PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:
1999 - 2143

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
B 60 R 25/04

(19)
ČESKÁ
REPUBLIKA

ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **06.11.1997**

(32) Datum podání prioritní přihlášky: **16.12.1996**

(31) Číslo prioritní přihlášky: **1996/19652256**

(33) Země priority: **DE**

(40) Datum zveřejnění přihlášky vynálezu: **12.01.2000**
(Věstník č. 1/2000)

(86) PCT číslo: **PCT/DE97/02579**

(87) PCT číslo zveřejnění: **WO98/26962**

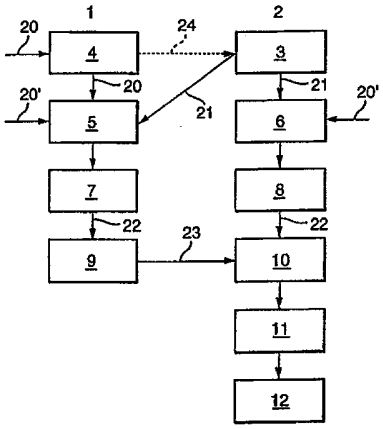
(71) Přihlašovatel:
ROBERT BOSCH GMBH, Stuttgart, DE;

(72) Původce:
Bitzer Wolfgang, Weissach, DE;

(74) Zástupce:
Hořejš Milan Dr. Ing., Národní 32, Praha 1,
110 00;

(54) Název přihlášky vynálezu:

Způsob zabezpečení přenosu dat



(57) Anotace:

Řešení se týká způsobu zabezpečení přenosu dat mezi alespoň dvěma řídicími jednotkami /1, 2/ ve vozidle, které jsou navzájem spojeny datovou sběrnicí, přičemž jedna z řídicích jednotek /1, 2/ přenáší v datové sběrnici sled /21/ náhodných bitů, které se uloží ve všech řídicích jednotkách /1, 2/, přičemž ve všech řídicích jednotkách /1, 2/ se vytvoří klíčový kód /22/ se sledem /21/ náhodných bitů a s vnitřním klíčem /20´/, a přičemž jednou z řídicích jednotek /1, 2/ se vytvoří a odešle zpráva /23/ zakódovaná klíčovým kódem /22/, která se v přijímacích řídicích jednotkách /1, 2/ klíčovým kódem /22/ přezkoumá z hlediska svého správného zakódování podle redundantní informace obsažené v zakódované zprávě /23/, která je přijímajícím jednotkám známá, a přečte se. Sled /21/ náhodných bitů se vytvoří z existujících senzorových dat řídicí jednotky /2/.

CZ 1999 - 2143 A3

01-992-99-Ho
PV 2143-99

Způsob zabezpečení přenosu dat

Oblast techniky

Vynález se týká způsobu zabezpečení přenosu dat mezi alespoň dvěma řídicími jednotkami ve vozidle, které jsou navzájem spojeny datovou sběrnicí, přičemž jedna z řídicích jednotek přenáší v datové sběrnici sled náhodných bitů, které se uloží ve všech řídicích jednotkách, přičemž ve všech řídicích jednotkách se vytvoří klíčový kód se sledem náhodných bitů a s vnitřním klíčem, a přičemž jednou z řídicích jednotek se vytvoří a odešle zpráva zakódovaná klíčovým kódem, která se v přijímajících řídicích jednotkách klíčovým kódem přezkoumá z hlediska svého správného zakódování podle redundantní informace obsažené v zakódované zprávě, která je přijímajícím jednotkám známá, a přečte se.

Dosavadní stav techniky

Takový způsob je v principu známý ze spisu EP 0 692 412 A2. Podobné způsoby jsou známé rovněž ze spisů DE-A 195 480 19, WO-A-96/20100 a EP-A-0 492 692. U řešení podle spisu WO-A-96/20100 se pro další zvýšení zabezpečení proti odposlechu provádí navíc kódování neboli šifrování sledu náhodných bitů.

Použití přenosu dat, při němž je zapotřebí zvlášť bezpečného přenosu dat mezi řídicími jednotkami, je rovněž známé ze spisu DE 44 42 103. Přitom se jedná o ochranu proti ukradení vozidla, u níž zábrana pro zabránění rozjezdu vozidla ovlivňuje uvolnění zařízení pro

řízení motoru. Pro uvolnění zařízení pro řízení motoru je nutno do zařízení pro zjišťování kódů vložit kód a tím aktivovat ovládací zařízení blokování. Datová komunikace mezi řídicími jednotkami probíhá po sběrnici nacházející se uvnitř vozidla. U dosavadního stavu techniky se sice provádí uvedení zábrany proti rozjezdu do činnosti prostřednictvím klíčového kódu, který je známý pouze uživateli, avšak komunikace mezi řídicí jednotkou zábrany proti rozjezdu a zařízením pro řízení motoru se provádí prostřednictvím sériového vedení pro přenos dat. Protože takovým uvolňovacím nebo blokovacím signálem je velmi jednoduchý signál, který v extrémním případě sestává z jednoho bitu, je možno s takovým signálem velmi lehce manipulovat. U takového způsobu by bylo proto možné přerušením spojovacího vedení zavést manipulační signál. Takový manipulační signál by se mohl získat jednoduchým způsobem opětovným nahráním signálu dříve tímto přenosovým vedením odebraného a zaznamenaného.

Podstata vynálezu

Výše uvedené nedostatky odstraňuje způsob zabezpečení přenosu dat mezi alespoň dvěma řídicími jednotkami ve vozidle, které jsou navzájem spojeny datovou sběrnicí, přičemž jedna z řídicích jednotek přenáší v datové sběrnici sled náhodných bitů, které se uloží ve všech řídicích jednotkách, přičemž ve všech řídicích jednotkách se vytvoří klíčový kód se sledem náhodných bitů a s vnitřním klíčem, a přičemž jednou z řídicích jednotek se vytvoří a odešle zpráva zakódovaná klíčovým kódem, která se v přijímajících řídicích jednotkách klíčovým kódem přezkoumá z hlediska svého správného zakódování podle redundantní informace obsažené v zakódované zprávě, která je přijímajícím jednotkám známá, a přečte se, podle vynálezu, jehož podstatou je, že sled náhodných bitů se vytvoří z existujících senzorových dat řídicí jednotky.

Výhodou způsobu podle vynálezu je, že přenos dat mezi řídicími jednotkami se provádí v kódované formě, a že takový přenos dat nemůže být jednoduše zmanipulován, když navíc sled náhodných bitů, který tvoří základ pro kódování, se získá ze senzorových dat získaných ve vozidle, která jsou ve sběrnici přístupná z toku dat. Proto přerušení spojovacího vedení a odposlech kódovaného signálu přenášeného tímto vedením nemůže vést k úspěchu. Rovněž záměna například řídicí jednotky za zábrany proti rozjezdu, stejně jako výměna řídicí jednotky motoru, nevede k úspěchu, protože klíče obsažené v těchto zařízeních již spolu nesouhlasí. Rovněž přerušení a opětovné připojení napětí baterie nemůže ovlivnit přenos dat. Rovněž vyčtení paměti řídicích jednotek a manipulace s interními klíči v nich uloženými nevede k náležité komunikaci mezi řídicími jednotkami. Dokonce ani současná výměna řídicí jednotky motoru a zařízení pro ovládání zábrany proti rozjezdu nevede k úspěchu, protože vždy chybí klíč známý pouze uživateli.

Prostřednictvím opatření uvedených v závislých nárocích 2 až 10 jsou umožněna výhodná další provedení a vylepšení způsobu definovaného v nároku 1. Zvlášť výhodné přitom je, že je možno mezi řídicími jednotkami použít způsob komunikace podle vynálezu pro zabezpečení komunikace mezi řídicí jednotkou zábrany proti rozjezdu a řídicí jednotkou řízení motoru.

Z důvodů bezpečnosti, aby se zabránilo uhodnutí sledu náhodných bitů zkoušením, by sled náhodných bitů měl mít délku 4 byty. Rovněž pro interní klíč, který se použije pro kódování zpráv mezi řídicími jednotkami, je výhodná délka alespoň 4 bytů.

Pro vytvoření kryptogramu ze získaného klíče se signálový byte sečte po bitech sčítáním modulo 2 s prvním klíčovým bytem, výsledek

se podrobí permutaci a její výsledek se potom podrobí dalšímu sčítání, popřípadě násobení dalšími byty klíčového bytu. Výsledný signálový byte sestává z jednotlivých výsledků kódovacích kroků. Způsob kódování podle vynálezu může pracovat s různými permutačními tabulkami. Permutaci je možno zejména uskutečnit rovněž násobením. Zvýšení zabezpečení kódování se dosáhne navzájem paralelně pracujícími kódovacími kroky.

Přehled obrázků na výkresech

Vynález bude dále blíže objasněn na příkladném provedení podle přiložených výkresů, na nichž obr. 1 znázorňuje průběh komunikace mezi dvěma řídicími jednotkami, obr. 2 uvedení řízení motoru v zábraně pro rozjezd do provozu a obr. 3 postup kódování.

Příklady provedení vynálezu

Komunikace mezi dvěma řídicími jednotkami 1 a 2 se podle obr. 1 uskuteční po vložení klíče neboli po přivedení klíčového signálu 20 do první řídicí jednotky 1, například do zábrany pro rozjezd. Tento klíčový signál 20 může být kódovaným klíčem, kódováním vloženým prostřednictvím čipové karty, rádiovým kódováním atd. Klíčový signál 20 se zábranou pro rozjezd v kroku 4 rozpozná a do datového vedení se předá budicí signál 24, oznamující, že existuje platný klíč. Tento budicí signál 24 plní funkci buzení druhé řídicí jednotky 2. Druhá řídicí jednotka 2 vytvoří v kroku 3 sled 21 náhodných bitů o délce n_t, tento sled 21 náhodných bitů uloží a přenese do první řídicí jednotky 1. Počet bitů ve sledu 21 náhodných bitů se musí zvolit tak, aby osoba, která má zařízení, respektive vozidlo, k dispozici, nebyla schopna zjistit zkoušením všechny možné odpovědi na veškeré sledy náhodných bitů a zaznamenat je. Když se uvažuje délka sledu 21 náhodných bitů v

závislosti na počtu možných permutací, vznikne pro jeden sled 21 náhodných bitů o délce 1 byte celkem 265 bytů, při délce 4 byty již počet čtyřikrát 256^4 = 17,2 Gbyte. Uložit takové množství dat není pro zloděje již snadné. Po přenosu sledu 21 náhodných bitů se v kroku 5, popřípadě v kroku 6, to znamená v obou řídicích jednotkách 1, 2, uvede současně do činnosti interním klíčem 20´ šifrovací generátor. Přitom interní klíč 20´ existuje jak v první řídicí jednotce 1, tak i v druhé řídicí jednotce 2. V případě správného uvedení do provozu je interní klíč 20´ pro obě zařízení stejný. Právě tato skutečnost však musí být nejprve komunikací přezkoušena. Délka interního klíče 20´ se musí zvolit tak velká, aby jeho zjištění zkoušením bylo vyloučeno. Neoprávněná osoba může přirozeně náhodou zachytit správný klíč již při prvním pokusu, avšak rovněž i při posledním možném pokusu. Vychází se z toho, že neoprávněná osoba by musela vyzkoušet polovinu všech možných interních klíčů 20´, aby dosáhla úspěchu. Porovnání časů, během nichž musí neoprávněná osoba vyzkoušet různé klíče, je uvedeno dále: při délce klíče 1 byte potřebuje neoprávněná osoba jedenapůlkrát 2^8 sekund = 128 sekund, když se předpokládá, že neoprávněná osoba vykoná jeden pokus za jednu sekundu. Zvětší-li se délka interního klíče 20´ na 2 byty, znamená to již asi 9 hodin, při zvětšení na 3 byty již 97 dní a při zvětšení na 4 byty již 69 let. Proto se zdá délka 3 byty dostatečnou délkou interního klíče 20´. Když se však vezme v úvahu ještě to, že paralelizováním a podobným způsobem se rychlost zvýší desetkrát nebo dokonce stokrát, je hodnota 4 byty pro toto použití přiměřená.

Interní klíč 20´ musí být jak v první řídicí jednotce 1, tak i v druhé řídicí jednotce 2, uložen tak, že jej nelze vyčíst. Pro neoprávněnou osobu rovněž nesmí být možné provést jeho změnu nebo přepsání. Jinak je nutno v případě nutné opravy rovněž umožnit výměnu vadných dílů, například řídicích zařízení nebo dílů řídicích

zařízení, a nově je uvést do činnosti. Proto je pro kódování pro uložení interního klíče 20´ v elektronice řídicích jednotek nutno vyvinout vyšší úsilí. Pomocí interního klíče 20´ a sledu 21 náhodných bitů se v krocích 7 a 8 vytvoří klíčový kód 22. Tento klíčový kód 22 slouží k zakódování zprávy vysílané z první řídicí jednotky 1 do druhé řídicí jednotky 2 a obráceně. První zpráva první řídicí jednotky 1 sestává z textu, v němž alespoň n_r bitů je neproměnných (redundantních), a který je druhé řídicí jednotce 2 znám. V kroku 9 se tento výsledný kryptogram o délce n_s bitů přenese. Délka n_s je délkou vyměněné informace, podle potřeby přídavně zakódované, včetně délky n_r redundantních bitů. Spojení zprávy s klíčovým kódem 22 v kroku 9 se může provést po bitech sčítáním modulo 2. V tomto případě nemusí sice neoprávněná osoba přídavně zakódované přenesené zprávě 23 rozumět a může ji interpretovat, avšak vždy ještě bity v určitých polohách jsou cíleně, a pro elektroniku vozidla popřípadě nepozorovaně, invertovány, a proto jsou povely zfalšovány. Toto opatření však nemusí být použito, když se provede přídavné zavedení zpětné vazby textu, která má za následek vytváření chyb. Když se potom přenese přídavná informace před neproměnnou identifikační značkou, tato identifikační značka se při libovolném zfalšování přídavné informace změní a pokus o manipulaci se v každém případě odkryje. Vytvoření komunikace je potom bezúspěšné. V kroku 10 se neproměnný sled bitů o délce n_r bitů, který je obsažen v přijmutém a odkódovaném kryptogramu, porovná s uloženým neproměnným sledem bitů, a tím se neproměnné n_r bity přezkoušejí na správnost. V dalším kroku 11 se při správném výsledku porovnání zbylý počet odkódovaných bitů nesoucích informaci, to jest n_s-n_r bitů zprávy 23, vyšle do například řídicí jednotky motoru a uvolní ji. Ukáže-li porovnání se zprávou 23, že došlo ke vzniku chyby, například pokusem o manipulaci, zůstane motor zablokován. Tímto způsobem je možno blokovat funkce řídicích jednotek.

Na obr. 2 je znázorněn průběh komunikace mezi zábranou proti rozjezdu a řídicím zařízením motoru. Kryptoalgoritmus v řídicím zařízení motoru se náhodnými ovlivňovacími veličinami, které jsou naznačeny šipkou, uvede do počátečního stavu. Řídicí zařízení motoru je v kroku 14 v aktivním stavu, zatímco v kroku 13 je zábrana proti rozjezdu zablokována. Kryptoalgoritmus v řídicím zařízení vyšle do řídicího zařízení zábrany proti rozjezdu signál ve formě alespoň 4 bytů, aby uvedl toto řídicí zařízení do činnosti a do kryptosynchronizace, viz krok 15. Řídicí zařízení zábrany proti rozjezdu se v kroku 17 uvede do činnosti a začne v kroku 18 přenášet do řídicího zařízení motoru informaci, zakódovanou libovolným počtem (n_s/8) bytů. Pravost informace se rozpozná tím, že může být správně odkódována. Pro přezkoušení této skutečnosti, a tudíž pro umožnění jízdy, musí být v přenesené informaci obsaženo dost redundantních n_r bitů, tedy informace, kterou přijímací strana již zná. Proto například by měla zakódovaná data, přenášená ze zábrany pro rozjezd do řídicího zařízení motoru, obsahovat alespoň 16 bitů dat, která jsou řídicímu zařízení motoru již známá, a která řídicí zařízení motoru po odkódování musí rozeznat. Mohlo by se jednat například o dva byty s 00 nebo 11 nebo jinou pevnou bitovou strukturou. V zakódovaných signálech nelze tyto oba byty rozeznat, přičemž tyto byty musí být v každém případě jinak zakódovány. Z tohoto důvodu nemohou být zfalšovány ani třetí osobou, která nezná klíčový kód 22. 16 redundantních bitů nemusí být přenášeno nutně uzavřeně ve formě dvou bytů, mohou být včleněny do zakódované přenášené informace libovolně. Potom musí být ověřeny v řídicím zařízení motoru jednotlivě porovnáním s očekávanou bitovou strukturou.

Na obr. 3 je znázorněn vlastní kryptoalgoritmus, který sestává ze čtyř stejných modulů 27, zapojených v řetězci. Na obr. 3 znamená znaménko + sčítání modulo 2 po bitech a znaménko * násobení modulo

257. Klíčový kód 22 má čtyři byty 28 a moduly 27 má výstupní byty 29. Ke vstupnímu bytu 26 každého modulu 27 se nejprve přičte po bitech sčítáním modulo 2 jeden byte 28 klíčového kódu 22, tedy jinými slovy každý byte vstupního bytu se spojí způsobem EXOR s rovnocenným bytem příslušného klíčového bytu. Výsledek se podrobí nelineární permutaci, a to z hlediska jak výpočtu modulo 256, tak i připočtením po bitech sčítáním modulo 2. Tyto permutace se nejlépe provádějí pomocí tabulky, která však všeobecně vyžaduje v paměti ROM mnoho místa. Téměř přesně tak dobře je možno uskutečnit permutaci násobením lichým číslem mezi 3 a 253 modulo 257, přičemž na výstupu se hodnota 256 nahradí výslednou hodnotou ze vstupní hodnoty 256, tedy hodnotou (256 * F) modulo 257. F je lichým faktorem. Výstupní byte 29 každého modulu 27, kromě posledního modulu 27, se přivádí vždy do vstupu následujícího modulu 27. Součet po bitech modulo 2 výstupních bytů 29 tvoří výstupní byte 23, který se použije pro zakódování nebo odkódování připočtením po bitech modulo 2 k nešifrovanému, popřípadě tajnému, bytu.

Další příklady provedení

Popsaný kryptoalgoritmus může být různými způsoby modifikován: Liché faktory F_I mohou být volně zvoleny v dalších rozsazích mezi 3 a 253 a pro každý modul 27 jinak. Přitom je výhodná volba středních hodnot. Do řetězce je možno, jak již bylo výše naznačeno, připojit další moduly 27, čímž se délka tajného kódu, avšak rovněž délka synchronizační předpony a délka vytváření chyb, příslušně zvětší. Je-li zapotřebí pouze zvětšení klíčového kódu 22 bez prodloužení synchronizace, je možno připojit paralelně i další řetězec, jehož vstup je spojen se vstupem prvního řetězce, a jehož výstupy se připočtou k výstupům prvního řetězce po bitech sčítáním modulo 2. Bylo-li by zapotřebí nekonečně dlouhého vytváření chyb, je možno po

dosažení synchronizace zaměnit konfiguraci vysílací strany za konfiguraci přijímací strany.

Způsob podle vynálezu umožňuje kódovanou komunikaci mezi řídicími zařízeními, mezi částmi řídicích zařízení nebo mezi jednotlivými elektronickými moduly prostřednictvím vhodného spojení. Způsob podle vynálezu může být použit jak pro přenos jednotlivých řídicích signálů, tak pro přenos velkých množství dat.

PATENTOVÉ NÁROKY

1. Způsob zabezpečení přenosu dat mezi alespoň dvěma řídicími jednotkami ve vozidle, které jsou navzájem spojeny datovou sběrnicí, přičemž jedna z řídicích jednotek přenáší v datové sběrnici sled (21) náhodných bitů, které se uloží ve všech řídicích jednotkách, přičemž ve všech řídicích jednotkách se vytvoří klíčový kód (22) se sledem (21) náhodných bitů a s vnitřním klíčem (20´), a přičemž jednou z řídicích jednotek se vytvoří a odešle zpráva (23) zakódovaná klíčovým kódem (22), která se v přijímajících řídicích jednotkách klíčovým kódem (22) přezkoumá z hlediska svého správného zakódování podle redundantní informace obsažené v zakódované zprávě (23), která je přijímajícím jednotkám známá, a přečte se, podle vynálezu, jehož podstatou je, že sled (21) náhodných bitů se vytvoří z existujících senzorových dat řídicí jednotky (2).

2. Způsob podle nároku 1, **vyznačující se tím,** že

- první řídicí jednotka (1) se uvede do provozu klíčovým signálem (20),
- první řídicí jednotkou (1) se v datové sběrnici potvrdí příjem klíčového signálu (20) budicím signálem (24),
- druhá řídicí jednotka (2) se budicím signálem (24) uvede do činnosti,
- z druhé řídicí jednotky (2) se provede přenos sledu (21) náhodných bitů do první řídicí jednotky (1),
- v obou řídicích jednotkách (1, 2) se pomocí sledu (21) náhodných bitů a interního klíče (20´) vytvoří klíčový kód (22)
- a z první řídicí jednotky se vyšle zpráva (23), která se ve druhé řídicí jednotce (2) přezkoumá klíčovým kódem (22) na správnost svého kódování.

3. Způsob podle nároku 1 nebo 2, **vyznačující se tím,** že první řídicí jednotka (1) je tvořena zábranou proti rozjezdu a druhá řídicí jednotka (2) je tvořena řízením motoru, přičemž při správném kódování zprávy (23), která se vyšle do řízení (2) motoru, dojde k uvolnění řízení motoru.

4. Způsob podle jednoho z nároků 1 až 3, **vyznačující se tím,** že pro sled (21) náhodných bitů se zvolí délka alespoň 4 byty.

5. Způsob podle jednoho z nároků 1 až 4, **vyznačující se tím,** že délka klíčového kódu (22) se stanoví s alespoň 4 byty.

6. Způsob podle jednoho z nároků 1 až 5, **vyznačující se tím,** že pro vytvoření zprávy (23) se k signálovému bytu (25) přičte v několika modulech (27), vždy po bitech, sčítáním modulo 2, jeden byte (28) klíčového kódu (22), načež se podrobí permutaci a výsledek se předá do dalšího modulu (28), přičemž po každém způsobovém kroku se příslušný výsledek (29) shrne do zakódovaného signálového bytu (23).

7. Způsob podle jednoho z nároků 1 až 6, **vyznačující se tím,** že permutace se provádí násobením modulo 257 hodnoty vstupního bytu faktorem Fi.

8. Způsob podle nároku 7, **vyznačující se tím,** že faktor Fi má hodnotu mezi 3 a 253 a je pro každý kódovací modul (27) volitelný libovolně.

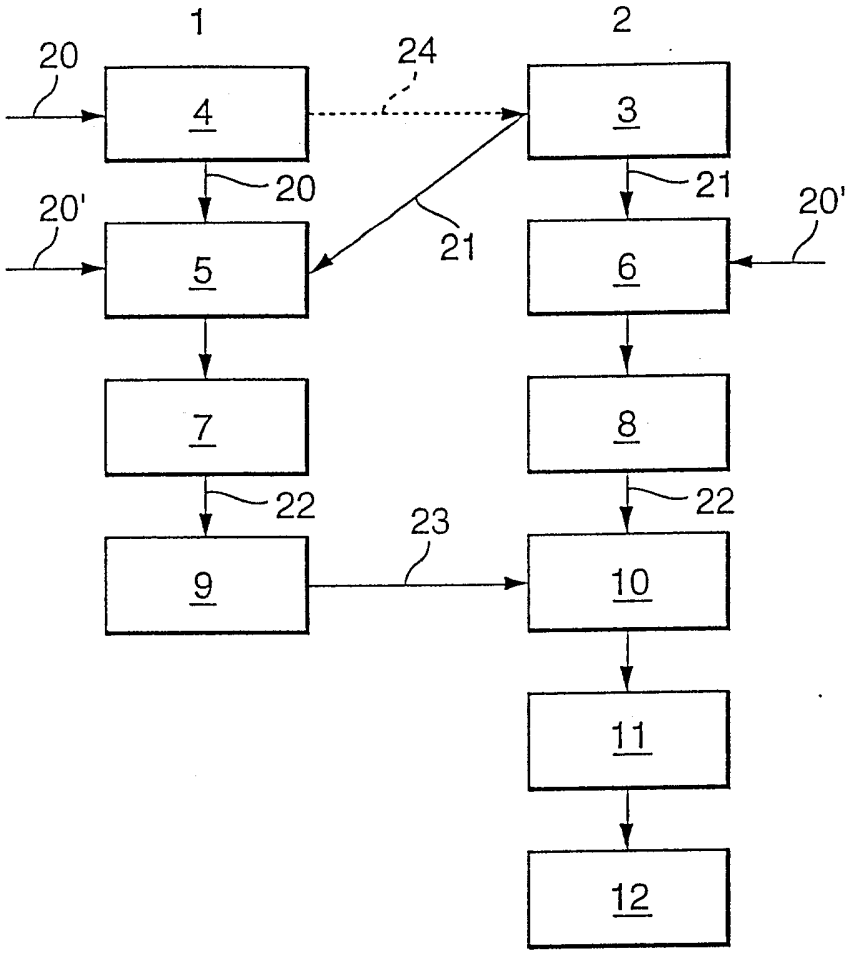
9. Způsob podle jednoho z nároků 1 až 7, **vyznačující se tím,** že kódování se provádí více paralelně navzájem pracujícími kryptogenerátorovými řetězci.

10. Způsob podle jednoho z nároků 1 až 9, **vyznačující se tím,** že při negativním výsledku přezkoušení se vytvoří hlášení o chybě a/nebo se přeruší funkce řídicích jednotek.

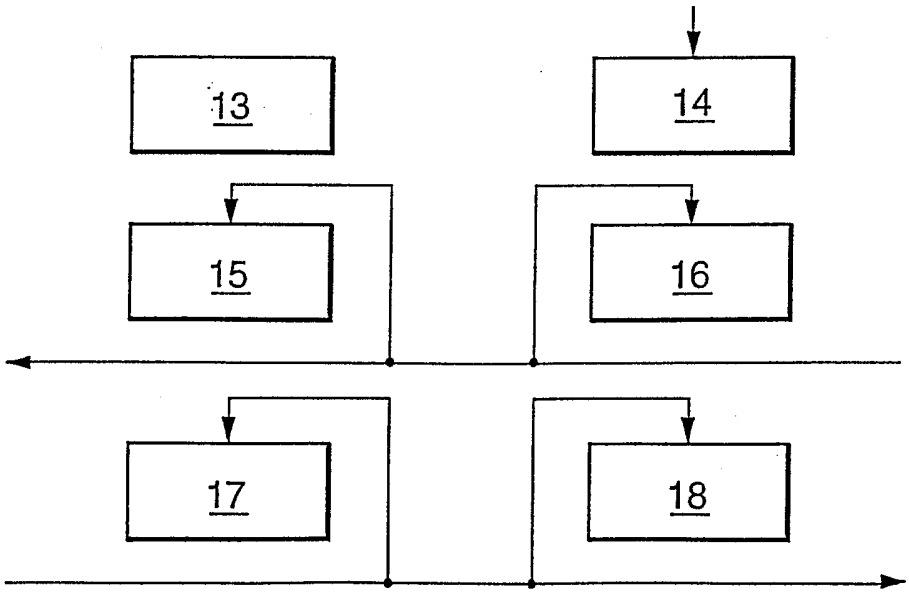
PV 2143-99
19.08.99

5784 3x)

obr. 1



obr. 2



57843 x)

obr. 3