SLOVENSKÁ REPUBLIKA

(19) **SK**

ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

PATENTOVÝ SPIS

(21) Číslo prihlášky: **50006-2012**
(22) Dátum podania prihlášky: **7. 2. 2012**
(31) Číslo prioritnej prihlášky: **PV 2011-142**
(32) Dátum podania prioritnej prihlášky: **17. 3. 2011**
(33) Krajina alebo regionálna organizácia priority: **CZ**
(40) Dátum zverejnenia prihlášky: **2. 10. 2013**
Vestník ÚPV SR č.: **10/2013**
(47) Dátum sprístupnenia patentu verejnosti: **8. 6. 2016**
(62) Číslo pôvodnej prihlášky v prípade vylúčenej prihlášky:
(67) Číslo pôvodnej prihlášky úžitkového vzoru v prípade odbočenia:
(86) Číslo podania medzinárodnej prihlášky podľa PCT:
(87) Číslo zverejnenia medzinárodnej prihlášky podľa PCT:
(96) Číslo podania európskej patentovej prihlášky:

(11) Číslo dokumentu:

288372

(13) Druh dokumentu: **B6**

(51) Int. Cl. (2016.01):

G06F 21/00
G06F 11/00
B61L 1/00
H04L 1/00
H04L 9/00

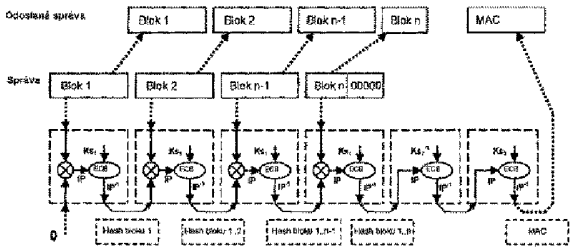
(73) Majiteľ: **AŽD Praha s. r. o., Praha, CZ;**

(72) Pôvodca: **Klapka Štěpán, doc. RNDr., Praha, CZ;**
Kárná Lucie, Mgr., Praha, CZ;
Súkup Jaroslav, Ing., Praha, CZ;
Harlenderová Magdaléna, RNDr., Olomouc, CZ;

(74) Zástupca: **Bachratá Magdaléna, Mgr., Bratislava, SK;**

(54) Názov: **Spôsob zachovania bezpečnostného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov**

(57) Anotácia:
Spôsob zachovania bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov, kde aspoň dve jednotky spoločne vytvárajú odtlačky dát, a pritom súčasne žiadna z nich sama osebe neumožňuje vytvorenie takéhoto dátového odtlačku. Podstata spočíva v tom, že postup vytvorenia odtlačku dát sa rozloží do postupností vytvárania čiastkových odtlačkov dát v stanovenom časovom slede, ktorých výsledkom je pôvodný odtlačok dát, a v prípade, keď sa zistí porucha v niektorej zo spolupracujúcich jednotiek, odmietne neporušená jednotka, ktorá spolupracuje s poškodenou jednotkou, vytvorenie čiastkového odtlačku dát.



SK 288372 B6

Oblasť techniky

Predložený vynález sa týka spôsobu zachovania bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov.

Doterajší stav techniky

Z celkového pohľadu je možné bezpečnosť kritických aplikácií na najvyššej úrovni rozdeliť na oblasť technickej a funkčnej bezpečnosti. Funkčná bezpečnosť sa v železničnej zabezpečovacej technike zaoberá predovšetkým dopravno-bezpečnostnými algoritmami, ktoré zaisťujú obmedzenie rizík vznikajúcich väčšinou mimo vlastného zabezpečovacieho zariadenia, predovšetkým v nadväzujúcej železničnej infraštruktúre, ako sú koľajové obvody, návestidlá, výhybky a podobne. Na druhej strane technická bezpečnosť je zameraná na riziká, ktoré vznikajú predovšetkým vplyvom poruchových stavov vlastného zabezpečovacieho zariadenia. Pri návrhu zabezpečovacích zariadení je teda z pohľadu technickej bezpečnosti nutné brať do úvahy vplyvy poruchových stavov na vlastnú bezpečnostnú funkciu zariadenia. V prípade uvažovania vplyvu ojedinelých poruchových stavov je pre systémy s vyššími požiadavkami na bezpečnosť potrebné zabezpečiť, aby zostali bezpečné v prípade akéhokoľvek druhu ojedinelého náhodného poruchového stavu hardvéru, ktorý je považovaný za možný. Tento princíp je známy ako bezpečnosť pri poruche (Fail-Safe) a môže byť dosiahnutý niekoľkými rôznymi spôsobmi, a to inherentne (vlastnou) bezpečnosťou pri poruche, zloženou bezpečnosťou pri poruche a reaktívnou bezpečnosťou pri poruche. Podľa princípu inherentnej bezpečnosti sa pri poruche dosahuje bezpečnosť tým, že žiadne hodnoverné druhy porúch jednotky (zariadenia) nie sú nebezpečné. Hodnovernosť porúch musí byť garantovaná napríklad fyzikálnymi vlastnosťami použitých súčiastok a ich zapojením. V tomto prípade je zvládnutie poruchy (detekcia a negácia) zaistené predovšetkým fyzikálnymi zákonmi.

Naproti tomu zložená a reaktívna bezpečnosť využíva detekciu na dosiahnutie bezpečnosti na zabránenie nebezpečenstvu. V prípade zloženej bezpečnosti je na detekciu poruchových stavov použitý hlasovací princíp. V prípade reaktívnej bezpečnosti je rýchla a hodnoverná detekcia zaistená špecializovanou jednotkou, ktorá je na tento účel navrhnutá. Táto špeciálna jednotka však nevykonáva priamo bezpečnostnú funkciu, ale len dohliada na správne vykonávanie bezpečnostnej funkcie hlavnej (funkčnej) jednotky. Ak je špeciálnou jednotkou detegované zlyhanie bezpečnostnej funkcie hlavnej jednotky, je špeciálnou jednotkou zabezpečené, že výstupy systému s vyššími požiadavkami na bezpečnosť prejdú do bezpečného stavu. Pri určitom zjednodušení sa dá povedať, že hlasovací princíp zo zloženej bezpečnosti je pri reaktívnej bezpečnosti nahradený kvalitou detekcie špeciálnej jednotky. Súčasné zabezpečovacie zariadenia pre vysoké riziká väčšinou využívajú všetky tri princípy a v niektorých prípadoch sa dá veľmi ťažko rozhodnúť, o ktorý z uvedených princípov práve ide.

V prípade zloženej bezpečnosti pri poruche vykonáva bezpečnostnú funkciu (dopravnobezpečnostné algoritmy) viac ako jedna jednotka (zariadenie), resp. časť zariadenia, v spolupráci s ostatnými jednotkami. V tomto prípade nezávislé jednotky rozhodujú väčšinovo, hlasujú o svojich výstupoch, svojich funkciách. Tak napríklad rozhodujú dve jednotky z dvoch, dve z troch, tri z piatich a pod. Zabezpečovacím zariadením môže byť napr. rádiobloková centrála systému ETCS (European Train Control System), ktorá v systéme dvoch jednotiek z troch (väčšinové rozhodovanie o výstupoch ich funkcií) vytvára povely pre vlaky, ktoré sú prenášané pomocou GSM komunikácie. Vzhľadom na možnosť útoku v GSM prenose musí byť použitá kryptografická ochrana pomocou blokovej šifry DES (Data Encryption Standard). Pre techniku zloženej bezpečnosti sa pri poruche požaduje, aby nebezpečný poruchový stav v jednej jednotke bol detegovaný a zvládnutý v dobe dostatočnej na to, aby sa zabránilo súhlasnému poruchovému stavu v druhej jednotke. Požaduje sa, aby poruchový stav bol zvládnutý skôr, než zlyhá zvolený postup detekcie (hlasovanie) vzhľadom k ďalšej degradácii systému.

Jedným z dôležitých postupov na zabezpečenie princípu zloženej bezpečnosti pri poruche je proces zvládnutia poruchy po jej detekcii. Obvykle sa používa nevratné odpojenie narušenej jednotky z ďalšej funkcie. Pretože k odpojeniu jednotky sa väčšinou odpojí napájacie napätie, vznikajú pri následnom bežnom štartovaní systému určité komplikácie. Ďalšou často používanou technikou je izolácia narušenej časti, napr. funkčným odpojením porušenej jednotky bez potreby odpájania hardvéru. Jednou z možností na implementáciu tohto spôsobu je existencia bezpečnostne relevantnej informácie, ktorá je nevyhnutná na vykonávanie bezpečnostne relevantnej činnosti, napr. uskutočňovanie zvolenej komunikácie medzi zabezpečovacími zariadeniami. Jedným spoločným prvkom, ktorým musia byť vysielané správy vybavené, je bezpečnostný kód, čo je tá časť správy, ktorá je pridaná k prenášaným dátam na účel kontroly ich integrity (celistvosti) a autenticity (pôvodnosti). Podľa svojej konštrukcie môže byť bezpečnostný kód kryptografický a nekryptografický. V patentovom dokumente CZ 296129 je forma bezpečnostného kódu prispôsobená potrebe zloženej bezpečnosti pri poruche, ale toto riešenie je obmedzené len na niektoré cyklické kódy, nemožno ho používať pre li-

neárne alebo kryptografické kódy. Nie je preto použiteľný pre prenosové systémy, kde nemožno vylúčiť útok na prenášané informácie, to znamená najmä na zmenu ich obsahu alebo zmenu autenticity. Na výpočet kryptografického bezpečnostného kódu sa síce dá použiť postup, uvedený v patentovom dokumente DE 102007032805 A1, ale len v stanovenej kompozícii, to znamená pre obmedzený počet bezpečnostných kódov, čo obmedzuje jeho využitie. Účelom predloženého vynálezu je postup, ktorý je možné adaptovať na takmer ľubovoľný typ bezpečnostného kódu, ktorý sa ďalej označuje ako odtlačok dát.

Podstata vynálezu

Predmetom tohto vynálezu je spôsob zachovania bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov, kde aspoň dve jednotky spoločne vytvárajú odtlačky dát a pritom súčasne každá z nich sama osebe, neumožňuje vytvorenie takéhoto dátového odtlačku. Podstata vynálezu spočíva v tom, že postup vytvorenia odtlačku dát sa rozloží do postupností vytvárania čiastkových odtlačkov dát v stanovenom časovom slede, ktorých výsledkom je pôvodný odtlačok dát, a v prípade, keď sa zistí porucha v niektorej zo spolupracujúcich jednotiek, odmietne neporušená jednotka, ktorá spolupracuje s poškodenou jednotkou, vytvorenie čiastkového odtlačku dát, čím sa znemožní vytvorenie pôvodného odtlačku dát. Pôvodný odtlačok dát je teda vytvorený len z postupnosti jednotiek, ktoré nemajú poruchu. Zabezpečovacím systémom, zahrnujúcim uvedené jednotky, môže byť rádiobloková centrála na riadenie vlakov prostredníctvom rádiovej komunikácie.

Odtlačky dát sú výsledkom funkcie, ktorá z daných pôvodných dát, vstupnej informácie, vytvára pomocou určitej definovanej redukcie reprezentatívnu dátovú vzorku k pôvodným dátam. Takúto funkciu je možné zostrojiť napríklad za použitia cyklického kódu tak, že za odtlačok položíme zvyšok po delení vstupnej informácie generujúcim polynómom cyklického kódu. Takýto dátový odtlačok potom slúži napríklad na kontrolu neporušenosti dát alebo kontrolu ich autenticity.

V prípade lineárnych kódov, keď sa na vytvorenie odtlačku dát použije generujúca matica, sa výsledný čiastkový odtlačok dát vytvára tak, že je permutáciou pôvodného odtlačku dát, pričom inverzná permutácia je rozložená na čiastkovú permutáciu, a tým vzniknú čiastkové transformácie, ktoré z výsledného čiastkového odtlačku dát vytvoria pôvodný odtlačok dát. Na tento účel postačí vykonať iba permutáciu stĺpcov generujúcej matice.

V prípade použitia blokovej šifry, ktorou sa vytvára pomocou metódy CBC (Cipher Block Chaining) pôvodný odtlačok CBC-MAC dát, sa modifikuje bloková šifra tak, že sa výsledný čiastkový odtlačok dát metódy CBC odlišuje od pôvodného odtlačku CBC-MAC dát a ďalšími čiastkovými transformáciami výsledného čiastkového odtlačku dát sa vytvorí pôvodný odtlačok CBC-MAC dát.

V prípade použitia blokovej šifry DES (Data Encryption Standard) sa vstupnou permutáciou pôvodného bloku dát, šifrovacej časti a výstupnou inverznou permutáciou zašifrovaného bloku dát sa táto výstupná inverzná permutácia rozloží na čiastkové permutácie, a tým vzniknú čiastkové transformácie, ktoré z výsledného čiastkového odtlačku dát vytvoria pôvodný odtlačok dát.

V prípade použitia blokovej šifry AES (Advanced Encryption Standard), ktorá sa vykonáva v blokoch výpočtu (rounds), pričom pre každý tento blok výpočtu sa uplatní špecifický kľúč, sa k šifrovaným dátam z pôvodného bloku dát pridáva v každom bloku výpočtu odlišný kľúč a kľúč posledného bloku výpočtu sa pridá ku kľúču prvého bloku výpočtu nasledujúceho kroku výpočtu metódy CBC, čím sa zabezpečí odlišnosť výsledného čiastkového odtlačku dát od pôvodného odtlačku dát, pričom ďalšou čiastkovou transformáciou sa výsledný odtlačok premení na tvar, kedy je permutáciou pôvodného odtlačku a inverzná permutácia sa rozloží do čiastkových permutácií, ktoré transformujú čiastkový odtlačok na pôvodný odtlačok.

V prípade použitia lineárnych kódov, kedy sa na vytvorenie odtlačku dát použije generujúca matica, sa pri overovaní odtlačku dát použije výsledný čiastkový odtlačok, ktorý sa pre neporušenú autentickú správu rovná prijatému odtlačku, získanému spoluprácou jednotiek, na ktorom je uskutočnená permutácia v inverznom poradí.

V prípade použitia systému overovacích polynómov, ktorých najmenší spoločný násobok sa rovná generujúcemu polynómu cyklického bezpečnostného kódu, sa tieto overovacie polynómy použijú na kontrolu neporušenosti a autenticity.

V prípade použitia blokovej šifry DES sa pri overovaní pôvodného odtlačku CBC-MAC dát použije inverzný postup pomocou trojice navzájom odlišných kľúčov K_{S1}, K_{S2}, K_{S3}, kedy prijatý pôvodný odtlačok CBC-MAC dát sa najprv dešifruje pomocou tretieho kľúča, a potom zašifruje pomocou druhého kľúča K_{S2}, pričom ak overovaný odtlačok je autentický a neporušený, potom sa výsledok týchto operácií zhoduje s odtlačkom správy vytvoreným pomocou prvého kľúča K_{S1}.

V prípade použitia blokovej šifry AES sa pri overovaní pôvodného odtlačku CBC-MAC dát použije inverzný postup, kedy prijatý pôvodný odtlačok CBC-MAC dát sa najprv dešifruje a potom pomocou funkcie XOR s posledným blokom dát sa upraví na CBC-MAC len predchádzajúcich blokov dát, pričom sa spätne

postupuje až k prvému bloku dát, keď pre autentickú a neporušenú správu sa výsledok výpočtu rovná inicializačnému vektoru.

Hlavná výhoda spôsobu zachovania bezpečného stavu pri poruche zabezpečovacích systémov so zloženou bezpečnosťou pri vytváraní dátových odtlačkov podľa tohto vynálezu, oproti doteraz známym riešeniam uvedeným v bode doterajšieho stavu techniky, spočíva v tom, že tento postup nevyžaduje špecializované hardvérové prostriedky na komparáciu alebo hlasovanie, ktoré by inak museli pracovať na princípe inherentnej bezpečnosti. Tento postup vedie k zjednodušeniu HW návrhu, zníženiu nákladov a nakoniec k zvýšeniu spoľahlivosti zabezpečovacích systémov.

Prehľad obrázkov na výkresoch

Na pripojených výkresoch sú znázornené príklady uskutočnenia predloženého vynálezu, nasleduje jeho podrobný opis s vysvetlením.

Binárny (n, k)-lineárny blokový systematický kód sa skladá z k informačných bitov (informačné časti) a $c = n - k$ kontrolných bitov (kontrolné časti), ktoré sú vo výslednej správe organizované podľa schémy na obrázku 1.

V prípade použitia blokovej šifry, ktorou sa vytvára pomocou metódy CBC (Cipher Block Chaining) pôvodný odtlačok CBC-MAC dát, sa modifikuje bloková šifra tak, že sa výsledný čiastkový odtlačok dát metódy CBC odlišuje od pôvodného odtlačku CBC-MAC dát a ďalším čiastkovými transformáciami čiastkového odtlačku dát sa vytvorí pôvodný odtlačok CBC- MAC dát. Pôvodný postup výpočtu CBC-MAC pomocou blokovej šifry DES je zrejmý zo schémy na obrázku 2. Technika výpočtu CBC-MAC je založená na tom, že inverzia vstupnej permutácie IP pre blokovú šifru DES nie je známa v žiadnej jednotke, a tak na dosiahnutie správneho výsledku je potrebná spolupráca medzi dvojicami jednotiek, ktoré potrebnú transformáciu vo vzájomnej spolupráci vytvoria, viď nasledujúca schéma na obrázku 3. Pôvodná schéma výpočtu blokovej šifry DES je zobrazená na obrázku 4.

Bloková šifra AES je obdobne ako DES vykonávaná v rundách (round), pozri obrázok 5 so štruktúrou výpočtu blokovej šifry AES.

Podľa dĺžky kľúča (128, 192 a 256 bitov) sa vykonáva príslušný počet cyklov (Nr = 10, 12 a 14 rund). Pred prvou rundou, a potom po každej runde je k stavovej informácii pridaná príslušná časť expandovaného kľúča, za pomoci operácie XOR. Pretože výpočet CBC-MAC je takisto založený na operácii XOR, je možné využiť komutatívnosť tejto operácie a preusporiadať výpočet CBC-MAC tak, že posledných 16B expandovaného kľúča sa už vopred upraví pomocou funkcie XOR s prvými 16B kľúča. Zmena vo výpočte je schematicky naznačená nasledovne (pôvodná na obrázku 6 a potom nová na obrázku 7).

V prípade blokovej šifry DES na overenie pôvodného odtlačku CBC-MAC dát pri príjme je možné využiť aj postup, ktorý nepoužije jeho znovuvytvorenie. Tento postup je založený na inverznom postupe pri vytváraní pôvodného odtlačku CBC-MAC dát, pomocou trojice navzájom odlišných kľúčov. Z prijatého telegramu je nutné pomocou tretieho kľúča K_{S3} dešifrovať (D) CBC-MAC, ďalej zašifrovať (E) pomocou druhého kľúča K_{S2}, a potom overiť, že výsledok zodpovedá odtlačku správy vytvoreného pomocou prvého kľúča K_{S1} (viď obrázok 8). Na schéme na obrázku 9 je opísaný systém vytvorenia odtlačku validnej (platnej) správy pre kontrolu jej integrity a autenticity, ktorý vyžaduje spoluprácu vždy dvoch jednotiek.

Príklady uskutočnenia vynálezu

Pod zloženou bezpečnosťou železničných zabezpečovacích systémov sa rozumie princíp, ktorý umožňuje zachovať ich bezpečnosť v prípadoch, keď bezpečnostnú funkciu vykonáva viac ako jedna jednotka v spolupráci s ďalšími nezávislými jednotkami. Napríklad, keď nezávislé jednotky väčšinovo rozhodujú o výstupoch svojich funkcií, to znamená dve z troch jednotiek, dve z dvoch, tri z piatich a pod.

Spôsob zachovania bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou na železnici pri vytváraní dátových odtlačkov bude v nasledujúcom texte opísaný pre prípady lineárnych kódov a blokovej šifry DES (Data Encryption Standard) a AES (Advanced Encryption Standard), ktorou sa vytvára pomocou metódy CBC (Cipher Block Chaining) pôvodný odtlačok CBC-MAC dát a bloková šifra sa modifikuje tak, že sa výsledný čiastkový odtlačok dát metódy CBC odlišuje od pôvodného odtlačku CBC-MAC dát a ďalšími čiastočnými transformáciami výsledného čiastkového odtlačku dát sa vytvorí pôvodný odtlačok CBC-MAC dát. Odtlačok dát je výsledkom funkcie, ktorá z daných pôvodných dát vytvorí pomocou určitej definovanej redukcie reprezentatívnu dátovú vzorku k pôvodným dátam. Zmyslom odtlačku dát je napríklad kontrola neporušenosti dát alebo kontrola ich autenticity.

Lineárny kód je definovaný generujúcou maticou, ktorá opisuje transformáciu pôvodných dát na odtlačok dát. Ako už bolo uvedené, odtlačky dát sú výsledkom funkcie, ktorá z daných pôvodných dát vytvára pomo-

cou určitej definovanej redukcie reprezentatívnu vzorku dát k pôvodným dátam a slúži napríklad na kontrolu neporušenosti dát. V nasledujúcich odsekoch je uvažovaný binárny *(n, k)*-lineárne blokový systematický kód, ktorý sa skladá z *k* informačných bitov (informačnej časti) a *c* = *n-k* kontrolných bitov (kontrolnej časti), ktoré sú vo výslednej správe organizované podľa schémy na obrázku 1.

Binárny *(n, k)*-lineárny (blokový) systematický kód je plne opísaný generujúcou binárnou maticou v nasledujúcom tvare. Každý riadkový vektor B_i s *c* bitmi je príslušným príspevkom do kontrolnej časti, ak je bit *i* správy nenulový.

$$G = [E, B] = \begin{bmatrix} 1 & 0 & \cdots & 0 & B_1 \\ 0 & 1 & \cdots & 0 & B_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & B_n \end{bmatrix} \qquad M = [E, BP] = \begin{bmatrix} 1 & 0 & \cdots & 0 & B_1P \\ 0 & 1 & \cdots & 0 & B_2P \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & B_nP \end{bmatrix}$$

Ak sa na bitoch riadku B_i matice *B* vykoná potrebná permutácia *P,* potom nová generujúca matica *M* už vytvára odtlačok, v ktorom sú bity príslušne poprehadzované. Výsledný čiastkový odtlačok dát je teda maticou *M* vytváraný tak, že je permutáciou pôvodného odtlačku dát, ktorá je určená maticou permutácie *P.* Z hľadiska teórie kódovania ide v tomto prípade o ekvivalentný lineárny kód. Vlastné násobenie generujúce maticou *M* systematického binárneho kódu potom predstavuje použitie operácie XOR pre pridanie vektorov B_i do kontrolnej časti. Z generujúcej matice *M* je teda pre výpočet potrebné uchovávať len maticu *BP.* Potrebné permutácie *P* na spoluprácu jednotiek sú súčasťou informácií v dátovej štruktúre, ktorá je označovaná ako reštartovacia značka. Spôsoby práce s reštartovacou značkou (bezpečnostne relevantnou informáciou) sú podrobne opísané v patentovom dokumente CZ 298373.

Pretože všetky cyklické kódy sú lineárne, možno opísaný postup použiť aj pre všetky cyklické kódy, ktoré sú vytvorené nad algebrickými telesami charakteristiky dva (GF (2^m)).

Všetky tieto kódy možno totiž chápať ako binárne lineárne kódy. Do tejto skupiny cyklických kódov patria zatiaľ všetky uvažované bezpečnostné kódy pri zvažovaných aplikáciách zabezpečovacích zariadení na železnici.

V prípade použitia blokovej šifry, ktorou sa vytvára pomocou metódy CBC (Cipher Block Chaining) pôvodný odtlačok CBC-MAC dát, sa modifikuje bloková šifra tak, že sa výsledný čiastkový odtlačok dát metódy CBC odlišuje od pôvodného odtlačku CBC-MAC dát a ďalšími čiastkovými transformáciami čiastkového odtlačku dát sa vytvorí pôvodný odtlačok CBC-MAC dát. Pôvodný postup výpočtu CBC-MAC pomocou blokovej šifry DES je zrejmý zo schémy na obrázku 2.

Výpočet pôvodného odtlačku CBC-MAC dát začína úpravou prvého 64-bitového bloku dát s inicializačným vektorom pomocou operácie XOR. Na výsledok je použitá bloková šifra DES (Data Encryption Standard) s kľúčom K_{S1}, pričom v rámci výpočtu DES je najprv použitá vstupná permutácia a po použití vlastného šifrovacieho postupu je použitá permutácia inverzná. K získanému výsledku sa pridá, za pomoci operácie XOR, ďalší 64-bitový blok dát a ďalej sa vo výpočte postupuje obdobným spôsobom. Ak sa permutácia obsiahnutá v algoritme DES vytkne pred operáciu XOR, získame tak postup, kde sa ušetrí v každom kroku výpočet jednej permutácie (inverzná permutácia). Inverzná permutácia sa použije len raz na konci výpočtu.

Nasledujúca technika výpočtu CBC-MAC je založená na tom, že inverzia vstupnej permutácie IP pre blokovú šifru DES nie je známa v žiadnej jednotke a tak na dosiahnutie správneho výsledku je potrebná spolupráca medzi dvojicami jednotiek, ktoré potrebnú transformáciu vo vzájomnej spolupráci vytvoria, viď nasledujúca schéma na obrázok 3. Pôvodná schéma výpočtu blokovej šifry DES je zobrazená na obrázku 4.

Štruktúra výpočtu (šifrovanie a dešifrovanie) blokovej šifry AES (Advanced Encryption Standard) má niekoľko zásadných odlišností oproti blokovej šifre DES. Prvá odlišnosť spočíva v tom, že šifrovanie a dešifrovanie sú špecializované nezámenné procedúry. Pretože na vytvorenie CBC-MAC je nevyhnutná len šifrovacia procedúra, možno sa v ďalšom výklade obmedziť iba na modifikáciu tejto procedúry na potreby zloženej bezpečnosti pri poruche. Ďalšia odlišnosť medzi AES a DES spočíva v tom, že AES nepoužíva žiadne vstupné a výstupné permutácie. Pri určitom úsilí možno permutácie do procedúry šifrovania AES zabudovať, ale to prináša navýšenie potrebného výpočtového výkonu. Preto je vhodnejšie modifikovať výpočet AES takým spôsobom, aby žiadny medzivýsledok nebol použiteľným odtlačkom a potrebné permutácie zabudovať až do finálnej procedúry výpočtu.

Bloková šifra AES sa obdobne ako DES vykonáva v rundách (round), viď obrázok 5, so štruktúrou výpočtu blokovej šifry AES. Podľa dĺžky kľúča (128, 192 a 256 bitov) sa vykonáva príslušný počet cyklov (Nr = 10, 12 a 14 rund). Pred prvou rundou, a potom po každej runde je stavová informácia upravená pomocou funkcie XOR s príslušnou časťou expandovaného kľúča. Pretože výpočet CBC-MAC je tiež založený na operácii XOR, je možné využiť komutatívnosť tejto operácie a preusporiadať výpočet CBC-MAC tak, že posledných 16B expandovaného kľúča sa už vopred upraví pomocou operácie XOR s prvými 16B kľúča. Zmena vo výpočte je schematicky naznačená nasledovne (pôvodná na obrázku 6 a potom nová na obrázku 7).

Oproti pôvodnému výpočtu (schéma na obrázku 6) je vždy po poslednej runde zároveň aplikovaná ako posledná, tak aj prvá časť expandovaného kľúča. Vďaka tomu je výsledok na konci výpočtu modifikovaný prvými 16B kľúča. Na tento výsledok sa vykonajú potrebné permutácie a na takto získaný medzivýsledok sa aplikuje časť kľúča, na ktorej je uskutočnená permutácia. Tým sa získa potrebný výsledný čiastkový odtlačok, ktorý už bude dokončený rovnakým spôsobom ako v ostatných prípadoch pri spolupráci určených jednotiek.

Postup výpočtu naznačený na schéme nová štruktúra výpočtu (obrázok 7) sa dá ďalej urýchliť tým, že pri expanzii kľúča sa ku kľúču pre poslednú rundu pridá, za pomoci operácie XOR, prvý kľúč. Vzhľadom na túto úpravu je od výpočtu druhého bloku ďalej ušetrená jedna aplikácia kľúča pred prvou rundou. Celý výpočet CBC-MAC sa teda rozpadne na tri časti. V počiatočnej časti je pred prvou rundou aplikovaná prvá časť expandovaného kľúča (to je prvých 16B tajného kľúča), a potom po každej runde ďalšia príslušná časť.

V opakovanom výpočte už nie je používaná prvá časť expandovaného kľúča a sú vždy aplikované len ostatné časti po každej runde. V záverečnej úprave sa na výsledok aplikuje permutácia a modifikuje sa prvou časťou expandovaného kľúča, na ktorej bola takisto vykonaná permutácia.

Základný princíp technickej bezpečnosti pri overovaní odtlačkov dát je založený na tom, že pri postupe overovania nevzniká správny odtlačok dát. Postup kontroly, ktorý by využíval opätovné vytvorenie odtlačku, je teda neprípustný. Takýto postup kontroly je jednoducho zneužiteľný na to, aby príjemca a overovateľ správnosti odtlačku také odtlačky prípadne vplyvom poruchy vytváral sám.

Pre acyklické lineárne kódy je možné postupovať tak, že pomocou uvedenej matice *M* je najprv vytvorený odtlačok, na ktorom je aplikovaná permutácia, a následne je porovnávaný s doručeným odtlačkom, na ktorý je aplikovaná inverzná permutácia, vytvorená spoluprácou potrebného počtu jednotiek. Tento postup je nutné použiť aj pri cyklických kódoch, ak príslušný generujúci polynóm nemožno rozdeliť na použiteľný systém faktorov. Tento typ lineárnych bezpečnostných kódov nebol doteraz požadovaný pre žiadnu aplikáciu.

Ak existuje systém polynómov (overovacích polynómov), ktorých najmenší spoločný násobok sa rovná generujúcemu polynómu cyklického bezpečnostného kódu, potom možno nahradiť postup overenia odtlačku generujúcim polynómom kontrolou pomocou overovacích polynómov. Tento postup je podrobne opísaný v patentovom dokumente CZ 296129.

Na overenie pôvodného odtlačku CBC-MAC dát s použitím blokovej šifry DES pri príjme je možné využiť aj postup, ktorý nevyužíva jeho znovuvytvorenie (čo je všeobecne odporúčaná technika). Tento postup je založený na inverznom postupe pri vytváraní pôvodného odtlačku CBC-MAC dát, pomocou trojice navzájom odlišných kľúčov. Z prijatého telegramu je nutné pomocou tretieho kľúča $\mathbf{K}_{S3}$ dešifrovať (D) CBC-MAC, ďalej zašifrovať (E) pomocou druhého kľúča $\mathbf{K}_{S2}$, a potom overiť, že výsledok zodpovedá odtlačku správy vytvoreného pomocou prvého kľúča $\mathbf{K}_{S1}$ (pozri obrázok 8).

Tento postup kontroly má obdobnú výhodu ako postup uvedený v predchádzajúcom odseku. Na overenie integrity a autenticity došlej správy nie je nutná spolupráca jednotiek, ktorá je nevyhnutná pre jej vytvorenie.

Na overenie pôvodného odtlačku CBC-MAC dát s použitím blokovej šifry AES pri príjme je možné využiť podobný postup, ktorý je uvedený v predchádzajúcom odseku. Je nutné z prijatého telegramu pomocou tajného kľúča dešifrovať blok s pôvodným odtlačkom CBC-MAC dát, a potom ďalej pokračovať v inverznom postupe (za pomoci operácie XOR vždy s posledným blokom dát), až bude zrekonštruovaný inicializačný vektor, ktorým začínal vlastný výpočet pôvodného odtlačku CBC-MAC dát. Ak dostaneme dohodnutú hodnotu, je prijatá správa integritná a autentická. Vzhľadom na to, že procedúru dešifrovania blokovej šifry AES je možné použiť bez obmedzenia v jednej jednotke, je tento postup kontroly uskutočniteľný bez spolupráce viacerých jednotiek.

Na kontrolu možno využiť aj nedokončený proces konštrukcie pôvodného odtlačku CBC-MAC na dátach prijatej správy. Ak sa výsledok pred záverečnou úpravou konštrukcie pôvodného odtlačku CBC-MAC dát upraví pomocou operácie XOR s prijatým pôvodným odtlačkom CBC-MAC dát, potom pre neporušenú autentickú správu je potrebné dostať prvých 16B použitého tajného kľúča.

Na schéme na obrázku 9 je opísaný systém vytvorenia odtlačku validnej (platnej) správy na kontrolu jej integrity a autenticity, ktorý vyžaduje spoluprácu vždy práve dvoch jednotiek. (Poznámka: Aby mohla daná jednotka vytvoriť odtlačok, potrebuje spoluprácu aspoň jednej ďalšej jednotky daného zariadenia. Zámer tohto faktu bude zrejmý z nižšie uvedeného.)

V systéme dva z troch sa na vytváraní odtlačku podieľajú tri jednotky A, B, C, pričom žiadna z nich nepozná kompletný postup jeho vytvorenia a odtlačok vzniká vynútenou spoluprácou vždy dvoch jednotiek. Z dát vytváranej správy u (na obrázku označené ako pole DATA) je vytvorený odtlačok F(u) nasledujúcim postupom, znázorneným na obrázku.

1. Každá z troch jednotiek A, B, C vytvorí z dát pomocou funkcie F_{PAIC} výsledný čiastkový odtlačok na kontrolu integrity, ktorý sa označuje PAIC (Primary Authorization Integrity Check). Funkcia F_{PAIC} vytvára výsledný čiastkový odtlačok dát, na ktorý je aplikovaná permutácia P_{PAIC} tak, že s dátami nevytvára validnú správu; t. j. je to zložené zobrazenie $F_{PAIC} = P_{PAIC} \circ \mathbf{F}$. Funkcia F_{PAIC} je vo všetkých troch jednotkách rovnaká a

musí byť implementovaná tak, aby nebolo možné jej neúplným uskutočnením vytvoriť platný odtlačok dát **F**(**u**). Nemožno teda najprv vykonať funkciu **F** a potom permutáciu P_{PAIC}; zložená funkcia FPAIC musí byť pre jednotku nerozložiteľná.

2. Jednotka A vykoná spracovanie poľa dát PAIC funkcií P_{AB1}, a tým vytvorí sekundárny autorizačný odtlačok SAICAB (Secondary Authorization Integrity Check), čo je čiastková transformácia výsledného čiastkového odtlačku. Táto funkcia vykoná permutáciu bitov poľa PAIC, ktorá je v rámci systému jedinečná; schopnosťou vykonať danú permutáciu disponuje iba jednotka A a možno ju použiť len na spoluprácu s jednotkou B. Zároveň vytvorí pomocou permutácie P_{ACI} druhý sekundárny autorizačný odtlačok $SAIC_{AC}$, určený pre spoluprácu s jednotkou C.

3. Súčasne vytvorí jednotka B z poľa PAIC pomocou permutácií P_{BA1} a P_{BC1} sekundárne autorizačné odtlačky $SAIC_{BA}$ a $SAIC_{BC}$, určené na spoluprácu s jednotkami A a C.

4. Súčasne vytvorí jednotka C z poľa PAIC pomocou permutácií P_{CA1} a P_{CB1} sekundárne autorizačné odtlačky $SAIC_{CA}$ a $SAIC_{CB}$, určené na spoluprácu s jednotkami A a B.

5. Každá z permutácií P_{XY1} (kde X a Y môžu nadobúdať hodnoty A, B a C) je v rámci systému jedinečná; pozná ju len jednotka X a možno ju použiť len na spoluprácu s jednotkou Y.

6. Nasleduje výmena sekundárnych odtlačkov (čiastkovou transformáciou výsledného čiastkového odtlačku) medzi jednotkami: jednotka A vyšle odtlačok $SAIC_{AB}$ jednotke B a odtlačok $SAIC_{AC}$ jednotke C; jednotka B vyšle odtlačok $SAIC_{BA}$ jednotke A a odtlačok $SAIC_{BC}$ jednotke C a konečne jednotka C vyšle odtlačok $SAIC_{CA}$ jednotke A a odtlačok $SAIC_{CB}$ jednotke B (pozri obrázok).

7. Jednotka A spracuje sekundárny autorizačný odtlačok $SAIC_{BA}$ (ktorý dostala od jednotky B) permutáciou P_{BA2}, čím vznikne finálny autorizačný odtlačok $FAIC_{BA}$. Zároveň aplikuje na autorizačný odtlačok $SAIC_{CA}$ (ktorý dostala od jednotky C) permutáciu P_{CA2}, čím vznikne finálny autorizačný odtlačok $FAIC_{CA}$.

8. Súčasne jednotka B vytvorí zo sekundárneho autorizačného odtlačku $SAIC_{AB}$ (ktorý dostala od jednotky A) pomocou permutácie P_{AB2} finálny autorizačný odtlačok $FAIC_{AB}$ a z autorizačného odtlačku $SAIC_{CB}$ (ktorý dostala od jednotky C) permutáciou P_{CB2} finálny autorizačný odtlačok $FAIC_{CB}$.

9. Konečne jednotka C vytvorí zo sekundárneho autorizačného odtlačku $SAIC_{AC}$ (ktorý dostala od jednotky A) pomocou permutácie P_{AC2} finálny autorizačný odtlačok $FAIC_{AC}$ a z autorizačného odtlačku $SAIC_{BC}$ (ktorý dostala od jednotky C) permutáciou P_{BC2} finálny autorizačný odtlačok $FAIC_{BC}$.

10. Každá z permutácií P_{XY2} (kde X a Y môžu nadobúdať hodnoty A, B a C) je opäť v rámci systému jedinečná; pozná ju len jednotka Y a možno ju použiť len na spracovanie sekundárneho odtlačku vytvoreného jednotkou X.

11. Permutácie P_{XY1} a P_{XY2} (X a Y môžu nadobúdať hodnoty A, B a C) sú zvolené tak, aby zložením permutácií P_{XY1} a P_{XY2} vznikla pre každú dvojicu X, Y rovnaká permutácia, a to permutácia P_{PAIC}^{-1} inverzná k permutácii P_{PAIC}. (t. j. $P_{AB1} \circ P_{AB2} = P_{AC1} \circ P_{AC2} = ... = P_{CB1} \circ P_{CB2} = P_{PAIC}^{-1}$). Vďaka tomu sú pri bezchybnej funkcii všetkých jednotiek všetky finálne odtlačky $FAIC_{XY}$ rovnaké. (Platí totiž napríklad $FAIC_{AB} = P_{AB2}(P_{AB1}(F_{PAIC}(\boldsymbol{u})))) = P_{PAIC}^{-1}(P_{PAIC}(\mathbf{F}(\boldsymbol{u})) = \mathbf{F}(\boldsymbol{u}))$.

Pred samotným začatím výpočtu odtlačku sa vykoná kontrola vzájomnej zhody poľa dát DATA medzi jednotkami. Rovnako pred pridaním poľa DATA k odtlačku FAIC sa jednotkou overí, či odtlačok FAIC zodpovedá údajom, ktoré zabezpečuje.

Priemyselná využiteľnosť

Vynález je využiteľný na zachovanie bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov.

PATENTOVÉ NÁROKY

1. Spôsob zachovania bezpečného stavu zabezpečovacích systémov so zloženou bezpečnosťou, najmä na železnici, pri vytváraní dátových odtlačkov, kde aspoň dve jednotky spoločne vytvárajú odtlačky dát a pritom súčasne žiadna z nich sama osebe neumožňuje vytvorenie takéhoto dátového odtlačku, **vyznačujúci sa tým,** že postup vytvorenia odtlačku dát sa rozloží do postupností vytvárania čiastkových odtlačkov dát v stanovenom časovom slede, ktorých výsledkom je pôvodný odtlačok dát, a v prípade, keď sa zistí porucha v niektorej zo spolupracujúcich jednotiek, odmietne neporušená jednotka, ktorá spolupracuje s poškodenou jednotkou, vytvorenie čiastkového odtlačku dát, čím sa znemožní vytvorenie pôvodného odtlačku dát.

2. Spôsob podľa nároku 1, **vyznačujúci sa tým,** že v prípade lineárnych kódov, kedy sa na vytvorenie odtlačku dát použije generujúca matica, sa výsledný čiastkový odtlačok dát vytvára tak, že je permutáciou pôvodného odtlačku dát, pričom inverzná permutácia je rozložená na čiastkové permutácie, a

tým vzniknú čiastkové transformácie, ktoré z výsledného čiastkového odtlačku dát vytvoria pôvodný odtlačok dát.

3. Spôsob podľa nároku 1, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia blokovej šifry, ktorou sa vytvára pomocou metódy reťazenia šifrovaného textu (CBC) pôvodný odtlačok CBC-MAC dát, sa modifikuje bloková šifra tak, že sa výsledný čiastkový odtlačok dát metódy CBC odlišuje od pôvodného odtlačku CBC-MAC dát a ďalšími čiastočnými transformáciami výsledného čiastkového odtlačku dát sa vytvorí pôvodný odtlačok CBC-MAC dát.

4. Spôsob podľa nároku 3, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia algoritmu na šifrovanie dát (DES) so vstupnou permutáciou IP pôvodného bloku dát, šifrovacou časťou a výstupnou inverznou permutáciou zašifrovaného bloku dát sa táto výstupná inverzná permutácia rozloží na čiastkové permutácie a tým vzniknú čiastkové transformácie, ktorými sa z výsledného čiastkového odtlačku dát vytvorí pôvodný odtlačok dát.

5. Spôsob podľa nároku 3, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia štandardu pokročilého šifrovania (AES), ktorý sa vykonáva v blokoch výpočtu, pričom pre každý tento blok výpočtu sa uplatní špecifický kľúč, sa k šifrovaným dátam z pôvodného bloku dát pridáva v každom bloku výpočtu odlišný kľúč a kľúč posledného bloku výpočtu sa pridá ku kľúču prvého bloku výpočtu nasledujúceho kroku výpočtu metódy CBC, čím sa zabezpečí odlišnosť výsledného čiastkového odtlačku dát od pôvodného odtlačku dát, pričom ďalšou čiastkovou transformáciou sa výsledný odtlačok premení na tvar, ktorý je permutáciou pôvodného odtlačku a inverzná permutácia sa rozloží na čiastkové permutácie, ktoré transformujú čiastkový odtlačok na pôvodný odtlačok.

6. Spôsob podľa nároku 2, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia lineárnych kódov, keď sa na vytvorenie odtlačku dát použije generujúca matica, sa pri overovaní odtlačkov dát použije výsledný čiastkový odtlačok, ktorý sa pre neporušenú autentickú správu rovná prijatému odtlačku, získanému spoluprácou aspoň dvoch jednotiek spoločne vytvárajúcich odtlačky dát, na ktorom je uskutočnená permutácia v inverznom poradí.

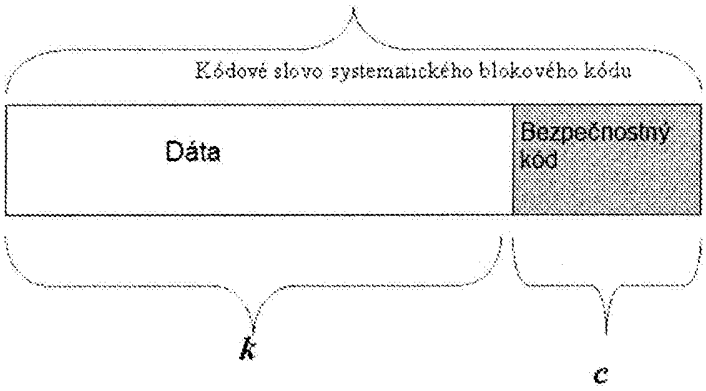
7. Spôsob podľa nároku 2, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia systému overovacích polynómov, ktorých najmenší spoločný násobok sa rovná generujúcemu polynómu cyklického bezpečnostného kódu, sa tieto overovacie polynómy použijú na kontrolu neporušenosti a autenticity.

8. Spôsob podľa nároku 4, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia blokovej šifry DES sa pri overovaní pôvodného odtlačku CBC-MAC dát použije inverzný postup pomocou trojice navzájom odlišných kľúčov ($\mathbf{K_{s1}}$, $\mathbf{K_{s2}}$, $\mathbf{K_{s3}}$), keď prijatý pôvodný odtlačok CBC-MAC dát sa najprv dešifruje pomocou tretieho kľúča ($\mathbf{K_{s3}}$), a potom zašifruje pomocou druhého kľúča ($\mathbf{K_{s2}}$), pričom ak overovaný odtlačok je autentický a neporušený, potom výsledok týchto operácií sa zhoduje s odtlačkom správy vytvoreným pomocou prvého kľúča ($\mathbf{K_{s1}}$).

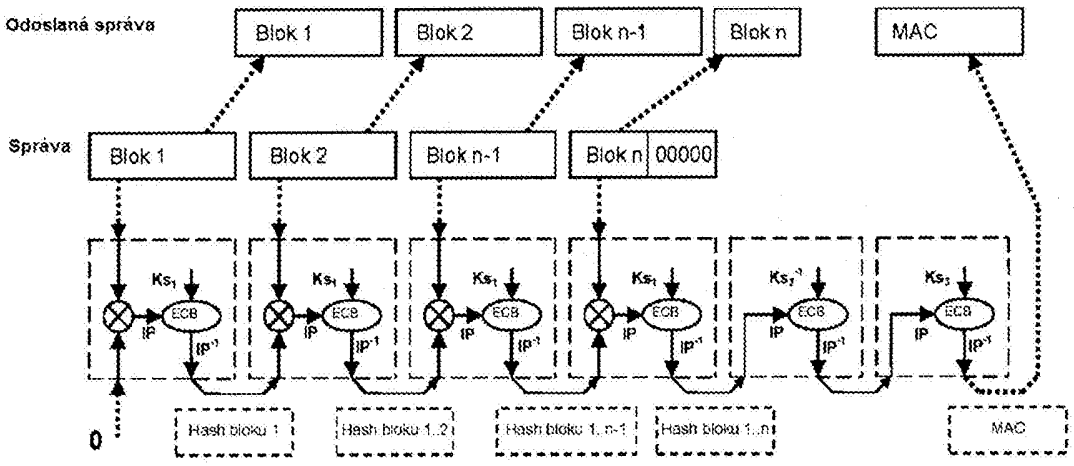
9. Spôsob podľa nároku 5, **v y z n a č u j ú c i s a t ý m ,** že v prípade použitia blokovej šifry AES sa pri overovaní pôvodného odtlačku CBC-MAC dát použije inverzný postup, keď prijatý pôvodný odtlačok CBC-MAC dát sa najprv dešifruje, a potom pomocou funkcie XOR s posledným blokom dát sa upraví na CBC-MAC len predchádzajúcich blokov dát, pričom sa spätne postupuje až k prvému bloku dát, keď sa pre autentickú a neporušenú správu výsledok výpočtu rovná inicializačnému vektoru.

10. Spôsob podľa niektorého z nárokov 1 až 9, **v y z n a č u j ú c i s a t ý m ,** že zabezpečovacím systémom, zahrnujúcim aspoň dve jednotky spoločne vytvárajúce odtlačky dát, je rádiobloková centrála na riadenie vlakov prostredníctvom rádiovej komunikácie.

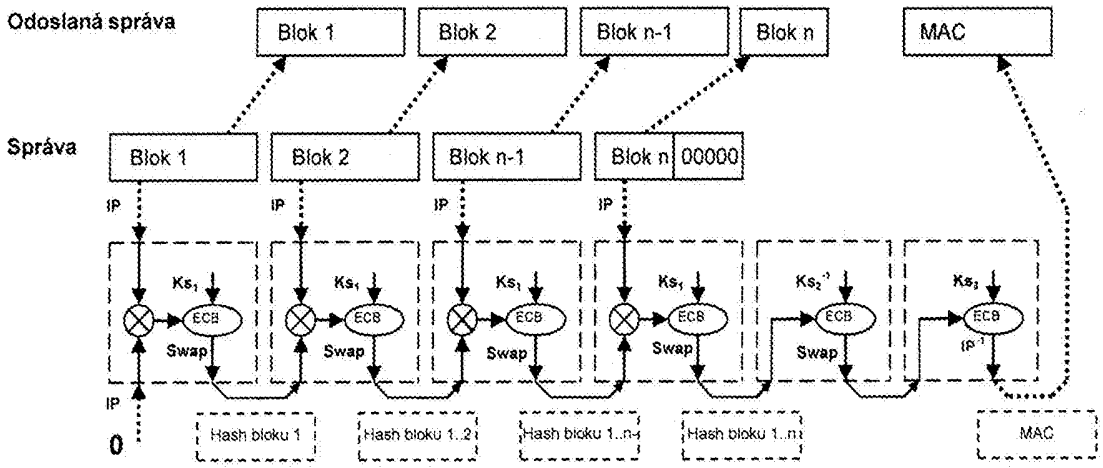
7 výkresov


Kódové slovo systematického blokového kódu
Dáta
Bezpečnostný kód
k
c

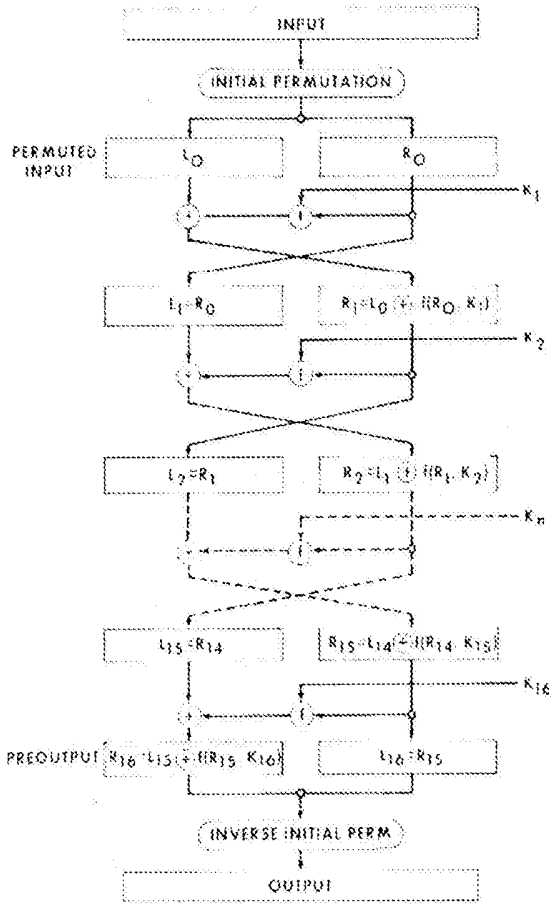
OBR. 1


Odoslaná správa
Blok 1
Blok 2
Blok n-1
Blok n
MAC
Správa
Blok 1
Blok 2
Blok n-1
Blok n
00000
ECB
IP
IP-1
0
Hash bloku 1
Hash bloku 1..2
Hash bloku 1..n-1
Hash bloku 1..n
MAC

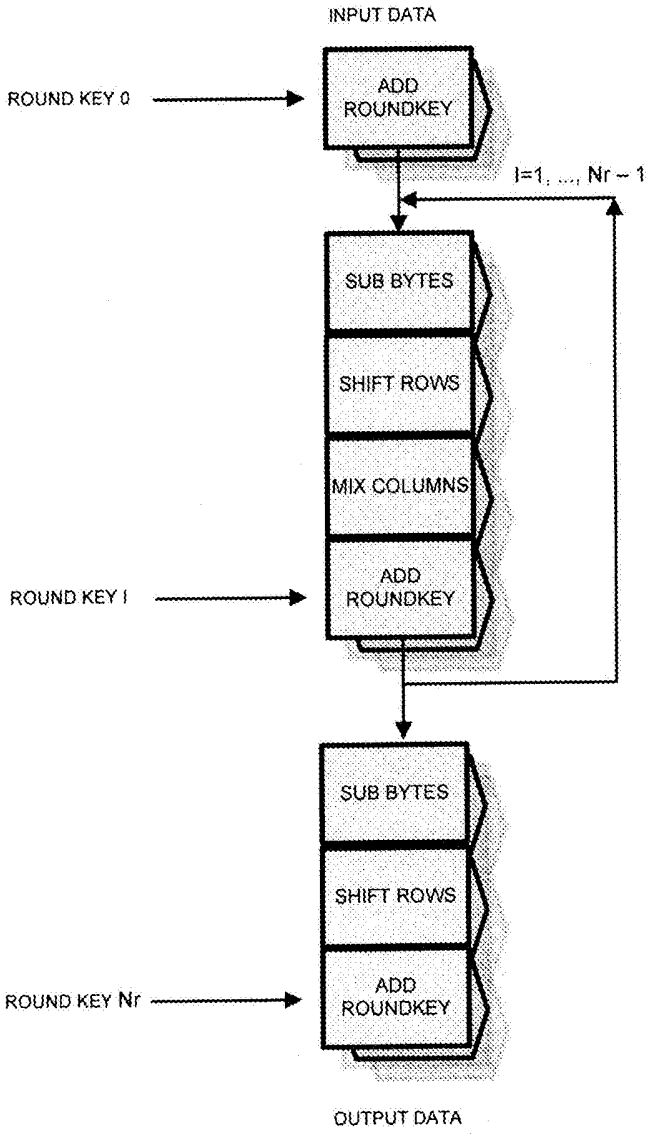
OBR. 2


Odoslaná správa
Blok 1
Blok 2
Blok n-1
Blok n
MAC
Správa
Blok 1
Blok 2
Blok n-1
Blok n 00000
IP
Ks1
ECB
Swap
Ks2-1
IP-1
0
Hash bloku 1
Hash bloku 1..2
Hash bloku 1..n-1
Hash bloku 1..n
MAC

OBR. 3

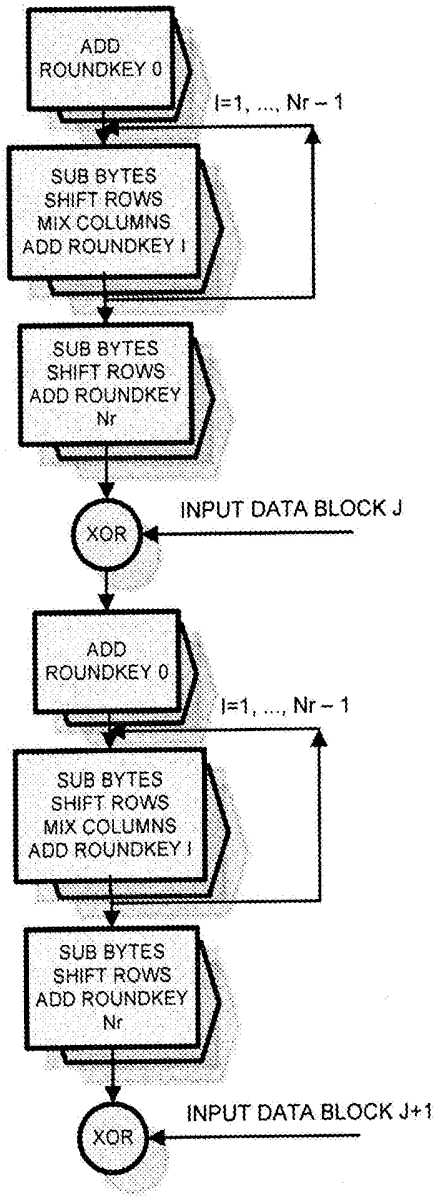

INPUT
INITIAL PERMUTATION
PERMUTED INPUT
L0
R0
K1
L1=R0
R1=L0 + f(R0, K1)
K2
L2=R1
R2=L1 + f(R1, K2)
Kn
L15=R14
R15=L14 + f(R14, K15)
K16
PREOUTPUT
R16=L15 + f(R15, K16)
L16=R15
INVERSE INITIAL PERM
OUTPUT

OBR. 4



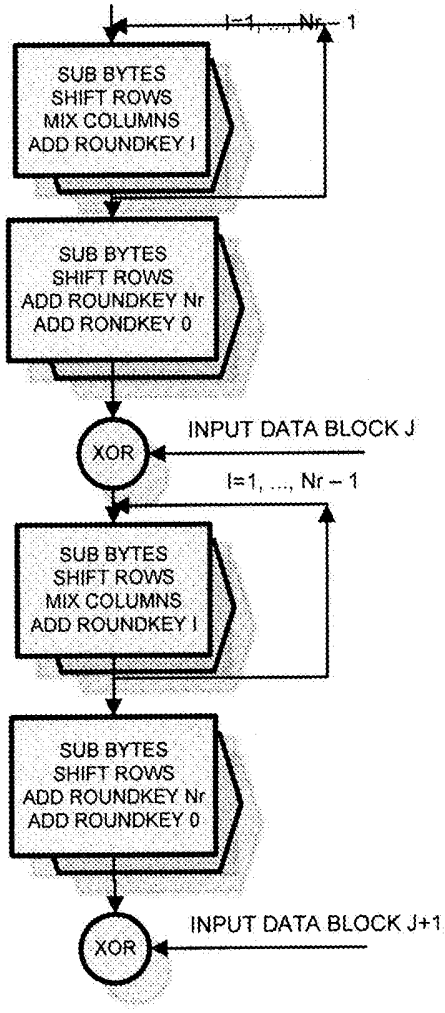
Štruktúra výpočtu blokovej šifry AES

OBR. 5



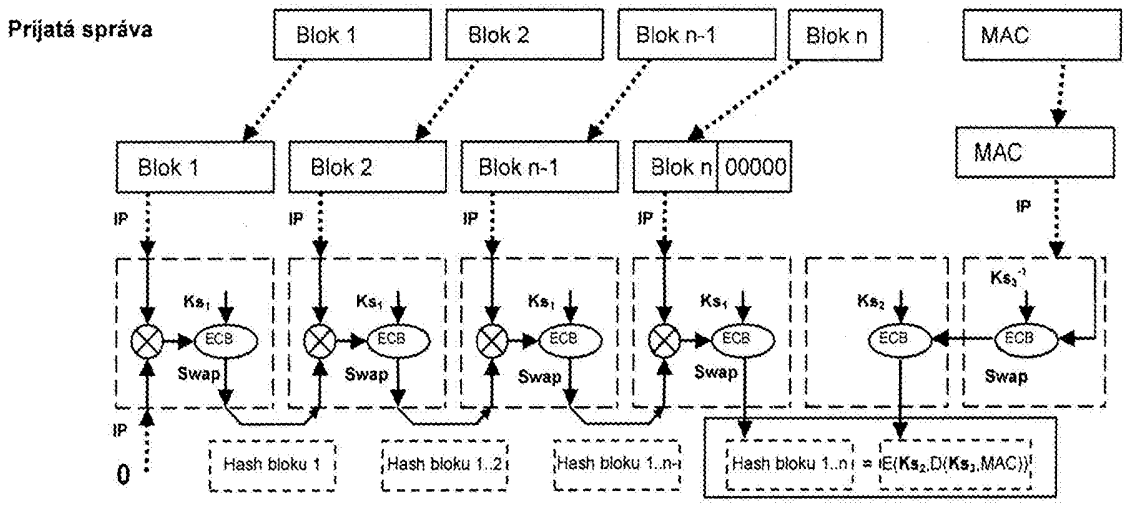
Štruktúra výpočtu CBC-MAC pomocou blokovej šifry AES

OBR. 6



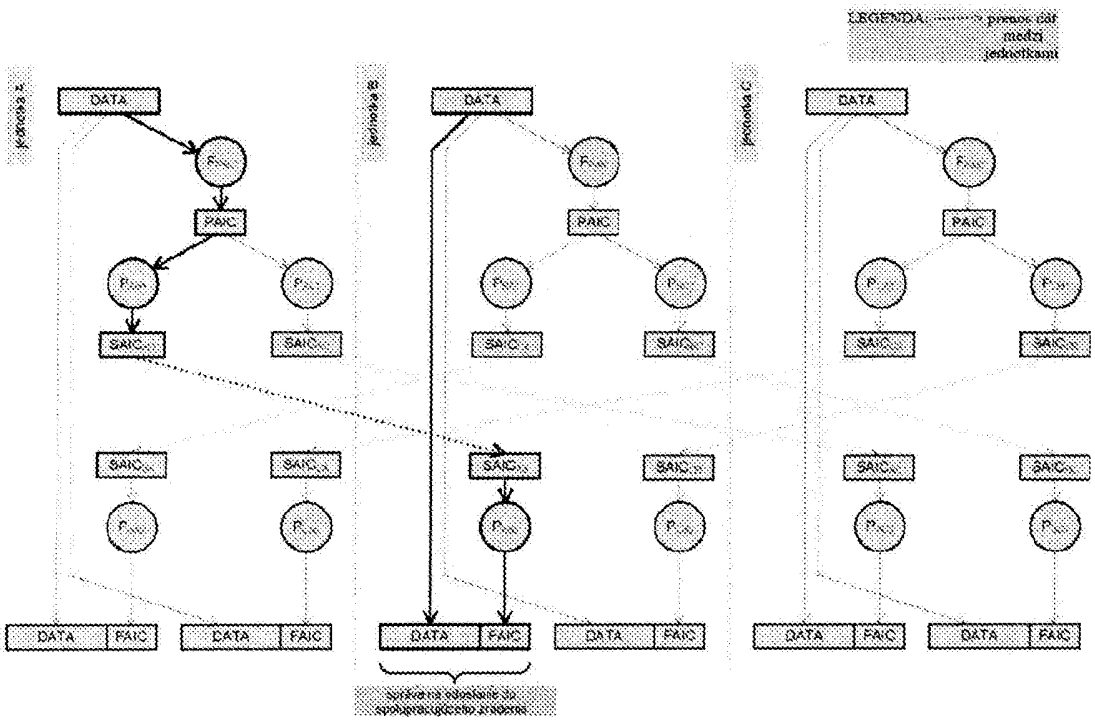
Nová štruktúra výpočtu pôvodného odtlačku dát CBC-MAC pomocou blokovej šifry AES

OBR. 7



Postup overenia pôvodného odtlačku CBC-MAC dát (DES)

OBR. 8



Vytvorenie odtlačku

OBR. 9

Koniec dokumentu