PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:
2003 - 1598

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
G 06 F 7/58

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **14.09.2001**

(32) Datum podání prioritní přihlášky: **08.12.2000**

(31) Číslo prioritní přihlášky: **2000/10061315**

(33) Země priority: **DE**

(40) Datum zveřejnění přihlášky vynálezu: **13.08.2003**
(Věstník č. 8/2003)

(86) PCT číslo: **PCT/EP01/10650**

(87) PCT číslo zveřejnění: **WO02/046912**

(71) Přihlašovatel:
DEUTSCHE TELEKOM AG, Bonn, DE;

(72) Původce:
Huber Klaus, Darmstadt, DE;
Heister Ulrich, Dieburg, DE;
Schaefer-Lorinser Frank, Ober-Ramstadt, DE;
Martin Tobias, Rabenau, DE;
Breitbach Thomas, Nickenich, DE;

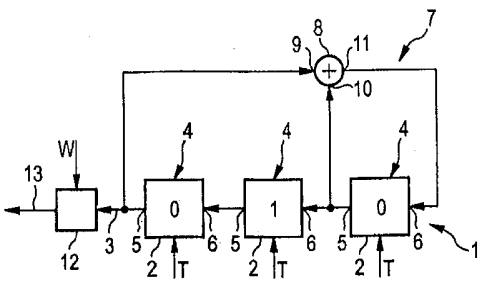
(74) Zástupce:
Fischer Michael Ing., Na Hrobci 5, Praha 2, 12800;

(54) Název přihlášky vynálezu:

Způsob a zařízení pro generování pseudonáhodné posloupnosti

(57) Anotace:

Prvky pseudonáhodné posloupnosti se posouvají posuvným registrem s více v sérii zapojenými paměťovými buňkami, tvořeným hardwarem nebo softwarem. S výstupními hodnotami alespoň dvou paměťových buněk se provádí početní operace a výsledek početní operace se ve zpětné vazbě přivádí na vstup jedné z paměťových buněk posuvného registru, přičemž podle řešení se prvky (γ) pseudonáhodné posloupnosti diskrétně logaritmují a s výhodou se diskrétní logaritmování provádí modifikovaně, při početní operaci výstupních hodnot posuvných registrů, vícekrát nebo se diskrétně logaritmuje podle tabulky, pomocí Zech-logaritmu, popřípadě Jacobi-logaritmu. Zařízení pro generování pseudonáhodné posloupnosti zahrnuje posuvný registr s více v sérii zapojenými paměťovými buňkami, zpětnovazební větví, která spojuje dva různé výstupy registru se vstupem registru a s obvodem realizujícím početní operaci s výstupními hodnotami registru. Obvod realizující početní operaci je ze vstupní strany spojen s výstupy registru a z výstupní strany se vstupem registru, vyznačující se obvodem (12) pro diskrétní logaritmování prvků (γ) presudonáhodné posloupnosti. Ve zpětnovazební větvi (7) je uspořádán obvod pro diskrétní logaritmování a vytváří obvod (8') realizující početní operaci, který diskrétně logaritmuje výstupní hodnoty stupňů (2) registru.



CZ 2003 - 1598 A3

PV 2003 - 1598
06.06.03

Způsob a zařízení pro generování pseudonáhodné posloupnosti

Oblast techniky

Vynález se týká způsobu generování pseudonáhodné posloupnosti, podle kterého se prvky pseudonáhodné posloupnosti posouvají posuvným registrem s více v sérii zapojenými paměťovými buňkami, tvořeným hardwarem nebo softwarem, s výstupními hodnotami alespoň dvou paměťových buněk se provádí početní operace a výsledek početní operace se ve zpětné vazbě přivádí na vstup jedné z paměťových buněk posuvného registru. Vynález se dále týká zařízení pro generování pseudonáhodné posloupnosti s posuvným registrem, zahrnujícím více v sérii zapojených paměťových buněk, zpětnovazební větví, která spojuje dva různé výstupy registru se vstupem registru, a s obvodem realizujícím početní operaci s výstupními hodnotami registru, přičemž je obvod realizující početní operaci ze vstupní strany spojen s výstupy registru a z výstupní strany se vstupem registru.

Dosavadní stav techniky

Při generování náhodných posloupností se zásadně rozlišují dvě varianty. Pravé náhodné posloupnosti se generují na základě fyzikálních efektů, například na základě radioaktivního rozpadu. Tyto pravé náhodné posloupnosti se mohou zejména používat v kryptografii. U jiných variant se pseudonáhodné posloupnosti generují pomocí zařízení, označovaného jako (pseudo)náhodný generátor. Toto zařízení se

může vytvořit například pomocí počítače, ve kterém probíhá příslušný algoritmus. Vedle této softwarové realizace se mohou pseudonáhodné posloupnosti generovat i pomocí hardware, realizovaného posuvnými registry, které jsou většinou spojeny lineární zpětnou vazbou. Základní rozdíl mezi pseudonáhodnými posloupnostmi a pravými náhodnými posloupnostmi může být tedy viděn v tom, že při znalosti obvodového uspořádání, popřípadě algoritmu, je možné opakování, popřípadě opětné generování téže samé pseudonáhodné posloupnosti. Způsob daného druhu a obvodové uspořádání pro generování pseudonáhodné posloupnosti jsou známy ze spisu EP 0 616 429 A1. Toto obvodové uspořádání je realizováno posuvným registrem se zpětnou vazbou, u kterého je uspořádáno více v sérii zapojených paměťových buněk (Flip-Flops). Alespoň dvě výstupní hodnoty různých paměťových buněk se přivedou do obvodu realizujícího početní operaci a tato početní operace se s nimi provede. Výsledek početní operace se vede zpět na vstup posuvného registru. Samozřejmě je použitelných více zpětnovazebních větví. Početní operace obou výstupních hodnot dvou paměťových buněk probíhá u známého způsobu, popřípadě u známého obvodového uspořádání, přičtením modulo 2, které se realizuje pomocí hradla exclusive-or. Tento známý způsob, popřípadě známé obvodové uspořádání, se například používá při tak zvaném proudovém šifrování. Cílem vynálezu je uvést další zdroj pro generování pseudonáhodné posloupnosti.

Podstata vynálezu

Nedostatky dosavadního stavu techniky podstatnou měrou odstraňuje a cíl vynálezu splňuje způsob generování

pseudonáhodné posloupnosti, podle kterého se prvky pseudonáhodné posloupnosti posouvají posuvným registrem s více v sérii zapojenými paměťovými buňkami, tvořeným hardwarem nebo softwarem, s výstupními hodnotami alespoň dvou paměťových buněk se provádí početní operace a výsledek početní operace se ve zpětné vazbě přivádí na vstup jedné z paměťových buněk posuvného registru, přičemž podle vynálezu se prvky (γ) pseudonáhodné posloupnosti diskrétně logaritmují. S výhodou se diskrétní logaritmování provádí modifikovaně. S výhodou se diskrétní logaritmování provádí již při početní operaci výstupních hodnot posuvných registrů. S výhodou se dále diskrétní logaritmování provádí vícekrát. S výhodou se diskrétně logaritmuje podle tabulky, zahrnující výstupní a výsledkové hodnoty. S výhodou se alespoň s jednou z výstupních hodnot, určených pro početní operaci, provede před touto početní operací předběžná početní operace s předem stanovitelnou hodnotou. S výhodou se jako předběžná početní operace provádí logická početní operace, výhodně sčítání. S výhodou se předběžná početní operace provádí na základě tabulky pro předběžnou početní operaci, zahrnující výstupní a výsledkové hodnoty, nebo pomocí logických obvodů. S výhodou se diskrétní logaritmování provádí pomocí Zech-logaritmu, popřípadě Jacobi-logaritmu. S výhodou se tabulka logaritmů odvozuje od Zech-logaritmu, popřípadě Jacobi-logaritmu. S výhodou se zpětná vazba realizuje tak, že se vytváří pseudonáhodná posloupnost o maximální délce periody. Nedostatky dosavadního stavu techniky podstatnou měrou odstraňuje a cíl vynálezu splňuje zařízení pro generování pseudonáhodné posloupnosti, s posuvným registrem, zahrnujícím více v sérii zapojených paměťových buněk, zpětnovazební větví, která spojuje dva různé výstupy registru se vstupem registru,

a s obvodem realizujícím početní operaci s výstupními hodnotami registru, přičemž je obvod realizující početní operaci ze vstupní strany spojen s výstupy registru a z výstupní strany se vstupem registru, vyznačující se obvodem pro diskrétní logaritmování prvků (γ) pseudonáhodné posloupnosti. S výhodou je ve zpětnovazební větvi uspořádán obvod pro diskrétní logaritmování a vytváří obvod realizující početní operaci, který diskrétně logaritmuje výstupní hodnoty stupňů registru. S výhodou je obvodem realizujícím početní operaci paměťový obvod, ve kterém je uložena tabulka logaritmů, zahrnující výstupní a výsledkové hodnoty. S výhodou je mezi jedním z výstupů registru a obvodem realizujícím početní operaci uspořádán obvod realizující předběžnou početní operaci, jehož jeden vstup je spojen s tímto výstupem stupně registru, jehož druhý vstup je ovladatelný předem stanovitelnou hodnotou, a jehož výstup je spojen se vstupem obvodu realizujícího početní operaci. S výhodou je obvodem realizujícím předběžnou početní operaci logický obvod. Prvky pseudonáhodné posloupnosti se diskrétně logaritmují. Tím oproti známému způsobu vzniká nová pseudonáhodná posloupnost. Výraz diskrétně logaritmovat znamená, že se nelogaritmuje pseudonáhodná posloupnost jako celek, nýbrž jednotlivé prvky pseudonáhodné posloupnosti. Může být při tom uvažováno, že se dvěma prvky pseudonáhodné posloupnosti logaritmováním spojí. Podle jednoho obzvláště výhodného příkladu provedení se diskrétně logaritmuje modifikovaně. Protože není logaritmus v nule definován, tak se -pokud nějaký prvek nabude hodnoty nula- logaritmování neprovádí, nýbrž se potom dosadí předem stanovitelná hodnota. Podle jednoho výhodného příkladu provedení se diskrétní logaritmování provádí již při provádění početní operace s výstupními hodnotami stupňů posuvného

registru. Zásadně by však také bylo myslitelné nejdříve generovat pseudonáhodnou posloupnost a následně na výstupu řetězce posuvného registru provádět diskrétní logaritmování, jak je to popsáno výše. Samozřejmě je možné provádět diskrétní logaritmování vícekrát. Tím se mohou zase generovat jiné pseudonáhodné posloupnosti. Podle jednoho výhodného příkladu provedení se předpokládá, že se diskrétně logaritmuje na základě tabulky logaritmů, zahrnující výstupní a výsledkové hodnoty. To znamená, že se výstupní hodnota paměťové buňky srovnává s hodnotami tabulky logaritmů, zvolí se výsledek, hodící se k výstupní hodnotě, a ten se jako výsledek početní operace dále předá na vstup paměťové buňky. Podle jednoho příkladu provedení se předpokládá, že se s jednou z těchto výstupních hodnot, se kterými se pak provádí početní operace, před touto početní operací, tedy před diskrétním logaritmováním, provede ještě předběžná početní operace s předem stanovitelnou hodnotou. Zejména je pro tuto předběžnou početní operaci uvažována logická početní operace, výhodně sčítání. Jestliže se tedy při sčítání provede s výstupní hodnotou posuvného registru početní operace s nulou, je tím zpětnovazební větev zapojena, popřípadě aktivní, protože se vždy dále předává výstupní hodnota posuvného registru. Jestliže se s výstupní hodnotou posuvného registru provede početní operace s jedničkou, mohla by se tím zpětnovazební větev odpojit. Samozřejmě jsou pro předběžnou početní operaci použitelné i jiné, od nuly nebo jedničky se lišící, předem stanovitelné hodnoty. Podle jednoho příkladu provedení se může předpokládat, že se předběžná početní operace provádí na základě tabulky pro předběžnou početní operaci, zahrnující výstupní a výsledkové hodnoty, nebo pomocí logických obvodů. Jeden obzvláště výhodný příklad provedení se vyznačuje tím, že

se diskrétní logaritmování provádí pomocí tak zvaného Zech-logaritmu, popřípadě Jacobi-logaritmu. Jestliže se diskrétní logaritmování provádí na základě výše zmíněné tabulky, jsou výsledkové hodnoty v této tabulce stanoveny pomocí Zech-logaritmu, popřípadě Jacobi-logaritmu. Tabulka logaritmů tedy spočívá na samo o sobě známých Zech-logaritmech, popřípadě Jacobi-logaritmech. Jeden obzvláště výhodný příklad provedení se vyznačuje tím, že je zpětná vazba realizována tak, že se vytváří pseudonáhodná posloupnost o maximální délce periody. To znamená, že se na určitých výstupech stupňů posuvného registru uvažuje alespoň jedna zpětnovazební větev. Pro stanovení zpětnovazebních připojení, popřípadě zpětnovazební větve, které poskytují maximální délku periody pseudonáhodné posloupnosti, jsou v příslušné literatuře známy tabulky (například W. Peterson, E. Weldon, Error-Correcting Codes, second Edition, MIT Press, Cambridge, seventh printing 1984 nebo R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press 1984). Zařízení pro generování pseudonáhodné posloupnosti zahrnuje více v sérii zapojených paměťových buněk, které tvoří posuvný registr. Dále je uvažována zpětnovazební větev, která spojuje dva různé výstupy registru se vstupem registru. Kromě toho je uspořádán obvod realizující početní operaci s výstupními hodnotami stupňů registru, který je ze vstupní strany spojen s výstupy registru a z výstupní strany se vstupem registru. Podle vynálezu se zařízení vyznačuje obvodem pro diskrétní logaritmování prvků pseudonáhodné posloupnosti. Zařízením podle vynálezu se tedy realizuje další zdroj pro generování pseudonáhodných posloupností, který poskytuje pseudonáhodné posloupnosti, které jsou rozdílné oproti náhodným posloupnostem, známým ze stavu techniky. Výhodný je příklad provedení, u kterého obvod

pro diskrétní logaritmování leží ve zpětnovazební větvi a vytváří obvod realizující početní operaci, který diskrétně logaritmuje výstupní hodnoty registrů. Alternativně se však také může uvažovat, že je obvod pro diskrétní logaritmování uspořádán na konci řetězce posuvného registru, jak je to výše vysvětleno v souvislosti se způsobem podle vynálezu. Výhodný je příklad provedení, u kterého je obvodem paměťový obvod, ve kterém je uložena tabulka logaritmů, zahrnující výstupní a výsledkové hodnoty. Alternativně může být obvod také realizován logickými moduly, tedy hardwarově. U jednoho příkladu provedení se předpokládá, že je mezi jedním z výstupů registru a obvodem realizujícím početní operaci uspořádán obvod realizující předběžnou početní operaci, jehož jeden vstup je ovladatelný tímto výstupem registru, jehož druhý vstup je ovladatelný předem stanovitelnou hodnotou, a jehož výstup je spojen se vstupem obvodu realizujícího početní operaci. Tím je myslitelné zapojit a odpojit, tedy aktivovat nebo deaktivovat zpětnovazební větev, popřípadě více zpětnovazebních větví. Obvod realizující předběžnou početní operaci může být logickým obvodem, zejména hradlem exclusive-or. Obvod realizující předběžnou početní operaci může však být u alternativního příkladu provedení realizován rovněž paměťovým obvodem, ve kterém jsou uloženy výsledky předběžné početní operace v závislosti na vstupních hodnotách.

Přehled obrázků na výkresech

Způsob a zařízení pro generování pseudonáhodné posloupnosti podle vynálezu jsou objasněny pomocí výkresů, na kterých znázorňuje obr. 1 lineárně zpětnovazebně zapojený

binární posuvný registr s obvodem pro diskrétní vytváření logaritmu, obr. 2 lineárně zpětnovazebně zapojený ternární posuvný registr s obvodem pro diskrétní vytváření logaritmu, obr. 3 obecný lineárně zpětnovazebně zapojený posuvný registr s obvodem pro diskrétní vytváření logaritmu, obr. 4 lineárně zpětnovazebně zapojený posuvný registr nad souborem GF (2^2) = GF (4), obr. 5 lineárně zpětnovazebně zapojený posuvný registr nad souborem GF (2^2) = GF (4), přičemž obvod pro diskrétní vytváření logaritmu je uspořádán ve zpětnovazební větvi a obr. 6 obecný lineárně zpětnovazebně zapojený posuvný registr, který má ve zpětnovazebních větvích obvod pro diskrétní vytváření logaritmu.

Příklady provedení

Obr. 1 znázorňuje pouze pro ilustraci sloužící příklad řetězce 1 posuvného registru, který má počet m v sérii zapojených paměťových buněk 4. Vstup jednoho stupně posuvného registru je tedy spojen s výstupem před ním zapojeného stupně posuvného registru. Tento poslední stupeň posuvného registru tvoří výstup 3 řetězce 1 posuvného registru, na kterém je snímatelná generovatelná pseudonáhodná posloupnost. Pro generování pseudonáhodných posloupností se ve většině případů používají tyto tak zvané lineárně zpětnovazebně zapojené řetězce 1 posuvných registrů, které mohou být vytvářeny v integrovaném tvaru hardwarově, tedy pomocí rychlých logických modulů, čímž se může dosáhnout velmi vysoké pracovní rychlosti. Jak již bylo výše zmíněno, znázorňuje obr. 1 jeden takovýto binární řetězec posuvného registru. Každý stupeň 2 posuvného registru je ovládán taktováním T, takže se při

každém taktu načte do paměťové buňky 4 hodnota, nacházející se na vstupu stupně 2 posuvného registru, a poskytne se na výstupu 5 registru prvek pseudonáhodné posloupnosti, odložený dříve v paměťové buňce 4. Pro taktování jsou zejména uspořádány centrální hodiny. Každá paměťová buňka je na obr. 1 opatřena vstupy 6. Ve zpětnovazební větvi 7 binárního řetězce 1 posuvného registru je uspořádán obvod 8 realizující početní operaci, jehož vstupy 9 a 10 jsou spojeny s výstupy 5 registru. Výstup 11 obvodu 8 realizujícího početní operaci je spojen se vstupem 6 jednoho stupně posuvného registru, výhodně prvního. U uvedeného příkladu provedení je obvodem realizujícím početní operaci sčítací zařízení, které sčítá výstupní hodnoty registrů, nacházejících se na vstupech 9 a 10, přičemž platí 0 + 0 = 0, 0 + 1 = 1 + 0 = 1 a 1 + 1 = 0 mod 2. Toto sčítání modulo 2 může být obzvláště jednoduše provedeno pomocí logického hradla, které je realizováno jako hradlo exklusive-or. Tím se ozřejmí, že při počátečním obsazení paměťových buněk 4 řetězce 1 posuvného registru, znázorněném na obr. 1, může být generována pseudonáhodná posloupnost s prvky 0100111010.... Tato pseudonáhodná posloupnost leží na výstupu 3 řetězce posuvného registru, popřípadě může být na tomto výstupu 3 snímána. Předpokládá se, že se pseudonáhodná posloupnost, poskytnutá na výstupu 3, diskrétně logaritmuje. K tomu účelu je za výstupem 3 zapojen logaritmický obvod 12, který provádí diskrétní logaritmování prvků pseudonáhodné posloupnosti. Pro diskrétní logaritmování se může uvažovat, že se provádí početní operace jednoho prvku pseudonáhodné posloupnosti s druhým prvkem pseudonáhodné posloupnosti. Může se však také uvažovat, že se provádí početní operace prvku pseudonáhodné posloupnosti s předem stanovitelnou hodnotou W, kterou lze přivést do obvodu 12. Na

výstupu 13 obvodu se potom vyskytuje diskrétně logaritmovaná pseudonáhodná posloupnost. Výhodně se provádí modifikované diskrétní logaritmování, to znamená, že pokud má prvek pseudonáhodné posloupnosti hodnotu 0, tak se obvod nastaví na předem stanovitelnou výsledkovou hodnotu, protože vytváření logaritmu v 0 není ze známých důvodů možné. Výhodou lineárně zpětnovazebně zapojeného řetězce 1 posuvného registru je to, že je relativně jednoduché určit parametry, aby se dosáhlo maximální možné délky periody pseudonáhodné posloupnosti. Jako parametr jsou zde uvedeny výstupy 5 registru, s jejímiž výstupními hodnotami se musí provést početní operace v obvodu 8 realizujícím početní operaci. Musí být tedy uvedeno umístění zpětnovazebních přípojů, přičemž je také třeba uvést, na který vstup 6 registru musí být přiveden výstup 11 obvodu realizujícího početní operaci. Binárně lineárně zpětnovazebně zapojený řetězec 1 posuvného registru o délce m, tedy počtu stupňů 2 posuvného registru, může generovat pseudonáhodnou binární posloupnost, která se opakuje teprve po $2^m - 1$ bitech. Tabulky se zpětnovazebními přípoji, které udávají maximální délku periody, můžeme nalézt v literatuře (například W. Peterson, E. Weldon, Error-Correcting Codes, second Edition, MIT Press, Cambrigde, seventh printing 1984 nebo R. Lidl, H. Niederreiter, Finite Fields, Cambrigde University Press, 1984). Samozřejmě je také možné místo binárních posloupností posuvného registru využívat nebinární posloupnosti. Jeden nebinární řetězec 1 posuvného registru je znázorněn na obr. 2. Na rozdíl od řetězce 1 posuvného registru podle obr. 1 je mezi vstupem 10 obvodu 8 realizujícího početní operaci a výstupem 5 registru doplňkově zapojen obvod 14 realizující předběžnou početní operaci. Ten má dva vstupy 15 a 16, jakož i výstup 17, který je připojen na vstup 10 obvodu 8 realizujícího početní

operaci. Obvod 14 realizující předběžnou početní operaci provádí u výhodného příkladu provedení násobení. U řetězce 1 posuvného registru představují tedy obvod 8 realizující početní operaci a obvod 14 realizující předběžnou početní operaci sčítání a násobení modulo 3, to znamená, že se provádí sčítání, popřípadě násobení čísel z množiny {0, 1, 2} a z výsledku, který je větší než 2, se substrahuje hodnota 3. Z toho vyplývá na výstupu 3 řetězce 1 posuvného registru pseudonáhodná posloupnost s prvky 00111021121010022201221202001.... Tato pseudonáhodná posloupnost se - tak jako u řetězce 1 posuvného registru podle obr. 1 - přivádí do logaritmického obvodu 12. Další rozdíl spočívá v tom, že je ve zpětnovazební větvi 7 uspořádán další násobící obvod 18, který je vytvořen identicky jako obvod 14 realizující předběžnou početní operaci. Vstup 19 násobícího obvodu je spojen s výstupem 11 obvodu 8 realizujícího početní operaci. Druhý vstup 20 násobícího obvodu získává pro funkci modulo 2 příslušný vstupní parametr. Výstup 21 násobícího obvodu 18 je spojen se vstupem 6 prvního stupně 2 posuvného registru. Ostatní stejné, popřípadě stejně působící části jako na obr. 1, jsou na obr. 2 opatřeny týmiž vztahovými značkami. Obr. 3 znázorňuje řetězec 1 posuvného registru, který jako abeceda GF(q) používá tak zvaný rozšiřující binární soubor s $q = 2^m$. Binární rozšiřující soubory jsou výhodné, protože tyto napomáhají zpracování dat v běžném binárním formátu. Lineárně zpětnovazebně zapojený řetězec 1 posuvného registru má potom tvar, znázorněný na obr. 3. Jsou zde tedy uspořádány - tak jako na obr. 2 - obvody 14 realizující předběžnou početní operaci, které leží vždy mezi výstupem jednoho stupně posuvného registru a vstupem obvodu 8 realizujícího početní operaci. Jak vyplývá z obr. 3, může být každý výstup 5

posuvného registru zpětnovazebně zapojen přes obvod 14 realizující předběžnou početní operaci a obvod 8 realizující početní operaci, tedy být veden na vstup 6 druhého stupně posuvného registru, přičemž se samozřejmě početní operace, prováděné v souvislosti s obr. 1 a obr. 2, provádějí v obvodech 14 realizujících předběžnou početní operaci a obvodech 8 realizujících početní operaci. Stejné, popřípadě stejně působící části, jsou na obr. 3 opatřeny stejnými vztahovými značkami jako na obr. 1 a obr. 2. Podle obr. 3 se v následujícím posuzuje řetězec 1 posuvného registru nad abecedou GF(q), přičemž GF(q) charakterizuje soubor s $q = p^m$ prvky, přičemž q představuje mocninu prvočísla. Ukazuje se, že struktura lineárně zpětnovazebně zapojených stupňů posuvného registru je ve srovnání se stavem techniky v podstatě zachována. Ovšem se, tak jak je to znázorněno na obr. 1 až obr. 4, operuje s pseudonáhodnou posloupností pomocí prostředků nepatrně modifikovaného diskrétního vytváření logaritmu, přičemž potřebné výpočetní operace pro vytváření logaritmu se ukládají do množiny čísel, ve které jsou potřebné operace snadno proveditelné většinou výpočetních automatů / procesorů. Místo násobení v obvodu 14 realizujícím předběžnou početní operaci se nyní provádí sčítání modulo $p^m - 1$, a místo sčítání v obvodu 8 realizujícím početní operaci příslušná náhradní operace, přičemž tato náhradní operace může být prováděna například s tabulkou. V obvodu 8 realizujícím početní operaci může být tedy obsažena paměť pro takovouto tabulku, ze které se v závislosti na vstupních hodnotách volí příslušná výsledková hodnota. Získané pseudonáhodné posloupnosti jsou různé od posloupností, které se generují zpětnovazebně zapojenými posuvnými registry podle stavu techniky. Na základě struktury lineárně zapojeného řetězce

posuvného registru se dá ovšem exaktně určovat délka periody pseudonáhodné posloupnosti. Délka periody je dána délkou periody podléhajícího posuvného registru. Jestliže se například vezme řetězec 1 posuvného registru, znázorněný na obr. 4, s počtem m = 3 stupně posuvného registru nad souborem GF (2^2) = (00, 01, 10, 11), tak se získá pseudonáhodná posloupnost s délkou periody $4^3 - 1 = 63$. Na obr. 4 jsou v paměťové buňce 4 každého stupně 2 posuvného registru znázorněny jednotlivé prvky souboru GF. Aby mohlo být s prvky souboru GF počítáno, mohou se v tomto souboru například použít obě dále uvedené tabulky pro sčítání a násobení. Tyto tabulky tedy obsahují výchozí hodnoty, jimž jsou jednoznačně přiřazeny příslušné výsledkové hodnoty. Tyto tabulky jsou tedy vyvolatelné a zpracovatelné v obvodech 8 realizujících početní operaci a obvodech 14 realizujících předběžnou početní operaci.

Tabulka sčítání

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Tabulka násobení

x	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Sčítání v binárních rozšiřovacích souborech GF je docela jednoduché, totiž pomocí komponentů realizované logické operace exklusiv-or, naproti tomu násobení je v rozšiřujících souborech komplikovanější. Může se provádět buď speciálními obvody nebo pomocí tabulek. S počátečním obsazením paměťových buněk 4, znázorněným na obr. 4, hodnotami 00, 00 a 01, se pro řetězec posuvného registru podle obr. 4 získá posloupnost 00 00 01 11 10 00 11 00 00 11 10 01 00 10 00 00 10 01 11 01.... Tato získaná pseudonáhodná posloupnost se - tak jako u výše uvedených příkladů podle obr. 1 a obr. 3 - diskrétně logaritmuje pomocí obvodu 12. Od popisu příslušných obrázků se tedy upouští. Místo obvodů 12, znázorněných na obr. 1 až obr. 4, pro omezené diskrétní vytváření logaritmu na výstupu 3 řetězce 1 posuvného registru, se v následujícím textu na základě obr. 5 a obr. 6 popisuje jeden výhodný příklad provedení řetězce 1 posuvného registru pro generování pseudonáhodných posloupností. Diskrétní transformací je - jak již bylo výše zmíněno - modifikované diskrétní vytváření logaritmů, které se dále níže podrobněji vysvětluje. Podstatný rozdíl vůči výše popisovaným příkladům provedení spočívá nyní v tom, použít struktury řetězce 1 posuvného registru lineárně zpětnovazebně zapojených stupňů 2 posuvného registru, provést početní operace v obvodu 8 realizujícím početní operaci a obvodu 14 realizujícím předběžnou početní operaci, nikoliv však tak, jak bylo výše popsáno, pomocí sčítání nebo násobení, nýbrž je nahradit diskrétním vytvářením logaritmu. To znamená, že se dosud na výstup 3 připojený obvod 12 nyní přeloží do zpětnovazební větve 7. Tím obvod 8 realizující početní operaci přebírá omezené diskrétní logaritmování. Potřebné výpočetní operace se překládají do číselné množiny, ve které mohou být potřebné početní operace výpočetními automaty / procesory

snadno prováděny. Místo násobení polem GAL v obvodu 14 realizujícím předběžnou početní operaci se v podstatě provádí sčítání modulo $p^m - 1$, a místo sčítání v obvodu 8 realizujícím početní operaci příslušná náhradní operace, která může být například prováděna pomocí logických modulů nebo také pomocí tabulky. Tato náhradní operace je na obr. 5 a obr. 6 vyznačena symbolem ~. Obvod 8´ realizující početní operaci ve zpětnovazební větvi 7, viz obr. 5, popřípadě obvody 8´ realizující početní operaci ve zpětnovazební větvi 7, viz obr. 6, provádějí tedy omezené diskrétní vytváření logaritmu. V obvodech 14 realizujících předběžnou početní operaci, popřípadě v obvodech 14´ realizujících předběžnou početní operaci, se naproti tomu provádí sčítání modulo $p^m - 1$. Funkce řetězců 1 posuvných registrů podle obr. 5 a obr. 6 se popisuje v následujícím textu. Je známo, že v konečném souboru GF (p^m) každého od 0 různého prvku γ souboru může být představena jako mocnina tak zvaného prvotního prvku α, to znamená, jako α^i pro $i = 0 \ldots p^m - 2$. Pro pole GAL GF (2^2) se například získá

i	$\gamma = \alpha^i$
0	01
1	10
2	11

Diskrétní logaritmus pro prvky γ souboru je definován následovně: $\log(\gamma) = i$ pro $\gamma = \alpha^i$, $i = 0 \ldots p^m-2$.
Jestliže se k tomu nyní ještě připojí násobení $\log(\gamma) = p^m-1$ pro $\gamma = 0$, tak se získá pro podstatu vynálezu vhodná, nepatrně modifikovaná definice diskrétního logaritmu.
Pro případ GF (2^2) se získá pro prvky γ následující tabulka:

γ	$\log(\gamma)$
00	11 (odpovídá 3)
01	00 (odpovídá 0)

10 01 (odpovídá 1)

11 10 (odpovídá 2)

Tabulka logaritmů

V této tabulce jsou celočíselné hodnoty log(γ) zobrazeny v binárním znázornění. Kvůli matematické korektnosti budiž zmíněno, že vytváření logaritmu vede na celočíselné hodnoty a nikoliv na prvky konečného souboru. To však není pro využití prvků, tedy bitů, pseudonáhodných posloupností relevantní. Zavedená definice pro logaritmus nuly vede k tomu, že logaritmická funkce se stane bijektivní (jednojednoznačnou) funkcí GF (p^m) na (0, 1, ... p^m-1). Logaritmováním pomocí diskrétního logaritmu o základu α = 10 se z pseudonáhodné posloupnosti, popisované v souvislosti s obr. 4, stane posloupnost 11 11 00 10 01 11 10 11 11 10 01 00 11 01 11 11 01 11 11 01 00 10 00 .... Tato posloupnost se dá generovat řetězcem 1 posuvného registru podle obr. 5.

Místo násobení v souboru pole GAL GF (q) = GF (2^2) se může v podstatě provádět sčítání modulo 2^2 - 1 = 3, a místo sčítání v konečném souboru operace ~, která se vysvětluje v následujícím textu. Počáteční obsazení paměťových buněk 4 podle obr. 4 se pomocí diskrétního logaritmu převede do počátečního obsazení paměťových buněk 4 obr. 5. Způsob se zejména hodí pro binární rozšiřující soubory. Pro čistě binární posuvný registr, viz obr. 1, to naproti tomu vede jen k záměně nul a jedniček. V následující tabulce jsou znázorněny početní operace v obvodu 8´ realizujícím početní operaci sčítání mod 3 a operaci ~ pro řetězec 1 posuvného registru podle obr. 5, tedy pro soubor GF (2^2).

(+) početní operace řetězce 1 posuvného registru podle obr. 5

(+)	00	01	10	11
00	00	01	10	11
01	01	10	00	11
10	10	00	01	11
11	11	11	11	11

~ početní operace řetězce 1 posuvného registru podle obr. 5

~	00	01	10	11
00	11	10	01	00
01	10	11	00	01
10	01	00	11	10
11	00	01	10	11

Obecný řetězec 1 posuvného registru pro binární rozšiřující soubor GF (2^m) je znázorněn na obr. 6. Pro řetězec 1 posuvného registru podle obr. 6 budiž ještě jednou souhrnně vyjádřeny jednotlivé kroky. Nejdříve se zvolí příslušný řetězec 1 posuvného registru podle obr. 3 s operacemi nad souborem GF (2^m). Následně se násobení polem GAL v podstatě nahradí sčítáním modulo $2^m - 1$. Rozdíl vůči sčítání modulo $2^m - 1$ je ten, že pro celé obsazení jedničkami leží výstup 3 rovněž celé obsazení jedničkami na výstupu. Sčítání GF (2^m) se nahrazuje operací ~, která se dá realizovat pomocí kombinační logiky nebo pomocí výše popsaných tabulek. Při realizování pomocí tabulek se může také použít Zech-logaritmus, popřípadě Jacobi-logaritmus. Aby se získal výsledek operace ~, může se potom dosadit:

$i \sim j = j \sim i = \log(\alpha^i + \alpha^i) = i + \log \alpha^{(i-z(i-j))}$ pro $i>j$

$i \sim j = 2^m - 1$ pro $i = j$,

přičemž je Zech-logaritmus definován rovnicí $\alpha^{z(k)} = 1 + \alpha^k$. Pro soubor GF ($2^2$) se potom získá následující tabulka logaritmů:

i	Z(i)
00	11
01	10
10	10
11	00

Souhrnně se dá pro všechny řetězce 1 posuvných registrů podle obr. 1 až obr. 5 uvést způsob generování pseudonáhodných posloupností. Tento způsob v podstatě spočívá v omezeném diskrétním vytváření logaritmu posloupností posuvného registru. Generování pseudonáhodných posloupností se u výhodného příkladu provedení neprovádí pomocí dodatečného vytváření logaritmu, viz obr. 1 až obr. 4, nýbrž výhodným způsobem přímo při generování pseudonáhodné posloupnosti, jak je to znázorněno na obr. 5 a obr. 6. Způsob je výhodný zejména tehdy, jestliže je velikost posuzované abecedy, tedy souboru, mocnina dvou, například 256, přičemž se dá tato abeceda znázornit pomocí bitů.

PV 2003 - 1598
06.06.03

P A T E N T O V É N Á R O K Y

1. Způsob generování pseudonáhodné posloupnosti, podle kterého se prvky pseudonáhodné posloupnosti posouvají posuvným registrem s více v sérii zapojenými paměťovými buňkami, tvořeným hardwarem nebo softwarem, s výstupními hodnotami alespoň dvou paměťových buněk se provádí početní operace a výsledek početní operace se ve zpětné vazbě přivádí na vstup jedné z paměťových buněk posuvného registru,
v y z n a č u j í c í s e t í m, že
prvky (γ) pseudonáhodné posloupnosti se diskrétně logaritmují.

2. Způsob podle nároku 1,
v y z n a č u j í c í s e t í m, že
diskrétní logaritmování se provádí modifikovaně.

3. Způsob podle nároku 1 nebo 2,
v y z n a č u j í c í s e t í m, že
diskrétní logaritmování se provádí již při početní operaci výstupních hodnot posuvných registrů.

4. Způsob podle některého z předcházejících nároků,
v y z n a č u j í c í s e t í m, že
diskrétní logaritmování se provádí vícekrát.

5. Způsob podle některého z předcházejících nároků,
v y z n a č u j í c í s e t í m, že
diskrétně se logaritmuje podle tabulky, zahrnující výstupní a výsledkové hodnoty.

6. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že alespoň s jednou z výstupních hodnot, určených pro početní operaci, se provede před touto početní operací předběžná početní operace s předem stanovitelnou hodnotou.

7. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že jako předběžná početní operace se provádí logická početní operace, výhodně sčítání.

8. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že předběžná početní operace se provádí na základě tabulky pro předběžnou početní operaci, zahrnující výstupní a výsledkové hodnoty, nebo pomocí logických obvodů.

9. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že diskrétní logaritmování se provádí pomocí Zech-logaritmu, popřípadě Jacobi-logaritmu.

10. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že tabulka logaritmů spočívá na Zech-logaritmu, popřípadě Jacobi-logaritmu.

11. Způsob podle některého z předcházejících nároků, v y z n a č u j í c í s e t í m, že zpětná vazba se realizuje tak, že se vytváří pseudonáhodná posloupnost o maximální délce periody.

12. Zařízení pro generování pseudonáhodné posloupnosti, s posuvným registrem, zahrnujícím více v sérii zapojených paměťových buněk, zpětnovazební větví, která spojuje dva různé výstupy registru se vstupem registru, a s obvodem realizujícím početní operaci s výstupními hodnotami registru, přičemž je obvod realizující početní operaci ze vstupní strany spojen s výstupy registru a z výstupní strany se vstupem registru,
v y z n a č u j í c í s e
obvodem (12) pro diskrétní logaritmování prvků (γ) pseudonáhodné posloupnosti.

13. Zařízení podle nároku 12,
v y z n a č u j í c í s e t í m, že
ve zpětnovazební větvi (7) je uspořádán obvod pro diskrétní logaritmování a vytváří obvod (8´) realizující početní operaci, který diskrétně logaritmuje výstupní hodnoty stupňů (2) registru.

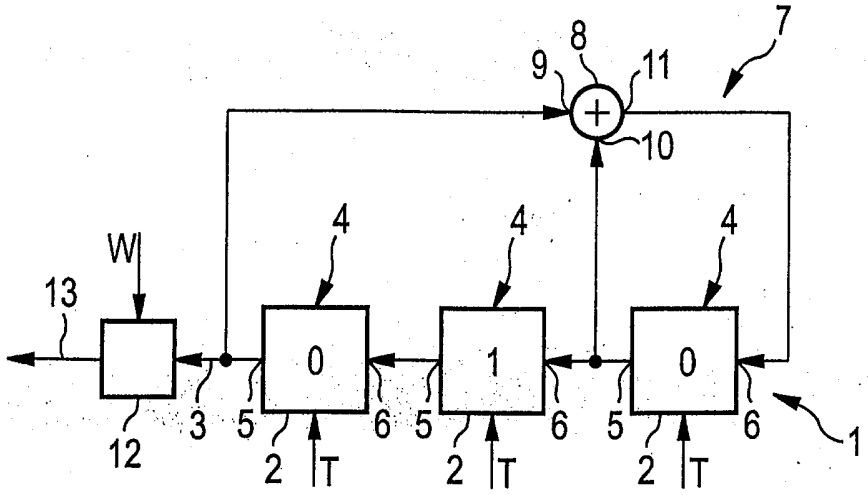
14. Zařízení podle nároku 12 nebo 13,
v y z n a č u j í c í s e t í m, že
obvodem (8´) realizujícím početní operaci je paměťový obvod, ve kterém je uložena tabulka logaritmů, zahrnující výstupní a výsledkové hodnoty.

15. Zařízení podle některého z nároků 12 až 14,
v y z n a č u j í c í s e t í m, že
mezi jedním z výstupů (5) registru a obvodem (8, 8´) realizujícím početní operaci je uspořádán obvod (14) realizující předběžnou početní operaci, jehož jeden vstup (15) je spojen s tímto výstupem (5) stupně registru, jehož druhý

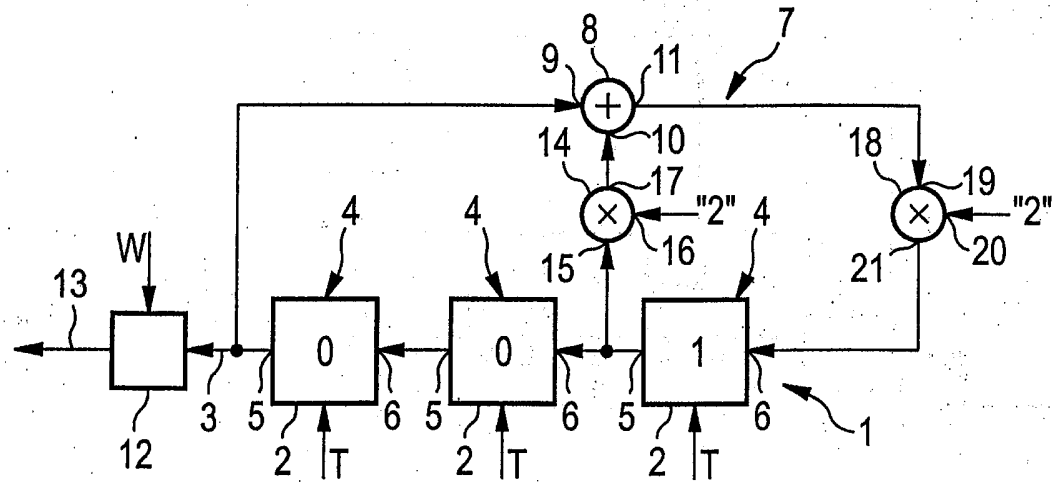
vstup (16) je ovladatelný předem stanovitelnou hodnotou, a jehož výstup (17) je spojen se vstupem (10) obvodu (8, 8´) realizujícího početní operaci.

16. Zařízení podle některého z nároků 12 až 15, v y z n a č u j í c í s e t í m, že obvodem (14) realizujícím předběžnou početní operaci je logický obvod.

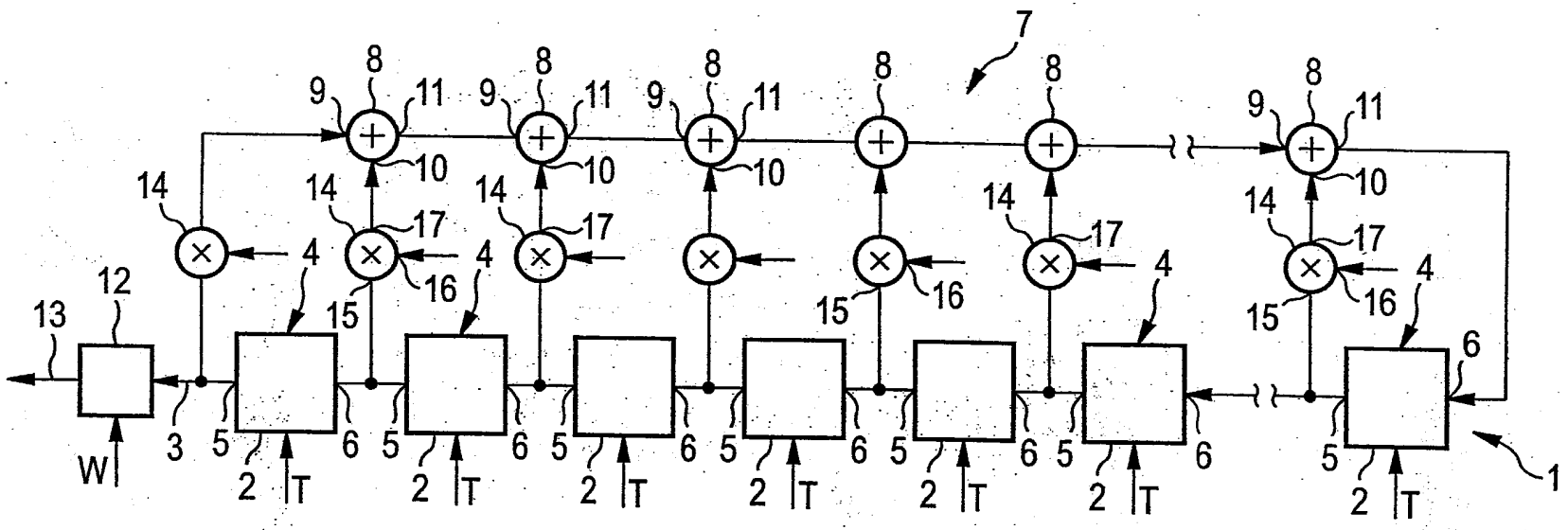
PV2003-1598
06.06.03



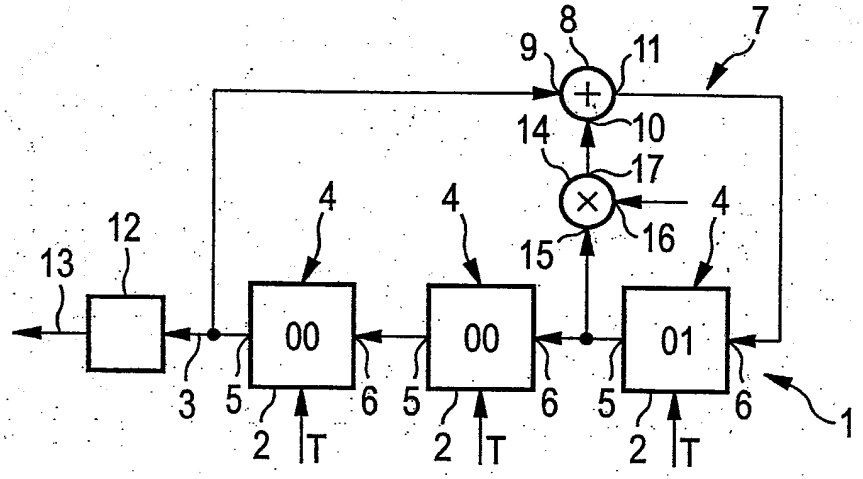
Obr. 1



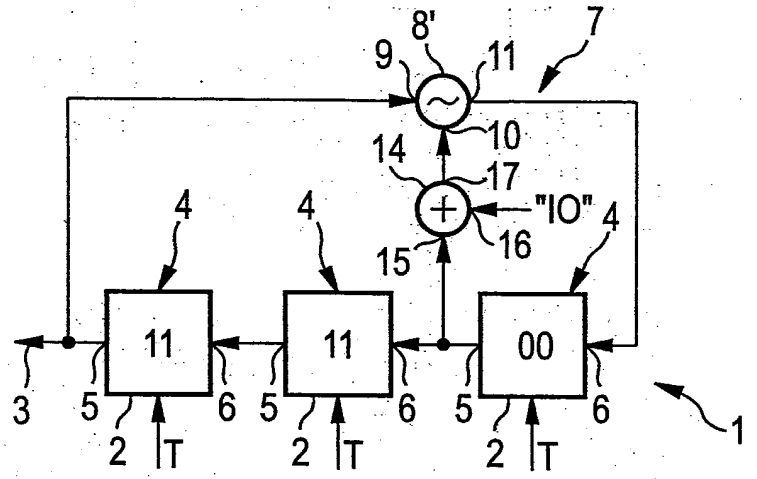
Obr. 2


7
8
9
11
10
14
17
16
15
4
12
13
W
3
5
2
T
6
1

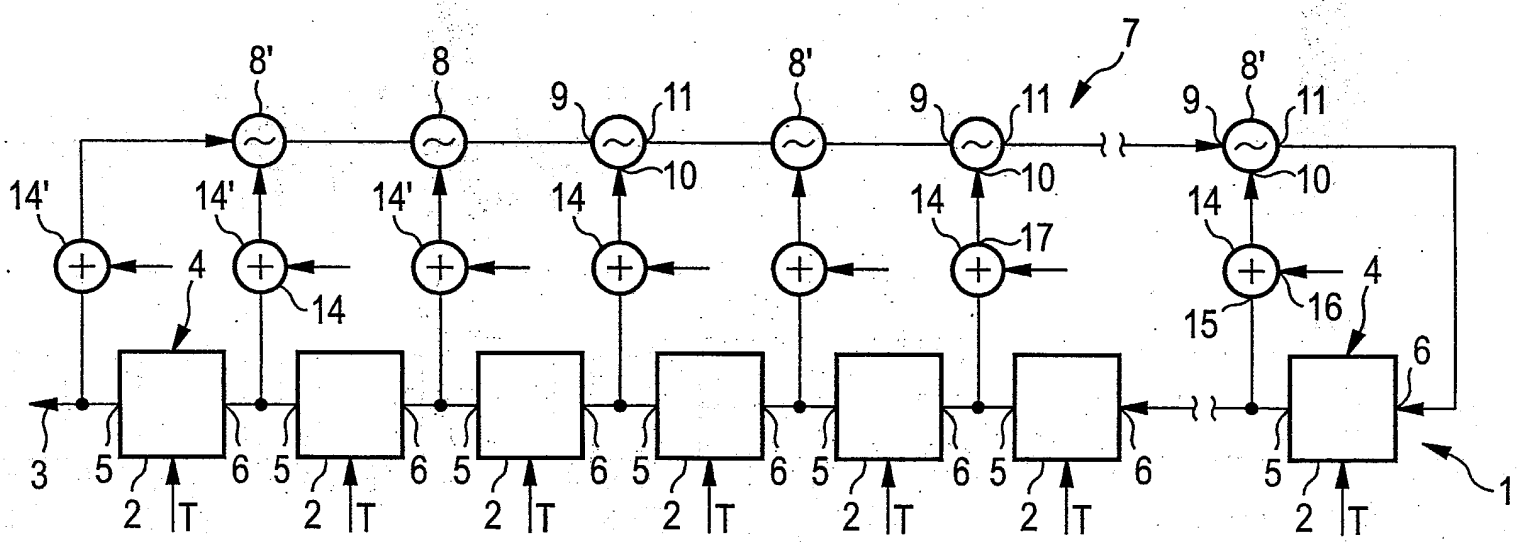
Obr. 3


8
9
11
7
14
10
17
16
15
4
12
13
00
00
01
3
5
2
T
6
1

Obr. 4


8'
9
11
7
10
14
17
"IO"
16
15
4
4
4
11
11
00
3
5
2
T
6
1

Obr. 5


8'
8
9
11
7
10
14'
14
17
4
15
16
6
3
5
2
T
1

Obr. 6