(19) REPUBLIKA SLOVENIJA
Urad RS za intelektualno lastnino

(10) SI 20349 A

(12) PATENT

(21) Številka prijave: 9820084

(51) MPK[6]: H04L 9/00

(22) Datum prijave: 19.06.1998

(45) Datum objave: 28.02.2001

(30) Prednostna pravica:
19.01.1998 RU 98 100 685

(86) Mednarodna patentna prijava:
19.06.1998 WO PCT/RU98/00182

(87) Objava mednarodne patentne prijave:
WO 99/36942, 22.07.1999

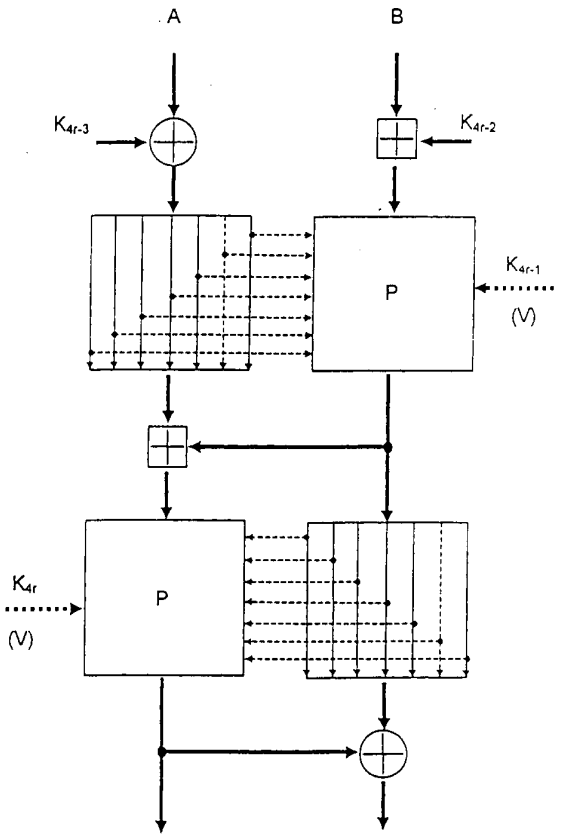
(72) Izumitelja: MOLDOVYAN Alexandr Andreevich, 188710, g. Vsevolozhsk, RU;
MOLDOVYAN Nikolai Andreevich, 188710, g. Vsevolozhsk, RU

(73) Nosilci: Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set",
Degtyarny pereulok, d. 6, stroenie 2, Moscow, GSP 103804, RU ;
MOLDOVYAN Alexandr Andreevich,
188710, g. Vsevolozhsk, ul Alexandrovskaja, d.88/2, kv.62, RU ;
MOLDOVYAN Nikolai Andreevich,
188710, g. Vsevolozhsk, Ul Alexandrovskaja, d.88/2, kv.62, RU

(74) Zastopnik: Dušan Borštar, univ.dipl.inž.str., Nova ulica 11, 1230 Domžale, SI

(54) POSTOPEK KRIPTOGRAFSKE PRETVORBE BINARNIH PODATKOVNIH BLOKOV

(57) Izum spada na področje električnih komunikacij in računalniških tehnik in se natančneje nanaša na kriptografske naprave in postopke za šifrirano zapisovanje digitalnih podatkov. Postopek obsega delitev podatkovnih blokov na N>=2 podblokov ter postopno konverzijo omenjenih podblokov s pomočjo vsaj ene operacije konverzije na i-tem podbloku, pri čemer je i=<N, omenjena operacija pa je odvisna od vrednosti j-tega podbloka, kjer je j=<N. Postopek je značilen po tem, da je operacija, ki je odvisna od vrednosti j-tega podbloka, operacija transpozicije bitov v i-ti podblok. Postopek je značilen tudi po tem, da se operacijo transpozicije bitov v i-tem podbloku, ki je odvisna od vrednosti j-tega podbloka, izvaja v skladu s tajnim ključem pred pričetkom konverzije i- tega podbloka. Še nadalje je postopek značilen po tem, da se operacijo transpozicije bitov v i-tem podbloku, ki je odvisna od vrednosti j-tega podbloka, izvaja v skladu s tajnim ključem pred pričetkom konverzije i-tega podbloka. Še nadalje je postopek značilen po tem, da je pred vsakokratno operacijo transpozicije bitov v i-ti podblok določen binarni vektor V, ki je odvisen od j-tega podbloka, pri čemer se omenjeno operacijo transpozicije bitov v i-tem podbloku izvaja v odvisnosti od vrednosti vektorja V. Binarni vector V je določen glede na njegovo vrednost med izvajanjem poprejšnjega koraka konverzije enega od podblokov kot tudi glede na vrednost j-tega podbloka.



SI 20349 A

Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich

MPK[6]: H 01 L 9/00

Postopek kriptografske pretvorbe binarnih podatkovnih blokov

Izum spada na področje električnih komunikacij in računalniške tehnologije, še zlasti na področje kriptografskih postopkov in naprav za šifriranje sporočil (informacij).

Stanje tehnike

Vse značilnosti obravnavanega postopka so povezane s sledečimi izrazi:

- varnostni ključ pomeni binarno informacijo, ki je znana edinole legitimnemu lastniku;
- kriptografska konverzija pomeni konverzijo oz. pretvorbo digitalnih podatkov, ki dopušča vpliv izvornega podatkovnega bita na množico izstopnih podatkovnih bitov, npr. z namenom zaščite podatkov pred nepooblaščenim čitanjem, generiranja elektronskega podpisa, generiranja modifikacije detekcijske kode; nekatere pomembne kriptografske konverzije so unilateralna konverzija, razbitje in šifriranje;

- razbitje informacij je določena metoda ustvarjanja takoimenovane razbite kode določene velikosti (običajno 128 bitov) za poljubno obsežna sporočila; postopki razbijanja so široko uporabljani in temeljijo na iterativnih funkcijah razbijanja s pomočjo blokovnih mehanizmov kriptografske konverzije podatkov (glej Lai X., Massey J.L. Hash Functions Based on Block Ciphers/ Workshop in the Theory and Applications of Cryptographic Techniques, EUROCRYPT'92, Madžarska, 24.-28. maj 1992, Proceedings, str. 53-66);
- šifriranje je postopek konverzije podatkov, ki je osnovan na tajnem ključu in ki pretvarja izvorno besedilo v šifrirano besedilo, ki predstavlja navidez naključno zaporedje, in iz katerega naj bi bilo takorekoč nemogoče razvozlati tajni ključ;
- dešifriranje je postopek, ki je obraten postopku šifriranja; dešifriranje zagotavlja povrnitev informacij, potem ko je znan tajni ključ;
- šifra je množica elementarnih korakov konverzije vstopnih podatkov z uporabo tajnega ključa; šifro je mogoče uporabiti v obliki računalniškega programa ali kot posebno napravo;
- binarni vektor predstavlja določeno sekvenco da-bitov in ne-bitov kot npr. 101100011; specifično strukturo binarnega vektorja je mogoče interpretirati kot binarno število ob predpostavki, da položaj vsakega bita ustreza binarnemu bitu, t.j. binarni vektor je možno primerjati z numerično vrednostjo, ki je enolično določena s strukturo binarnega vektorja;
- kriptoanaliza je postopek ugotavljanja tajnega ključa z namenom omogočanja nepooblaščenega dostopa do šifrirane informacije ali ustvarjanja postopka, ki naj bi omogočil dostop do šifrirane informacije brez ugotavljanja tajnega ključa;
- unilateralna konverzija je takšna konverzija vstopnega podatkovnega bloka L-bitov v izstopni podatkovni blok L-bitov, ki omogoča enostavno izračunavanje izstopnega podatkovnega bloka v odvisnosti od vstopnega podatkovnega bloka, medtem ko izračunavanja vstopnega bloka, ki bi se pretvarjal v naključno izbran izstopni blok, v bistvu ne prakticirajo;

- unilateralna funkcija pomeni funkcijo vrednosti, ki jo je mogoče enostavno izračunati na osnovi danega argumenta, vendar pa izračunavanje argumenta na osnovi dane funkcije predstavlja težak računski problem; unilateralne funkcije se uporabljajo kot proceduralno zaporedje unilateralne konverzije določenih vstopnih blokov (argumenta), katerega izstopno vrednost se predpostavi kot funkcijsko vrednost;
- kriptografska rezistenca predstavlja stopnjo varnosti zaščite šifrirane informacije in predstavlja intenziteto, merjeno s številom elementarnih operacij, ki so potrebne za ponovno vzpostavitev informacije na osnovi kriptograma, potem ko je znan algoritem konverzije, vendar brez poznavanja tajnega ključa; v primeru unilateralnih konverzij kriptografska rezistenca pomeni kompleksnost izračunavanja vrednosti vstopnega bloka glede na njegovo izstopno vrednost;
- ciklične operacije v odvisnosti od konvertiranih podblokov ali v odvisnosti od binarnega vektorja so operacije cikličnega zamika za določeno število bitov, ki je določeno glede na vrednost podbloka ali glede na vrednost binarnega vektorja; operacije cikličnega zamika proti levi (desni) so označene s simbolom "<<<" (">>>"), tako na primer navedba B_1<<<B_2 označuje operacijo cikličnega zamika proti levi podbloka B_1 za število bitov, ki je enako vrednosti binarnega vektorja B_2; podobne operacije so osnova za šifro RC5;
- enkratna operacija je operacija, ki se izvrši na osnovi enega operanda (podatkovni blok ali binarni vektor); vrednost podbloka po izvršitvi določene enkratne operacije je odvisna zgolj od začetne vrednosti; primer enkratne operacije je npr. seštevanje, odštevanje, množenje itd.

Znani so postopki blokovnega šifriranja podatkov, gl. npr. US standard DES (National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, januar 1977. Ta postopek šifriranja podatkovnih blokov obsega generiranje tajnega ključa, delitev podatkovnega bloka na dva podbloka L in R ter alternativno spreminjanje slednjega z izvajanjem tkzv.

operacije seštevanja bita za bitom z modulom 2 na podbloku L in binarnem vektorju, ki je generiran kot izstopna vrednost določene funkcije F glede na vrednost podbloka R. Zatem pride do medsebojne zamenjave blokov. V tem postopku je uporabljena funkcija F, ki temelji na transpoziciji in vstavljanju, kar se vrši na podbloku R. Ta postopek daje visoko stopnjo konverzije, kadar se ga vrši preko posebnega elektronskega vezja.

Vendar pa najbolj relevantni postopki iz stanja tehnike uporabljajo tajni ključ majhne dolžine (56 bitov), zaradi česar so izpostavljeni kriptoanalizi v smislu iskanja ustreznega ključa. Slednje je povezasno z visoko zmogljivimi sodobnimi računalniki, ki pa se sicer možično uporabljajo.

Glede na tehnično vsebino je obravnavanemu postopku najbližji postopek, ki je bil uporabljen pri šifri RC5 in opisan v delu (R-Rivest, The RC% Encryption Algorithm/ Fast Software Encryprion, secon international Workshop Proceedings (Leuven, Belgija, 14.-16. december 1994), Lecture Notes in Computer Science, v. 1008, Springer Verlag, 1995, str. 86-96. Najbližji postopek po stanju tehnike obsega generiranje tajnega ključa v obliki množice podključev, delitev vstopnih podatkov na podbloka A in B, kot tudi izmenično konverzijo podblokov. Transformacija podblokov poteka z izvajanjem enkratnih in dvakratnih operacij na njima. Kot dvakratne uperacije so uporabljene operacije prištevanja z modulom 2^n, pri čemer velja n = 8, 16, 32, 64 in takoimenovanega seštevanja z modulom 2 bita za bitom. Kot enkratna operacija je uporabljena operacija cikličnega zamika proti levi, pri čemer je število bitov, pri katerih je konvertirani podblok zamaknjen, odvisno od vrednostii preostalega podbloka, to pa določa odvisnost operacije cikličnega zamikanja v vsakokratnem koraku konverzije vstopnega bloka od začetne vrednosti vstopnega podatkovnega bloka. Dvakratna operacija se izvaja na podbloku in podključu kot tudi na dveh podblokih. Značilnost najbližjega postopka

po stanju tehnike je uporaba operacije cikličnega zamikanja bitov pri enem od podblokov v odvisnosti od vrednosti preostalega podbloka.

Podblok, na primer podblok B, se konvertira kot sledi. Na podblokih A in B se izvaja operacija ("⊕") sumiranja bita za bitom z modulom 2, po tej operaciji dobljena vrednost pa se prenese v podblok B. To je mogoče zapisati kot relacijo:

$$B \leftarrow B \oplus A,$$

pri čemer označba ← ponazarja operacijo prenosa. Zatem se na podbloku B izvede operacijo cikličnega zamikanja na številu bitov, ki je enako vrednosti podbloka A:

$$B \leftarrow B <<< A.$$

Zatem se na podbloku in enem od podključev izvrši operacijo sumiranja z modulom 2^n: $B \leftarrow (b + s) \bmod 2^n$, pri čemer n predstavlja dolžino podbloka v bitih, nato pa se na podoben način konvertira $i \leq N$. Pri obeh podblokih se izvrši več takšnih korakov konverzije.

Ta postopek omogoča visoko stopnjo šifriranosti, kadar se ga uporabi v obliki računalniškega programa ali v obliki elektronskih šifrirnih naprav. Vendar pa je to najbližje stanje tehnike povezano tudi z nekaterimi pomanjkljivostmi, in sicer ni zagotovljena visoka rezistenca konverzije kriptografskih podatkov v smislu diferencialne in linearne kriptoanalize (Kaliski B.S., Yin Y.L. On Differential and Linear Cryptanalysis of the RC5 Encrypton Algorythm, Advances in Cryptology-CRYPTO'95 Proceedings, Springer-Verlag, 1995, str. 171-184). Ta pomanjkljivost izhaja iz dejstva, da je učinkovitost uporabe operacij, ki so odvisne od podatkov, predvidenih za konverzijo, z namenom povečanja rezistence šifriranja glede na znane kriptoanalitične metode, zmanjšana zaradi dejstva, ker je število potencialno razpoložljivih verzij operacij cijkličnega zamikanja enako številu binarnih bitov podbloka n in ne presega 64.

Izum temelji na nalogi razvoja postopka kriptografske konverzije binarnih podatkovnih blokov, kjer naj bi konverzijo vstopnih podatkov izvršili na tak način, da bi se povečalo število različnih verzij operacije, ki je odvisna od za konverzijo predvidenega bloka, s tem pa naj bi se povečala rezistenca v smislu diferencialne in linearne kriptoanalize.

Opis izuma

Cilj je dosežen z dejstvom, da postopek kriptografske konverzije binarnih podatkovnih blokov obsega delitev podatkovnih blokov na $N \geq 2$ podblokov, izmenično konverzijo podblokov z izvajanjem vsaj ene operacije konverzije na i-tem podbloku, kjer je $i \leq N$, pri čemer je ta operacija odvisna od vrednosti j-tega podbloka, kjer je $j \leq N$, razen tega pa novo značilnost po izumu predstavlja tudi dejstvo, da se kot operacijo, ki je odvisna od vrednosti j-tega podbloka, izvaja operacijo transpozicije bitov i-tega podbloka.

Zahvaljujoč takšni rešitvi se poveča število možnih verzij od vrednosti j-tega podbloka odvisnih operacij, s čimer je omogočeno povečanje rezistence kriptografske konverzije glede na diferencialno in linearno kriptoanalizo.

Prav tako predstavlja novo značilnost, da se operacija transpozicije bitov i-tega podbloka, ki je odvisna od vrednosti j-tega podbloka, izvaja v odvisnosti od tajnega ključa, in sicer pred pričetkom konverzije i-tega bloka.

Zahvaljujoč tej rešitvi modifikacija operacije transpozicije bitov i-tega podbloka, ki je odvisna od vrednosti j-tega podbloka, ni vnaprej določena, kar omogoča še nadaljnje povečanje rezistence kriptografske konverzije glede na diferencialno in linearno kriptoanalizo ter hkrati dopušča zmanjšanje števila konverzijskih operacij ter pri tem poveča stopnjo šifriranosti.

Nova značilnost je tudi ta, da se pred izvajanjem vsakokratne operacije transpozicije bitov i-tega podbloka, kar je odvisno od j-tega podbloka, dodatno generira tudi binarni vektor V, medtem ko se operacija transpozicije bitov i-tega podbloka izvaja v odvisnosti od vrednosti V, pri čemer se binarni vektor generira v odvisnosti od svoje vrednosti v času izvajanja predhodnega koraka konverzije pri enem od podblokov kot tudi od vrednosti j-tega podbloka.

Zahvaljujoč tej rešitvi se poveča kriptografska rezistenca proti vdorom, ki so posledica onesposobitve šifrirne naprave.

V nadaljevanju bo bistvo izuma podrobneje pojasnjeno na osnovi njegovih primerov izvedbe v povezavi s priloženimi skicami.

Kratek opis skic

Sl. 1 kaže splošno shemo kriptografske konverzije v skladu s postopkom po izumu.

Sl. 2 shematično kaže strukturo upravljanih transpozicijskih blokov.

Sl. 3 kaže strukturo upravljanih transpozicijskih blokov s 32-bitnimi vstopnimi informacijami.

Sl. 4 kaže blokovno shemo elementarne pretvorbe.

Sl. 5 kaže tabelo vstopnih in izstopnih signalov elementarne pretvorbe, pri čemer je kontrolni signal u = 1.

Sl. 6 predstavlja tabelo vstopnih in izstopnih signalov elementarne upravljane pretvorbe, pri čemer je vrednost kontrolnega signala u = 1.

Prednostne izvedbe izuma

Izum bo obrazložen s pomočjo posplošene sheme konverzije podatkovnih blokov, temelječe na postopku po izumu, ki je prikazana na sl. 1.

Pri tem pomeni P kontroliran transpozicijski blok, A in B sta konvertirana podbloka, K_{4r}, K_{4r-1}, K_{4r-2}, K_{4r-3}, so elementi n-bitnega tajnega ključa (n-bitni podključi); V je binarni vektor, ki je generiran v odvisnosti od vstopnih podatkov; simbol $\oplus$ označuje operacijo sumiranja bita za bitom z modulom 2, simbol $\otimes$ označuje operacijo sumiranja z modulom n, kjer je n dolžina podatkovnega podbloka v bitih. Poudarjene polne črte označujejo potek prenosa n-bitnih signalov, tenke polne črte označujejo prenos posameznega bita, tenke prekinjene črte označujejo prenos posameznega kontrolnega bita. Poudarjene prekinjene črte označujejo potek n kontrolnih signalov, n kontrolnih signalov predstavlja bite podključa ali bite binarnega vektorja. Uporaba bitov podključa kot kontrolne signale ima za posledico določeno modifikacijo operacije transpozicije bitov podbloka v odvisnosti od vrednosti vstopnega bloka, kar še dodatno poveča rezistenco kriptografske konverzije.

Sl. 1 kaže en cikel konverzije. Mogoče je izvesti od 2 do 16 in še več ciklov, in sicer v odvisnosti od specifične implementacije kontroliranega transpozicijskega bloka in zahtevane konverzijske stopnje. Takšno shemo postopkov kriptografske konverzije je mogoče uporabiti za šifrirno in unilateralno konverzijo. Pri slednji tajni ključ ni uporabljen in namesto signalov podključa se v kontrolni vstop bloka P vodi signale binarnega vektorja V, generirane v odvisnosti od vrednosti podblokov, predvidenih za konvertiranje v vmesnih korakih konverzije. Pri šifriranju je med izvajanjem posameznih šifrirnih ciklov mogoče uporabiti taisto pri n-bitnih podključih K_4, K_3, K_2 in K_1. V tem primeru, ko je tipična dolžina podbloka n = 32, znaša dolžina tajnega ključa 128 bitov. Če uporabimo daljši tajni ključ, v vsakem ciklu lahko uporabimo K_{4r}, K_{4r-1}, K_{4r-2} in K_{4r-3}. Na primer, kadar je številka cikla r = 3, so v prvem ciklu uporabljeni podključi K_4, K_3, K_2 in K_1, v drugem ciklu so uporabljeni podključi K_8, K_7, K_6 in K_5, v tretjem ciklu pa podključi K_{12}, K_{11}, K_{10} in K_9.

Možnosti tehnične uporabe obravnavanega postopka so razložene s sledečimi posebnimi primeri.

Primer 1

Ta primer se nanaša na uporabo postopka za šifriranje podatkov. Tajni ključ je predstavljen v obliki štirih podključev K_{4r}, K_{4r-1}, K_{4r-2} in K_{4r-3}. En šifrirni cikel je opisan s sledečim proceduralnim zaporedjem:

1. Konvertiranje podbloka A v skladu z enačbo

$$A \leftarrow A \oplus K_{4r-3},$$

2. Konvertiranje podbloka B v skladu z enačbo

$$B \leftarrow B \otimes K_{4r-2},$$

3. V odvisnosti od vrednosti podbloka A in podključa K_{4r-1} se izvrši transpozicijo bita podbloka B.

4. Konvertiranje podbloka A v skladu z enačbo

$$A \leftarrow A \otimes B$$

5. V odvisnosti od vrednosti podbloka B in podključa K_{4r} se izvrši transpozicijo bita podbloka A.

6. Konvertiranje podbloka B v skladu z enačbo

$$B \leftarrow B \oplus A.$$

Primer 2

Ta primer opisuje en cikel unilateralne konverzije v skladu s sledečim proceduralnim zaporedjem.

1. Generiranje binarnega vektorja V

$$V \leftarrow B <<< B$$

2. Konvertiranje podbloka B v skladu z enačbo

$$B \leftarrow B \otimes V.$$

3. Generiranje binarnega vektorja V v iodvisnosti od njegove vrednosti v predhodnem koraku ter od vrednosti podblokov A in B v skladu s formulo:

$$V \leftarrow (V <<< A) \oplus (B <<< 13)$$

4. Konvertiranje podbloka A v skladu z enačbo

$$A \leftarrow A \oplus V.$$

5. V odvisnosti od vrednosti A in V se izvrši transpozicija bitov podbloka B.

6. Podblok A se konvertira po enačbi:

$$A \leftarrow A \otimes B.$$

7. Generira se binarni vektor V:

$$V \leftarrow (V <<< B) \oplus (A <<< 11)$$

8. V odvisnosti od vrednosti B in V se izvrši transpozicija bitov podbloka A.

9. Podblok B se konvertira po enačbi:

$$B \leftarrow B \oplus A.$$

Sl. 2 kaže možno izvedbo kontroliranega transpozicijskega bloka z uporabo množice elementarno pretvorjenih S. Izvedba ustreza bloku P z 8-bitnim vstopom podatkovnih signalov in 8-bitnim vstopom kontrolnih signalov, označenih s črtkanimi črtami podobno kot na sl. 1.

Število različnih verzij operacije transpozicije je enako številu možnih kodirnih kombinacij na kontrolnem izhodu in pri bloku P s strukturo, kakršna je prikazana na sl. 2 znaša $2^8 = 256$, kar presega število cikličnih oparacij zamikanja, uporabljeno pri najbližjem postopku po stanju tehnike. Z uporabo podobnega postopka je mogoče izvesti shemo bloka P poljubnih dimenzij vstopnih podatkov in vstopnega kontrolnega signala, še zlasti pri bloku s 32-bitnim vstopom podatkov in 32-bitnim vstopom kontrolnega signala. V nazadnje omenjenem primeru dosežemo število različnih variacij operacij transpozicije, ki je enako $2^{32} = 10^9$.

Sl. 3 kaže strukturo kontrolnega transpozicijskega bloka s 32-bitnim vstopom podatkov in 79-bitnim kontrolnim vstopom. Kontrolni transpozicijski blok vrši enkratno transpozicijo vstopnih binarnih bitov za vsako možno vrednost kodne kombinacije na kontrolnem vstopu, katerih število znaša 2^{79} . Eksterni vstopi informacij kontrolnega transpozicijskega bloka so označeni z i1, i2, ..., i32, eksterni izhodi so označeni z o1, o2, ..., o32, kontrolni vstopi pa so označeni s c1, c2, ..., c79. Elementarna stikala S so povezana na tak način, da tvorijo matrico, sestoječo iz 31 vrstic. V prvi vrstici je vključenih 31 elementarnih stikal, v drugi vrstici 30, v tretji 29 itd. V vsaki nadaljnji vrstici se število elementarnih stikal zmanjša za 1. V spodnji vrstici 31 je priključeno 1 elementarno stikalo.

Vrstica s številom j $\neq$ 31 ima 33 j-vstopov in 32j-kontrolnih vstopov. Zadnji (najbolj desni) izstop j-te vrstice je eksterni izstop kontrolnega transpozicijskega bloka, preostalih 32 j-izstopov j-te vrstice pa je priključenih na ustrezne vstope (j+1)-te vrstice. Zadnja 31. vrstica ima dva izstopa in oba sta eksterna izstopa kontrolnega transpozicijskega bloka. Enoten (u=1) kontrolni signal je voden izključno na en kontrolni vstop vsake vrstice. Izpolnjevanju teh zahtev služijo binarni dešifratorji 32. reda F_1, F_2, ...F_{15} ter binarni dešifrator 16. reda F_{16}. Dešifratorji F_1, F_2, ...F_{15} imajo pet kontrolnih vstopov, na katere je vodena poljubna 5-bitna koda, kot tudi 32 izstopov. Dešifratorji generirajo enoten signal zgolj na izstopu. Na preostalih 31 vstopih je nastavljen nični signal. Dešifrator F_{16} ima 4 kontrolne vstope, kamor je vodena poljubna 4-bitna signalna koda, in hkrati 16 izstopov, pri čemer je na zgolj enem nastavljen enoten signal. Pri vseh dešifratorjih F_1, F_2, ...F_{15} in F_{16} vsaka vstopna binarna koda definira enolično možno število izstopov, pri katerih je nastavljen enoten signal (u = 1).

Del izstopov dešifratorja F_h, kjer je h $\leq$ 15 je priključen na kontrolne vstope h-te vrstice (vstopi 32 - h), medtem ko je del vstopov priključen na kontrolne vstope (32

- h)-te vrstice (preostali dešifrirni izstopi h). Kontrolni signal u = 1 je v vsaki vrstici nastavljen za zgolj enem elementarnem stikalu. Vstop vrstice, ki je priključen na desni vstop elementarnega stikala, kamor je voden enoten kontrolni signal, komutira z eksternim izstopom kontrolnega transpozicijskega bloka, ki ustreza tej vrstici. Če je enoten kontrolni signal voden na najbolj levo stikalo, eksterni izstop kontrolnega transpozicijskega bloka (bloka P) komutira z najbolj levim vstopom vrstice. Prva vrstica komutira z enim od eksternih vstopov i1, i2, ..., i32 bloka P z eksternim izstopom o1, medtem ko preostalih 31 eksternih izstopov komutira z vstopi druge vrstice. Druga vrstica s preostalim 31 eksternim vstopom komutira z eksternim izstopom o2, medtem ko preostalih 30 eksternih vstopov komutira z vstopi 3. vstice, itd. Takšna struktura bloka P uporablja enolično transpozicijo vstopnih bitov za vsako vrednost binarne kode, dovedene na 79-bitni kontrolni vstop bloka P.

Možna je npr. tudi naslednja verzija uporane kontrolnega 79-bitnega vstopa v kriptograpski konverzijski shemi, ki je prikazana na sl. 1. Npr. 32 bitov je uporabljenih kot kontrolni signali podbloka B in 47 bitov pripada tajnemu ključu. Za slednje je mogoče uporabiti npr. 32 bitov podključa K_{4r-1} in 15 bitov podključa K_{4r-2}. V tem primeru se potem, ko je v šifrirno napravo vnešen tajni ključ, v odvisnosti od 47 bitov tega tajnega ključa, generira ena od 2^{47} modifikacij transpozicijskih operacij bitov, kar je odvisno od vrednosti vstopnega bloka. Pri tem vsaka modifikacija te operacije obsega 2^{32} različnih operacij transpozicije bitov bloka A, katerih izbor je določen z vrednostjo bloka B. Izbira modifikacije ni vnaprej določena, ker je določena s tajnim ključem. To še dodatno poveča rezistenco kriptografske konverzije. Če so pri šifrirni napravi uporabljeni 4 bloki P s strukturo, kakršna je prikazana na sl. 3, potem število možnih kombinacij modifikacij transpozicijskih operacij, nastavljenih na P v odvisnosti od tajnega ključa, ob uporabi tajnega ključa dolžine vsaj 188 bitov lahko znaša do $(2^{47})^4 = 2^{188}$.

Sl. 4 kaže delovanje elementarnega stikala, pri čemer u predstavlja kontrolni signal, a in b sta vstopna podatkovna signala, c in d pa sta izstopna podatkovna signala.

Tabeli 5 in 6 ponazarjata odvisnost izstopnih signalov od vstopnih in kontrolnih signalov. Iz omenjenih tabel izhaja, da je, kadar je u = 1, vrstica a komutirana z vrstico c, vrstica b pa z vrstico d. Kadar je u = 0, je vrstica a komutirana z vrstico d, vrstica b pa z vrstico d.

Zahvaljujoč enostavni strukturi sodobna planarna tehnologija proizvodnje integriranih vezij omogoča enostavno izdelavo kriptografskih mikroprocesorjev, ki obsegajo kontrolirane transpozicijske bloke s 32- ali 64 bitnim vstopom.

Gornji primeri kažejo, da je gornji postopek kriptografske konverzije binarnih podatkovnih blokov tehnično izvedljiv ter omogoča rešitev zastavljenega problema.

Industrijska uporabljivost

Obravnavani postopek je npr. mogoče realizirati v specializiranih kriptografskih mikroprocesorjih za stopnjo šifriranosti reda 1 Gbit/s, kar zadostuje za šifriranje podatkov med prenašanjem preko hitrih komunikacijskih kanalov iz optičnih vlaken v realnem času.

Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich

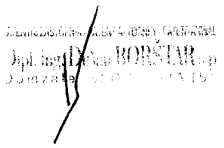
PATENTNI ZAHTEVKI

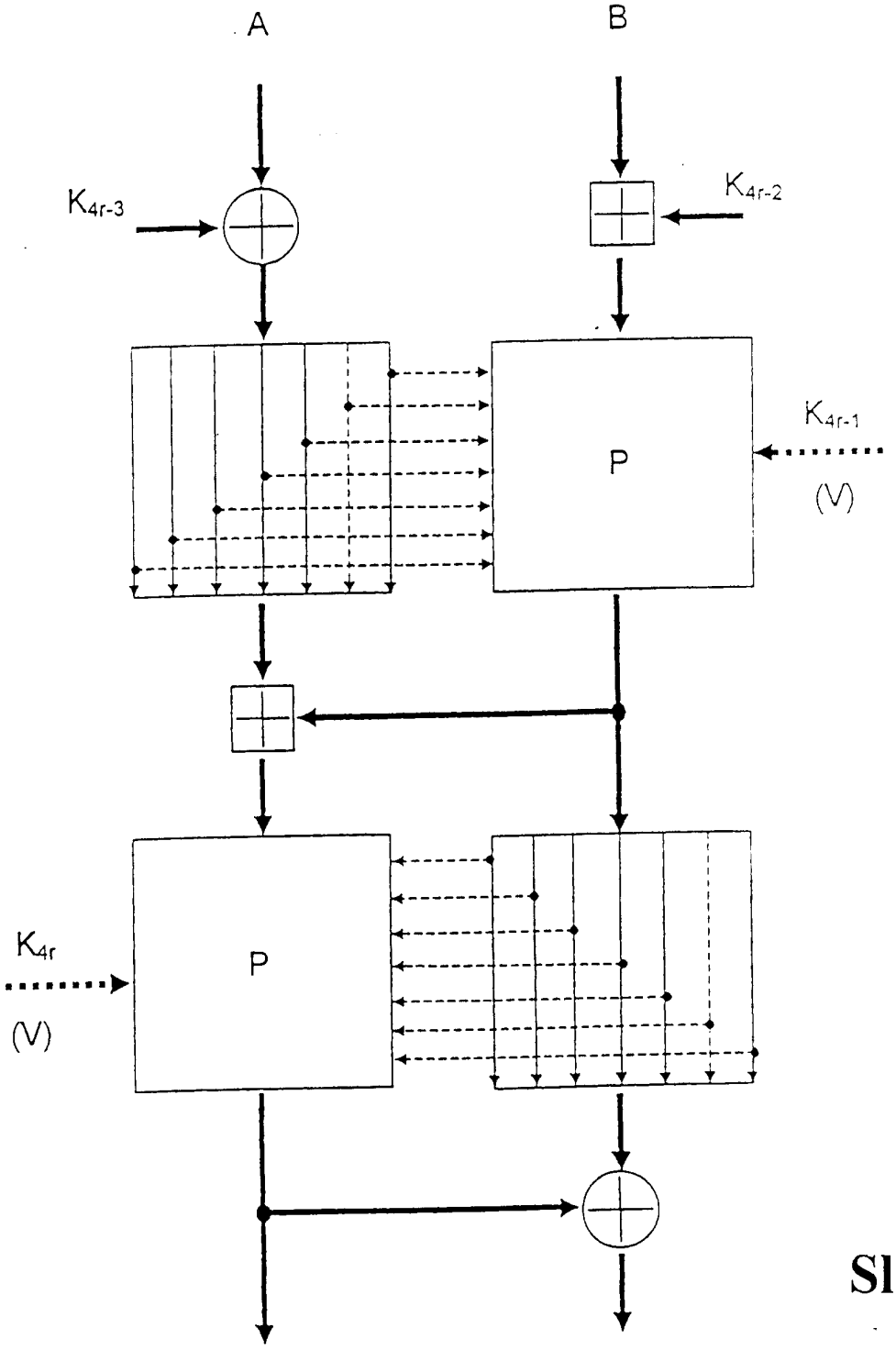
1. Postopek kriptografske konverzije binarnih podatkovnih blokov, obsegajoč delitev omenjenih podatkovnih blokov na $N \geq 2$ podblokov, izmenično konvertiranje omenjenih blokov z učinkovanjem na i-ti podblok, pri čemer je $i \leq N$, vsaj eno operacijo konverzije v odvisnosti od vrednosti j-tega podbloka, označen s tem, da je operacija transpozicije bitov i-tega podbloka uporabljena kot operacija, ki je odvisna od vrednosti j-tega podbloka, kjer je $j \leq N$.

2. Postopek po zahtevku 1, označen s tem, da se omenjeno operacijo transpozicije bitov omenjenega i-tega podbloka, ki je odvisna od vrednosti j-tega podbloka, generira v odvisnosti od tajnega ključa pred pričetkom konverzije i-tega podbloka.

3. Postopek po zahtevku 1, označen s tem, da se pred izvajanjem vsakokratne operacije transpozicije bitov omenjenega i-tega podbloka, ki je odvisna od vrednosti omenjenega j-tega podbloka, dodatno generira še binarni vektor V, omenjeno operacijo transpozicije bitov omenjenega i-tega podbloka pa se izvrši v odvisnocti od vrednosti V, pri čemer se omenjeni binarni vektor generira v odvisnosti od njegove vrednosti v času izvajanja predhodnega koraka enega od omenjenih podblokov ter v odvisnosti od vrednosti j-tega podbloka.

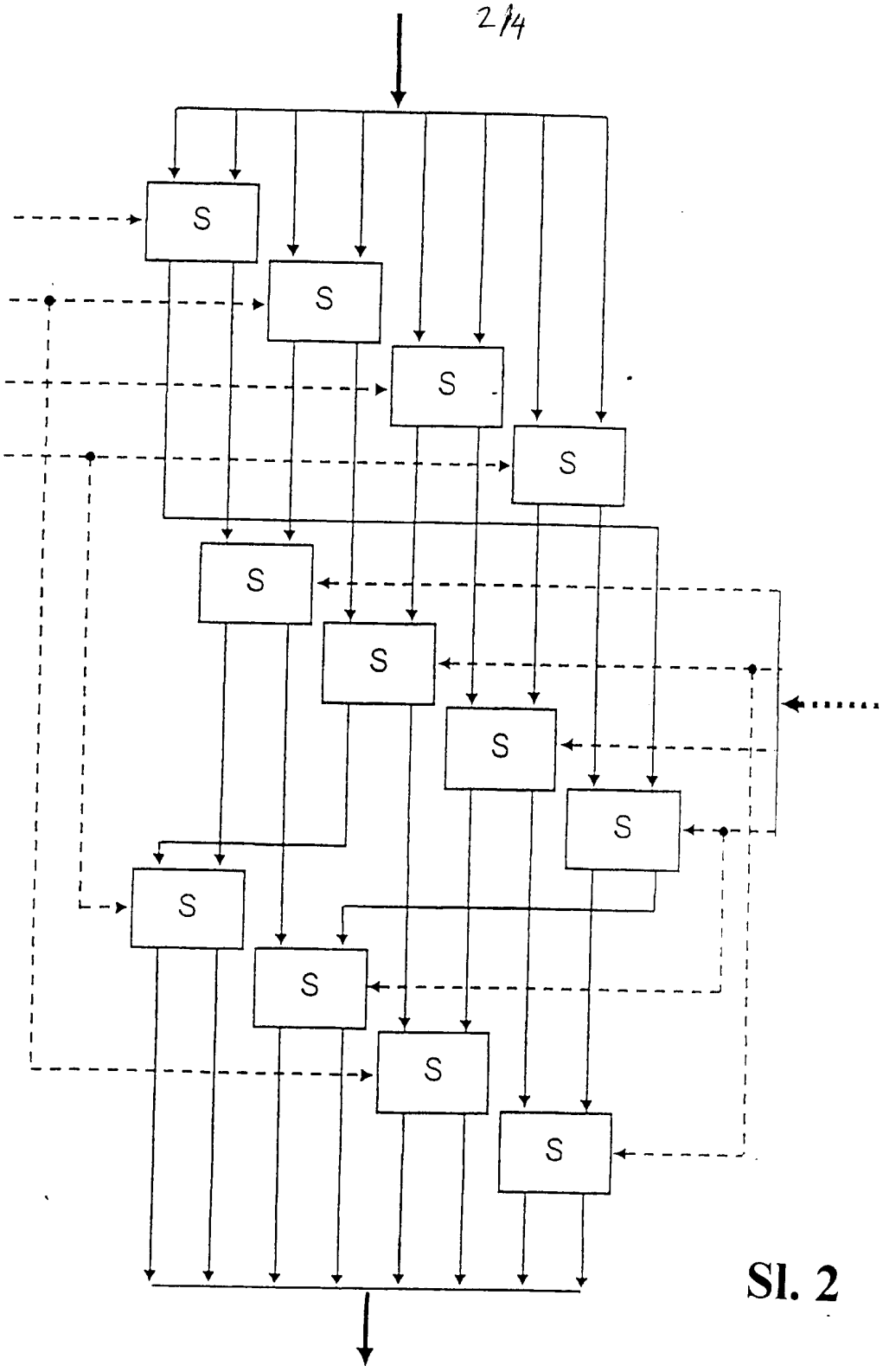
Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich





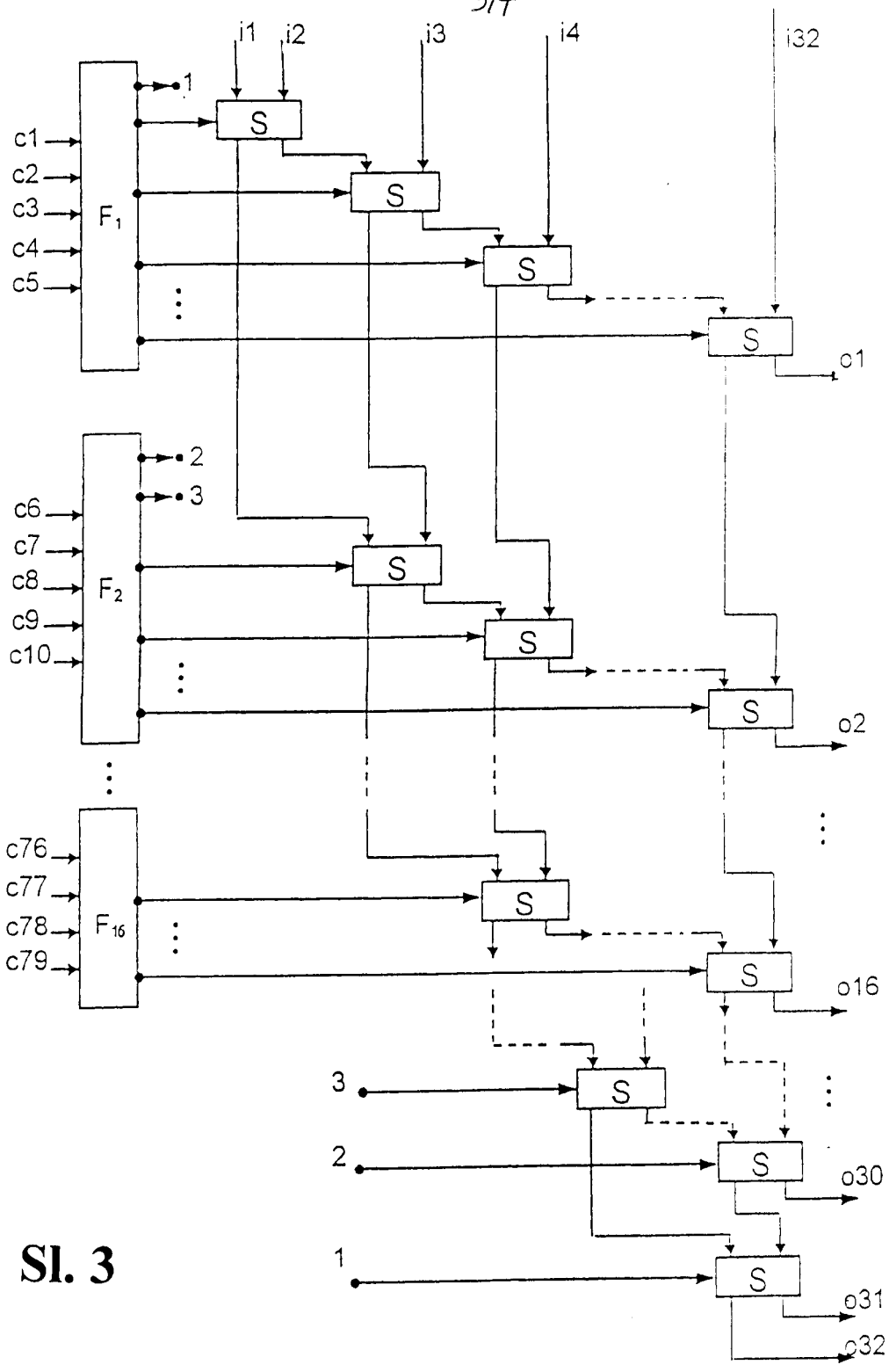
Sl. 1

Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich



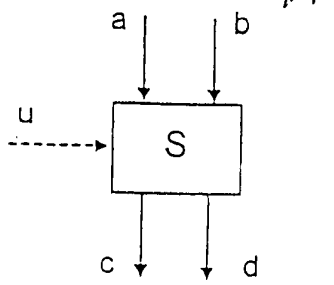
Sl. 2

Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich



Sl. 3

Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich



Sl. 4

u=1

VSTOP		IZSTOP	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

Sl. 5

u=0

VSTOP		IZSTOP	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

Sl. 6

Za:
Otkrytoe aktsionernoe obschestvo "Moskovskaya Gorodskaya Telefonnaya Set
MOLDOVYAN Alexandr Andreevich
MOLDOVYAN Nikolai Andreevich