Octrooiraad

(12) A **Terinzagelegging** (11) **8403416**

Nederland (19) NL

(54) **Elektronisch sleutelgeheugenmoduul.**

(51) Int.Cl⁴.: G09C 1/00, H04K 1/02, H04L 9/04.

(71) Aanvrager: ANT Nachrichtentechnik GmbH te Backnang, Bondsrepubliek Duitsland.

(74) Gem.: Ir. G.F. van der Beek c.s.
NEDERLANDSCH OCTROOIBUREAU
Joh. de Wittlaan 15
2517 JR 's-Gravenhage.

(21) Aanvrage Nr. 8403416.

(22) Ingediend 8 november 1984.

(32) Voorrang vanaf 10 november 1983.

(33) Land van voorrang: Bondsrepubliek Duitsland (DE).

(31) Nummer van de voorrangsaanvrage: P 3340582 .

(62) - -

(43) Ter inzage gelegd 3 juni 1985.

De aan dit blad gehechte stukken zijn een afdruk van de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en).

T

Elektronisch sleutelgeheugenmoduul

Elektronische codeerinrichtingen die voor het coderen van gegevens of spraak worden toegepast, vereisen als geheim element een zogenaamde grondsleutel.

Deze grondsleutel wordt bij moderne codeerinrichtingen via een elektrische of optische koppelinrichting ingevoerd en in een elektronisch geheugen opgeslagen en/of voor het vooraf instellen van het codeeralgoritme gebruikt.

Voor de overdracht en voor het invoeren van de sleutel kunnen verschillende gegevensdragers en invoerinrichtingen worden toegepast, bijvoorbeeld ponsbanden en ponsbandlezers. In toenemende mate worden hiervoor elektronische, draagbare geheugenmodulen toegepast, waarin de sleutel of sleutels in bijvoorbeeld RAM-geheugens worden vastgelegd, die door een batterij worden gebufferd. Deze geheugenmodulen kunnen thans worden ingestoken in het met één of meer sleutels te laden codeerinrichting om de sleutel over de op deze wijze tot stand gebrachte verbinding over te dragen.

Aangezien de grondsleutel(s) het belangrijkste geheime element in de codeertechniek voorstellen, is het van belang een misbruik resp. verraad van de vastgelegde sleutel op betrouwbare wijze te verhinderen.

Thans tracht men dit in het algemeen te bereiken door organisatorische maatregelen. Men vertrouwt het overdragen van het sleutelmateriaal slechts toe aan bijzonder verbonden en betrouwbaar personeel.

Het zou uiteraard beter zijn om een werkwijze te vinden, waarbij een verraad van het sleutelmateriaal tijdens het transport met technische middelen, onafhankelijk van de betrouwbaarheid van het personeel wordt verhinderd.

Een diefstal van het volledige, met de geheime sleutels geladen sleutelmoduul zal direkt worden opgemerkt, aangezien het moduul in dit geval niet bij de ontvanger terechtkomt. De sleutels zouden dan in het geheel niet worden gebruikt en zouden dus voor de dief waardeloos zijn.

Een andere mogelijkheid om de sleutels te stelen zou echter kunnen zijn, dat deze sleutels tijdens het transport door middel van een geschikte hulpinrichting uit het geheugenmoduul worden gekopiëerd. Ook een inrichting in het sleutelgeheugenmoduul die een meermalen uitlezen van een sleutel verhindert, doordat deze, na de uitvoer van de sleutel, deze in het geheugen direkt wist, biedt hier geen wezenlijk grotere

veiligheid. De dief zou de gekopiëerde sleutel weer in het sleutelgeheugenmoduul kunnen terugschrijven, of een sleutelgeheugenmoduul dat een gelijk uiterlijk heeft en gelijk functioneert, met de gestolen sleutels kunnen laden en dit moduul aan de rechtmatige ontvanger kunnen overhandigen.

De uitvinding heeft daarom ten doel de mogelijkheid om de inhoud van een sleutelgeheugenmoduul te kopiëren, met technische middelen op betrouwbare wijze te verhinderen.

In de fig. 1 en 2 is dit schematisch weergegeven. Het sleutelgeheugenmoduul is met het verwijzingsnummer 1 aangegeven. Dit bevat het gegevensgeheugen 2 en de daarop aangesloten sleutelgenerator 3. De instelling vooraf van de sleutelgenerator wordt uitgevoerd door middel van gegevens B die van buitenaf direkt kunnen worden toegevoerd aan de ingang 4 tezamen met uit het gegevensgeheugen 2 afgenomen gegevens A die via de ingang 8 aan de sleutelrekeninrichting 3 kan worden toegevoerd. De sleutelgenerator 3 bezit een uitgang 5 via welke een door de sleutelgenerator 3 opgewekte grondsleutel C aan een aangesloten codeerinrichting wordt toegevoerd. Het gegevensgeheugen 2 heeft een externe ingang 6 voor het laden; er is echter geen uitgang voor het uitlezen van zijn inhoud buiten het sleutelgeheugenmoduul 1 aanwezig. Het gegevensgeheugen 2 kan in een aantal geheugengebieden a, b ...f worden verdeeld, die van buitenaf via de ingang 7 kunnen worden geadresseerd. Men zal het geheugen bij voorkeur zodanig uitvoeren, dat de inhoud daarvan na een voorafbepaald aantal $n \geq 1$ uitleesbewerkingen automatisch wordt gewist. Als geheugen is een zogenaamde RAM met voeding door een ingebouwde batterij geschikt. Als sleutelgenerator 3 dient een blokversleutelgenerator die bij voorkeur als DES (vergelijk Nat. Bur. Stand. (US) Fed. Info. Process. Stand. Publ. (FIPS PUB) 46, 17 pagina's (1977, jan. 15)) is uitgevoerd. Men kan de van het gegevensgeheugen 2 afgenomen gegevens A en de van buitenaf toegevoerde gegevens B aan de beide ingangen 4 en 8 van de sleutelgenerator 3 in gemengde vorm toevoeren en/of vooraf bij elkaar optellen (moduul 2).

Uit het Europese octrooischrift 22.069 is het weliswaar bekend om het sleutelgeheugenmoduul (aldaar "Schlüsselbehälter" genoemd) met een kwartsklok uit te voeren, die de sleutel slechts gedurende bepaalde "tijdvensters" voor het uitlezen vrijgeeft en dus een onbevoegd uitlezen van de opgeslagen sleutels voorafgaand aan de voorafbepaalde tijd verhindert.

Dit heeft echter enige nadelen, dat in het bijzonder de opgeslagen sleutels slechts op de voorafbepaalde tijdstippen kunnen worden ge-

bruikt. De geheugenmodulen kunnen dus niet "op voorhand" worden geladen en ter beschikking worden gesteld. Dit vereist ingewikkelde organisatorische maatregelen. Bij de werkwijze volgens de uitvinding resp. de schakeling volgens de uitvinding worden deze nadelen vermeden.

De basisgedachte van de uitvinding bestaat daarin, dat het sleutelgeheugenmoduul nooit zijn eigenlijke geheugeninhoud direkt kan uitvoeren, maar dat een uit te voeren grondsleutel eerst bij afroep door de te laden sleutelinrichting door een in het sleutelgeheugenmoduul geïntegreerde sleutelgenerator uit een in het sleutelmoduul opgeslagen geheime "bronsleutel" en een "hulpsleutel" die uit de te laden sleutelinrichting aan het sleutelgeheugenmoduul wordt toegevoerd, wordt berekend. Een ontsleutelen van een kryptogram is dus slechts mogelijk wanneer bij de ontvanger dezelfde grondsleutel en om dit te bereiken dezelfde bronsleutel en hulpsleutel als bij de afzender aanwezig zijn. De bronsleutel kan niet worden uitgelezen en dus niet door een dief worden gekopiëerd. De hulpsleutel wordt eerst opgewekt, wanneer gewaarborgd is dat het sleutelgeheugenmoduul bij de rechtmatige ontvanger is aangekomen. De dief heeft dus ook geen mogelijkheid reeds vooraf een later gebruikte grondsleutel te kunnen uitvoeren. Wanneer de hulpsleutel uit bijvoorbeeld 30 bits bestaat, dan is de waarschijnlijkheid dat de dief door uitproberen toevallig op een juiste grondsleutel komt, gelijk aan 2^{-30} of kleiner dan 10^{-10}.

De hulpsleutel kan daarbij bij het voortbrengen van een kryptogram door middel van een toevalsbitreeksgenerator worden opgewekt en tezamen met het kryptogram naar de ontvanger worden overgedragen. Er kan hiervoor ook de bij de meeste sleutelinrichtingen toch al vereiste "spreuksleutel" of "initieervariabele" mede worden gebruikt.

CONCLUSIES

1. Sleutelgeheugenmoduul, met het kenmerk, dat dit een van buitenaf elektrisch laadbaar en wisbaar gegevensgeheugen (2) bevat en een sleutelgenerator (3) bezit, die door middel van gegevens (A) uit dit gegevensgeheugen (2) en van buitenaf direkt toe te voeren gegevens (B) vooraf kan worden ingesteld en dat een uitgang (5) aanwezig is, via welke een door deze sleutelgenerator (3) opgewekte grondsleutel (C) aan een aangesloten sleutelinrichting kan worden toegevoerd, waarbij het gegevensgeheugen (2) een externe ingang (6) voor het laden daarvan, maar geen uitgang voor het uitlezen van zijn inhoud buiten het sleutelgeheugenmoduul (1) bezit.

2. Sleutelgeheugenmoduul volgens conclusie 1, met het kenmerk, dat het gegevensgeheugen (2) is verdeeld in een aantal geheugengebieden (a, b ...f) die van buitenaf adresseerbaar zijn (7 fig. 2).

3. Sleutelgeheugenmoduul volgens conclusie 1 of 2, met het kenmerk, dat de inhoud van een geheugengebied (a, b, ...f) van het gegevensgeheugen na een voorafbepaald aantal van n uitleesbewerkingen wordt gewist, waarbij $n \geq 1$ is.

4. Sleutelgeheugenmoduul volgens één van de voorafgaande conclusies, met het kenmerk, dat het gegevensgeheugen (2) met een RAM met een voeding door een ingebouwde batterij is uitgevoerd.

5. Sleutelgeheugenmoduul volgens één van de voorafgaande conclusies, met het kenmerk, dat als sleutelgenerator (3) een blokversleutelgenerator wordt toegepast, waarbij de gegevens A uit het gegevensgeheugen (2) aan de sleutelgeneratoringang en de van buitenaf direkt toe te voeren gegevens (B) aan de ingang voor begrijpelijke resp. geheime tekst worden toegevoerd en waarbij de aan de uitgang (5) afgegeven grondsleutel (C) wordt afgenomen van de uitgang voor geheime resp. begrijpelijke tekst.

6. Sleutelgeheugenmoduul volgens conclusie 5, met het kenmerk, dat de aan het gegevensgeheugen (2) afgenomen gegevens (A) en de van buitenaf toe te voeren gegevens (B) aan de beide ingangen (8, 9) van de sleutelgenerator (3) volgens een gemengde volgorde worden toegevoerd en/of ook ten dele vooraf bij elkaar worden opgeteld (modulo 2).

=====

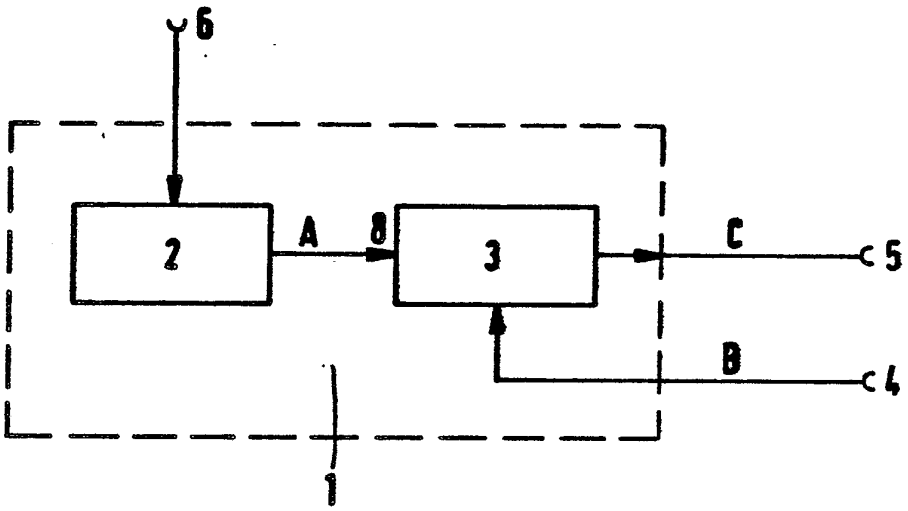

FIG. 1