PATENTOVÝ SPIS

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2011-142**
(22) Přihlášeno: **17.03.2011**
(40) Zveřejněno: **23.05.2012**
(Věstník č. 21/2012)
(47) Uděleno: **12.04.2012**
(24) Oznámení o udělení ve Věstníku: **23.05.2012**
(Věstník č. 21/2012)

(11) Číslo dokumentu:
303 209
(13) Druh dokumentu: **B6**
(51) Int. Cl.:

G06F 21/00	(2006.01)
G06F 11/14	(2006.01)
B61L 1/20	(2006.01)
H04L 1/22	(2006.01)
H04L 9/28	(2006.01)

(56) Relevantní dokumenty:
DE 102007032805 A; WO 2010148528 A; WO 2006051355 A; EP 1197418 B; EP 0725511 B; WO 2007079700 A.
Štěpán Klapka: Úloha detekčních kódů v železniční zabezpečovací technice, České vysoké učení technické v Praze, Fakulta dopravní, 2009.

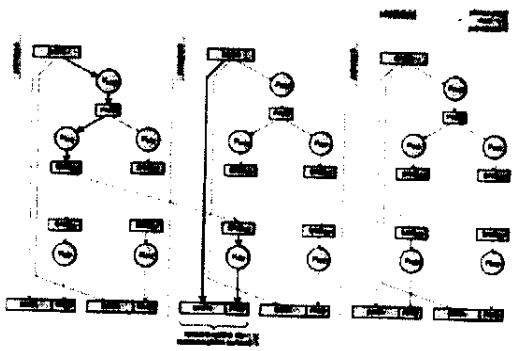
(73) Majitel patentu:
AŽD Praha s. r. o., Praha, CZ

(72) Původce:
Klapka Štěpán Doc. RNDr., Praha 10, CZ
Kárná Lucie Mgr., Praha 5, CZ
Súkup Jaroslav Ing., Praha 10, CZ
Harlenderová Magdaléna RNDr., Olomouc, CZ

(74) Zástupce:
Pavel Reichel a kol., Ing. Pavel Reichel, Lopatecká 14, Praha 4, 14700

(54) Název vynálezu:
Způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků

(57) Anotace:
Způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků, kde alespoň dvě jednotky společně vytvářejí otisky dat a přitom současně žádná z nich sama o sobě neumožňuje vytvoření takového datového otisku. Podstata řešení spočívá v tom, že postup vytvoření otisku dat se rozloží do posloupností vytváření dílčích otisků dat ve stanoveném časovém sledu, jejichž výsledkem je původní otisk dat, a v případě, kdy se zjistí porucha v některé ze spolupracujících jednotek, odmítne neporušená jednotka, která spolupracuje s porušenou jednotkou, vytvoření dílčího otisku dat.



CZ 303209 B6

Způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků

Oblast techniky

Předložený vynález se týká způsobu zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků.

Dosavadní stav techniky

Z celkového pohledu lze bezpečnost kritických aplikací na nejvyšší úrovni rozdělit na oblast technické a funkční bezpečnosti. Funkční bezpečnost se v železniční zabezpečovací technice především zabývá dopravně bezpečnostními algoritmy, které zajišťují omezení rizik vznikajících většinou mimo vlastní zabezpečovací zařízení, především v navazující železniční infrastruktuře jako jsou kolejové obvody, návěstidla, výhybky apod. Na druhé straně technická bezpečnost je zaměřena na rizika, která vznikají především vlivem poruchových stavů vlastního zabezpečovacího zařízení. Při návrhu zabezpečovacích zařízení je tedy z pohledu technické bezpečnosti nutné brát v úvahu vlivy poruchových stavů na vlastní bezpečnostní funkci zařízení. V případě uvažování vlivu ojedinělých poruchových stavů je pro systémy s vyššími požadavky na bezpečnost nutné zajistit, aby zůstaly bezpečné v případě jakéhokoli druhu ojedinělého náhodného poruchového stavu hardware, který je považován za možný. Tento princip je známý jako bezpečnost při poruše (Fail–Safe) a může ho být dosahováno několika různými způsoby, a to inherentní (vlastní) bezpečností při poruše, složenou bezpečností při poruše a reaktivní bezpečností při poruše. Podle principu inherentní bezpečnosti se při poruše dosahuje bezpečnosti tím, že žádné hodnověrné druhy poruch jednotky (zařízení) nejsou nebezpečné. Hodnověrnost poruch musí být garantována například fyzikálními vlastnostmi použitých součástek a jejich zapojením. V tomto případě je zvládnutí poruchy (detekce a negace) zajištěno především fyzikálními zákony.

Naproti tomu složená a reaktivní bezpečnost využívá detekce k dosažení bezpečnosti pro zabránění nebezpečí. V případě složené bezpečnosti je k detekci poruchových stavů použit hlasovací princip. V případě reaktivní bezpečnosti je rychlá a hodnověrná detekce zajištěna specializovanou jednotkou, která je k tomuto účelu navržena. Tato speciální jednotka však nevykonává přímo bezpečnostní funkci, ale jen dohlíží na správné vykonávání bezpečnostní funkce hlavní (funkční) jednotky. Jeli speciální jednotkou detekováno selhání bezpečnostní funkce hlavní jednotky, je speciální jednotkou zajištěno, že výstupy systému s vyššími požadavky na bezpečnost přejdou do bezpečného stavu. Při určitém zjednodušení se dá říci, že hlasovací princip ze složené bezpečnosti je u reaktivní bezpečnosti nahrazen kvalitou detekce speciální jednotky. Současná zabezpečovací zařízení pro vysoká rizika většinou využívají všech tří principů a u některých případů se dá velice obtížně rozhodnout, o který z uvedených principů se právě jedná.

V případě složené bezpečnosti při poruše vykonává bezpečnostní funkci (dopravně bezpečnostní algoritmy) více než jedna jednotka (zařízení), resp. část zařízení, ve spolupráci s ostatními jednotkami. V tomto případě nezávislé jednotky rozhodují většinově, hlasují o svých výstupech, svých funkcích. Tak například rozhodují dvě jednotky ze dvou, dvě ze tří, tři z pěti apod. Zabezpečovacím zařízením může být např. radiobloková centrála systému ETCS (European Train Control System), která v systému dvou jednotek ze tří (většinové rozhodování o výstupech jejich funkcí) vytváří povely pro vlaky, které jsou přenášeny pomocí GSM komunikace. Vzhledem k možnosti útoku v GSM přenosu musí být použito kryptografické ochrany pomocí blokové šifry DES (Data Encryption Standard). Pro techniku složené bezpečnosti se při poruše požaduje, aby nebezpečný poruchový stav v jedné jednotce byl detekován a zvládnut v době dostatečné k tomu, aby se zabránilo souhlasnému poruchovému stavu v druhé jednotce. Požaduje se, aby poruchový stav byl zvládnut dříve, než selže zvolený postup detekce (hlasování) vzhledem k další degradaci systému.

Jedním z důležitých postupů pro zajištění principu složené bezpečnosti při poruše je proces zvládnutí poruchy po její detekci. Obvykle se používá nevratné odpojení porušené jednotky z další funkce. Protože k odpojení jednotky se většinou odpojí napájecí napětí, vznikají při následném běžném startování systému určité komplikace. Další často používanou technikou je izolace porušené části, např. funkčním odpojením porušené jednotky bez potřeby odpojování hardware. Jednou možností pro implementaci tohoto způsobu je existence bezpečnostně relevantní informace, která je nezbytná pro vykonávání bezpečnostně relevantní činnosti, např. provádění zvolené komunikace mezi zabezpečovacími zařízeními. Jedním společným prvkem, kterým musí být vysílané z právy vybaveny, je bezpečnostní kód, což je ta část zprávy, která je přidána k přenášeným datům za účelem kontroly jejich integrity (neporušenosti) a autenticity (původnosti). Podle své konstrukce může být bezpečnostní kód kryptografický a nekryptografický. V patentovém dokumentu CZ 296129 je forma bezpečnostního kódu přizpůsobena potřebě složené bezpečnosti při poruše, ovšem toto řešení je omezeno pouze na některé cyklické kódy, nelze ho používat pro lineární nebo kryptografické kódy. Není proto použitelný pro přenosové systémy, kde nelze vyloučit útok na přenášené informace, to znamená zejména na změnu jejich obsahu nebo změnu autenticity. Pro výpočet kryptografického bezpečnostního kódu je sice možné použít postup uvedený v patentovém dokumentu DE 102007032805 A1, ale pouze ve stanovené kompozici, to znamená pro omezený počet bezpečnostních kódů, což omezuje jeho využití. Účelem předloženého vynálezu je postup, který je možné adaptovat na téměř libovolný typ bezpečnostního kódu, který je dále označován jako datový otisk.

Podstata vynálezu

Předmětem tohoto vynálezu je způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků, kde alespoň dvě jednotky společně vytvářejí otisky dat a přitom současně každá z nich sama o sobě neumožňuje vytvoření takového datového otisku. Podstata vynálezu spočívá v tom, že postup vytvoření otisku dat se rozloží do posloupností vytváření dílčích otisků dat ve stanoveném časovém sledu, jejichž výsledkem je původní otisk dat, a v případě, kdy se zjistí porucha v některé ze spolupracujících jednotek, odmítne neporušená jednotka, která spolupracuje s porušenou jednotkou, vytvoření dílčího otisku dat, čímž se znemožní vytvoření původního otisku dat. Původní otisk dat je tedy vytvořen pouze z posloupnosti jednotek, které nemají poruchu. Zabezpečovacím systémem, zahrnujícím výše uvedené jednotky, může být radiobloková centrála pro řízení vlaků prostřednictvím rádiové komunikace.

Otisky dat jsou výsledkem funkce, která z daných původních dat, vstupní informace, vytváří pomocí určité definované redukce reprezentativní datový vzorek k původním datům. Takovou funkci lze sestrojit například za použití cyklického kódu tak, že za otisk položíme zbytek po dělení vstupní informace generujícím polynomem cyklického kódu. Takový datový otisk pak slouží např. pro kontrolu neporušenosti dat nebo kontrolu jejich autenticity.

V případě lineárních kódů, kdy se k vytvoření otisku dat použije generující matice, se výsledný dílčí otisk dat vytváří tak, že je permutací původního otisku dat, přičemž inverzní permutace je rozložena na dílčí permutace a tím vzniknou dílčí transformace, které z výsledného dílčího otisku dat vytvoří původní otisk dat. Za tím účelem postačí provést pouze permutaci sloupců generující matice.

V případě použití blokové šifry, kterou se vytváří pomocí metody CBC (Cipher Block Chaining) původní otisk CBC–MAC dat, se modifikuje bloková šifra tak, že se výsledný dílčí otisk dat metody CBC odlišuje od původního otisku CBC–MAC dat a dalšími dílčími transformacemi výsledného dílčího otisku dat se vytvoří původní otisk CBC–MAC dat.

V případě použití blokové šifry DES (Data Encryption Standard) se vstupní permutací původního bloku dat, šifrovací částí a výstupní inverzní permutací zašifrovaného bloku dat, se tato výstupní inverzní permutace rozloží na dílčí permutace a tím vzniknou dílčí transformace, které z výsledného dílčího otisku dat vytvoří původní otisk dat.

V případě použití blokové šifry AES (Advanced Encryption Standard), která se provádí v blocích výpočtu (rounds), přičemž pro každý tento blok výpočtu se použije specifický klíč, se k zašifrovaným datům z původního bloku dat přidává v každém bloku výpočtu odlišný klíč, a klíč posledního bloku výpočtu se přidá ke klíči prvního bloku výpočtu následujícího kroku výpočtu metody CBC, čímž se zajistí odlišnost výsledného dílčího otisku dat od původního otisku dat, přičemž další dílčí transformací se výsledný otisk přemění do tvaru, kdy je permutací původního otisku a inverzní permutace se rozloží do dílčích permutací, které transformují dílčí otisk na původní otisk.

V případě použití lineárních kódů, kdy se k vytvoření otisku dat použije generující matice, se při ověřování otisku dat použije výsledný dílčí otisk, který se pro neporušenou autentickou zprávu rovná přijatému otisku, získanému spoluprací jednotek, na kterém je provedena permutace v inverzním pořadí. V případě použití systému ověřovacích polynomů, jejichž nejmenší společný násobek se rovná generujícímu polynomu cyklického bezpečnostního kódu, se tyto ověřovací polynomy použijí pro kontrolu neporušenosti a autenticity.

V případě použití blokové šifry DES se při ověřování původního otisku CBC–MAC dat použije inverzního postupu pomocí trojice navzájem odlišných klíčů K_{s1}, K_{s2}, K_{s3}, kdy přijatý původní otisk CBC–MAC dat se nejprve dešifruje pomocí třetího klíče K_{s3} a pak zašifruje pomocí druhého klíče K_{s2}, přičemž pokud ověřovaný otisk je autentický a neporušený, pak výsledek těchto operací se shoduje s otiskem zprávy vytvořeným pomocí prvního klíče K_{s1}.

V případě použití blokové šifry AES se při ověřování původního otisku CBC–MAC dat použije inverzního postupu, kdy přijatý původní otisk CBC–MAC dat se nejprve dešifruje a pak pomocí funkce XOR s posledním blokem dat se upraví na CBC–MAC pouze předcházejících bloků dat, přičemž se zpětně postupuje až k prvnímu bloku dat, kdy pro autentickou a neporušenou zprávu je výsledek výpočtu roven inicializačnímu vektoru.

Hlavní výhoda způsobu zachování bezpečného stavu při poruše zabezpečovacích systémů se složenou bezpečností při vytváření datových otisků podle tohoto vynálezu, oproti doposud známým řešením uvedeným v bodě dosavadního stavu techniky, spočívá v tom, že tento postup nevyžaduje specializované hardwarové prostředky pro komparaci nebo hlasování, které by jinak musely pracovat na principu inherentní bezpečnosti. Tento postup vede ke zjednodušení HW návrhu, snížení nákladů a nakonec ke zvýšení spolehlivosti zabezpečovacích systémů.

Přehled obrázků na výkresech

Na připojených výkresech jsou znázorněny příklady provedení předloženého vynálezu, následuje jeho podrobný popis s vysvětlením. Binární (n,k)–lineární blokový systematický kód se skládá z k informačních bitů (informační části) a $c = n–k$ kontrolních bitů (kontrolní části), které jsou ve výsledné zprávě organizovány podle schématu na Obr. 1.

V případě použití blokové šifry, kterou se vytváří pomocí metody CBC (Cipher Block Chaining) původní otisk CBC–MAC dat, se modifikuje bloková šifra tak, že se výsledný dílčí otisk dat metody CBC odlišuje od původního otisku CBC–MAC dat a dalšími dílčími transformacemi dílčího otisku dat se vytvoří původní otisk CBC–MAC dat. Původní postup výpočtu CBC–MAC pomocí blokové šifry DES je patrný ze schématu na Obr. 2. Technika výpočtu CBC–MAC je založena na tom, že inverze vstupní permutace IP pro blokovou šifru DES není známa v žádné jednotce, a tak k dosažení správného výsledku je nutná spolupráce mezi dvojicemi jednotek,

které potřebnou transformaci ve vzájemném spolupráci vytvoří, viz následující schéma na Obr. 3. Původní schéma výpočtu blokové šifry DES je zobrazeno na Obr. 4. Bloková šifra AES je obdobně jako DES vykonávána v rundách (round), viz Obr. 5 se strukturou výpočtu blokové šifry AES.

Podle délky klíče (128, 192 až 256 bitů) je vykonáván příslušný počet cyklů (Nr = 10, 12 a 14 rund). Před první, a pak po každé rundě je ke stavové informaci přidána příslušná část expandovaného klíče, za pomocí operace XOR. Protože výpočet CBC–MAC je rovněž založen na operaci XOR, je možné využít komutativnosti této operace a přeuspořádat výpočet CBC–MAC tak, že posledních 16B expandovaného klíče se již předem upraví pomocí funkce XOR s prvními 16B klíče. Změna ve výpočtu je schematicky naznačena následovně (původní na Obr. 6 a pak nová na Obr. 7).

V případě blokové šifry DES pro ověření původní otisku CBC–MAC dat při příjmu je možné využít i postup, který nepoužije jeho znovuvytvoření. Tento postup je založen na inverzním postupu při vytváření původního otisku CBC–MAC dat, pomocí trojice navzájem odlišných klíčů. Z přijatého telegramu je nutné pomocí třetího klíče K_{s3} dešifrovat (D) CBC–MAC, dále zašifrovat (E) pomocí druhého klíče K_{s2} a pak ověřit, že výsledek odpovídá otisku zprávy vytvořeného pomocí prvního klíče K_{s1} (viz Obr. 8). Na schématu na Obr. 9 je popsán systém vytvoření otisku validní zprávy pro kontrolu její integrity a autenticity, který vyžaduje spolupráci vždy dvou jednotek.

Příklady provedení vynálezu

Pod složenou bezpečností železničních zabezpečovacích systémů se rozumí princip, který umožňuje zachovat jejich bezpečnost v případech, kdy bezpečnostní funkci vykonává více než jedna jednotka ve spolupráci s dalšími nezávislými jednotkami. Například když nezávislé jednotky většinově rozhodují o výstupech svých funkcí, to znamená dvě ze tří jednotek, dvě ze dvou, tři z pěti apod.

Způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností na železnici při vytváření datových otisků bude v následujícím textu popsán pro případy lineárních kódů a blokové šifry DES (Data Encryption Standard) a AES (Advanced Encryption Standard), kterou se vytváří pomocí metody CBS (Cipher Block Chaining) původní otisk CBC–MAC dat a bloková šifra se modifikuje tak, že se výsledný dílčí otisk dat metody CBC odlišuje od původního otisku CBC–MAC dat a dalšími dílčími transformacemi výsledného dílčího otisku dat se vytvoří původní otisk CBC–MAC dat. Otisk dat je výsledkem funkce, která z daných původních dat vytvoří pomocí určité definované redukce reprezentativní datový vzorek k původním datům. Smyslem otisku dat je například kontrola neporušenosti dat nebo kontrola jejich autenticity.

Lineární kód je definován generující maticí, která popisuje transformaci původních dat na otisk dat. Jak již bylo uvedeno, otisky dat jsou výsledkem funkce, která z daných původních dat vytváří pomocí určité definované redukce reprezentativní vzorek dat k původním datům a slouží např. pro kontrolu neporušenosti dat. V následujících odstavcích je uvažován binární (n,k)–lineární blokový systematický kód, který se skládá z k informačních bitů (informační části) a $c = n–k$ kontrolních bitů (kontrolní části), které jsou ve výsledné zprávě organizovány podle schématu na Obr. 1.

Binární (n,k)–lineární (blokový) systematický kód je plně popsán generující binární maticí v následujícím tvaru. Každý řádkový vektor B_i o c bitech je příslušným příspěvkem do kontrolní části, pokud je bit i zprávy nenulový.

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

Pokud se na bity řádky B_i matice B provede potřebná permutace P, pak nová generující matice M již vytváří otisk, ve kterém jsou bity příslušně zpřeházeny. Výsledný dílčí otisk dat je tedy maticí M vytvářen tak, že je permutací původního otisku dat, která je určena maticí permutace P. Z hlediska teorie kódování jde v tomto případě o ekvivalentní lineární kód. Vlastní násobení generující maticí M systematického binárního kódu pak představuje použití operace XOR pro přidání vektorů B_i do kontrolní části. Z generující matice M je tedy pro výpočet potřebné uchovávat jen matici BP. Potřebné permutace P pro spolupráci jednotek jsou součástí informací v datové struktuře, která je označovaná jako restartovací značka. Způsoby práce s restartovací značkou (bezpečnostně relevantní informací) jsou podrobně popsány v patentovém dokumentu CZ 298373.

Protože všechny cyklické kódy jsou lineární, lze výše popsaný postup použít i pro všechny cyklické kódy, které jsou vytvořeny nad algebraickými tělesy charakteristiky dvě ($FG(2^m)$). Všechny tyto kódy lze totiž chápat jako binární lineární kódy. Do této skupiny cyklických kódů patří zatím všechny uvažované bezpečnostní kódy u zvažovaných aplikací zabezpečovacích zařízení na železnici.

V případě použití blokové šifry, kterou se vytváří pomocí metody CBC (Cipher Block Chaining) původní otisk CBC–MAC dat, se modifikuje bloková šifra tak, že se výsledný dílčí otisk dat metody CBC odlišuje od původního otisku CBC–MAC dat a dalšími dílčími transformacemi dílčího otisku dat se vytvoří původní otisk CBC–MAC dat. Původní postup výpočtu CBC–MAC pomocí blokové šifry DES je patrný ze schématu na Obr. 2.

Výpočet původního otisku CBC–MAC dat začíná úpravou prvního 64–bitového bloku dat s inicializačním vektorem pomocí operace XOR. Na výsledek je použita bloková šifra DES (Data Encryption Standard) s klíčem Ks_1, přičemž v rámci výpočtu DES je nejprve použita vstupní permutace a po použití vlastního šifrovacího postupu je použita permutace inverzní. K získanému výsledku je přidán, za pomocí operace XOR, další 64–bitový blok dat a dále se ve výpočtu postupuje obdobným způsobem. Pokud se permutace obsažená v algoritmu DES vytkne před operaci XOR, získáme tak postup, kde se ušetří v každém kroku výpočet jedné permutace (inverzní permutace). Inverzní permutace je použita jen jednou na konci výpočtu.

Následující technika výpočtu CBC–MAC je založena na tom, že inverze vstupní permutace IP pro blokovou šifru DES není známa v žádné jednotce, a tak k dosažení správného výsledku je nutná spolupráce mezi dvojicemi jednotek, které potřebnou transformaci ve vzájemné spolupráci vytvoří, viz následující schéma na Obr. 3. Původní schéma výpočtu blokové šifry DES je zobrazeno na Obr. 4.

Struktura výpočtu (šifrování a dešifrování) blokové šifry AES (Advanced Encryption Standard) má několik zásadních odlišností oproti blokové šifře DES. První odlišnost spočívá v tom, že šifrování a dešifrování jsou specializované nezáměnné procedury. Protože pro vytvoření CBC–MAC je nezbytná jen šifrovací procedura, lze se v dalším výkladu omezit pouze na modifikaci této procedury pro potřeby složené bezpečnosti při poruše. Další odlišnost mezi AES a DES spočívá v tom, že AES nepoužívá žádné vstupní a výstupní permutace. Za určitého úsilí lze permutace do procedury šifrování AES zabudovat, ale to přináší navýšení potřebného výpočetního výkonu. Proto je vhodnější modifikovat výpočet AES takovým způsobem, aby žádný mezivýsledek nebyl použitelným otiskem a potřebné permutace zabudovat až do finální procedury výpočtu.

Bloková šifra AES je obdobně jako DES vykonávána v rundách (round), viz Obr. 5 se strukturou výpočtu blokové šifry AES. Podle délky klíče (128, 192 a 256 bitů) je vykonáván příslušný počet cyklů (Nr = 10, 12 a 14 rund). Před první, a pak po každé rundě je stavová informace upravena pomocí funkce XOR s příslušnou částí expandovaného klíče. Protože výpočet CBC–MAC je rovněž založen na operaci XOR, je možné využít komutativnosti této operace a přeuspořádat výpočet CBC–MAC tak, že posledních 16B expandovaného klíče se již předem upraví pomocí operace XOR s prvními 16B klíče. Změna ve výpočtu je schematicky naznačena následovně (původní na Obr. 6 a pak nová na Obr. 7). Oproti původnímu výpočtu (schéma na Obr. 6) je vždy po poslední rundě zároveň aplikována jak poslední, tak první část expandovaného klíče. Díky tomu je výsledek na konci výpočtu modifikován prvními 16B klíče. Na tento výsledek se provedou potřebné permutace, a na takto získaný mezivýsledek se aplikuje část klíče, na které je provedena permutace. Tím se získá potřebný výsledný dílčí otisk, který již bude dokončen stejným způsobem jako v ostatních případech při spolupráci určených jednotek.

Postup výpočtu naznačený na schématu „nová struktura výpočtu" (Obr. 7) se dá dále urychlit tím, že při expanzi klíče se ke klíči pro poslední rundu přidá, za pomocí operace XOR, první klíč. Vzhledem k této úpravě je od výpočtu druhého bloku dále ušetřena jedna aplikace klíče před první rundou. Celý výpočet CBC–MAC se tedy rozpadne na tři části. V počáteční části je před první rundou aplikována první část expandovaného klíče (to je prvních 16B tajného klíče), a pak po každé rundě další příslušná část.

V opakovaném výpočtu již není používána první část expandovaného klíče a jsou vždy aplikovány jen ostatní části po každé rundě. V závěrečné úpravě je na výsledek aplikována permutace a je modifikován první částí expandovaného klíče, na které byla také provedena permutace.

Základní princip technické bezpečnosti při ověřování otisků dat je založen na tom, že při postupu ověřování nevzniká správný otisk dat. Postupy kontroly, který by využíval opětovné vytvoření otisku, je tedy nepřípustný. Takový postup kontroly je jednoduše zneužitelný pro to, aby příjemce a ověřovatel správnosti otisku takové otisky případně vlivem poruchy vytvářel sám.

Pro acyklické lineární kódy je možné postupovat tak, že pomocí výše uvedené matice M je nejprve vytvořen otisk, na kterém je aplikována permutace, a následně je porovnáván s došlým otiskem, na který je aplikována inverzní permutace, vytvořená ve spolupráci potřebného počtu jednotek. Tento postup je nutné použít i u cyklických kódů, pokud příslušný generující polynom nelze rozdělit na použitelný systém faktorů. Tento typ lineárních bezpečnostních kódů nebyl doposud pro žádnou aplikaci požadován.

Pokud existuje systém polynomů (ověřovacích polynomů), jejichž nejmenší společný násobek je roven generujícímu polynomu cyklického bezpečnostního kódu, pak lze nahradit postup ověření otisku generujícím polynomem kontrolou pomocí ověřovacích polynomů. Tento postup je podrobně popsán v patentovém dokumentu CZ 296129.

Pro ověření původního otisku CBC–MAC dat s použitím blokové šifry DES při příjmu je možné využít i postup, který nepoužije jeho znovuvytvoření (což je obecně doporučovaná technika). Tento postup je založen na inverzním postupu při vytváření původního otisku CBC–MAC dat, pomocí trojice navzájem odlišných klíčů. Z přijatého telegramu je nutné pomocí třetího klíče K_{s3} dešifrovat (D) CBC–MAC, dále zašifrovat (E) pomocí druhého klíče K_{s2} a pak ověřit, že výsledek odpovídá otisku zprávy vytvořeného pomocí prvního klíče K_{s1} (viz Obr. 8).

Tento postup kontroly má obdobnou výhodu, jako postup uvedený v předešlém odstavci. K ověření integrity a autenticity došlé zprávy není nutná spolupráce jednotek, která je nezbytná pro její vytvoření.

Pro ověření původního otisku CBC–MAC dat s použitím blokové šifry AES při příjmu, je možné využít obdobný postup, který je uveden v předcházejícím odstavci. Je nutné z přijatého telegramu pomocí tajného klíče dešifrovat blok s původním otiskem CBC–MAC dat a pak dále pokračovat v inverzním postupu (za pomocí operace XOR vždy s posledním blokem dat, ...), až bude zrekonstruován inicializační vektor, kterým začínal vlastní výpočet původního otisku CBC–MAC dat. Pokud dostaneme dohodnutou hodnotu, je obdržená zpráva integritní a autentická. Vzhledem k tomu, že proceduru dešifrování blokové šifry AES je možné použít bez omezení v jedné jednotce, je tento postup kontroly proveditelný bez spolupráce více jednotek.

Ke kontrole lze využít i nedokončený proces konstrukce původního otisku CBC–MAC na datech přijaté zprávy. Pokud se výsledek před závěrečnou úpravou konstrukce původního otisku CBC–MAC dat upraví pomocí operace XOR s přijatým původním otiskem CBC–MAC dat, pak pro neporušenou autentickou zprávu je zapotřebí dostat prvních 16B použitého tajného klíče.

Na schématu na Obr. 9 je popsán systém vytvoření otisku validní zprávy pro kontrolu její integrity a autenticity, který vyžaduje spolupráci vždy právě dvou jednotek. (Poznámka: Pro to, aby mohla daná jednotka vytvořit otisk, potřebuje spolupráci alespoň jedné další jednotky daného zařízení. Záměr tohoto faktu bude zřejmý z níže uvedeného).

V systému „dva ze tří" se na vytváření otisku podílejí tři jednotky A, B, C, přičemž žádná z nich nezná kompletní postup jeho vytvoření a otisk vzniká vynucenou spoluprací vždy dvou jednotek. Postup tedy probíhá až v šesti různých posloupnostech. Z dat vytvářené zprávy u (na obrázku označeno jako pole DATA) je vytvořen otisk F(u) následujícím postupem, znázorněným na obrázku

1. Každá ze tří jednotek A, B, C vytvoří z dat pomocí funkce F_{PAIC} výsledný dílčí otisk pro kontrolu integrity, který se označuje PAIC (Primary Authorization Integrity Check). Funkce F_{PAIC} vytváří výsledný dílčí otisk dat, na který je aplikována permutace P_{PAIC} tak, že s daty nevytváří validní zprávu; tj. je to složené zobrazení $F_{PAIC} = P_{PAIC} \circ F$. Funkce F_{PAIC} je ve všech třech jednotkách stejná a musí být implementována tak, aby bylo možné jejím neúplným provedením vytvořit platný otisk dat $F(u)$. Nelze tedy nejprve provést funkci F a potom permutaci P_{PAIC}; složená funkce F_{PAIC} musí být pro jednotku nerozložitelná.
2. Jednotka A provede zpracování pole dat PAIC funkcí P_{AB1} a tím vytvoření sekundární autorizační otisk $SAIC_{AB}$ (Secondary Authorization Integrity Check), což je dílčí transformace výsledného dílčího otisku – tato funkce provede permutaci bitů pole PAIC, která je v rámci systému jedinečná; schopností vykonat danou permutaci disponuje pouze jednotka A a lze ji použít pouze pro spolupráci s jednotkou B. Zároveň vytvoří pomocí permutace P_{AC1} druhý sekundární autorizační otisk $SAIC_{AC}$, určený pro spolupráci s jednotkou C.
3. Současně vytvoří jednotka B z pole PAIC pomocí permutací P_{BA1} a P_{BC1} sekundární autorizační otisky $SAIC_{BA}$ a $SAIC_{BC}$, určené pro spolupráci s jednotkami A a C.
4. Současně vytvoří jednotka C z pole PAIC pomocí permutací P_{CA1} a P_{CB1} sekundární autorizační otisky $SAIC_{CA}$ a $SAIC_{CB}$, určené pro spolupráci s jednotkami A a B.
5. Každá z permutací P_{XY1} (kde X a Y mohou nabývat hodnot A, B a C) je v rámci systému jedinečná; zná ji pouze jednotka X a lze ji použít pouze pro spolupráci s jednotkou Y.
6. Následuje výměna sekundárních otisků (dílčích transformací výsledného dílčího otisku) mezi jednotkami: jednotka A vyšle otisk $SAIC_{AB}$ jednotce B a otisk $SAIC_{AC}$ jednotce C; jednotka B vyšle otisk $SAIC_{BA}$ jednotce A a otisk $SAIC_{BC}$ jednotce C a konečně jednotka C vyšle otisk $SAIC_{CA}$ jednotce A otisk $SAIC_{CB}$ jednotce B (viz obrázek).
7. Jednotka A zpracuje sekundární autorizační otisk $SAIC_{BA}$ (který dostala od jednotky B) permutací P_{BA2}, čímž vznikne finální autorizační otisk $FAIC_{BA}$. Zároveň aplikuje na autorizační otisk $SAIC_{CA}$ (který dostala od jednotky C) permutací P_{CA2}, čímž vznikne finální autorizační otisk $FAIC_{CA}$.

8. Současně jednotka B vytvoří ze sekundárního autorizačního otisku $SAIC_{AB}$ (který dostala od jednotky A) pomocí permutace P_{AB2} finální autorizační otisk $FAIC_{AB}$ a z autorizačního otisku $SAIC_{CB}$ (který dostala od jednotky C) permutaci P_{CB2} finální autorizační otisk $FAIC_{CB}$.

9. Konečně jednotka C vytvoří ze sekundárního autorizačního otisku $SAIC_{AC}$ (který dostala od jednotky A) pomocí permutace P_{AC2} finální autorizační otisk $FAIC_{AC}$ a z autorizačního otisku $SAIC_{BC}$ (který dostala od jednotky C) permutací P_{BC2} finální autorizační otisk $FAIC_{BC}$.

10. Každá z permutací P_{XY2} (kde X a Y mohou nabývat hodnot A, B a C) je opět v rámci systému jedinečná; zná ji pouze jednotka Y a lze ji použít pouze pro zpracování sekundárního otisku vytvořeného jednotkou X.

11. Permutace P_{XY1} a P_{XY2} (X a Y mohou nabývat hodnot A, B a C) jsou zvoleny tak, aby složením permutací P_{XY1} a P_{XY2} vznikla pro každou dvojici X, Y stejná permutace, a to permutace P_{PAIC}^{-1} inverzní k permutaci P_{PAIC} (tj. $P_{AB1} \circ P_{AB2} = P_{AC1} \circ P_{AC2} = \ldots = P_{CB1} \circ P_{CB2} = P_{PAIC}^{-1}$). Díky tomu jsou při bezchybné funkci všech jednotek všechny finální otisky $FAIC_{XY}$ stejné. (Platí totiž například $FAIC_{AB} = P_{AB2}(P_{AB1}(F_{PAIC}(u))) = P_{PAIC}^{-1}(P_{PAIC}(F(u)) = F(u)$.

Před samotným zahájením výpočtu otisku je provedena kontrola vzájemné shody pole dat DATA mezi jednotkami. Rovněž tak před přidáním pole DATA k otisku FAIC je jednotkou ověřeno, zda otisk FAIC odpovídá datům, která zabezpečuje.

Průmyslová využitelnost

Vynález je využitelný pro zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků.

PATENTOVÉ NÁROKY

1. Způsob zachování bezpečného stavu zabezpečovacích systémů se složenou bezpečností, zejména na železnici, při vytváření datových otisků, kde alespoň dvě jednotky společně vytvářejí otisky dat a přitom současně žádná z nich sama o sobě neumožňuje vytvoření takového datového otisku, **vyznačující se tím**, že postup vytvoření otisku dat se rozloží do posloupností vytváření dílčích otisků dat ve stanoveném časovém sledu, jejichž výsledkem je původní otisk dat, a v případě, kdy se zjistí porucha v některé ze spolupracujících jednotek, odmítne neporušená jednotka, která spolupracuje s porušenou jednotkou, vytvoření dílčího otisku dat, čímž se znemožní vytvoření původního otisku dat.

2. Způsob podle nároku 1, **vyznačující se tím**, že v případě lineárních kódů, kdy se k vytvoření otisku dat použije generující matice, se výsledný dílčí otisk dat vytváří tak, že je permutací původního otisku dat, přičemž inverzní permutace je rozložena na dílčí permutace a tím vzniknou dílčí transformace, které z výsledného dílčího otisku dat vytvoří původní otisk dat.

3. Způsob podle nároku 1, **vyznačující se tím**, že v případě použití blokové šifry, kterou se vytváří pomocí metody CBC (Cipher Block Chaining) původní otisk CBC–MAC dat, se modifikuje bloková šifra tak, že se výsledný dílčí otisk dat metody CBC odlišuje od původního otisku CBC–MAC dat a dalšími dílčími transformacemi výsledného dílčího otisku dat se vytvoří původní otisk CBC–MAC dat.

4. Způsob podle nároku 3, **vyznačující se tím**, že v případě použití blokové šifry DES (Data Encryption Standard) se vstupní permutací IP původního bloku dat, šifrovací částí a

výstupní inverzní permutací zašifrovaného bloku dat, se tato výstupní inverzní permutace rozloží na dílčí permutace a tím vzniknou dílčí transformace, kterými se z výsledného dílčího otisku dat vytvoří původní otisk dat.

5. Způsob podle nároku 3, **vyznačující se tím**, že v případě použití blokové šifry AES (Advanced Encryption Standard), která se provádí v blocích výpočtu (rounds), přičemž pro každý tento blok výpočtu se použije specifický klíč, se k zašifrovaným datům z původního bloku dat přidává v každém bloku výpočtu odlišný klíč, a klíč posledního bloku výpočtu se přidá ke klíči prvního bloku výpočtu následujícího kroku výpočtu metody CBC, čímž se zajistí odlišnost výsledného dílčího otisku dat od původního otisku dat, přičemž další dílčí transformací se výsledný otisk přemění do tvaru, který je permutací původního otisku a inverzní permutace se rozloží do dílčích permutací, které transformují dílčí otisk na původní otisk.

6. Způsob podle nároku 2, **vyznačující se tím**, že v případě použití lineárních kódů, kdy se k vytvoření otisku dat použije generující matice, se při ověřování otisku dat použije výsledný dílčí otisk, který se pro neporušenou autentickou zprávu rovná přijatému otisku, získanému spoluprací jednotek podle nároku 1, na kterém je provedena permutace v inverzním pořadí.

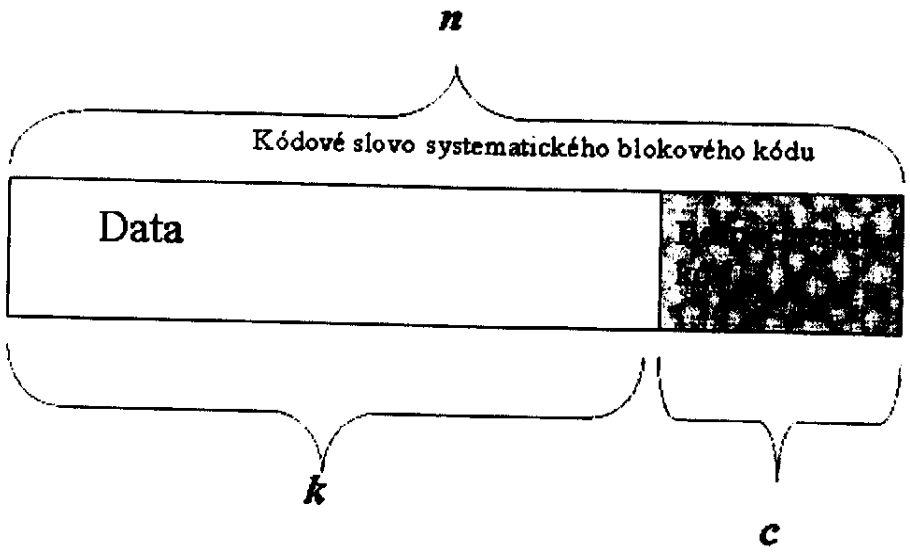
7. Způsob podle nároku 2, **vyznačující se tím**, že v případě použití systému ověřovacích polynomů, jejichž nejmenší společný násobek se rovná generujícímu polynomu cyklického bezpečnostního kódu, se tyto ověřovací polynomy použijí pro kontrolu neporušenosti a autenticity.

8. Způsob podle nároku 4, **vyznačující se tím**, že v případě použití blokové šifry DES se při ověřování původního otisku CBC–MAC dat použije inverzního postupu pomocí trojice navzájem odlišných klíčů (K_{s1}, K_{s2}, K_{s3}), kdy přijatý původní otisk CBC–MAC dat se nejprve dešifruje pomocí třetího klíče (K_{s3}) a pak zašifruje pomocí druhého klíče (K_{s2}), přičemž pokud ověřovaný otisk je autentický a neporušený, pak výsledek těchto operací se shoduje s otiskem zprávy vytvořeným pomocí prvního klíče (K_{s1}).

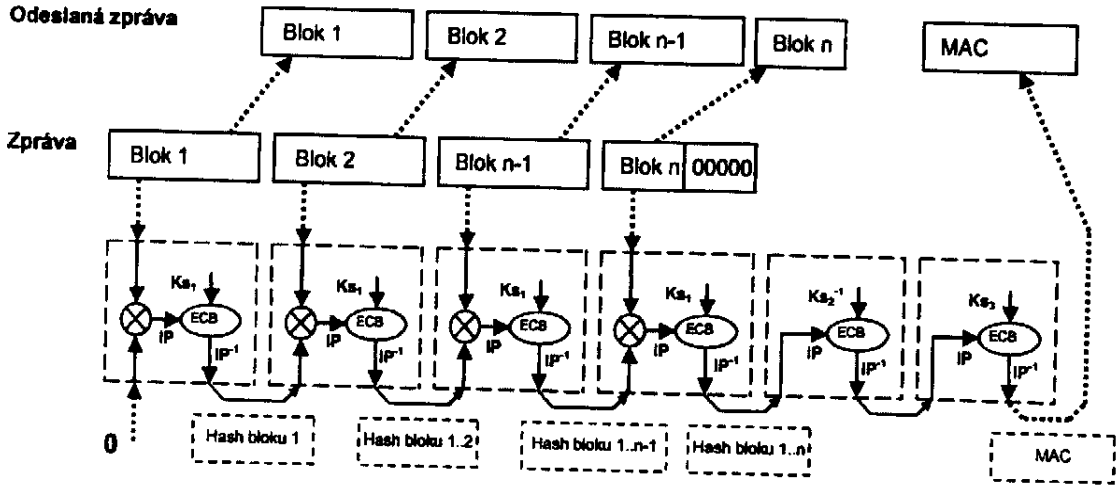
9. Způsob podle nároku 5, **vyznačující se tím**, že v případě použití blokové šifry AES se při ověřování původního otisku CBC–MAC dat použije inverzního postupu, kdy přijatý původní otisk CBC–MAC dat se nejprve dešifruje a pak pomocí funkce XOR s posledním blokem dat se upraví na CBC–MAC pouze předcházejících bloků dat, přičemž se zpětně postupuje až k prvnímu bloku dat, kdy pro autentickou a neporušenou zprávu je výsledek výpočtu roven inicializačnímu vektoru.

10. Způsob podle některého z nároků 1 až 9, **vyznačující se tím**, že zabezpečovacím systémem, zahrnujícím jednotky podle nároku 1, je radiobloková centrála pro řízení vlaků prostřednictvím rádiové komunikace.

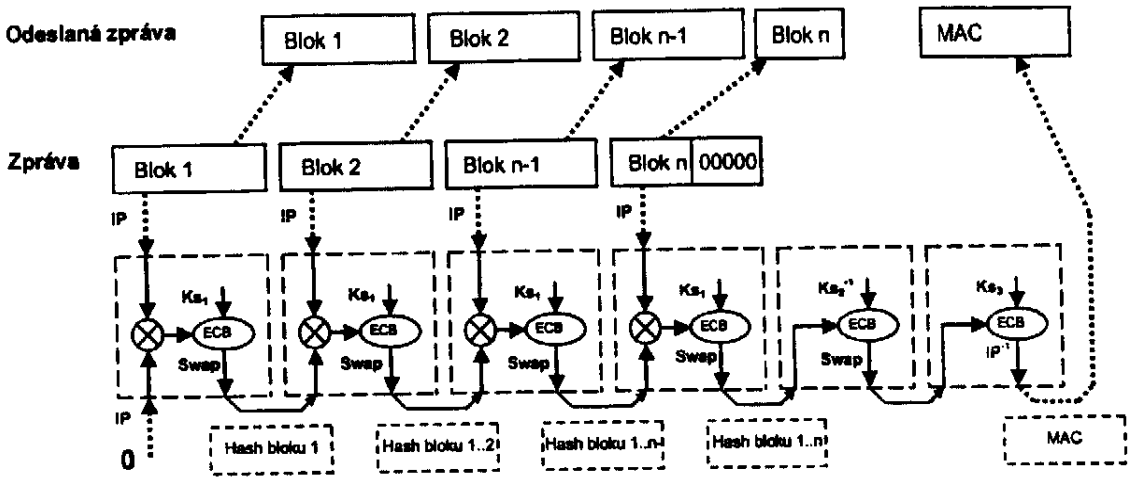
7 výkresů


n
Kódové slovo systematického blokového kódu
Data
k
c

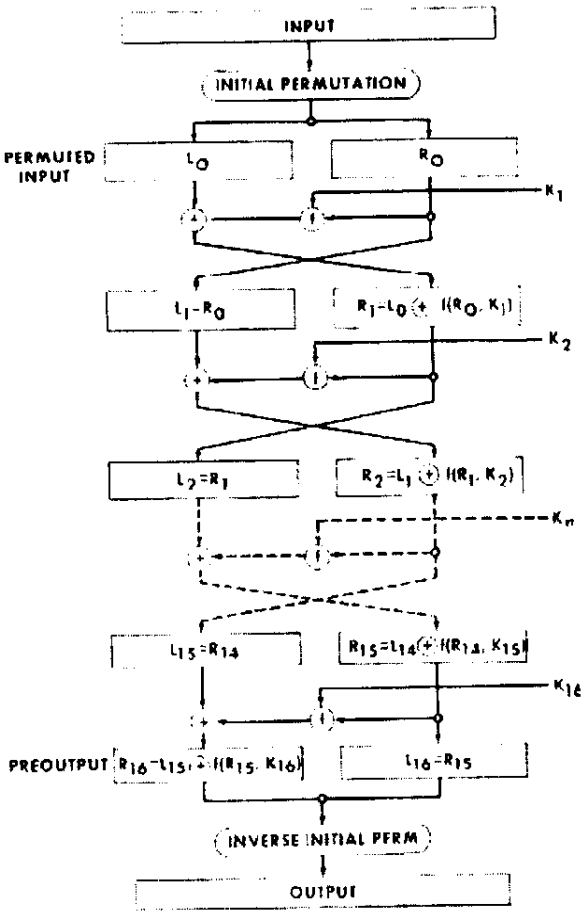
OBR.1


Odesílaná zpráva
Blok 1
Blok 2
Blok n-1
Blok n
MAC
Zpráva
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

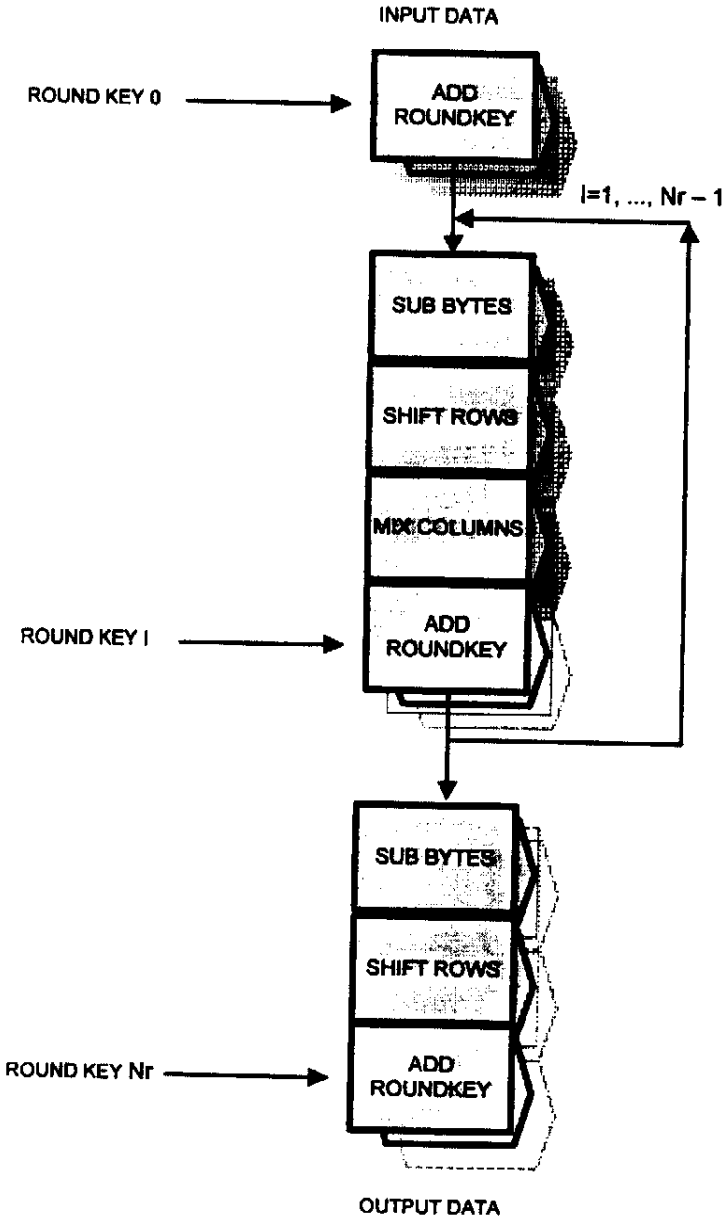
OBR.2


Odeslaná zpráva
Blok 1
Blok 2
Blok n-1
Blok n
MAC
Zpráva
Blok 1
Blok 2
Blok n-1
Blok n 00000
IP
ECB
Swap
IP-1
0
Hash bloku 1
Hash bloku 1..2
Hash bloku 1..n-1
Hash bloku 1..n
MAC

OBR.3

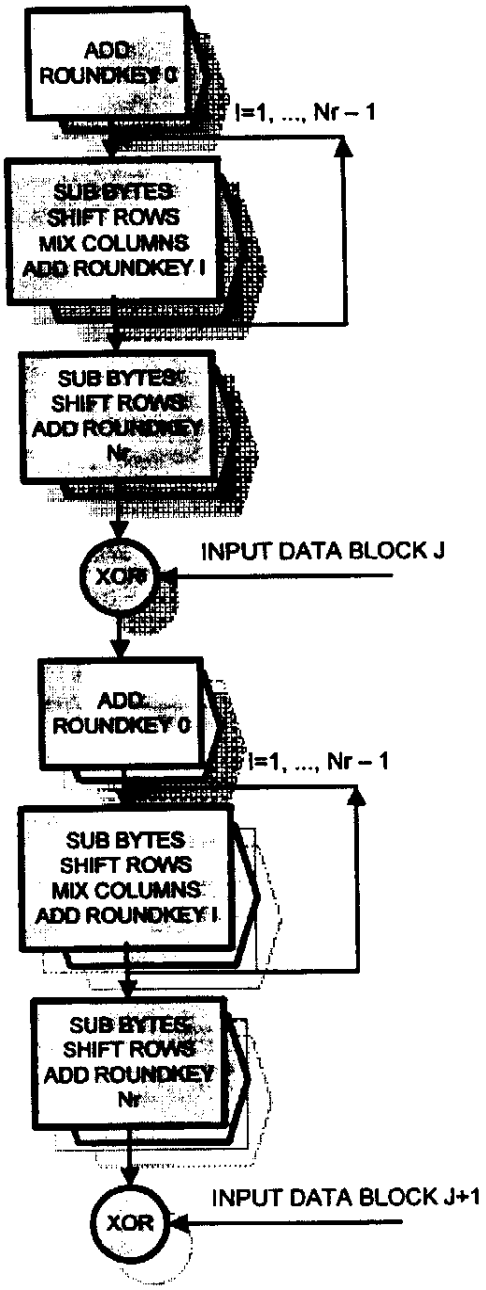

INPUT
INITIAL PERMUTATION
PERMUTED INPUT
PREOUTPUT
INVERSE INITIAL PERM
OUTPUT

OBR.4



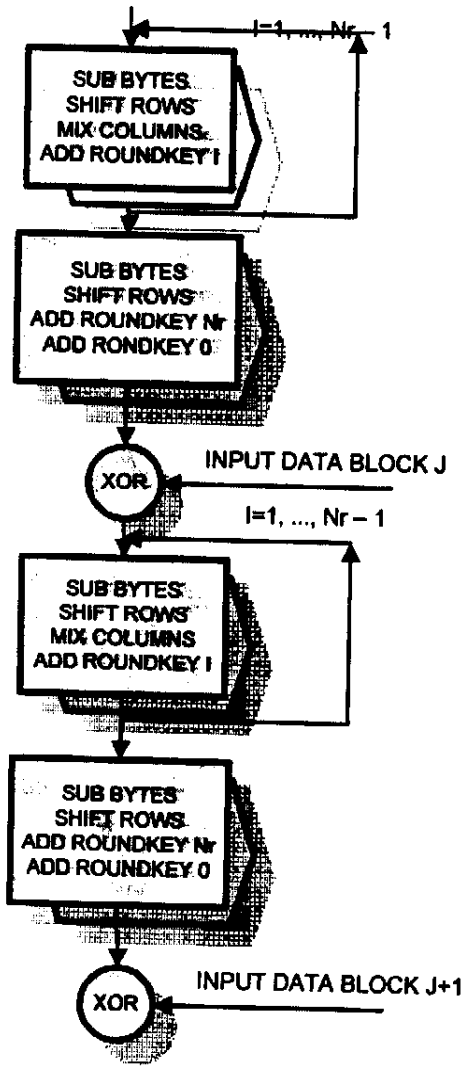
Struktura výpočtu blokové šifry AES

OBR.5



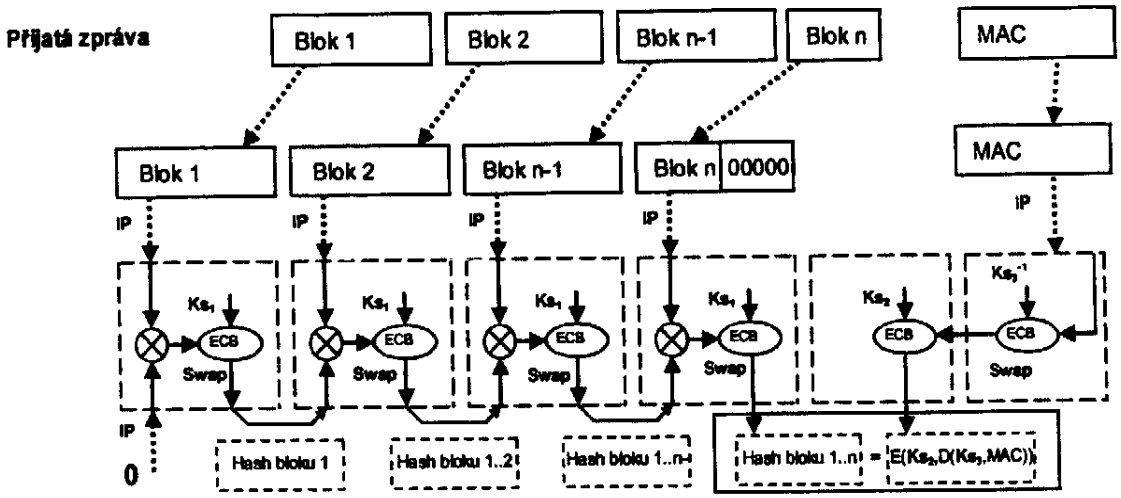
Struktura výpočtu CBC-MAC pomocí blokové šifry AES

OBR.6



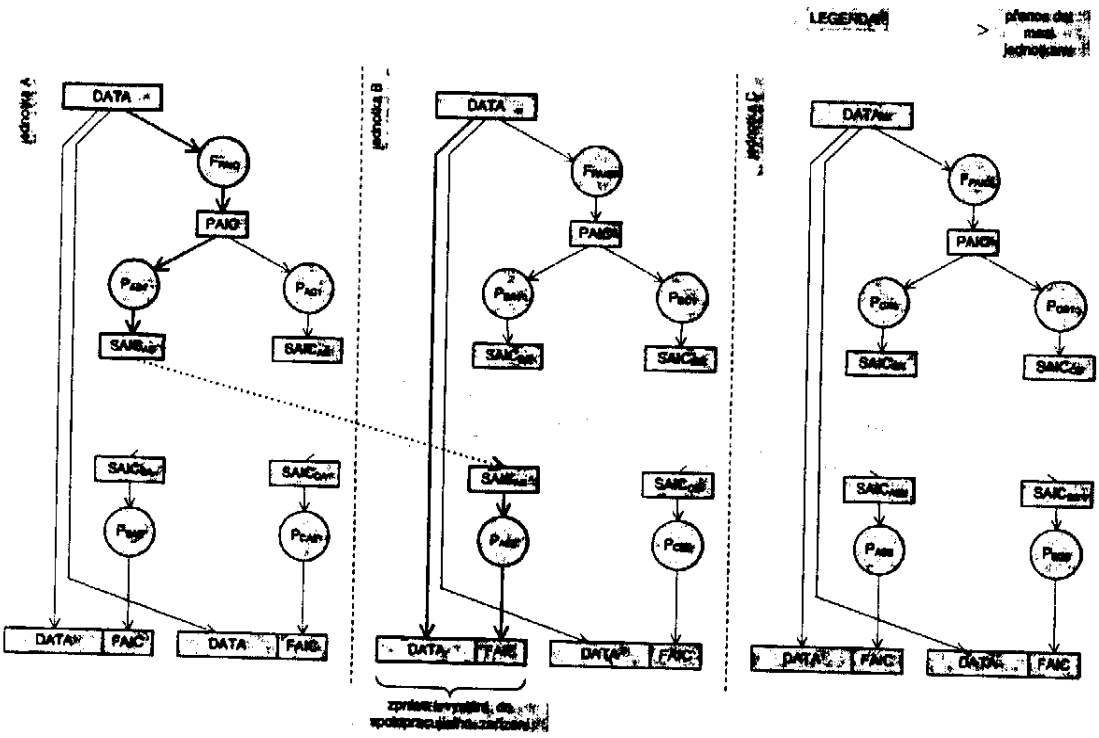
Nová struktura výpočtu původního otisku dat CBC-MAC pomocí blokové šifry AES

OBR.7



Postup ověření původního otisku CBC-MAC dat (DES)

OBR.8



Vytvoření otisku

OBR.9

Konec dokumentu