
Octrooiraad



⑫ A **Terinzagelegging** ⑪ **8903111**

Nederland

⑲ **NL**

⑤4 **Geheugenkaart met vluchtig datageheugen.**

⑤1 Int.Cl.⁵: G06K 19/073, G07F 7/12.

⑦1 Aanvrager: N.V. Philips' Gloeilampenfabrieken te Eindhoven.

⑦4 Gem.: Ir. J.E.M. Galama c.s.
Internationaal Octrooibureau B.V.
Prof. Holstlaan 6
5656 AA Eindhoven.

②1 Aanvraag Nr. 8903111.

②2 Ingediend 20 december 1989.

③2 - -

③3 - -

③1 - -

⑥2 - -

④3 Ter inzage gelegd 16 juli 1991.

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

N.V. Philips' Gloeilampenfabrieken te Eindhoven
Geheugenkaart met vluchtig datageheugen.

De uitvinding heeft betrekking op chip-geheugenkaart met een chip die voorzien is van een datageheugen en van detectiemiddelen om de geheugenkaart onklaar te maken in responsie op een niet door de geheugenkaart geautoriseerde actie voor het verkrijgen van toegang tot
5 het datageheugen.

Een dergelijke chip-geheugenkaart is bekend uit het artikel "Smart Card" van A.J. Selezneff in "Philips Telecommunications and Data Systems review", Volume 45, nr.4, December 1987. De chip zelf (ook wel 'geïntegreerde schakeling' genaamd) is geplaatst op een
10 gedrukte circuitplaat (printed circuit film), waarbij de circuitplaat contactvlakken bevat voor de invoer en uitvoer van data. De geïntegreerde schakeling en de circuitplaat is als één geheel aangebracht in de plastic geheugenkaart. De geïntegreerde schakeling bevat een centrale besturingseenheid en een datageheugen dat voor opslag
15 van gegevens kan dienen maar tevens een programma kan bevatten voor de bewerking van de gegevens of voor de aansturing van de centrale besturingseenheid; het woord 'data' heeft hier een ruime betekenis. Het datageheugen is als een EPROM-geheugen (Electrically Programmable Read Only Memory) uitgevoerd, waarbij de data met behulp van ultra-violet
20 licht worden gewist. Het datageheugen kan ook als een EEPROM-geheugen (Electrically Erasable Programmable Read Only Memory) zijn uitgevoerd, waarbij de data door een 'erase'-spanning worden uitgewist. Beide geheugens hebben de eigenschap dat het geheugen data bewaart ook wanneer het geheugen niet met een voedingsbron is verbonden.

25 Een van de niet geautoriseerde acties is een actie die niet overeenkomt met het vooraf vastgestelde protocol waarmee een geautoriseerde gebruiker toegang verkrijgt tot het datageheugen om data in te schrijven of te uit te lezen. Dit protocol behelst het toevoeren van een codewoord aan de geheugenkaart door de gebruiker. Met behulp van
30 in het datageheugen opgeslagen identificatiecodes wordt het aan de geheugenkaart aangeboden codewoord onderzocht door de detectiemiddelen. Indien de identificatie correct blijkt te zijn wordt toegang tot het

89 03 111.

datageheugen verleend. Wanneer de identificatie echter niet correct blijkt te zijn wordt geen toegang tot het datageheugen verleend, en indien bijvoorbeeld drie keer achter elkaar een foute identificatie is geconstateerd wordt het datageheugen via de detectiemiddelen onklaar gemaakt. Het onklaar maken van het datageheugen gebeurt afhankelijk van het type datageheugen door het bestralen van de geïntegreerde schakeling met ultra-violet licht of door het elektrisch wissen van de datacellen in het datageheugen.

Een verdere ongeautoriseerde actie is het verwijderen van de plastic oppervlaktelaag tegenover de geïntegreerde schakeling. Hierdoor kan men de geïntegreerde schakeling uit de geheugenkaart lichten of is het mogelijk om met behulp van elektronenmicroscopen of met behulp van andere analytische methoden data in het datageheugen uit te lezen. Ook is het dan mogelijk om het datageheugen via daarvoor bestemde contactvlakken op de circuitplaat te adresseren en uit te lezen. Uit de aldus verkregen data kunnen de identificatiegegevens gededuceerd worden.

De uitvinding beoogt een verbeterde bescherming van de data in het datageheugen en beoogt ongeautoriseerde toegang tot de data in het datageheugen te voorkomen.

De geheugenkaart volgens de uitvinding heeft het kenmerk dat de geheugenkaart een voedingsbron bevat voor het voeden van het datageheugen waarbij het datageheugen een vluchtig geheugen is, en dat de geheugenkaart een schakelaar bevat met een eerste toestand en met een tweede toestand waarbij de detectiemiddelen bij detectie van een niet geautoriseerde actie de schakelaar vanuit de eerste toestand in de tweede toestand brengen om de geheugenkaart onklaar te maken.

De uitvinding is berust op het inzicht dat het gebruiken van een vluchtig datageheugen dat slechts data bewaart in het geval dat het geheugen verbonden is met een voedingsbron. Deze voedingsbron dient om de gehele geïntegreerde schakeling van spanning te voorzien. Indien de detectiemiddelen een ongeautoriseerde actie detecteren om toegang tot het datageheugen te verkrijgen, wordt het voeden van het datageheugen door de voedingsbron afgebroken met als resultaat dat de data in het datageheugen instantaan uitgewist worden. Wanneer de schakelaar tussen de voedingsbron en het datageheugen aangebracht is, wordt het voeden van het datageheugen afgebroken door eenvoudig de

schakelaar te openen. In het geval dat de schakelaar parallel aan de voedingsbron aangebracht is, wordt door het sluiten van de schakelaar de voedingsbron kortgesloten met als resultaat dat de voedingsbron vernietigd wordt en dat het voeden van het datageheugen door de
5 voedingsbron wordt afgebroken.

Het wissen van het EPROM-datageheugen volgens de stand der techniek gebeurt door de geïntegreerde schakeling met ultra-violet licht te bestralen. Het nadeel hiervan is dat dit tijd kost en dat de gehele schakeling gewist wordt in plaats van het datageheugen sec. Het
10 EEPROM-datageheugen wordt gewist door het toevoeren van een 'erase'-spanning aan de datacellen in het datageheugen. Dit kost tijd en stroom. Met de maatregelen volgens de uitvinding wordt bereikt dat het gehele datageheugen in één slag zonder stroomverbruik gewist wordt.

Een uitvoeringsvorm van de geheugenkaart volgens de
15 uitvinding is gekenmerkt doordat de detectiemiddelen voorzien zijn van een ingang voor het ontvangen van een extern toegevoerd codewoord en van een uitgang om de schakelaar in de tweede toestand te brengen in responsie op het niet corresponderen van het codewoord met een in het datageheugen opgeslagen identificatiecode. Na detectie van bijvoorbeeld
20 drie maal een foute identificatie bij het uitwisselen van identificatiegegevens zal het gehele datageheugen uitgewist worden.

Een verdere uitvoeringsvorm van de geheugenkaart volgens de uitvinding is gekenmerkt doordat de detectiemiddelen een licht-detector bevatten voor het detecteren van een lichthoeveelheid per
25 tijdseenheid die groter is dan een vooraf bepaalde waarde en voor het in responsie daarop in de tweede toestand brengen van de schakelaar.

In het geval dat met een elektronenmicroscop of andere methoden getracht wordt het datageheugen uit te lezen, dient eerst een plastic oppervlaktelaag verwijderd te worden waarmee de geïntegreerde
30 schakeling en daarmee tevens het datageheugen bedekt is. Zodra dit gebeurt, wordt door de licht-detector een grote toename van de lichthoeveelheid per tijdseenheid gedetecteerd die een vooraf vastgestelde waarde overschrijdt. In responsie op het overschrijden van deze waarde wordt de schakelaar geopend. Deze waarde wordt zodanig
35 gekozen dat de gedetecteerde lichthoeveelheid per tijdseenheid onder deze waarde blijft zolang het gehele oppervlak van de lichtdetector bedekt is door een plastic oppervlaktelaag. Een geschikte uitvoering van

89 03 111

een licht-detector is een detector in de vorm van een licht-gevoelige p-n junctie, omdat de lichtdetector dan tegelijk met het datageheugen geïntegreerd kan worden zodat een extra component niet nodig is.

De uitvinding en haar voordelen zullen thans worden
5 toegelicht aan de hand van de tekening.

Daarbij toont:

Figuur 1: een "exploded view" van een geheugenkaart
volgens de uitvinding;

Figuur 2: schematische doorsnede van de geheugenkaart in
10 Figuur 1;

Figuur 3: een eerste schematische uitvoeringsvorm van de
geheugenkaart in Figuur 1;

Figuur 4: een tweede schematische uitvoeringsvorm van de
gheugenkaart in Figuur 1.

15 De geheugenkaart 1 in figuur 1 bevat een uitsparing 4
(recess) waarin een geïntegreerde schakeling 2 tezamen met een
gedrukte circuitplaat 3 (printed circuit film) wordt vastgelijmd. De
gedrukte circuitplaat 3 is voorzien van contactvlakken 5 voor de invoer
en uitvoer van data naar en van de geïntegreerde schakeling 2.

20 In figuur 2 is een sterk uitvergroete doorsnede van de
geheugenkaart 1 in figuur 1 weergegeven. De geheugenkaart van plastic 77
bevat twee tegen elkaar aan gelijmde gedeelten 6 en 7, waarbij deel 6 is
voorzien van de uitsparing 4. In deze uitsparing 4 in plastic deel 6 is
de geïntegreerde schakeling 2, de gedrukte circuitplaat 3 en een
25 voedingsbron 8 aangebracht, waarbij voedingsbron 8 met de
geïntegreerde schakeling 2 is verbonden.

In figuur 3 is geheugenkaart 1 met de geïntegreerde
schakeling 2 een voedingsbron 8 weergegeven. De schakeling 2 bevat een
I/O-eenheid 13 voor invoer en uitvoer van data via de gedrukte
30 circuitplaat 3 (printed circuit film), een centrale besturingseenheid 9,
een datageheugen 10, een schakelaar 12 en een lichtdetektor 14. De I/O
eenheid 13 is via een bus 11 verbonden met de centrale besturingseenheid
9 en het datageheugen 10. Deze bus 11 verbindt tevens besturingseenheid
9 en datageheugen 10 met elkaar. De schakelaar 12, die via de centrale
35 besturingseenheid 9 schakelbaar is, verbindt datageheugen 10 met
voedingsbron 8. De schakelaar 12 kan zijn uitgevoerd met een transistor
die in de ene toestand geleidt en in de andere toestand spert. Verder is

89 03 111.

lichtdetector 14 gekoppeld met besturingseenheid 9 om bij detectie van een ongeautoriseerde actie via besturingseenheid 9 schakelaar 12 te activeren. Deze lichtdetector 14 wordt later in de beschrijving beschreven.

5 Het datageheugen 10 is een vluchtig geheugen, dat wil zeggen dat het geheugen 10 slechts de opgeslagen data bewaart zolang het geheugen via de gesloten schakelaar 12 (eerste toestand) door de voedingsbron 8 voorzien wordt van een voedingsspanning. Het vluchtig geheugen 10 kan worden uitgevoerd als een CMOS-SRAM (Complementary Metal
10 Oxide Semiconductor Static Random Access Memory). Het voordeel van CMOS-SRAM is dat de dissipatie zeer klein is.

De centrale besturingseenheid 9 opent de schakelaar 12 bij detectie van een ongeautoriseerde actie om toegang tot het datageheugen 10 te verkrijgen. De besturingseenheid 9 bevat daartoe
15 detectiemiddelen of ontvangt een detectiesignaal (bijvoorbeeld van lichtdetector 14). Als gevolg van het openen van schakelaar 12 (tweede toestand) wordt het datageheugen 2 gewist.

In Figuur 4 is een uitvoeringsvorm van de geheugenkaart 1 schakeling 1 weergegeven, waarbij schakelaar 12 parallel is aangebracht
20 aan de voedingsbron 8 en datageheugen 10 in tegenstelling tot Figuur 3 waarbij schakelaar 12 tussen voedingsbron 8 en datageheugen 10 geplaatst is. In alle overige opzichten is geheugenkaart 1 in Figuur 4 identiek uitgevoerd als in Figuur 3. In de eerste toestand van schakelaar 12 in Figuur 4 is schakelaar 12 open. Wanneer als gevolg van een gedetecteerde
25 ongeautoriseerde actie schakelaar 12 gesloten wordt (tweede toestand) wordt voedingsbron 8 kortgesloten en daardoor vernietigd. Het datageheugen 10 verkrijgt dan geen voedingsspanning en wordt ten gevolge daarvan gewist.

Het datageheugen 10 dient voor het opslaan van gegevens
30 zoals bijvoorbeeld bankrekeningnummers en banksaldi. Dit is van belang bij gebruik van de geheugenkaarten voor het afrekenen van gekochte artikels in winkels. Tevens kan het datageheugen 10 het programma bevatten voor de besturing van de centrale besturingseenheid 9. Het woord "data" heeft hier dus een ruime betekenis.

35 Wanneer dus het datageheugen 10 gewist wordt is direct ook de geheugenkaart onklaar gemaakt. In het hierna volgende worden een aantal ongeautoriseerde acties beschreven, die aanleiding geven om

89 03 111.

schakelaar 12 in de tweede toestand te brengen, zodat het datageheugen 10 gewist wordt.

Het datageheugen 10 kan een al dan niet versleutelde identificatiecode bevatten om toegang tot het datageheugen 10 te bewaken. De detectiemiddelen in besturingseenheid 9 vergelijken deze identificatiecode met een via de I/O-eenheid 13 toegevoerd codewoord (PIN-code (Personal Identification Number)) om te bepalen of toegang tot het datageheugen verleend mag worden. Een andere mogelijkheid om de toegang tot het datageheugen 10 te bewaken is door middel van een in het datageheugen 10 opgeslagen programma dat het toegevoerde codewoord versleutelt en via de I/O eenheid 13 naar een externe (niet in de figuren 3 en 4 weergegeven) centrale controle-eenheid verstuurd ter verificatie. Een voorbeeld van een dergelijk programma is het DES-algoritme, waarbij twee sleutels ter codering gebruikt worden; één in de geheugenkaart en de andere in de centrale controle-eenheid ter decodering van de versleutelde identificatiecode. Wanneer het aangeboden codewoord niet correspondeert met opgeslagen identificatiecode of niet voldoet volgens het DES-algoritme, wordt toegang tot het datageheugen 10 door de detectiemiddelen in besturingseenheid 9 geblokkeerd. Indien bijvoorbeeld drie maal achter elkaar door de detectiemiddelen een onjuist toegevoerd codewoord geconstateerd is, wordt schakelaar 12 in de tweede toestand gebracht via een signaal afkomstig van besturingseenheid 9.

Bij geautoriseerd gebruik van de geheugenkaart 1 zullen de geheugenplaatsen in datageheugen 10 in een bepaalde volgorde geadresseerd worden door de besturingseenheid 9. Indien op de adresingang van datageheugen 10 door de detectiemiddelen in besturingseenheid 9 een hiervan afwijkende volgorde gedetecteerd wordt, zal schakelaar 12 in de tweede toestand gebracht worden.

Het is ook mogelijk specifieke adressen te definiëren in het datageheugen 10 die bij normaal gebruik door een daartoe geautoriseerd persoon niet gebruikt worden. Wanneer door de detectiemiddelen gedetecteerd wordt dat deze adressen toch uitgelezen worden, is dit een indicatie dat met een niet geautoriseerde actie data worden uitgelezen.

Behalve dat ongeautoriseerde acties gedetecteerd worden met behulp van detectiemiddelen in de centrale besturingseenheid 9,

8903111

kunnen ook ongeautoriseerde acties gedetecteerd worden met behulp van een lichtdetector 14. Deze lichtdetector 14 is bij voorkeur een lichtgevoelige p-n junctie. Het voordeel hiervan is dat de lichtdetector 14 tegelijk met het datageheugen 10 mee geïntegreerd kan worden zodat
5 geen extra component nodig is. Wanneer getracht wordt het datageheugen 10 uit te lezen met behulp van een elektronenmicroscop of via andere analytische methoden zal de plastic oppervlaktelaag 77 of de geïntegreerde schakeling uit de geheugenkaart verwijderd moeten worden. Dit heeft tot gevolg dat door de lichtdetector 14 een
10 lichthoeveelheid per seconde gedetecteerd wordt die een vooraf bepaalde waarde overschrijdt. Met andere woorden, in responsie op het overschrijden van de vooraf bepaalde grens van de lichthoeveelheid per seconde wordt de besturingseenheid 9 via lichtdetector 14 geactiveerd om de schakelaar 12 in de tweede toestand te brengen, met als resultaat dat
15 het datageheugen 10 gewist wordt.

89 03 111.

CONCLUSIES

1. Chip-geheugenkaart met een chip die voorzien is van een datageheugen en van detectiemiddelen om de geheugenkaart onklaar te maken in responsie op een niet door de geheugenkaart geautoriseerde actie voor het verkrijgen van toegang tot het datageheugen,
5 met het kenmerk dat de geheugenkaart een voedingsbron bevat voor het voeden van het datageheugen waarbij het datageheugen een vluchtig geheugen is, en dat de geheugenkaart een schakelaar bevat met een eerste toestand en met een tweede toestand waarbij de detectiemiddelen bij detectie van een niet geautoriseerde actie de schakelaar vanuit de
10 eerste toestand in de tweede toestand brengen om de geheugenkaart onklaar te maken.
2. Geheugenkaart volgens conclusie 1, met het kenmerk dat de voedingsbron via de schakelaar met de datageheugen verbonden is, waarbij de eerste toestand en de tweede toestand van de schakelaar
15 respectievelijk een gesloten en een open schakelaar representeren.
3. Geheugenkaart volgens conclusie 1, met het kenmerk dat de schakelaar parallel aan de voedingsbron is gekoppeld, waarbij de eerste toestand en de tweede toestand van de schakelaar respectievelijk een open en een gesloten schakelaar representeren.
- 20 4. Geheugenkaart volgens conclusie 1,2 of 3, met het kenmerk dat de detectiemiddelen voorzien zijn van een ingang voor het ontvangen van een extern toegevoerd codewoord en van een uitgang om de schakelaar in de tweede toestand te brengen in responsie op het niet corresponderen van het codewoord met een in het datageheugen opgeslagen
25 identificatiecode.
5. Geheugenkaart volgens conclusie 1,2,3, of 4, met het kenmerk dat de detectiemiddelen gekoppeld zijn met de adresingang van het datageheugen om in responsie op een vooraf bepaald adreswoord of bij afwijking van een vooraf bepaalde combinatie van adreswoorden op de
30 adresingang de schakelaar in de tweede toestand te brengen.
6. Geheugenkaart volgens conclusie 1,2,3,4 of 5, met het kenmerk dat de detectiemiddelen een licht-detector bevatten voor het detecteren van een lichthoeveelheid per tijdseenheid die groter is dan een vooraf bepaalde waarde en voor het in responsie daarop in de tweede
35 toestand brengen van de schakelaar.
7. Geheugenkaart volgens conclusie 6, met het kenmerk dat de licht-detector voorzien is van een gebied met een licht-gevoelige p-n

89 03 111

junctie.

8. Geheugenkaart volgens conclusie 6 of 7, met het kenmerk dat de licht-gevoelige p-n junctie met het datageheugen is meegeïntegreerd.

5 9. Geheugenkaart volgens een der voorafgaande conclusies, met het kenmerk dat het datageheugen gevormd wordt door een CMOS Statisch Random Access Memory.

10. Chip geschikt voor gebruik in een chip-geheugenkaart volgens één der voorafgaande conclusies.

10 11. Chip volgens conclusie 10, met het kenmerk dat de chip voorzien is van een lichtgevoelige p-n junctie.

12. Chip volgens conclusie 11, met het kenmerk dat de lichtgevoelige p-n junctie met het datageheugen is meegeïntegreerd.

8903 111.

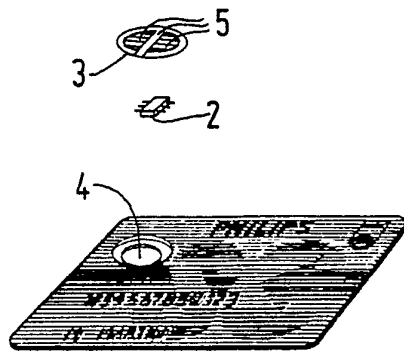


FIG.1

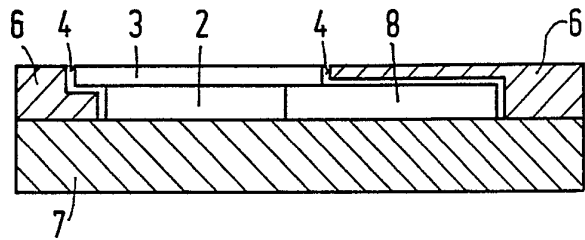


FIG.2

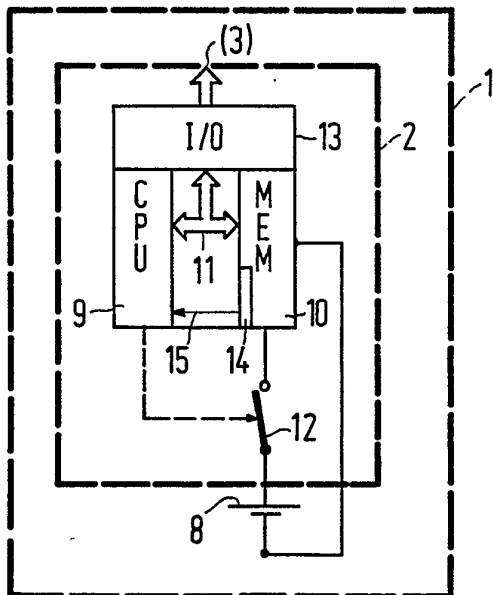


FIG.3

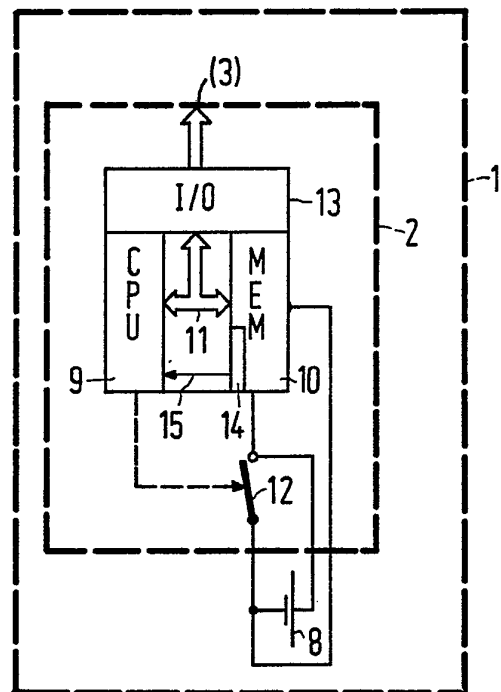


FIG.4