer beliebigen zehnelementigen mathematischen Gruppe nacheinander verknüpft; das letzte Ergebnis ist die gesuchte Ziffer. Die vorher ungleichmäßige statistische Verteilung der 210 Dezimalziffern wird damit

vergleichmäßigt. Der gesamte Vorgang wird für jede der Stellen Z2 bis Z4 der PIN erneut durchgeführt.

[0020] Für die erste Ziffer der PIN werden analog 36 Hexadezimalziffern erzeugt, die mit je einer anderen der 36 möglichen Abbildungen der Hexadezimalziffern in die Menge der Ziffern 1 bis 9 in eine Ziffer zwischen 1 und 9 abgebildet werden. Die 36 Dezimalziffern werden mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 zu der ersten Ziffer der PIN verknüpft. Es lassen sich damit 9000 unterschiedliche PINs erzeugen, die annähernd gleichmäßig verteilt sind. Bei der Erzeugung von 10^5 PINs betrugen die maximalen Ungleichmäßigkeiten etwa 1,5 Prozent, was die Wahrscheinlichkeit, daß eine PIN zufällig erraten wird, nicht nennenswert gegenüber dem theoretischen Minimalwert erhöht. Das Verfahren arbeitet damit sehr zuverlässig.

[0021] Zur Anwendung in diesem Verfahren eignen sich grundsätzlich alle mathematischen Gruppen, die zehn Elemente aufweisen. Bekannte Vertreter sind die additive Gruppe der ganzen Zahlen Modulo 10, $Z_{10,+}$, die multiplikative Gruppe der ganzen Zahlen Modulo 11, Z_{11}^{*}, sowie die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks D5, die sogenannte Diedergruppe. Im letzten Falle wird den einzelnen Elementen der Gruppe je eine Dezimalziffer zugeordnet, mit der sich rechnen läßt.

Patentansprüche

1. Verfahren zur maschinellen Ableitung von Personen-Identifikations-Nummern (PINs) für eine große Anzahl von Geldkarten oder anderen sicherheitsbedürftigen Einrichtungen, wobei die PINs aus einer Anzahl N dezimaler Ziffern bestehen, die jeweils einer Geldkarte oder einer sicherheitsbedürftigen Einrichtung zugeordnet sind, aus einer auf der Geldkarte oder Einrichtung gespeicherten binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode, **dadurch gekennzeichnet, daß** eine statistisch gleichmäßige Verteilung der PINs auf den zur Verfügung stehenden Zahlenbereich **dadurch** erzielt wird, daß zur Erstellung der Ziffern der PIN folgende Schritte ausgeführt werden:

   - aus der binären Zahl der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus 210 hexadezimalen Ziffern besteht,
   - jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen Abbildungen hexadezimaler Ziffern in dezimale Ziffern, in eine dezimale Ziffer umgesetzt,
   - die 210 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:

   - aus der binären Zahl der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus 36 hexadezimalen Ziffern besteht,
   - jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
   - die 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der 210 Ziffern verwendet wird.

4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der 210 Ziffern verwendet wird.

5. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen dieser Gruppe eine andere dezimale Ziffer zugeordnet wird.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, daß** der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den fünf Spiegelungen um die fünf Symmetrieachsen des

Fünfecks die Ziffern 5 bis 9 zugeordnet werden.

Claims

1. Method for machine derivation of personal identification numbers (PINs) for a large number of debit cards or other instruments requiring security, said PINs consisting of a number N of decimal digits, each said PIN being assigned - from a binary number with L places stored on the debit card or instrument, in particular a person-specific binary code - to a debit card or instrument requiring security, **characterized in that** a statistically uniform distribution of the PINs over the range of available numbers is achieved **in that** the following steps are carried out to generate the digits of the PIN:

   - a pseudorandom number consisting of 210 hexadecimal digits is generated from the binary number of length L,
   - each hexadecimal digit of said number is transformed into a decimal digit by a different one of the 210 possible mathematical mappings of hexadecimal digits to decimal digits,
   - to make uniform the probability of occurrence of the particular digit of the pin, the 210 decimal digits of the number thus generated are combined with one another, by a group operation of an arbitrary mathematical group of order 10, into a decimal digit representing the particular digit of the PIN.

2. Method according to claim 1, **characterized in that** the following steps are carried out to generate the first digit of the PIN:

   - a pseudorandom number consisting of 36 hexadecimal digits is generated from the binary number of length L,
   - each hexadecimal digit of said number is transformed into a digit from 1 through 9 by a different one of the 36 possible mathematical mappings of hexadecimal digits to the digits 1 through 9,
   - to make uniform the probability of occurrence of the particular digit of the pin, the 36 decimal digits of the number thus generated are combined with one another, by a group operation of an arbitrary mathematical group of order 9, into a nonzero decimal digit representing the first digit of the PIN.

3. Method according to claim 1 or 2, **characterized in that** the additive group of the integers modulo 10 is used to combine the 210 digits.

4. Method according to claim 1 or 2, **characterized in that** the multiplicative group of the integers modulo 11 is used to combine the 210 digits.

5. Method according to claim 1 or 2, **characterized in that** the group of symmetry mappings of a regular pentagon (dihedral group) is used to combine the 210 digits, each of the ten symmetry mappings of said group being assigned to a different decimal digit.

6. Method according to claim 5, **characterized in that** the digit 0 is assigned to the identity mapping, the digits 1 through 4 are assigned to the four rotations about the center point of the pentagon, and the digits 5 through 9 are assigned to the five reflections about the five axes of symmetry of the pentagon.

Revendications

1. Procédé de dérivation automatique de numéros d'identification personnels (PIN) pour un grand nombre de cartes de paiement ou autres dispositifs demandant sécurisation, les PIN étant constitués d'un nombre N de chiffres décimaux, chacun assigné à une carte de paiement ou à un dispositif demandant sécurisation, d'un nombre binaire de L chiffres mémorisé sur la carte de paiement ou le dispositif, notamment d'un code binaire personnel, **caractérisé en ce qu'**une répartition statistiquement homogène des PIN sur la gamme des nombres disponibles est assurée par les opérations suivantes à effectuer pour la détermination des chiffres du PIN :

   - à partir du nombre binaire de longueur L, un nombre pseudo-aléatoire est généré, composé de 210 chiffres hexadécimaux,
   - chaque chiffre hexadécimal de ce nombre est transformé en un chiffre décimal chaque fois avec une fonction mathématique différente parmi les 210 fonctions possibles entre chiffres hexadécimaux et chiffres décimaux,
   - pour homogénéisation de la probabilité d'occurrence des différents chiffres du PIN, les 210 chiffres décimaux

du nombre ainsi généré sont combinés par une opération de groupe d'un groupe mathématique quelconque d'ordre 10 en un chiffre décimal qui représente le chiffre correspondant du PIN.

2. Procédé selon la revendication 1, **caractérisé en ce que** l'on procède de la manière suivante pour déterminer le premier chiffre du PIN :

   - à partir du nombre binaire de longueur L, un nombre pseudo-aléatoire est généré, composé de 36 chiffres hexadécimaux,
   - chaque chiffre hexadécimal de ce nombre est transformé en un chiffre de 1 à 9 chaque fois avec une fonction mathématique différente parmi les 36 fonctions possibles entre chiffres hexadécimaux et les chiffres 1 à 9,
   - pour homogénéisation de la probabilité d'occurrence des différents chiffres du PIN, les 210 chiffres décimaux du nombre ainsi généré sont combinés par une opération de groupe d'un groupe mathématique quelconque d'ordre 9 en un chiffre décimal différent de zéro, qui représente le premier chiffre du PIN.

3. Procédé selon l'une des revendications 1 ou 2, **caractérisé en ce que** le groupe additif des entiers modulo 10 est utilisé pour la combinaison des 210 chiffres.

4. Procédé selon l'une des revendications 1 ou 2, **caractérisé en ce que** le groupe multiplicatif des entiers modulo 11 est utilisé pour la combinaison des 210 chiffres.

5. Procédé selon l'une des revendications 1 ou 2, **caractérisé en ce que** le groupe des fonctions symétriques d'un pentagone régulier (groupe dièdre) est utilisé pour la combinaison des 210 chiffres, chacune des dix fonctions symétriques de ce groupe se voyant assigner un autre chiffre décimal.

6. Procédé selon la revendication 5, **caractérisé en ce que** le chiffre 0 est assigné à la fonction identique, les chiffres 1 à 4 aux quatre rotations autour du centre du pentagone et les chiffres 5 à 9 aux cinq réflexions par rapport aux cinq axes de symétrie du pentagone.

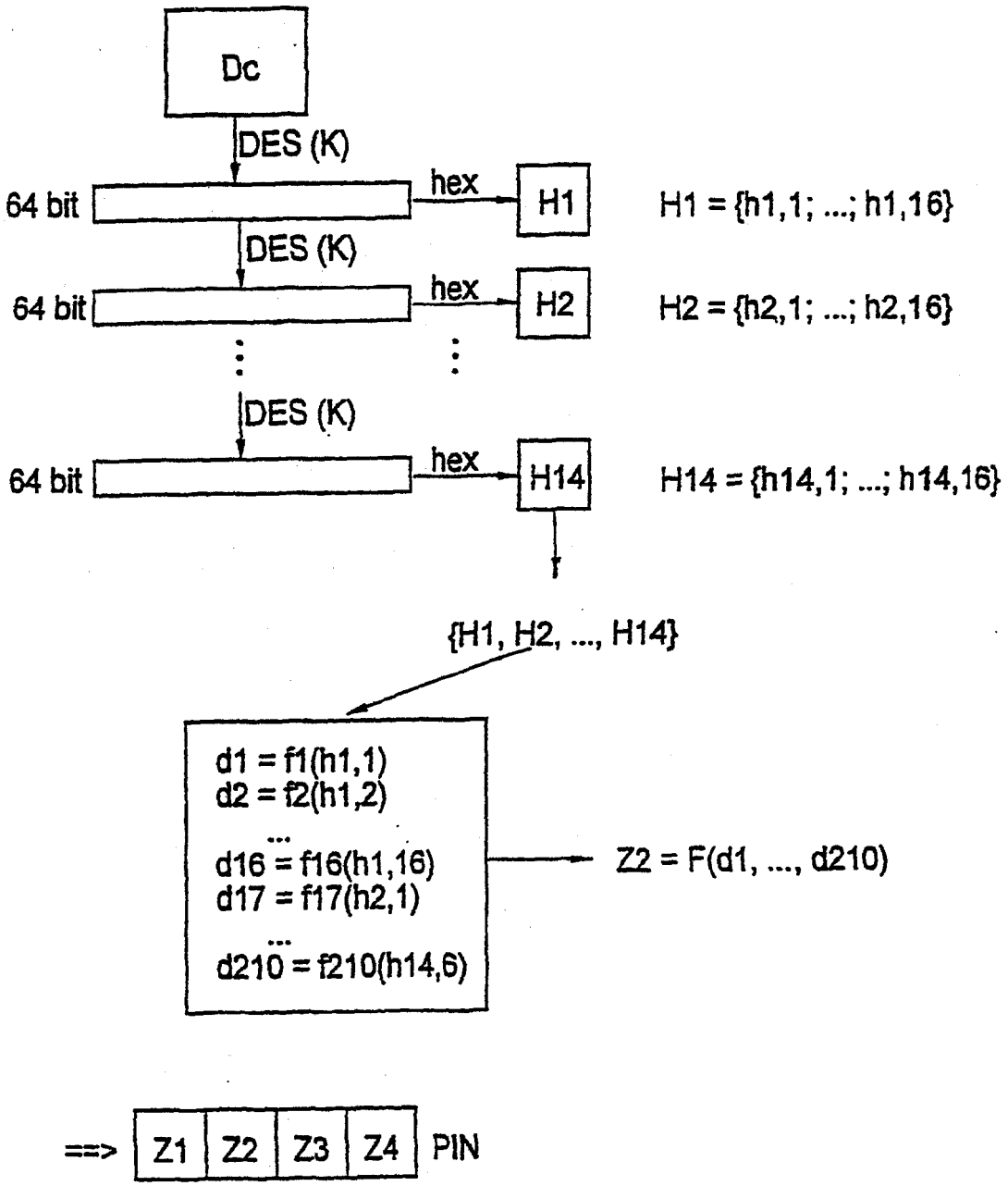
Dc
DES (K)
64 bit
hex
H1
H1 = {h1,1; ...; h1,16}
DES (K)
64 bit
hex
H2
H2 = {h2,1; ...; h2,16}
DES (K)
64 bit
hex
H14
H14 = {h14,1; ...; h14,16}
{H1, H2, ..., H14}
d1 = f1(h1,1)
d2 = f2(h1,2)
...
d16 = f16(h1,16)
d17 = f17(h2,1)
...
d210 = f210(h14,6)
Z2 = F(d1, ..., d210)
==>
Z1
Z2
Z3
Z4
PIN

Fig. 1