HU 000022499 0 B1

(19) HU

MAGYAR KÖZTÁRSASÁG
Magyar Szabadalmi Hivatal

(11) Lajstromszám: 224 990 (13) B1

SZABADALMI LEÍRÁS

(21) A bejelentés ügyszáma: **P 00 02429**
(22) A bejelentés napja: **1999. 05. 25.**

(40) A közzététel napja: **2000. 11. 28.**
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlöny és Védjegyértesítőben: **2006. 05. 29.**

(51) Int. Cl.: ***H04Q 7/00*** *(2006.01)*

(86) A nemzetközi (PCT) bejelentési szám:
PCT/DE 99/01531
(87) A nemzetközi közzétételi szám: **WO 9962275**

(30) Elsőbbségi adatok:
198 23 532.1 1998. 05. 26. DE

(72) Feltaláló:
Dupre, Michael, Sankt Augustin (DE)

(73) Jogosult:
DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn (DE)

(74) Képviselő:
Mák András, S. B. G. & K. Budapesti Nemzetközi Szabadalmi Iroda, Budapest

(54) **Előfizetői azonosító modul, valamint eljárás annak vezérlésére**

(57) Kivonat

A találmány tárgya előfizetői azonosító modul (SIM), valamint eljárás annak vezérlésére mobil rádiótelefonos hálózathoz. Az eljárás azon alapszik, hogy a mobil rádiótelefonos hálózat egy vagy több meghatározott vezérlőértéket ad le az előfizetői azonosító modulra, amelyek az előfizetői azonosító modulon belül meghatározott hatásokat vagy folyamatokat váltanak ki. Vezérlőértékekként meghatározott, a mobil rádiótelefonos hálózat által a szabályszerű hitelesítés végett az előfizetői azonosító modulra leadott véletlen értékeket (vezérlő RAND-eket) alkalmaznak.

HU 224 990 B1

A találmány tárgya előfizetői azonosító modul, valamint eljárás annak vezérlésére mobil rádiótelefonos hálózathoz.

A mobilállomások a valamennyi rádió- és átviteltechnikai feladat ellátására szolgáló mobil rádiótelefonos végberendezésből és egy ezzel összeköthető előfizetői azonosító modulból (SIM=*S*ubscriber *I*dentity *M*odule) állnak. Az előfizetői azonosító modult többnyire egy csipkártya képezi, amely az előfizetői viszonyt a mobil rádiótelefonos hálózat üzemeltetőjének igazolja. Az előfizetői azonosító modulon fontos egyéni előfizetői adatok vannak tárolva, amelyek lehetővé teszi a mobil rádiótelefonos szolgáltatások használatát. Az előfizetői azonosító modul tartalmazza a nemzetközi mobilelőfizető-azonosítót (IMSI=*I*nternational *M*obile *S*ubscriber *I*dentity), az egyéni és titkos előfizetői kulcsot (Ki), egy hitelesítési algoritmust (A3), egy adatkulcs-előállító algoritmust (A8), egy személyi azonosító számot (PIN), és más állandó, valamint ideiglenes adatokat.

Az előfizetői azonosító modulokat a mobil rádiótelefonos hálózat üzemeltetőjének egy úgynevezett személyre szabó (perszonalizáló) központjában a nemzetközi mobilelőfizető-azonosítóval (IMSI), az egyéni és titkos előfizetői kulccsal (Ki) előzetesen személyre szabják, és az előfizetőnek kiadják. Az előfizetői azonosító modulon állandó jelleggel tárolt adatok változtatása például aktualizálási folyamatokhoz vagy a biztonság szempontjából fontos tökéletesítések végett ezután általában nem lehetséges vagy csak a személyre szabó központban lehetséges. Ha sok előfizető előfizetői azonosító moduljának adatait kell megváltoztatni, akkor ez nagyon munkaigényes és költséges feladat.

Találmányunk célja olyan eljárás előfizetői azonosító modul vezérlésére mobil rádiótelefonos hálózatokban, amely szigorú biztonsági követelményeket teljesít és egyszerűen megvalósítható.

Ezt a feladatot a találmány értelmében a legáltalánosabban olyan eljárással oldjuk meg, amelynek során a mobil rádiótelefonos hálózat egy vagy több meghatározott vezérlőértéket ad le az előfizetői azonosító modulnak, amelyek az előfizetői azonosító modulon belül meghatározott hatásokat vagy folyamatokat váltanak ki. Vezérlőértékekként meghatározott véletlen értékeket alkalmazunk vezérlő RAND-ek formájában, és az előfizetői azonosító modulban ellenőrizzük, hogy a fogadott vezérlőértékek olyan speciális vezérlő RAND-ek-e, amelyek mind az előfizetői azonosító modulnak a mobil rádiótelefonos hálózat felé történő hitelesítésére, mind pedig bizonyos hatások vagy folyamatok kiváltására alkalmasak az előfizető-azonosító modulon belül.

Ehhez az eljáráshoz a találmány értelmében olyan előfizetői azonosító modult (SIM) alkalmazunk, amelynek egy vagy több meghatározott vezérlőérték vétele után az előfizetői azonosító modulban meghatározott eseményeket vagy folyamatokat kiváltó eszköze van. Az előfizetői azonosító modulon összehasonlítási RAND formájában legalább egy összehasonlítási érték biztonságosan tárolva van, vagy az előfizetői azonosító modulon tárolt adatokból számítható. Vezérlőértékekként meghatározott véletlen értékeket alkalmazunk vezérlő RAND-ek formájában, amelyek mind az előfizető-azonosító modulnak a mobil rádiótelefonos hálózat felé történő hitelesítésére, mind pedig az előfizető azonosító modulon belül bizonyos események vagy folyamatok kiváltására alkalmasak. Az előfizetői azonosító modul olyan eszközöket is tartalmaz, amelyek alkalmasak a meghatározott esemény vagy folyamat kiváltása előtt a vezérlő RAND-ek ellenőrzésére a vezérlő RAND-ek és az előfizetői azonosító modulon tárolt összehasonlítási RAND-ek összehasonlításával.

Az előfizetői modulban egy hatás vagy folyamat kiváltása előtt ellenőrizzük ezeket a vett vezérlőértékeket (vezérlő RAND-eket) úgy, hogy a vezérlőértékeket összehasonlítjuk meghatározott, az előfizetői azonosító modulon rendelkezésre álló összehasonlítási értékekkel (összehasonlítási RAND-ekkel). Az előfizetői azonosító modulon ehhez legalább egy összehasonlítási érték rendelkezésre áll, amely vagy fix mennyiségként tárolva van, vagy számítható. A kártyák egyéni vezérlő/összehasonlítási RAND-jeit például úgy kaphatjuk meg, hogy ezeket az előfizetői azonosító modulon implementált A3/A8 biztonsági algoritmusok alapján a Ki titkos kulcs és/vagy további fixen tárolt Z mennyiségek alapján határozzuk meg.

Az összehasonlítás gyors elvégezhetősége végett az összehasonlítási érték az előfizetői azonosító modulon tárolható.

Emellett minden előfizetői azonosító modulhoz több vezérlőérték van fenntartva, amelyek egy-egy meghatározott hatást vagy folyamatot váltanak ki az előfizetői azonosító modulon. Egy sor megengedett vezérlőérték van a mobil rádiótelefonos hálózat alkalmas helyén, például a hitelesítő-központban fenntartva, amelyek meghatározott előfizetői azonosító modulokhoz és meghatározott hatásokhoz vannak hozzárendelve.

A mobil rádiótelefonos hálózat biztonságának fokozása végett például az előfizetői azonosító modulon különböző A3/A8 biztonsági algoritmusokat lehet tárolni, amelyek között megfelelő vezérlőérték vétele révén át lehet kapcsolni.

Ugyanígy lehetséges több Ki titkos kulcs tárolása a előfizetői azonosító modulkártyán, vagy ezek származtatása egy ott tárolt Ki titkos kulcsból, és ezek között megfelelő vezérlőérték vétele révén át lehet kapcsolni.

Minden kiváltandó hatás vagy folyamat nemcsak egyetlen vezérlő RAND-del, hanem vezérlő RAND-ek egy csoportjához tartozó egy vezérlő RAND-del is kiváltható. Ekkor a vezérlő RAND-nek csak egy részét használjuk, úgyhogy az egymást követő vezérlő RAND-ek különböznek egymástól, de a vezérlőbitjeik közösek.

A találmány előnye, hogy az előfizetői azonosító modulon végzendő hatások és folyamatok ilyen „távvezérléséhez" nem kell járulékos vezérlőértékeket átvinni, amelyeket egyébként könnyen lehet azonosítani, és amelyekkel könnyen vissza lehet élni. A minden hitelesítéskor átvitt véletlen szám vezérlőértékként való alkalmazása ezt mint olyat felismerhetetlenné teszi. A vezérlőértékek „szokásos" RAND értékekként jelen-

nek meg, amelyeket a hálózat a hitelesítés végett az előfizetői azonosító modulnak lead. A GSM-protokollokat sem kell módosítani.

Találmányunkat a következőkben egy kiviteli alakja alapján ismertetjük részletesen. Ennek során világossá válnak a találmány további jellemzői és előnyei.

A hitelesítési folyamat a GSM mobil rádiótelefonos hálózatokban úgy történik, hogy a mobil rádiótelefonos hálózat hitelesítő-központja (AC) egy RAND véletlen számot küld az előfizetői azonosító modulra, és ez egy A3/A8 algoritmus és a Ki titkos kulcs alapján egy SRES'=A3/A8 (Ki, RAND) eredményt számít ki, és ezt visszaküldi a hitelesítő-központnak. A hitelesítő-központ szintén ismeri a Ki titkos kulcsot, és ugyanazzal az A3/A8 algoritmussal kiszámít egy SRES értéket, és ezt az értéket összehasonlítja az előfizetői azonosító modul által szállított SRES' értékkel. A két érték megegyezése esetén az előfizetői azonosító modul hitelesítetté válik.

Az előfizetői azonosító modulkártyának két különböző, vagy akár több A3/A8 algoritmusa van, amelyeknek kifelé ugyanazok az interfészeik, és a RAND, a Ki titkos kulcs és az SRES hossza azonos. Emellett az előfizetői azonosító modulnak csak egy Ki titkos kulcsa, vagy A3/A8 algoritmusonként egy saját Ki titkos kulcsa lehet.

Ha a hálózat üzemeltetője például biztonsági okokból meg akarja változtatni az alkalmazott A3/A8 algoritmust, akkor a hitelesítő-központban kezdeményezheti egy különleges RAND véletlen szám előállítását, amely egyidejűleg egy találmány szerinti vezérlőértéket képez, és amelyet a következőkben vezérlő RAND-nek is nevezünk. A vezérlő RAND kiváltja az A3/A8 algoritmus átkapcsolását az előfizetői azonosító modulkártyában. A hitelesítő-központ által a hitelesítéshez kiszámított SRES értékek már az új algoritmuson alapszanak, amely a vezérlő RAND-re van alkalmazva. A vezérlő RAND tehát egyrészt az előfizetői azonosító modul szabályszerű hitelesítésére, másrészt az alkalmazott A3/A8 kódolóalgoritmusok átkapcsolására szolgál.

A vezérlő RAND-ként szolgáló RAND-nek kártyánként egyéninek és biztosnak kell lennie. Ezért például az A3/A8-ból (Ki, Ki) adódó érték vezérlő RAND-ként alkalmazható. Az A3/A8 (Ki, Ki) érték kártyánként egyéni, és csak az ismeri, aki a Ki titkos kulcsot ismeri. Vezérlőfunkciókra szolgáló RAND véletlen szám kiszámításához tehát a Ki titkos kulcsot használjuk, amit csak az előfizetői azonosító modul és a hálózat ismer. Elegendő ennek a Ki titkoskulcs-értéknek csak egy részével vezérelni, hogy ne kelljen ennek az értéknek valamennyi bitjét alkalmazni. Ekkor vezérlő RAND például minden olyan RAND, amelynek az első n bitje megegyezik az A3/A8 (Ki, Ki) érték első n bitjével.

Az A3/A8 (Ki, Ki) érték már a kártya személyre szabásakor kiszámítható és biztonságosan tárolható. A hitelesítő-központ által küldött RAND-nél minden hitelesítés előtt kimaszkoljuk a nem alkalmazott biteket, és az eredményt összehasonlítjuk a vezérlő RAND-nek az előfizetői azonosító modulon kiszámított és adott esetben ott biztonságosan tárolt értékével. Ha a kártya által számított összehasonlítási érték megegyezik a vett vezérlő RAND-del, akkor a vezérlő RAND hitelesítve van, és az előfizetői azonosító modulon kiválthatja a hozzárendelt hatásokat vagy folyamatokat. Ha az A3/A8 algoritmus már ki van cserélve, akkor normális hitelesítési folyamat zajlik le. Az ugyanahhoz a vezérlő RAND-csoporthoz tartozó ismét vett vezérlő RAND-et mint ilyent, nem vesszük figyelembe.

A hitelesítő-központ az előfizetői azonosító modulnak küldött RAND véletlen számot rendszerint tisztán véletlenszerűen állítja elő. Ha egy vezérlő RAND alkalmazott bitjeinek n száma eléggé nagy, akkor elmaradhat annak vizsgálata, hogy vajon a véletlenszerűen előállított RAND fenntartott vezérlő RAND vagy nem az. Ha az n értéket nagyon nagyra választjuk, akkor valószínűtlen, hogy a hitelesítő-központ a mindennapos hitelesítéshez véletlenül olyan RAND-et állít elő, amely megegyezik egy fenntartott RAND-del. Ha az algoritmust módosítani kell, akkor a hitelesítő-központnak egymás után többször kell hitelesítést végeznie vezérlő RAND-ekkel, hogy összeköttetési problémák esetén biztos legyen arról, hogy a előfizetői azonosító modul ezt a vezérlő RAND-et meg is kapja.

Ha a hitelesítés egy idegenhelyzet-regiszteren (VLR=Visitor Location Register) át történik, akkor ez először tovább használja a régi, a honos helyzetregisztertől (HLR=Home Location Register) kapott, három bitből álló hitelesítő csoportjait, és valamikor megtalálja a honos helyzetregiszter, illetőleg a hitelesítő-központ által előre adott vezérlő RAND-et. Az idegenhelyzet-regiszter nem tudja, hogy vezérlő RAND-ről van szó. Az előfizetői azonosító modul csak ekkor kapcsolja át az algoritmust. Az előfizetői azonosító modulban az átkapcsolás időpontja ezért bizonyos körülmények között jóval később van, mint az átkapcsolás időpontja a hitelesítő-központban. Ha az előfizető honi hálózatán belül változtatja az idegenhelyzet-regisztert, akkor átveszi, és tovább alkalmazza a legutóbbi idegenhelyzet-regiszterben tárolt RAND/SRES értékeket. Az idegenhelyzet-regiszter váltása vagy többszöri váltása ezért nem kritikus, és nem késlelteti az algoritmus átkapcsolását az előfizetői azonosító modulban.

Ugyanilyen eljárással lehet módosítani az előfizetői azonosító modulban a Ki titkos kulcsot is. Ehhez az új Ki titkos kulcs már biztonságosan tárolva lehet az előfizetői azonosító modulon, vagy a régi Ki-ből definiált számítási eljárással származtatható.

A Ki titkos kulcs átkapcsolásához szükséges vezérlő RAND-ek értéke különbözik az A3/A8 algoritmusok átkapcsolásához használt vezérlő RAND-ekétől, és például egy másik matematikai eljárással vezethetők le. Egy vezérlő RAND állhat az A3/A8 (Ki, Ki XOR Z) eredmény első n bitjéből, ahol Z tetszőleges, de fix érték, amely az előfizetői azonosító modulon van tárolva. A hitelesítő-központnak már az első vezérlő RAND előállítása után az új Ki titkoskulcs-értékkel kell tovább dolgoznia, és az előfizetői azonosító modul is már az új Ki titkos kulcsot használja a hitelesítéshez, amelyet ugyancsak a vett vezérlő RAND-del kell végrehajtani.

SZABADALMI IGÉNYPONTOK

1. Eljárás előfizetői azonosító modul (SIM) vezérlésére mobil rádiótelefonos hálózatban, melynek során a mobil rádiótelefonos hálózat egy vagy több meghatározott vezérlőértéket ad le az előfizetői azonosító modulnak, amelyek az előfizetői azonosító modulon belül meghatározott eseményeket vagy folyamatokat váltanak ki, *azzal jellemezve,* hogy vezérlőértékekként meghatározott véletlen értékeket alkalmazunk vezérlő RAND-ek formájában, ahol az előfizető-azonosító modulban ellenőrizzük, hogy a fogadott vezérlőértékek olyan speciális vezérlő RAND-ek-e, amelyek mind az előfizető-azonosító modulnak a mobil rádiótelefonos hálózat felé történő hitelesítésére, mind pedig bizonyos események vagy folyamatok kiváltására alkalmasak az előfizető-azonosító modulon belül.

2. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy egy esemény vagy egy folyamat kiváltásához különböző vezérlő RAND-ek egy csoportját használjuk.

3. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy egy vezérlő RAND több különböző eseményt vagy folyamatot vált ki.

4. Az 1–3. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az előfizetői azonosító modulban egy esemény vagy folyamat kiváltása előtt ellenőrizzük ezeket a vett vezérlő RAND-eket úgy, hogy a vezérlő RAND-eket összehasonlítjuk meghatározott, az előfizetői azonosító modulon összehasonlítási RAND-ek formájában rendelkezésre álló összehasonlítási értékekkel.

5. Az 1–4. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az összehasonlítási RAND-eket fixen tároljuk az előfizetői azonosító modulon.

6. Az 1–5. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az összehasonlítási RAND-eket az előfizetői azonosító modulon tárolt adatok alapján számítjuk ki.

7. Az 1–6. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az összehasonlítási RAND-et az előfizetői azonosító modulon implementált A3/A8 biztonsági algoritmusokkal, a titkos Ki kód és/vagy további fixen tárolt Z mennyiségek függvényeként határozzuk meg.

8. Az 1–7. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy minden előfizetői azonosító modulhoz több vezérlő RAND van fenntartva, amelyek egy-egy meghatározott eseményt vagy folyamatot váltanak ki az előfizetői azonosító modulon.

9. Az 1–8. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy a mobil rádiótelefonos hálózat alkalmas helyén egy sor megengedett vezérlő RAND van fenntartva, amelyek meghatározott előfizetői azonosító modulokhoz és meghatározott eseményekhez vannak hozzárendelve.

10. Előfizetői azonosító modul (SIM) az 1–9. igénypontok szerinti eljárásban való alkalmazáshoz, amelynek egy vagy több meghatározott vezérlőérték vétele után az előfizetői azonosító modulban meghatározott eseményeket vagy folyamatokat kiváltó eszköze van, *azzal jellemezve,* hogy

az előfizetői azonosító modulon összehasonlítási RAND formájában legalább egy összehasonlítási érték biztonságosan tárolva van, vagy az előfizetői azonosító modulon tárolt adatokból számítható,

vezérlőértékekként meghatározott véletlen értékeket alkalmazunk vezérlő RAND-ek formájában, amelyek mind az előfizető-azonosító modulnak a mobil rádiótelefonos hálózat felé történő hitelesítésére, mind pedig az előfizető-azonosító modulon belül bizonyos események vagy folyamatok kiváltására alkalmasak, és

az előfizetői azonosító modul olyan eszközöket tartalmaz, amelyek alkalmasak a meghatározott esemény vagy folyamat kiváltása előtt a vezérlő RAND-ek ellenőrzésére a vezérlő RAND-ek és az előfizetői azonosító modulon tárolt összehasonlítási RAND-ek összehasonlításával.

11. A 10. igénypont szerinti előfizetői azonosító modul, *azzal jellemezve,* hogy eszközöket tartalmaz az összehasonlítási RAND-ek meghatározására az előfizetői azonosító modulon implementált A3/A8 biztonsági algoritmusokkal, a titkos Ki kód és/vagy további fixen tárolt Z mennyiségek függvényeként.

12. A 10. vagy 11. igénypont szerinti előfizetői azonosító modul, *azzal jellemezve,* hogy az előfizetői azonosító modulon különböző A3/A8 biztonsági algoritmusok vannak tárolva, és eszközt tartalmaz a biztonsági algoritmusok közötti átkapcsolásra megfelelő vezérlő RAND vétele esetén.

13. A 10. vagy 11. igénypont szerinti előfizetői azonosító modul, *azzal jellemezve,* hogy több titkos Ki kód van az előfizetői azonosító modulon (SIM) tárolva, vagy egy ott tárolt titkos Ki kódból származtatva, és eszköze van a titkos Ki kódok közötti átkapcsolásra megfelelő vezérlő RAND vétele esetén.

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna főosztályvezető-helyettes
Windor Bt., Budapest