PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:
2000 -2653

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
H 04 L 9/00

(19) ČESKÁ REPUBLIKA

(22) Přihlášeno: **19.06.1998**

(32) Datum podání prioritní přihlášky: **19.01.1998**

(31) Číslo prioritní přihlášky: **1998/98100685**

(33) Země priority: **RU**

(40) Datum zveřejnění přihlášky vynálezu: **14.03.2001**
(Věstník č. 3/2001)

(86) PCT číslo: **PCT/RU98/00182**

(87) PCT číslo zveřejnění: **WO99/36942**

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

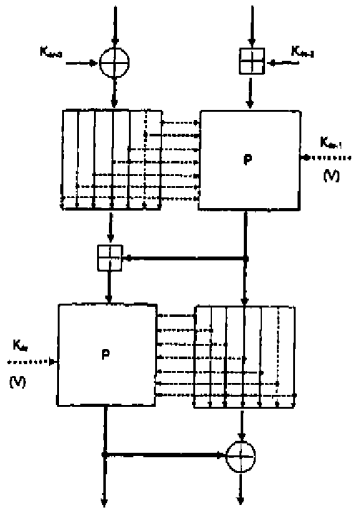
(71) Přihlašovatel:
OTKRYTOE AKTSIONERNOE OBSCHESTVO "MOSKOVSKAYA GORODSKAYA TELEFONNAYA CET", Moscow, RU;
MOLDOVYAN Alexandr Andreevich, Vsevolozhsk, RU;
MOLDOVYAN Nikolay Andreevich, Vsevolozhsk, RU;

(72) Původce:
Moldovyan Alexandr Andreevich, Vsevolozhsk, RU;
Moldovyan Nikolay Andreevich, Vsevolozhsk, RU;

(74) Zástupce:
PATENTSERVIS PRAHA a.s., Jivenská 1, Praha 4, 14000;

(54) Název přihlášky vynálezu:

Způsob kryptografické konverze binárních datových bloků



(57) Anotace:

Způsob kryptografické konverze binárních datových bloků používající dělení zmíněných datových bloků do N≥2 podbloků, postupnou konverzi zmíněných datových bloků prací s i-tým podblokem, kde i≤N a kde alespoň jedna operace konverze závisí na hodnotě j-tého podbloku, kde j≤N. Operace závisející na hodnotě j-tého podbloku je transpoziční operací bitů a i-tém podbloku, která závisí na hodnotě j-tého podbloku a je provedena podle tajného klíče před zahájením konverze i-tého podbloku. Tato metoda se rovněž vyznačuje tím, že binární vektor V je určen před momentální transpoziční operací bitů i-tého podbloku, závisejícího n j-tém podbloku, přičemž transpoziční operace i-tého podbloku je provedena podle hodnoty vektoru V. Binární vektor V je určen podle své hodnoty při provádění předchozího konverzního kroku jednoho z podbloků a podle hodnoty j-tého podbloku.

CZ 2000 - 2653 A3

Způsob kryptografické konverze binárních datových bloků

Oblast techniky

Tento vynález se týká oblasti elektrických komunikací a počítačové technologie, zvláště se pak týká kryptografických metod a zařízení pro kryptování zpráv (informací).

Dosavadní stav techniky

Všechny popisy nárokovaných metod používají následující terminologii:

- tajný klíč je binární informace známá pouze legitimnímu vlastníkovi;
- kryptografická konverze je konverze digitálních dat, která umožňuje působení zdrojových datových bitů na množství výstupních datových bitů na příklad za účelem generování digitálního podpisu, generování kódu příznaku změny; mezi důležité metody kryptografické konverze patří unilaterální konverze, hešování a šifrování;
- hešování informací je metoda vytvářející takzvaný hešovací kód pevné délky (typicky 128 bitů) pro zprávy jakékoliv délky; velmi rozšířené jsou hešovací metody založené na iterativních hešovacích funkcích používajících blokový mechanismus kryptografické konverze informací (viz Lai X., Massey J.L. Hash Functions Based on Block Ciphers/ Workshop on the Theory and Applications of Cryptographic

Techniques. EUROCRYPT'92, Hungary, May 24-28, Proceedings, p.53-66);

- šifrování je proces konverze informace, který závisí na tajném klíči a který převádí zdrojový text do zašifrované formy reprezentované pseudonáhodnou posloupností znaků, ze které je prakticky nemožné získat původní informaci bez znalosti tajného klíče;
- dešifrování je proces, který je reverzní k procesu šifrování; dešifrování provádí znovusestavení informace podle kryptogramu, kde tajný klíč je znám;
- šifra je posloupnost elementárních kroků konverzí vstupních dat s použitím tajného klíče; šifrovač může být implementován jako počítačový program nebo jako speciální zařízení;
- binární vektor je určitá sekvence bitů zapnuto vypnuto, jako například 1011010011; určitá struktura binárního vektoru může být interpretována jako binární číslo, pokud řekneme, že pozice každého bitu odpovídá binárnímu bitu, t.j. binární vektor může být porovnáván s numerickou hodnotou, která je jednoznačně určena strukturou binárního vektoru;
- kryptoanalýza je metoda výpočtu tajného klíče pro získání neautorizovaného přístupu k zašifrovaným informacím nebo vyvíjení metody, která zajistí přístup k zašifrované infromaci bez výpočtu tajného klíče;
- unilaterální konverze je taková konverze vstupního datového bloku o L-bitech do výstupního datového bitu o L-bitech, která umožňuje jednoduše vypočítat výstupní datový blok ze vstupního datového bloku, kde transformace vstupního datového bloku do náhodně zvoleného výstupního bloku je prakticky neproveditelná;
- unilaterální funkce je funkce, jejíž hodnota je jednoduše vypočítatelná z daného argumentu, nicméně kde výpočet argumentu k danému výsledku funkce je výpočetně složitý

problém; unilaterální funkce jsou implementovány jako procedurální sekvence unilaterálních konverzí určitého vstupního bloku (argument) jehož výstupní hodnota je považována za hodnotu funkce;

- kryptografická odolnost je měření bezpečností ochrany šifrované informace a reprezentuje práci potřebnou k zotavení informace z kryptogramu, kde konverzní algoritmus je známý, ale tajný klíč není znám; v případě unilaterálních konverzí je kryptografickou odolností míněna složitost výpočtu hodnoty vstupních bloku podle výstupního bloku;
- cyklické operace posuvu závisející na převáděných podblocích nebo závisející na binárním vektoru jsou operace cyklického posuvu na několika bitech určených hodnotou podbloku nebo hodnotou binárního vektoru; operace cyklického posuvu vlevo (vpravo) jsou označeny symbolem '<<<'('>>>'), například zápis B1<<<B2 označuje operaci cyklického posuvu vlevo podbloku B1 na počtu bitů rovnému hodnotě binárního vektoru B2; podobné operace jsou základem šifry RC5;
- jednostranná operace je operace provedená na jednom operandu (datovém bloku nebo binárním vektoru); hodnota podbloku po provedení určité dané jednostranné operace závisí pouze na počáteční hodnotě; příkladem jednostranných operací je sčítání, odčítání, násobení atp;

Jsou známy metody blokového šifrování dat, viz např. US standard DES (National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, January 1977). Tato metoda šifrování datových bloků se skládá z generování tajného klíče, rozdělování konvertovaných datových bloků do dvou podbloků L a R a střídání zmíněného tak, že se vykonává operace suma bit-k-bitu modulo 2 podbloku L a binárního vektoru, který je generován jako výstupní hodnota určité funkce F podle hodnoty podblo-

ku R. Potom jsou bloky vyměněny. Funkce F v této metodě je implementována prováděním transpozice a operace stlačování vykonávaná na podbloku R. Tato metoda má vysokou rychlost konverze, je-li realizována jako specializovaný elektronický obvod.

Nicméně nejbližší známá metoda z dosavadního stavu techniky používá tajný klíč malé velikosti (56 bitů), což ji činí prolomitelnou kryptoanalýzou založeno na hledání klíče, který funguje. Tato posledně zmíněná metoda je spojená s vyskou výkonností moderních masově využívaných počítačů.

Nejbližší metodou k nárokované metodě pro kryptografickou konverzi binárních datových bloků podle své technické podstaty je metoda implementovaná v šifře RC5 a popsaná v práci (R.Rivest, The RC5 Encryption Algorithm/ Fast Software Encryption, second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, v.1008, Springer-Verlag, 1995, pp.86-96). Nejbližší metoda z dosavadního stavu techniky se skládá z generování tajného klíče ve formě sady podklíčů a dále z rozdělování vstupních datových bloků do podbloků A a B a střídavé konverze podbloků. Podbloky jsou transformovány pomocí provádění jednostranných a dvoustranných operací. Jako dvoustranné operace jsou použity operace sčítání modulo 2^n, kde n=8, 16, 32, 64 a operace sčítání modulo 2 bit-k-bitu. Jako jednostranné operace je použita operace cyklického posuvu vlevo, kde počet bitů, o které se posun provede závisí na hodnotě jiného podbloku, toto určuje závislost operace cyklického posunu v prováděném kroku konverze podbloku na počáteční hodnotě vstupního datového bloku. Dvoustranná operace se provádí na podbloku a podklíči stejně tak jako na dvou podblocích. Charakteristické v metodách ze stávajícího stavu techniky je použití cyklických operací bitového posuvu na jednom podbloku v závislosti na hodnotě jiného podbloku.

Podblok, například podblok B, je konvertován následovně. Je provedena operace modulo 2 bit-k-bitu ("⊕") na podblocích A a B a hodnota obdržená z této operace je přiřazena podbloku B. Toto se zapisuje jako relace:

$B \leftarrow B \oplus A,$

kde symbol "←" označuje operaci přiřazení. Poté je na podbloku B provedena operace cyklického bitového posuvu o počet bitů rovný hodnotě podbloku A:

$B \leftarrow B <<< A.$

Poté je provedena na podbloku a jednom z podklíčů S operace součet modulo 2^n:

$B \leftarrow (B + S) \bmod 2^n$

kde n je délka podbloku v bitech. Poté je stejným způsobem konvertován podblok A. Několik takových konverzních kroků je provedeno na obou podblocích.

Tato metoda poskytuje vysokou rychost šifrování, je-li implementována jako počítačový program nebo jako elektronické šifrovací zařízení. Nicméně tyto nejbližší metody z dosavadního stavu techniky mají také některé nevýhody, zvláště pak neposkytují vysokou odolnost kryptografické datové konverze vůči diferenciální a lineární kryptoanalýze (Kaliski B.S., Yin Y.L. On Differential and Linear Cryptoanalysis of the RC5 Encryption Algorithm. Advances in Cryptology-CRYPTO'95 Proceedings, Springer-Verlag, 1955, pp. 171-184). Tato nevýhoda je daná faktem, že efektivita operací závisí na datech, které se konvertují, způsobem jakým se zvyšuje odolnost šifry v známých kryptoanalytických metodých, kde tato odolnost je snižována počtem potencionálně proveditelných variant cyklických operací posuvu, což je počet binárních bitů podbloku n, která nepřesahuje 64.

Podstata vynálezu

Podstata vynálezu je formována úlohou vyvinout metodu kryptografické konverze binárních bloků dat, kde vstupní datové konverze by byly ovlivňovány takovým způsobem, aby bylo zajištěno zvýšení počtů možných variant operace, která závisí na konvertovaném bloku a čímž se zvýší odolnost vůči diferenciální a lineární kryptoanalýze.

Tohoto cíle je dosaženo faktem, že v metodě kryptografické konverze binárních datových bloků, které se vyznačují dělením datových bloků do N≥2 podbloků, dále střídavým konvertováním podbloků operacemi na i-tém podbloku, kde i<=N, a to alespoň jednou konverzní operací, kde zmíněná operace závisí na hodnotě j-tého podbloku, kde j<=N, kde nová vlastnost v souladu s předkládaným vynálezem je fakt, že tak jako operace závisí na hodnotě j-tého podbloku, tak je použito operace transpozice bitů i-tého podbloku.

S pomocí tohoto způsobu, je počet možných verzí j-tého podbloku vyšší, což pomáhá zvětšit kryptografickou odolnost konverze vůči diferenciální a lineární cryptoanalýze.

Novost spočívá také v tom, že operace transpozice bitů i-tého podbloku, která závisí na hodnotě j-tého podbloku je vytvářena na základě tajného klíče před zahájením konverze i-tého podbloku.

Pomocí tohoto řešení modifikace operace transpozice bitů i-tého podbloku, která závisí na hodnotě j-tého podbloku není předurčena, což poskytuje další zlepšení odolnosti kryptografické konverze vůči diferenciální a lineární kryptoanalýze s umožňuje zredukovat počet konverzních operací a tím zvýšit rychlost konverze.

Novost spočívá také v tom, že před provedením aktuální operace transpozice bitů i-tého podbloku, která závisí na hodnotě j-tého podbloku, je navíc vygenerován binární vektor V, kde operace transpozice bitů i-tého podbloku je prováděna v

závislosti na hodnotě V, kde binární vektor je generován v závislosti na hodnotě v době provádění předchozího kroku konverze pro jeden z podbloků a na hodnotě j-tého podbloku.

Díky tomuto řešení je dosaženo další zlepšené odolnosti proti útokům založeným na rozboru šifrovacího zařízení.

V dalším textu bude podstata vynálezu vyjasněna detailně pomocí realizací vynálezu společně s odkazy na přiložené obrázky.

Seznam obrázků na výkrese

Obr.1 ukazuje zobecněný diagram kryptografické konverze v souladu s předkládaným vynálezem.

Obr.2 zobrazuje schematickou strukturu řídícího bloku transpozicí.

Obr.3 reprezentuje strukturu řízeného transpozičního bloku s 32-bitovým vstupem.

Obr.4 zobrazuje blokový diagram elementarního přepínače.

Obr.5 ukazuje tabulku vstupních a výstupních signálů elementárního přepínače když řídící signál u=1.

Obr.6 zobrazuje tabulku vstupních a výstupních signálů elementárního přepínače když řídící signál u=0.

Příklady provedení vynálezu

Nyní bude vynále vysvětlen v zobecněném diagramu blokové konverze dat nárokované metody podle Obr.1, kde

P je řízený transpoziční blok; A a B jsou konvertované n-bitové podbloky; K_{4r}, K_{4r-1}, K_{4r-2}, K_{4r-3}, jsou n-bitové elementy tajného klíče (n-bitové podklíče); V je binární vektor generovaný na základě vstupních dat; symbol ⊕ znamená operaci bitový součet modulo 2; značka □⊕ označuje operaci součtu modulo n, kde n délka datového podbloku v bitech. Silné nepřerušované čáry označují n-bitovou signální přenosovou sběrnici, tenké nepřerušované čáry označují přenos jednoho bitu, tlusté tečkované čáry označují přenos jednoho řídícího bitu. Silné tečkované čáry označují n bitovou řídící přenosovou sběrnici, n řídících signálů, což jsou bity podklíče nebo bity binárního vektoru. Použití bitů podklíče jako řídících signálů zajišťuje vytváření specifické modifikace operace transponující podblok závislou na hodnotě vstupního bloku, což dále zlepšuje kryptografickou odolnost konverze.

Obr.1 ukazuje jedno kolo konverze. V závislosti na specifické implementaci řízeného transpozičního bloku a požadované rychlosti konverze, může být použito od 2 do 16 kol. Toto schema kryptografické konverzní procedury může být použito pro šifrování a jednosměrné konverze. V posledně zmíněném případě není tajný klíč použit a narozdíl o signálů podklíče je na vstup bloku P přiveden vektor V vygenerovaný na základě hodnotu konvertovaného v mezilehlých konverzních krocích. Při šifrování mohou být použity stejné čtyři n-bitové podklíče K_4, K_3, K_2, K_1 při každém kole šifrování. V tomto případě, kde je typická velikost podbloku n=32, délka tajného klíče je 128 bitů. Když je použit tajný klíč o větší délce, každé kolo může použít K_{4r}, K_{4r-1}, K_{4r-2}, a K_{4r-3}. Na příklad, je-li číslo kola r=3,

první kolo použije podklíče K_4, K_3, K_2, K_1 a druhé kolo potom K_8, K_7, K_6, K_5, třetí kolo pak použije podklíče K_{12}, K_{11}, K_{10}, K_9.

Možnosti technických implementací nárokované metody jsou popsány se svými specifickými implementacemi.

Příklad 1:

Tento příklad se týká metody pro šifrování dat. Tajný klíč je prezentován ve formě čtyř podklíčů K_{4r}, K_{4r-1}, K_{4r-2}, a K_{4r-3}. Jedno kolo šifrování je popsáno jako následující procedurální posloupnost:

1. Konvertuj podblok A podle výrazu:

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

   kde "$\leftarrow$" značí operaci přiřazení.

2. Konvertuj podblok B podle výrazu:

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

3. V závislosti na hodnotě podbloku A a na podklíči K_{4r-1} ovlivni transpozici bitu v podbloku.

4. Konvertuj podblok A podle výrazu:

   $A \leftarrow A \oplus B$

5. V závislosti na hodnotě podbloku B a na podklíči K_{4r} ovlivni transpozici bitů v podbloku A.

5. Konvertuj podblok B podle výrazu:

   $B \leftarrow B \oplus A$

Příklad 2:

Tento příklad popisuje jedno kolo jednosměrné konverze podle následující procedurální posloupnosti:

1. Generuj binární vektor V:

   $V \leftarrow A \lll B$.

2. Konvertuj podblok B podle výrazu:

   $B \leftarrow B \otimes V$.

3. Generuj binární vektor V v závislosti na jeho hodnotě z předchozího kroku a na hodnotách podbloků A a B podle vzorce:

   $V \leftarrow (V \lll A) \oplus (B \lll 13)$.

4. Konvertuj podblok A podle výrazu:

   $A \leftarrow A \oplus V$.

5. V závislosti na hodnotě A a V ovlivni transpozici bitů v podbloku B.

6. Konvertuj podblok A podle výrazu:

   $A \leftarrow A \otimes B$.

7. Generuj binární vektor V:

   $V \leftarrow (V \lll B) \oplus (A \lll 11)$.

8. V závislosti na hodnotách B a V ovlivni transpozici bitů v podbloku A.

9. Konvertuj podblok B podle výrazu:

   $B \leftarrow B \oplus A$.

Obr.2 ukazuje možnou realizaci řízeného transpozičního bloku s použitím elementárních přepínačů S. Tato realizace odpovídá bloku P s 8-bitovým vstupem pro datové signály a 8-bitovým vstupem pro řídící signály označené tečkovanými čarami podobně jako na Obr.1.

Počet různých verzí operace transpozice je roven počtu možných kódových kombinací na řídícím vstupu a je to pro blok P se strukturou na Obr.2 $2^8=256$, což je více než počet cyklických operací posunu použitých v nejbližších podobných metodách se stávajícího stavu techniky. S použitím podobné metody je možné vymyslet schema pro blok P libovolnou velikostí vstupních dat a řídících signálů, zvláště pak blok P s 32-bitovým vstupem prodata a 32-bitovým vstupem pro řídící signály. V posledně zmíněném případě je dosaženo počtu různých variací operace transpozice roven $2^{32} > 10^9$.

Obr.3 ukazuje strukturu bloku řízené transpozice mající 32-bitový datový vstup a 79-bitový řídící vstup. Tento blok řízené transpozice implementuje unikátní transpozici vstupních binárních bitů pro každou možnou hodnotu kódové kombinace na řídícím vstupu, kde těchto možností je 2^{79}. Externí informace vstupující do transpozičního bloku je označena jako i1, i2,…, i32, externí výstupy jsou označeny jako o1, o2, … , o32, a ří-

dící vstupy jsou označeny jako c1, c2, … , c79. Elementární přepínače S jsou spojeny takovým způsobem, že tvoří matici z 31 řad.V první řadě je spojeno 31 elementárních přepínačů, ve druhé řadě 30, ve třetí řadě 29 atd. V každé další řadě je počet elementárních přepínačů menší o jeden. V nejnižší řadě 31 je zapojen 1 elementární přepínač.

Počet j≠31 řad má 33 vstupů j, 33 výstupů j a 32 řídících vstupů j. Poslední (nejpravější) výstup j-té řady je externí výstup řídícího transpozičního bloku, zbývajících 32 výstupů j z j-té řady je zapojeno do odpovídajících vstupů řady (j+1). Poslední řada 31 ma dva výstupy oba z nich jsou externí výstupy řízené transpoziční jednotky. Samostatný řídící signál (u=1) je přiveden do maximálně jednoho řídícího vstupu v každé řadě. K tomuto slouží binární 32 bitové dešifrátory F_1, F_2,…, F_{15} a binární 16 bitový dešifrátor F_{16}. Dešifrátory F_1, F_2,…, F_{15} mají pět externích řídících vstupů do kterých je přiveden libovolný 5-bitový binární kód a 32 výstupů. Dešifrátor generuje unitární signál jen na jednom výstupu. Na zbývajících 31 vstupech zůstává signál nula. Dešifrátor F_{16} má 4 výstupy na které je přivedena libovolná binární hodnota a 16 výstupů, kde pouze na jednom z nich je unitární hodnota jedna. Pro všechny dešifrátory F_1, F_2,…, F_{15} a F_{16} platí, že každá binární hodnota na vstupu definuje unikátní možnou výstupní hodnotu ve které je unitární signál (u=1) nastaven.

Část výstupu dešifrátorů F_h, kde h<=15, je připojena na řídící vstupy h-té řady (32 vstupů h), zatímco část vstupů je připojena na řídící vstupy (32-h) řad (zbývající výstupy dešifrátoru). Řídící signál (u=1) je nastaven v každé řadě na nejvýše jeden elementární přepínač. Vstup řady připojený k pravému vstupu elementárního přepínače, kde kterému je přiveden unitární řídící signál je zaměněn externím výstupem řízeného transpozičního bloku vedoucího k této řadě. Jestliže je unitární řídící signál přiveden k nejlevějšímu elementárnímu přepínači, potom externí výstup z řízeného transpo-

zičního bloku (blok P) je zaměněn s nejlevější vstupem řady. První řada zamění jeden z externích vstupů i1, i2, …, i32 bloku P s externím výstupem o1, zatímco zbývajících 31 externích vstupů se zamění se vstupy druhé řady. Druhá řada přivede jeden ze zbývajících 31 externích vstupů na externí výstup o2, zatímco zbývajících 30 externích vstupů je přivedeno na vstupy třetí řady atd. Tato struktura bloku P implementuje unikátní transpozici vstupních bitů pro každou hodnotu binárního kódu přivedeného na 79-bitový řídící vstup bloku P.

Například je možná následující verze použití 79-bitového vstupu v schematu kryptografické konverze, viz Obr.1. 32 bitů je použito jako řídící signály, například podbloku B a 47 bitů tajného klíče. Podobně může být například použito 32 bitů podklíče K_{4r-1} a 15 bitů podklíče K_{4r-2}. V tomto případě, když je zadán tajný klíč do šifrovacího zařízení, v závislosti na těchto 47 šifrovacích bitech je vygenerována jedna z 2^{47} různých modifikací operace bitové transpozice, v závislosti na hodnotě vstupního bloku. Zde každá modifikace této operace zahrnuje 2^{32} různých operací transpozice bitů podbloku A, kde jejich výběr je dán hodnotou podbloku B. Výběr modifikace je nepředvídatelný, protože je určen tajným klíčem. Toto dále zvyšuje odolnost kryptografické konverze. Jestliže šifrovací zařízení použije 4 bloky P se strukturou z Obr.3, potom počet možných kombinací modifikací transpozičních operací na bloku P závisí na tajném klíči a může nastaven až na $(2^{47})^4=2^{188}$ - s použitím tajného klíče s délkou alespoň 188 bitů.

Obr.4 vyjasňuje funkci elementárního přepínače, kde u je řídící signál, a a b jsouvstupní datové signály a c a d jsou výstupní datové signály.

Tabulky na Obr.5 a 6 demonstrují závislosti výstupních signálů na vstupních a řídících signálech. Z těchto tabulek je zřejmé, že když je u=1, vstup a je přiveden na výstup c a

vstup b na výstup d. Když je u=0, vstup a je přiveden na výstup d a vstup b na výstup d.

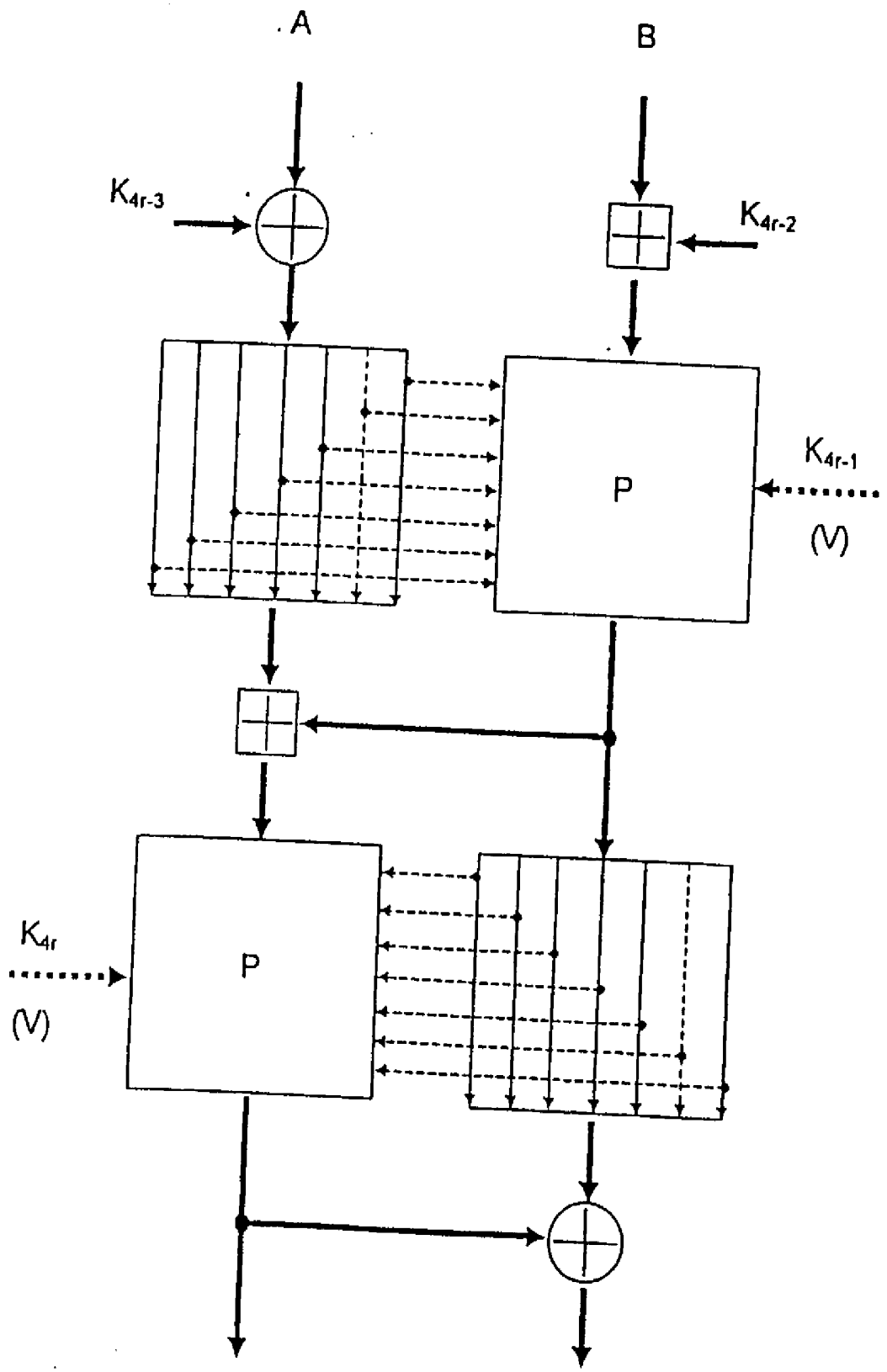
Tato jednoduchá struktura umožňuje moderním planárním technologiím výroby integrovaných obvodů lehce vyprodukovat kryptografické mikroprocesory obsahující řízené transpoziční bloky s velikostí vstupních dat 32 a 64 bitů.

Výše uvedené příklady ukazují, že předkládaná metoda pro kryptografickou konverzi binárních datových bloků je technicky proveditelná a řeší problémy zmíněné v úvodu.

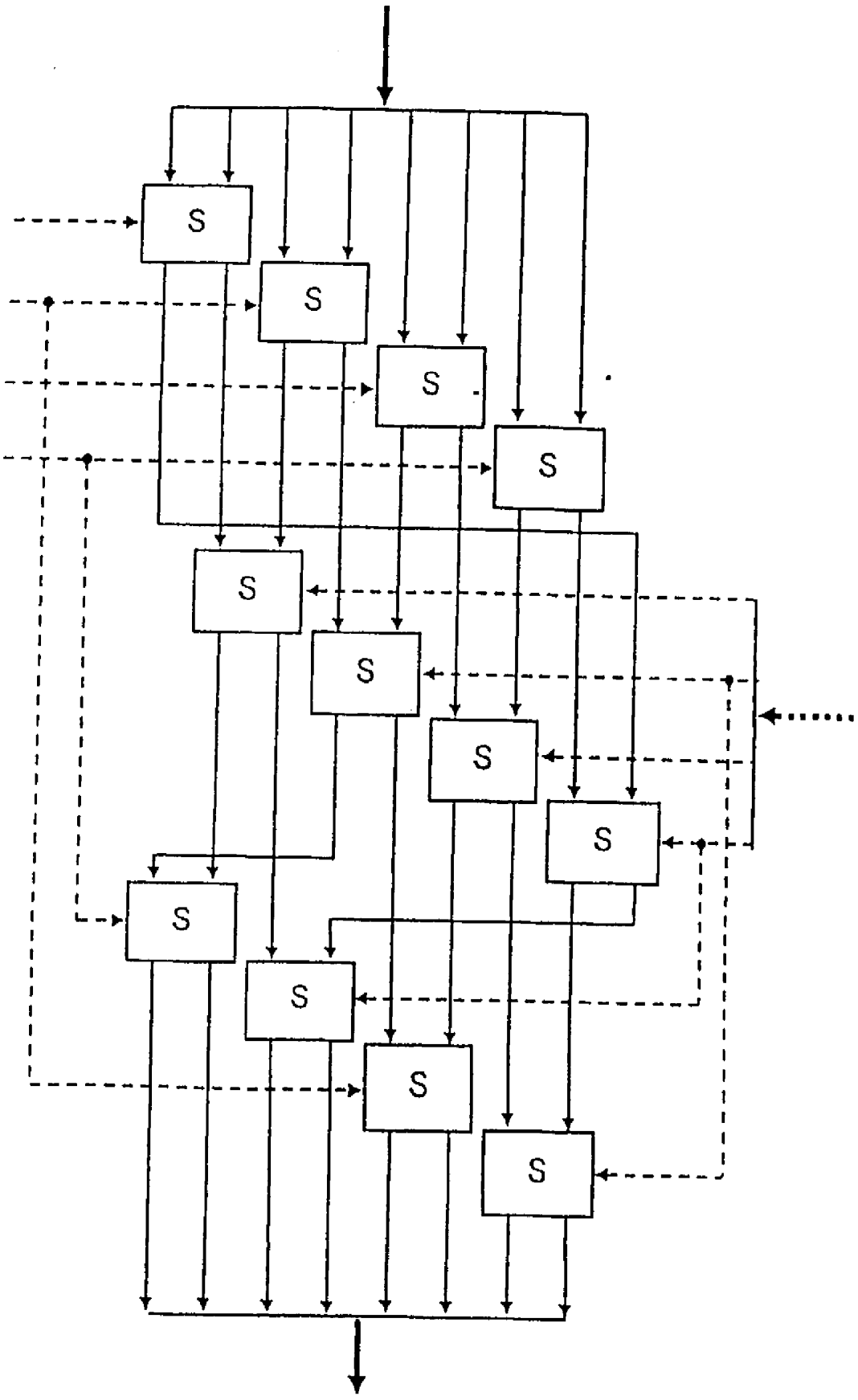
Nárokovaná metoda může být realizována například jako specializovaný kryptografický procesor s rychlostí šifrování v řádu 1 Gbit/sec, což je postačující pro šifrování dat přenášených ve vysokorychlostních komunikačních kanálech optických vláken v reálném čase.

P A T E N T O V É N Á R O K Y

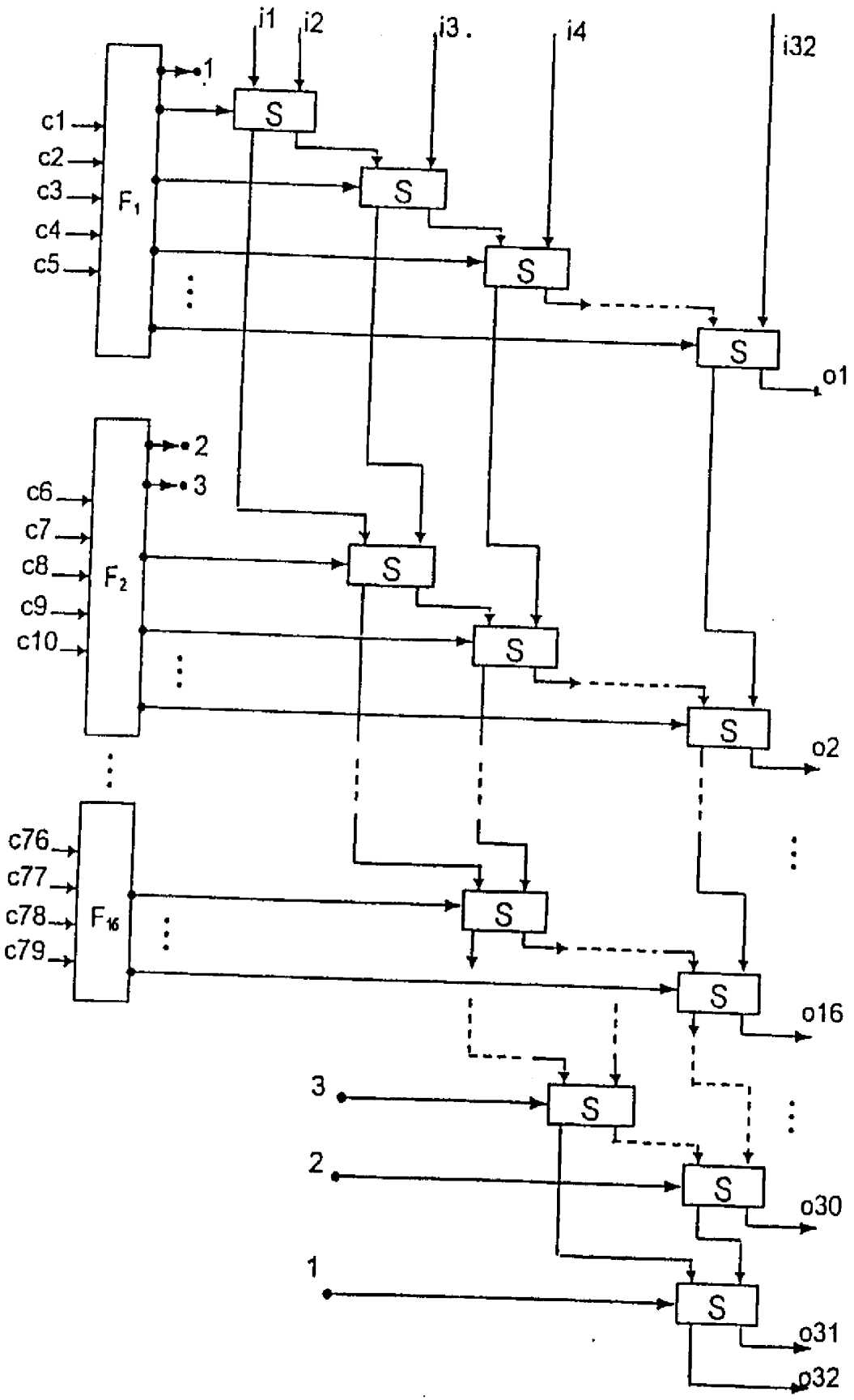
1. Způsob kryptografické konverze binárních datových bloků používající metodu dělení zmíněných datových bloků do N≥2 podbloků, střídavou konverzi zmíněných datových bloků prací s i-tým podblokem, kde i≤N a kde alespoň jedna operace konverze závisí na hodnotě j-tého podbloku, v y z n a č u j í c í s e t í m , že operace transpozice bitů i-tého podbloku je použita jako operace závislá na hodnotě j-tého podbloku, kde j≤N.
2. Způsob podle nároku 1, v y z n a č u j í c í s e t í m, že zmíněná operace transponování bitů zmíněného i-tého podbloku, která závisí na hodnotě j-tého podbloku je generována v závislosti na tajném klíči před začátkem konverze i-tého podbloku.
3. Způsob podle nároku 1, v y z n a č u j í c í s e t í m, že před provedením aktuální operace transponování bitů zmíněného i-tého podbloku, který závisí na hodnotě zmíněného j-tého podbloku, je dále vygenerován binární vektor V s tím, že zmíněná operace transpozice bitů zmíněného i-tého podbloku je prováděna v závislosti na hodnotě V, kde zmíněný binární vektor je vygenerován v závislosti na jeho hodnotě v čase provádění předchozího kroku konverze zmíněných podbloků a závisí na hodnotě j-tého podbloku.



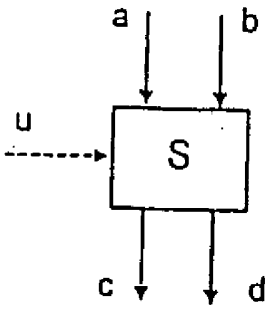
obr. 1



obr. 2


i1
i2
i3.
i4
i32
1
c1
c2
c3
c4
c5
F1
S
o1
2
3
c6
c7
c8
c9
c10
F2
o2
c76
c77
c78
c79
F16
o16
3
2
1
o30
o31
o32

obr. 3



obr. 4

u=1

VSTUP		VÝSTUP	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

obr. 5

u=0

VSTUP		VÝSTUP	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

obr. 6