

G06F 21/33 (2013.01)
G06F 21/62 (2013.01)
H04L 9/32 (2006.01)

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLVÉHO
VLASTNICTVÍ

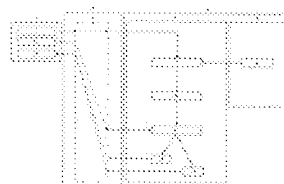
(21) Číslo přihlášky: 2019-607
(22) Přihlášeno: 26.09.2019
(40) Zveřejněno: 14.04.2021
(Věstník č. 15/2021)
(47) Uděleno: 23.06.2021
(24) Oznámení o udělení ve věstníku: 04.08.2021
(Věstník č. 31/2021)

(56) Relevantní dokumenty:
Michel Daydé, José M.L.M. Palma, Álvaro L.G.A. Couthino, Esther Pacitti, João Correia Lopes: High Performance Computing for Computational Science - VECPAR 2006: 7th International Conference, Rio de Janeiro, Brazil, June 10-13, 2006.
US 2019019366 A1; US 2011296188 A1; US 2018241548 A1.

(73) Majitel patentu:
Univerzita Tomáše Bati ve Zlíně, Zlín, CZ
VIAVIS a.s., Ostrava, Vítkovice, CZ

(72) Původce:
prof. Mgr. Roman Jašek, Ph.D., Zlín, CZ
Ing. Milan Oulehla, Brno, Slatina, CZ
Ing. Petr Žáček, Zlín, CZ
Mgr. Jan Krňávek, Ph.D., Zábřeh, CZ
Ing. Vladimír Lazecký, Hradec nad Moravicí, CZ
Ing. Jacek Makowski, Bohumín, Nový Bohumín, CZ
Ing. Tomáš Malík, Ostrava, Petřkovice, CZ
Ing. Jiří Malík, Mikulůvka, CZ

(74) Zástupce:
UTB ve Zlíně, Ing. Dana Kreizlová, nám. T. G.
Masaryka 5555, 760 01 Zlín



(54) Název vynálezu:
**Systém ověření identity a licencí pro práci s
vysoce citlivými daty**

(57) Anotace:
Systém má v hardware (1) klienta uložen jednoznačný identifikátor (2), který je přes přenosové prostředí (3) skrze protokol (4) vyšší vrstvy spojen se serverem (5), kde je ve vyhodnocovacím bloku (6) napojen na dosazovací a výpočtový blok (7), a současně soustava (8) w formovaných polynómů uložená v persistentní paměti (9) serveru (5) je rovněž spojena s dosazovacím a výpočtovým blokem (7), jehož výstupem je vypočtený klíč (10). Současně je v hardware (1) klienta uložen lokální klíč (11), který je přes přenosové prostředí (3) skrze protokol (4) vyšší vrstvy spojen se srovnávacím blokem (12) klíčů, na jehož vstup je také napojen vypočtený klíč (10). Srovnávací blok (12) klíčů je skrze svůj kladný výstup (13) i záporný výstup (14) spojen přes přenosové prostředí (3) prostřednictvím protokolu (4) vyšší vrstvy s blokem (15) zpracování odpovědi, uloženým v hardware (1) klienta. Systém při vysoké úrovni zabezpečení poskytuje požadovanou rychlost odezvy i pro velký počet uživatelů a/nebo licencí, a to bez podstatného navýšení nároků na prostorovou/paměťovou náročnost výpočetních prostředků.

Systém ověření identity a licencí pro práci s vysoce citlivými daty

Oblast techniky

5

Vynález se týká systému pro ověření identity a licencí pro dostupnost a nakládání se zabezpečenými daty, která jsou vázána selektivním nebo placeným přístupem. Řešení je přednostně určeno pro práci s vysoce citlivými daty, jako jsou vojenské a policejní aplikace, dále například autorizace bankovních operací, licence softwarových produktů, zabezpečení vstupů do budov a další analogické aplikace.

10

Dosavadní stav techniky

15 Dosud známé a používané systémy zabezpečení chráněných souborů nebo pro autentizaci klientů či licencí jsou založeny například na systému elektronického podpisu, kvalifikovaného certifikátu a podobně. Tyto systémy využívají k zabezpečení převážně metod standardní asymetrické kryptografie, která je založena na principu diskrétního logaritmu nebo na faktorizaci velkých čísel. Přitom se uplatňuje využití polynomů ve standardním tvaru

20

$$p_i(x) = q_{p-1}x^{p-1} + q_{p-2}x^{p-2} + \dots + q_2x^2 + q_1x + q_0.$$

Standardní polynomy nejsou dobře použitelné pro vyšší hodnoty proměnné p (počet uživatelů a/nebo licencí), vzhledem k tomu, že počet členů, hodnoty koeficientů polynomu i hodnoty jednotlivých exponentů neúnosně narůstají. Tím se značně zvyšují nároky na práci systému a 25 úměrně tomu i čas odezvy, potřebný pro komplexní zabezpečení. Dalším negativním důsledkem při potřebě použití polynomů vysokých stupňů je prostorová/paměťová náročnost daná nutností udržovat takové polynomy v persistentní paměti příslušných výpočetních prostředků.

30 Náhradní řešení eliminující či redukující tyto nevýhody jsou vedena v podstatě dvěma směry. Jedním z nich je snaha urychlit výpočet polynomu pomocí tzv. Hornerova schématu. Tento způsob řešení sice vede k částečnému urychlení procesu autentizace/autorizace, ale neodstraňuje problém související s velkým počtem parametrů.

35 Druhou navrhovanou cestou zjednodušení a zrychlení procesu verifikace je omezení polynomu na výrazně nižší stupeň. Tímto způsobem je sice možno dosáhnout časového i kapacitního odlehčení celého procesu, současně však je otevřena vyšší možnost neoprávněného vstupu, neboť koeficienty takového redukovaného polynomu lze odhadnout například pomocí Newtonovy interpolace.

40 Úkolem vynálezu je vytvořit takový systém pro ověření identity a licencí při práci se zabezpečenými daty, který při vysoké úrovni zabezpečení poskytuje požadovanou rychlost odezvy i pro velký počet uživatelů a/nebo licencí (pro vysoké hodnoty proměnné p), a to bez podstatného navýšení nároků na prostorovou/paměťovou náročnost výpočetních prostředků.

45

Podstata vynálezu

Uvedené nevýhody a nedostatky dosud známých zabezpečovacích systémů do značné míry odstraňuje systém ověření identity a licencí pro práci s vysoce citlivými daty podle vynálezu. 50 Podstata vynálezu spočívá v tom, že systém má v hardware klienta uložen jednoznačný identifikátor, spojený přes přenosové prostředí skrze protokol vyšší vrstvy se serverem, kde je ve vyhodnocovacím bloku napojen na dosazovací a výpočtový blok. S dosazovacím a výpočtovým blokem je současně spojena také soustava w formovaných polynomů uložená v persistentní paměti serveru; přitom výstupem dosazovacího a výpočtového bloku je vypočtený klíč. V hardware klienta 55 je zároveň uložen lokální klíč, který je přes přenosové prostředí skrze protokol vyšší vrstvy spojen

se srovnávacím blokem klíčů, na jehož vstup je také napojen vypočtený klíč; srovnávací blok klíčů má kladný výstup i záporný výstup spojený přes přenosové prostředí prostřednictvím protokolu vyšší vrstvy s blokem zpracování odpovědi, který je uložen v hardware klienta.

- 5 Systém ověření identity a licenci podle vynálezu má s výhodou ve vyhodnocovacím bloku před dosazovací a výpočtový blok předřazen vyhledávací blok, do něž je společně s jednoznačným identifikátorem připojen blok matice x -mat, uložený v persistentní paměti serveru, přičemž vyhledávací blok je společně se soustavou w formovaných polynomů připojen k dosazovacímu a výpočtovému bloku.

10

Systém ověření identity a licenci podle vynálezu má s výhodou v persistentní paměti serveru uloženou permutaci ρ , která je spojena s vypočteným klíčem, s nímž je současně spojen také blok matice x -mat.

- 15 Hlavní předností systému ověření identity a licenci pro práci s vysoce citlivými daty podle vynálezu je mimořádné zjednodušení výpočtu/zpracování vstupních dat uživatele a s tím spojené velmi rychlé a zároveň bezpečné přihlášení do chráněného systému vysoce citlivých dat. Je to umožněno charakterem zde užívaného polynomu, kdy dalším důsledkem a významným přínosem takto dosaženého odlehčení výpočetní kapacity zabezpečovacího systému je možnost prakticky libovolného navýšení počtu uživatelů/licenci – řádově v milionech – bez patrného dopadu na délku odezvy systému. Bezpečnost systému podle vynálezu je navíc posílena tím, že klíče a licence jsou rozděleny do dvou částí a verifikace probíhá vzdáleně na serveru. Bezpečnost systému je dále navýšena tím, že pokus o neoprávněnou manipulaci s jedním sloupcem matice v bloku matice x -mat vyvolá zablokování několika jiných lokálních klíčů.

25

Objasnění výkresů

- 30 K přiblížení podstaty zabezpečovacího systému podle vynálezu slouží jeho znázornění na přiložených výkresech, kde značí:

- obr. 1 – schéma systému podle příkladu 1 – základní provedení,
- obr. 2 – schéma systému podle příkladu 2 – výhodné provedení,
- 35 – obr. 3 – schéma systému podle příkladu 3 – optimální provedení,–
- obr. 4 – standardní polynom pro hodnotu $p = 1009$ (ve formátu pdf),
- 40 – obr. 5 – grafické srovnání výpočetní náročnosti u systému dle příkladu 3 a S,
- obr. 6 – grafické znázornění vztahu bitové bezpečnosti a velikosti prvočísla p .

45 Příklady uskutečnění vynálezu

Příklad 1

- 50 Jak je zřejmé z obr. 1, tento systém ověření identity a licenci pro práci s vysoce citlivými daty má v hardware 1 klienta uložen jednoznačný identifikátor 2, který je přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy spojen se serverem 5, kde je ve vyhodnocovacím bloku 6 napojen na dosazovací a výpočtový blok 7. Soustava 8 w polynomů uložená v persistentní paměti 9 serveru 5 je rovněž spojena s dosazovacím a výpočtovým blokem 7, jehož výstupem je vypočtený klíč 10. V hardware 1 klienta je zároveň uložen lokální klíč 11, který je přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy spojen se srovnávacím blokem 12 klíčů, na jehož vstup je také napojen

55

vypočtený klíč 10. Srovnávací blok 12 klíčů má kladný výstup 13 i záporný výstup 14 spojený přes přenosové prostředí 3 prostřednictvím protokolu 4 vyšší vrstvy s blokem 15 zpracování odpovědi, který je rovněž uložen v hardware 1 klienta.

- 5 Tento systém pracuje tak, že z hardware 1 klienta je vyslán jednoznačný identifikátor 2 přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy na server 5, konkrétně do vyhodnocovacího bloku 6. Vyhodnocovací blok 6 dosadí transformovaný jednoznačný identifikátor 2 do dosazovacího a výpočtového bloku 7 jako proměnné do soustavy 8 w polynomů. Na základě výsledků po dosazení do soustavy 8 w polynomů vytvoří vypočtený klíč 10. Ten je ve srovnávacím bloku 12 klíčů porovnán s lokálním klíčem 11, který je získán přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy od hardware 1 klienta. V případě kladného výstupu 13 je ověření úspěšné, v opačném případě je ověření zamítnuto. Výsledek ověření získaný přes kladný výstup 13 nebo záporný výstup 14 je přenosovým prostředím 3 skrze protokol 4 vyšší vrstvy předán do bloku 15 zpracování odpovědi, který je rovněž uložen v hardware 1 klienta.

- 15 Řešení popsané v příkladu 1 poskytuje ve srovnání se stávajícími systémy zabezpečení vysokou rychlost odezvy i pro vysoké hodnoty proměnné p (počet uživatelů a/nebo licenci), a to bez podstatného navýšení nároků na prostorovou/paměťovou náročnost výpočetních prostředků. Využití konečných těles, které bude blíže popsáno v závěrečné části příkladu 3, zabraňuje podvodnému vložení dalšího uživatele/licence, což je významný bezpečnostní rys navrhovaného systému.

Příklad 2

- 25 Jak je zřejmé z obr. 2, tento systém ověření identity a licenci pro práci s vysoce citlivými daty má v hardware 1 klienta také uložen jednoznačný identifikátor 2, lokální klíč 11 i blok 15 zpracování odpovědi. Server 5 opět obsahuje vyhodnocovací blok 6, ve kterém je dosazovací a výpočtový blok 7 s výstupem - vypočteným klíčem 10 spojeným se srovnávacím blokem 12 klíčů. V persistentní paměti 9 serveru 5 uložená soustava 8 w polynomů je rovněž spojena s dosazovacím a výpočtovým blokem 7. Také následná struktura jeho výstupních vazeb od srovnávacího bloku 12 klíčů až k bloku 15 zpracování odpovědi je shodná jako v příkladu 1.

- Tento systém má navíc ve vyhodnocovacím bloku 6 před dosazovací a výpočtový blok 7 předřazen vyhledávací blok 16, do něž je společně s jednoznačným identifikátorem 2 připojen blok 17 matice x -mat, uložený v persistentní paměti 9 serveru 5; přitom vyhledávací blok 16 je společně se soustavou 8 w polynomů připojen k dosazovacímu a výpočtovému bloku 7.

- 40 Tento systém pracuje tak, že z hardware 1 klienta je vyslán jednoznačný identifikátor 2 přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy na server 5, konkrétně do vyhodnocovacího bloku 6. Vyhodnocovací blok 6 vyhledá v bloku 17 matice x -mat příslušný sloupec. Hodnoty prvků z vyhledaného sloupce dosazovací a výpočtový blok 7 dosadí jako proměnné do soustavy 8 w polynomů. Na základě výsledků po dosazení do soustavy 8 w polynomů vytvoří vypočtený klíč 10. Ten je ve srovnávacím bloku 12 klíčů porovnán s lokálním klíčem 11, který je získán přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy od hardware 1 klienta. V případě kladného výstupu 13 je ověření úspěšné, v opačném případě je ověření zamítnuto. Výsledek ověření získaný přes kladný výstup 13 nebo záporný výstup 14 je přenosovým prostředím 3 skrze protokol 4 vyšší vrstvy předán do bloku 15 zpracování odpovědi, který je rovněž uložen v hardware 1 klienta.

- 50 Díky zařazení bloku 17 matice x -mat se do vyhodnocovacího bloku 6 nedosazuje přímo transformovaný jednoznačný identifikátor 2, ale na jeho základě je vyhledán v bloku 17 matice x -mat příslušný sloupec, který je pak dosazen do soustavy 8 w polynomů. Uvedené řešení dále zvyšuje úroveň bezpečnosti, aniž by se zvyšovala výpočetní náročnost.

Příklad 3

Jak je zřejmé z obr. 3, tento systém ověření identity a licenci pro práci s vysoce citlivými daty obsahuje všechny součásti uvedené v příkladu 2 ve stejném uspořádání a se shodnými vazbami. Navíc má tento systém v persistentní paměti 9 serveru 5 uloženou permutaci p 18, která je spojena s vypočteným klíčem 10, se kterým je současně spojen také blok 17 matice x -mat.

Tento systém pracuje tak, že z hardware 1 klienta je vyslán jednoznačný identifikátor 2 přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy na server 5, konkrétně do vyhodnocovacího bloku 6. Vyhodnocovací blok 6 vyhledá v bloku 17 matice x -mat příslušný sloupec. Hodnoty prvků z vyhledaného sloupce dosadí dosazovací a výpočtový blok 7 jako proměnné do soustavy 8 w polynomů. Na základě permutace p 18 a výsledků po dosazení do soustavy 8 w polynomů jsou vyhledány v bloku 17 matice x -mat příslušné hodnoty, které tvoří vypočtený klíč 10. Ten je ve srovnávacím bloku 12 klíčů porovnán s lokálním klíčem 11, který je získán přes přenosové prostředí 3 skrze protokol 4 vyšší vrstvy od hardware 1 klienta. V případě kladného výstupu 13 je ověření úspěšné, v opačném případě je ověření zamítnuto. Výsledek ověření získaný přes kladný výstup 13 nebo záporný výstup 14 je přenosovým prostředím 3 skrze protokol 4 vyšší vrstvy předán do bloku 15 zpracování odpovědi, který je rovněž uložen v hardware 1 klienta.

Výše uvedené řešení představuje optimální provedení systému ověření identity a licenci pro práci s vysoce citlivými daty. Díky využití permutace p 18 současně s blokem 17 matice x -mat je tato matice chráněna před škodlivou manipulací, protože neoprávněná manipulace s jedním sloupcem zneplatní více lokálních klíčů. To má za následek zvýšení bezpečnosti oproti řešení uvedeném v příkladu 2.

Systémy ověření identity a licenci pro práci s vysoce citlivými daty podle vynálezu využívají k výpočetním/ověřovacím operacím specificky vytvořené polynomy, které budou dále nazývány formované polynomy.

Formované polynomy jsou vytvořeny nahrazením běžných koeficientů q , užívaných ve standardním polynomu, pomocí sestavy koeficientů a , b , přičemž formované polynomy mají zásadně odlišný způsob/formu zápisu a také výpočtu než standardní polynomy. Formovaný polynom má méně členů než standardní polynom a jeho výpočet má konstantní počet cyklů bez ohledu na zvyšující se hodnoty p (počet uživatelů a/nebo licenci), což významně zkracuje a zrychluje ověřovací operace. Při výpočtu formovaných polynomů systém pracuje s podstatně schůdnějšími hodnotami koeficientů a exponentů, a to – zejména pokud jde o exponenty - značně snižuje výpočetní náročnost. Tím se šetří čas operace i kapacita výpočetních prostředků.

Uvedené účinky z hlediska zrychlení/zjednodušení výpočtu jsou tím zřetelnější, čím vyšší je počet uživatelů/licenci/subsystémů, zapojených do systému. Podstatný je přínos již při hodnotě $p = 37$ a s navyšováním tohoto počtu úspora pracovního času i kapacity mimořádně rychle narůstá (viz obr. 5). Při vysokých hodnotách p je úspora natolik mimořádná, že by formované polynomy mohly být nazývány „magickými polynomy“.

Příklad S – srovnávací

Pro názornost se uvádí příklad stávajícího zabezpečovacího systému pro podobné účely, pracujícího na bázi polynomů ve standardním tvaru:

$$p_i(x) = q_{p-1}x^{p-1} + q_{p-2}x^{p-2} + \dots + q_2x^2 + q_1x + q_0.$$

Dále budou uvedeny příkladné zápisy standardních polynomů pro různé hodnoty p .

Roznásobený polynom (standardní tvar) nad tělesem $\mathbb{Z}_{101}$:

$$\begin{aligned}
(x) = & 25x^{100} + 73x^{99} + 92x^{98} + 48x^{97} + 83x^{96} + 100x^{95} + 75x^{94} + 83x^{92} + 17x^{91} + 93x^{90} \\
& + 30x^{89} + 74x^{88} + 40x^{87} + 25x^{86} + 38x^{85} + 78x^{84} + 73x^{83} + 69x^{82} + 91x^{81} \\
& + 4x^{80} + 84x^{79} + 4x^{78} + 61x^{77} + 98x^{76} + 19x^{75} + 100x^{74} + 91x^{73} + 5x^{72} \\
& + 69x^{71} + 36x^{70} + 91x^{69} + 76x^{68} + 81x^{67} + 53x^{66} + 81x^{65} + 91x^{64} + 82x^{63} \\
& + 86x^{62} + 87x^{61} + 59x^{60} + 3x^{59} + 38x^{58} + 94x^{57} + 84x^{56} + 57x^{55} + 20x^{54} \\
& + 97x^{53} + 31x^{52} + 21x^{51} + 30x^{50} + 11x^{49} + 93x^{48} + 26x^{47} + 70x^{46} + 26x^{45} \\
& + 19x^{44} + 73x^{43} + 99x^{42} + 52x^{41} + 19x^{40} + 80x^{39} + 55x^{38} + 51x^{37} + 22x^{36} \\
& + 41x^{35} + 75x^{34} + 28x^{33} + 19x^{32} + 17x^{31} + 95x^{30} + 32x^{29} + 91x^{28} + 64x^{27} \\
& + 79x^{26} + 13x^{25} + 86x^{24} + 45x^{23} + 26x^{22} + 42x^{21} + 87x^{20} + 23x^{19} + 52x^{18} \\
& + 3x^{17} + 6x^{16} + 87x^{15} + 78x^{14} + 89x^{13} + 44x^{12} + 45x^{11} + 16x^{10} + 38x^9 \\
& + 2x^8 + 25x^7 + 15x^6 + 7x^5 + 94x^4 + 15x^2 + 55x + 39
\end{aligned}$$

Roznásobený polynom (standardní tvar) nad tělesem $\mathbb{Z}_{311}$:

$$\begin{aligned}
p(x) = & 18x^{302} + 8x^{301} + 122x^{300} + 6x^{299} + 198x^{298} + 20x^{297} + 110x^{296} + 92x^{295} + 64x^{294} + \\
& 149x^{293} + 269x^{292} + 304x^{291} + 278x^{290} + 36x^{289} + 117x^{288} + 304x^{287} + 223x^{286} + 193x^{285} + \\
& 123x^{284} + 44x^{283} + 88x^{282} + 60x^{281} + 122x^{280} + 302x^{279} + 16x^{278} + 271x^{277} + 237x^{276} + \\
& 73x^{275} + 55x^{274} + 192x^{273} + 250x^{272} + 186x^{271} + 171x^{270} + 2x^{269} + 124x^{268} + 28x^{267} + \\
& 237x^{266} + 256x^{265} + 42x^{264} + 155x^{263} + 194x^{262} + 176x^{261} + 145x^{260} + 189x^{259} + 51x^{258} + \\
& 208x^{257} + 216x^{256} + 124x^{255} + 308x^{254} + 119x^{253} + 190x^{252} + 196x^{251} + 130x^{250} + \\
& 292x^{249} + 244x^{248} + 278x^{247} + 132x^{246} + 59x^{245} + 168x^{244} + 175x^{243} + 238x^{242} + 178x^{241} + \\
& 235x^{240} + 58x^{239} + 226x^{238} + 267x^{237} + 104x^{236} + 29x^{235} + 161x^{234} + 291x^{233} + 162x^{232} + \\
& 231x^{231} + 123x^{230} + 15x^{229} + 49x^{228} + 92x^{227} + 307x^{226} + 47x^{225} + 60x^{224} + 257x^{223} + \\
& 97x^{222} + 38x^{221} + 139x^{220} + 6x^{219} + 68x^{218} + 142x^{217} + 114x^{216} + 145x^{215} + 171x^{214} + \\
& 22x^{213} + 93x^{212} + 11x^{211} + 216x^{210} + 68x^{209} + 147x^{208} + 269x^{207} + 43x^{206} + 261x^{205} + \\
& 82x^{204} + 64x^{203} + 203x^{202} + 287x^{201} + 207x^{200} + 38x^{199} + 158x^{198} + 56x^{197} + 162x^{196} + \\
& 103x^{195} + 217x^{194} + 108x^{193} + 308x^{192} + 230x^{191} + 278x^{190} + 114x^{189} + 131x^{188} + \\
& 169x^{187} + 87x^{186} + 50x^{185} + 232x^{184} + 88x^{183} + 166x^{182} + 182x^{180} + 291x^{178} + 157x^{177} + \\
& 234x^{176} + 299x^{175} + 118x^{174} + 58x^{173} + 283x^{172} + 20x^{171} + 208x^{170} + 175x^{169} + 165x^{168} + \\
& 157x^{167} + 190x^{166} + 96x^{165} + 43x^{164} + 36x^{163} + 41x^{162} + 153x^{161} + 151x^{160} + 173x^{159} + \\
& 190x^{158} + 291x^{157} + 294x^{156} + 58x^{155} + 217x^{154} + 128x^{153} + 178x^{152} + 174x^{151} + 88x^{150} + \\
& 96x^{149} + 172x^{148} + 122x^{147} + 189x^{146} + 113x^{145} + 113x^{144} + 48x^{143} + 282x^{142} + 310x^{141} + \\
& 241x^{140} + 245x^{139} + 186x^{138} + 57x^{137} + 174x^{136} + 178x^{135} + 78x^{134} + 151x^{133} + 125x^{132} + \\
& 26x^{131} + 37x^{130} + 46x^{129} + 243x^{128} + 95x^{127} + 146x^{126} + 237x^{125} + 223x^{124} + 14x^{123} + \\
& 153x^{122} + 282x^{121} + 170x^{120} + 237x^{119} + 128x^{118} + 33x^{117} + 31x^{116} + 144x^{115} + 37x^{114} + \\
& 177x^{113} + 195x^{112} + 181x^{110} + 206x^{109} + 225x^{108} + 81x^{107} + 128x^{106} + 173x^{105} + 310x^{104} + \\
& 94x^{103} + 197x^{102} + 160x^{101} + 75x^{100} + 243x^{99} + 18x^{98} + 108x^{97} + 27x^{96} + 126x^{95} + \\
& 191x^{94} + 89x^{93} + 62x^{92} + 37x^{91} + 133x^{90} + 9x^{89} + 95x^{88} + 157x^{87} + 100x^{86} + 273x^{85} + \\
& 164x^{84} + 276x^{83} + 147x^{82} + 125x^{81} + 6x^{80} + 191x^{79} + 159x^{78} + 205x^{77} + 111x^{76} + \\
& 143x^{75} + 34x^{74} + 210x^{73} + 78x^{72} + 141x^{71} + x^{70} + 26x^{69} + 252x^{68} + 138x^{67} + 66x^{66} + \\
& 142x^{65} + 161x^{64} + 44x^{63} + 240x^{62} + 187x^{61} + 53x^{60} + 281x^{59} + 125x^{58} + 118x^{57} + \\
& 263x^{56} + 237x^{55} + 241x^{54} + 304x^{53} + 109x^{52} + 17x^{51} + 271x^{50} + 53x^{49} + 30x^{48} + 267x^{47} + \\
& 77x^{46} + 165x^{45} + 106x^{44} + 39x^{43} + 248x^{42} + 273x^{41} + 172x^{40} + 231x^{39} + 217x^{38} + \\
& 247x^{37} + 156x^{36} + 302x^{35} + 286x^{34} + 31x^{33} + 56x^{32} + 201x^{31} + 211x^{30} + 230x^{29} + \\
& 186x^{28} + 187x^{27} + 204x^{26} + 229x^{25} + 137x^{24} + 11x^{23} + 171x^{22} + 221x^{21} + 109x^{20} + \\
& 28x^{19} + 239x^{18} + 194x^{17} + 243x^{16} + 299x^{15} + 91x^{14} + 99x^{13} + 257x^{12} + 32x^{11} + 8x^{10} + \\
& 109x^9 + 250x^8 + 217x^7 + 142x^6 + 183x^5 + 90x^4 + 269x^3 + 189x^2 + 153x + 198.
\end{aligned}$$

Roznásobený polynom (standardní tvar) nad tělesem $\mathbb{Z}_{1009}$ je vzhledem k jeho rozsahu a objemu dat uveden samostatně jako příloha ve formátu pdf – viz obr. 4. Z obrázku, který názorně

ilustruje složitost výrazu, je zřejmá náročnost výpočtu hodnoty standardního polynomu, jak z hlediska kapacity výpočetních prostředků, tak také dopad složitosti na rychlost výpočtu a odezvu systému.

- 5 Na rozdíl od standardních polynomů s právě uvedenými problémy a nedostatky využití formovaných polynomů v systému podle vynálezu umožňuje rychlé výpočty, které mají konstantní počet cyklů i pro velké množství uživatelů, licenci a subsystémů. Na obr. 5 je znázorněno srovnání výpočetní náročnosti hodnot formovaných polynomů (příklad 3) a polynomů ve standardním tvaru (příklad S). Graf názorně ukazuje úsporu času odezvy i odlehčení kapacity výpočetních prostředků zejména při vyšších hodnotách p .

- 15 Navzdory výpočetní rychlosti bezpečnost zůstává u systému podle vynálezu stále na vysoké úrovni. Z hlediska bezpečnosti je přínosné, že serverové klíče pro uživatele/licenci/subsystém jsou reprezentovány sloupci v bloku 17 matice x -mat uložené na serveru 5, přičemž vypočtený klíč 10 v případě využití permutace ρ 18 není přímým výsledkem výpočtu samotných formovaných polynomů, ale je podle nich následně vyhledán v bloku 17 matice x -mat. Výsledky polynomů ani vypočítané klíče nesmí být uloženy na serveru. Je tedy obtížné odvodit blok 17 matice x -mat z polynomů a lokálních klíčů 11, pokud by byly odcizeny.

- 20 Bezpečnost systému podle vynálezu je demonstrována na obr. 6, který znázorňuje vztah bitové bezpečnosti a velikosti prvočísla p . Vyjádření bitové bezpečnosti znamená konzervativní odhad počtu formovaných polynomů vzhledem ke zvolenému prvočíslu p , kdy bitová bezpečnost je vypočtena z předpokladu využití útoku hrubou silou, a tedy vyzkoušení všech různých kombinací. Pro 128bitový klíč se jedná o 2^{128} kombinací; pokud budeme volit prvočíslo $p = 31$, pak počet různých formovaných polynomů je porovnatelný s počtem kombinací klíčů délky 121 bitů, tedy přibližně 2^{121} . V bezpečnosti symetrické kryptografie lze považovat klíče s délkou 128 bitů za bezpečné, k čemuž se $p = 31$ pouze přibližuje, ale hned další prvočíslo 37 o hodnotu přesahuje, konkrétně má bitovou bezpečnost 131 bitů. Pokud se podíváme na prvočíslo 10007, tak lze bitovou bezpečnost připodobnit 390 bitům. Tuto hodnotu lze v současné době považovat za dostatečně bezpečnou s ohledem na existenci kvantových počítačů, kde se uvažuje snížení bitové bezpečnosti na polovinu. Navíc je nutné si uvědomit, že bitová bezpečnost je vztažena pouze k jednotlivým formovaným polynomům, nikoliv k celé soustavě w polynomů, se kterou systém podle vynálezu pracuje a která je ve svých výhodných variantách bezpečnější.

35

Průmyslová využitelnost

- 40 Systém pro ověření identity a licenci pro práci se zabezpečenými daty podle vynálezu je určen pro generování a ověřování unikátních licenčních či identifikačních klíčů, určených pro potvrzení platnosti softwarových licencí či jedinečnou identifikaci uživatele, prvků internetu věcí, užití systémů spojených s rozhodovacími pravomocemi, ať už ve vojenství nebo v bankovním sektoru. Systém tedy najde uplatnění zejména pro verifikaci uživatelů elektronických datových systémů s mimořádně vysokou potřebou bezpečnosti a zároveň velmi rychlé odezvy, jako jsou systémy pro vojenské účely, bezpečnostní složky, integrovaný záchranný systém a další související oblasti.
- 45 Nabízí se však jeho využití také v civilních aplikacích, například pro zabezpečení budov, ale i pro běžné účely, jako jsou vstupenky, jízdenky a podobné aplikace.

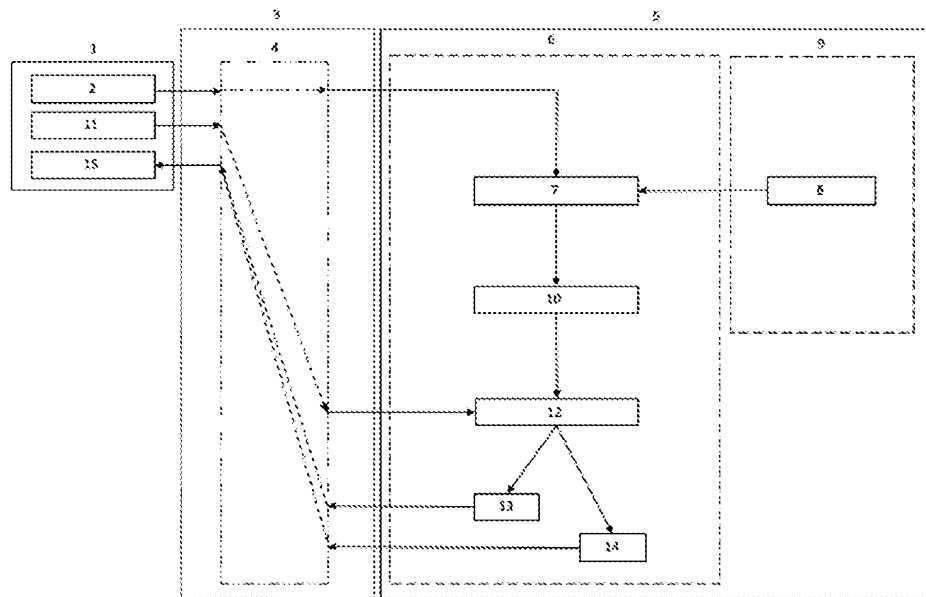
PATENTOVÉ NÁROKY

1. Systém pro ověření identity a licenci při vstupu a práci s elektronickým souborem vysoce citlivých dat, zahrnující přístupové hardwarové zařízení klienta s vloženým identifikátorem a klíčem, které je připojeno přes přenosové prostředí k zabezpečenému serveru, **vyznačující se tím**, že má v hardware (1) klienta uložen jednoznačný identifikátor (2), který je přes přenosové prostředí (3) skrze protokol (4) vyšší vrstvy spojen se serverem (5), kde je ve vyhodnocovacím bloku (6) napojen na dosazovací a výpočtový blok (7), a současně soustava (8) *w* formovaných polynomů uložená v persistentní paměti (9) serveru (5) je rovněž spojena s dosazovacím a výpočtovým blokem (7); výstupem dosazovacího a výpočtového bloku (7) je vypočtený klíč (10); současně je v hardware (1) klienta uložen lokální klíč (11), který je přes přenosové prostředí (3) skrze protokol (4) vyšší vrstvy spojen se srovnávacím blokem (12) klíčů, na jehož vstup je také napojen vypočtený klíč (10); srovnávací blok (12) klíčů je skrze svůj kladný výstup (13) i záporný výstup (14) spojen přes přenosové prostředí (3) prostřednictvím protokolu (4) vyšší vrstvy s blokem (15) zpracování odpovědi, uloženým v hardware (1) klienta.
2. Systém pro ověření identity a licenci uživatelů podle nároku 1, **vyznačující se tím**, že ve vyhodnocovacím bloku (6) je před dosazovací a výpočtový blok (7) předřazen vyhledávací blok (16), do něž je společně s jednoznačným identifikátorem (2) připojen blok (17) matice *x-mat*, uložený v persistentní paměti (9) serveru (5), přičemž vyhledávací blok (16) je společně se soustavou (8) *w* formovaných polynomů připojen k dosazovacímu a výpočtovému bloku (7).
3. Systém pro ověření identity a licenci uživatelů podle nároku 1 nebo 2, **vyznačující se tím**, že v persistentní paměti (9) serveru (5) je uložena permutace ρ (18), která je spojena s vypočteným klíčem (10), s nímž je současně spojen také blok (17) matice *x-mat*.

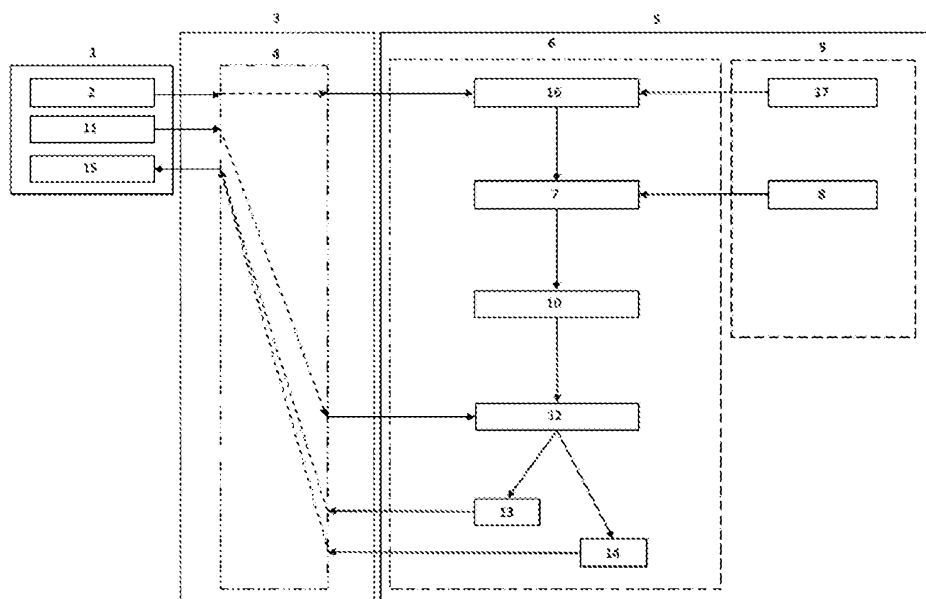
7 výkresů

Seznam vztahových značek:

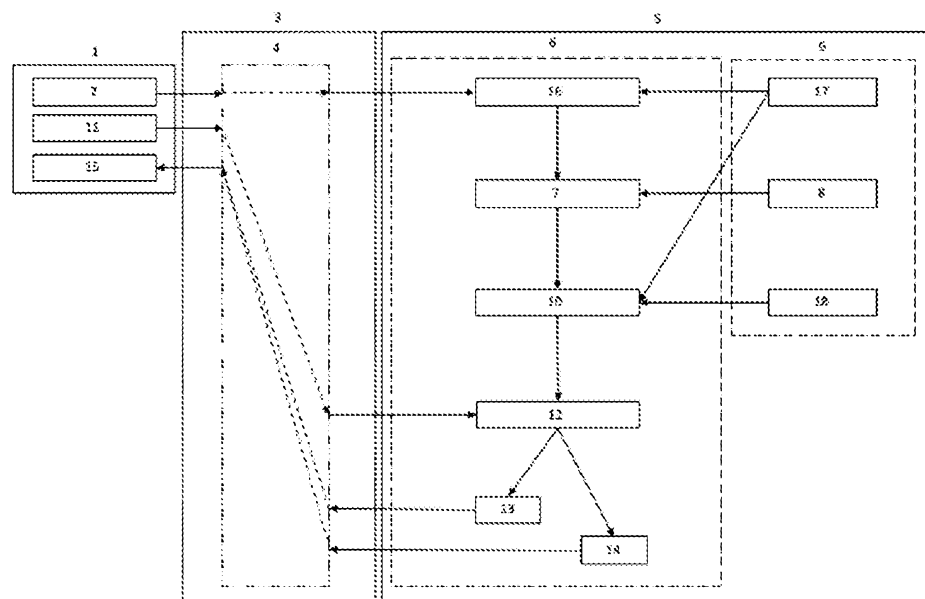
- 1 – hardware klienta
- 2 – jednoznačný identifikátor
- 3 – přenosové prostředí
- 4 – protokol vyšší vrstvy
- 5 – server
- 6 – vyhodnocovací blok
- 7 – dosazovací a výpočtový blok
- 8 – soustava *w* polynomů
- 9 – persistentní paměť (serveru)
- 10 – vypočtený klíč
- 11 – lokální klíč
- 12 – srovnávací blok klíčů
- 13 – kladný výstup (srovnávacího bloku klíčů)
- 14 – záporný výstup (srovnávacího bloku klíčů)
- 15 – blok zpracování odpovědi
- 16 – vyhledávací blok
- 17 – blok matice *x-mat*
- 18 – permutace ρ



Obr. 1



Obr. 2



Obr. 3

Roznásobený polynom (standardní tvar) nad tělesem $\mathbb{Z}_{1009}$:

$$\begin{aligned}
 p(x) = & 637x^{918} + 302x^{917} + 434x^{916} + 105x^{915} + 876x^{914} + 261x^{913} + 353x^{912} + \\
 & 622x^{911} + 358x^{910} + 184x^{909} + 509x^{908} + 163x^{907} + 680x^{906} + 227x^{905} + 420x^{904} + \\
 & 989x^{903} + 115x^{902} + 366x^{901} + 942x^{900} + 934x^{899} + 758x^{898} + 181x^{897} + 43x^{896} + \\
 & 541x^{895} + 734x^{894} + 858x^{893} + 261x^{892} + 198x^{891} + 1006x^{890} + 867x^{889} + \\
 & 280x^{888} + 267x^{887} + 326x^{886} + 246x^{885} + 1002x^{884} + 855x^{883} + 842x^{882} + 44x^{881} + \\
 & 814x^{880} + 843x^{879} + 505x^{878} + 288x^{877} + 635x^{876} + 580x^{875} + 263x^{874} + 819x^{873} + \\
 & 310x^{872} + 144x^{871} + 242x^{870} + 626x^{869} + 367x^{868} + 121x^{867} + 480x^{866} + 557x^{865} + \\
 & 546x^{864} + 923x^{863} + 815x^{862} + 230x^{861} + 427x^{860} + 753x^{859} + 505x^{858} + 961x^{857} + \\
 & 264x^{856} + 801x^{855} + 676x^{854} + 43x^{853} + 217x^{852} + 313x^{851} + 749x^{850} + 846x^{849} + \\
 & 124x^{848} + 375x^{847} + 898x^{846} + 865x^{845} + 384x^{844} + 684x^{843} + 583x^{842} + 782x^{841} + \\
 & 838x^{840} + 794x^{839} + 1003x^{838} + 1007x^{837} + 452x^{836} + 794x^{835} + 260x^{834} + \\
 & 940x^{833} + 196x^{832} + 717x^{831} + 240x^{830} + 719x^{829} + 769x^{828} + 942x^{827} + 943x^{826} + \\
 & 979x^{825} + 482x^{824} + 756x^{823} + 669x^{822} + 194x^{821} + 141x^{820} + 258x^{819} + 477x^{818} + \\
 & 529x^{817} + 582x^{816} + 118x^{815} + 612x^{814} + 501x^{813} + 835x^{812} + 527x^{811} + 194x^{810} + \\
 & 224x^{809} + 774x^{808} + 363x^{807} + 762x^{806} + 621x^{805} + 715x^{804} + 584x^{803} + 401x^{802} + \\
 & 602x^{801} + 205x^{800} + 594x^{799} + 941x^{798} + 738x^{797} + 318x^{796} + 201x^{795} + 912x^{794} + \\
 & 810x^{793} + 798x^{792} + 148x^{791} + 913x^{790} + 746x^{789} + 473x^{788} + 16x^{787} + 916x^{786} + \\
 & 996x^{785} + 649x^{784} + 654x^{783} + 87x^{782} + 64x^{781} + 497x^{780} + 455x^{779} + 239x^{778} + \\
 & 237x^{777} + 74x^{776} + 719x^{775} + 134x^{774} + 751x^{773} + 251x^{772} + 534x^{771} + 912x^{770} + \\
 & 814x^{769} + 940x^{768} + 217x^{767} + 289x^{766} + 965x^{765} + 666x^{764} + 74x^{763} + 815x^{762} + \\
 & 444x^{761} + 780x^{760} + 298x^{759} + 217x^{758} + 48x^{757} + 763x^{756} + 711x^{755} + 582x^{754} + \\
 & 10x^{753} + 131x^{752} + 343x^{751} + 769x^{750} + 862x^{749} + 538x^{748} + 986x^{747} + 477x^{746} + \\
 & 515x^{745} + 993x^{744} + 728x^{743} + 272x^{742} + 563x^{741} + 835x^{740} + 519x^{739} + 80x^{738} + \\
 & 493x^{737} + 207x^{736} + 250x^{735} + 766x^{734} + 630x^{733} + 252x^{732} + 187x^{731} + 980x^{730} + \\
 & 812x^{729} + 358x^{728} + 358x^{727} + 255x^{726} + 266x^{725} + 660x^{724} + 957x^{723} + 467x^{722} + \\
 & 922x^{721} + 579x^{720} + 814x^{719} + 907x^{718} + x^{717} + 551x^{716} + 160x^{715} + 761x^{714} + \\
 & 158x^{713} + 728x^{712} + 326x^{711} + 866x^{710} + 55x^{709} + 661x^{708} + 490x^{707} + 494x^{706} + \\
 & 584x^{705} + 1002x^{704} + 755x^{703} + 617x^{702} + 74x^{701} + 280x^{700} + 763x^{699} + 508x^{698} + \\
 & 281x^{697} + 341x^{696} + 709x^{695} + 773x^{694} + 805x^{693} + 822x^{692} + 294x^{691} + 847x^{690} + \\
 & 189x^{689} + 103x^{688} + 494x^{687} + 650x^{686} + 863x^{685} + 26x^{684} + 642x^{683} + 181x^{682} + \\
 & 794x^{681} + 499x^{680} + 380x^{679} + 428x^{678} + 659x^{677} + 285x^{676} + 917x^{675} + 409x^{674} + \\
 & 701x^{673} + 844x^{672} + 575x^{671} + 909x^{670} + 460x^{669} + 615x^{668} + 613x^{667} + 803x^{666} + \\
 & 899x^{665} + 636x^{664} + 866x^{663} + 345x^{662} + 891x^{661} + 846x^{660} + 1004x^{659} + 86x^{658} + \\
 & 172x^{657} + 475x^{656} + 747x^{655} + 365x^{654} + 260x^{653} + 348x^{652} + 604x^{651} + 826x^{650} + \\
 & 966x^{649} + 338x^{648} + 502x^{647} + 275x^{646} + 48x^{645} + 767x^{644} + 672x^{643} + 46x^{642} + \\
 & 456x^{641} + 70x^{640} + 660x^{639} + 928x^{638} + 47x^{637} + 599x^{636} + 941x^{635} + 145x^{634} + \\
 & 940x^{633} + 186x^{632} + 4x^{631} + 354x^{630} + 839x^{629} + 633x^{628} + 70x^{627} + 710x^{626} + \\
 & 799x^{625} + 40x^{624} + 725x^{623} + 23x^{622} + 459x^{621} + 600x^{620} + 465x^{619} + 720x^{618} + \\
 & 752x^{617} + 719x^{616} + 638x^{615} + 381x^{614} + 687x^{613} + 497x^{612} + 115x^{611} + 443x^{610} + \\
 & 13x^{609} + 756x^{608} + 983x^{607} + 462x^{606} + 993x^{605} + 700x^{604} + 7x^{603} + 428x^{602} + \\
 & 909x^{601} + 694x^{600} + 64x^{599} + 726x^{598} + 294x^{597} + 873x^{596} + 940x^{595} + 880x^{594} + \\
 & 382x^{593} + 71x^{592} + 926x^{591} + 574x^{590} + 935x^{589} + 84x^{588} + 996x^{587} + 600x^{586} + \\
 & 683x^{585} + 455x^{584} + 769x^{583} + 865x^{582} + 249x^{581} + 470x^{580} + 74x^{579} + 396x^{578} +
 \end{aligned}$$

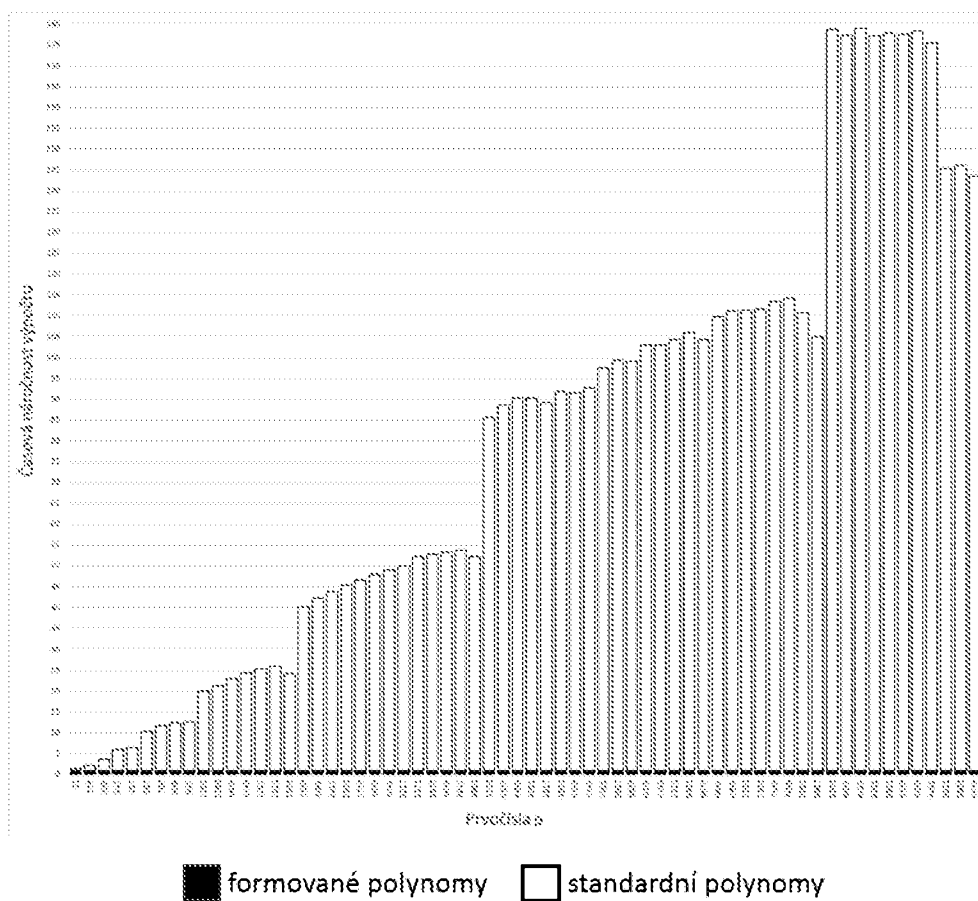
Obr. 4

$241x^{577} + 794x^{576} + 508x^{575} + 451x^{574} + 266x^{573} + 532x^{572} + 682x^{571} + 104x^{570} +$
 $877x^{569} + 310x^{568} + 393x^{567} + 556x^{566} + 313x^{565} + 30x^{564} + 880x^{563} + 953x^{562} +$
 $211x^{561} + 87x^{560} + 272x^{559} + 211x^{558} + 947x^{557} + 417x^{556} + 754x^{555} + 574x^{554} +$
 $908x^{553} + 896x^{552} + 672x^{551} + 204x^{550} + 985x^{549} + 634x^{548} + 713x^{547} + 799x^{546} +$
 $152x^{545} + 327x^{544} + 786x^{543} + 85x^{542} + 18x^{541} + 70x^{540} + 362x^{539} + 292x^{538} +$
 $666x^{537} + 68x^{536} + 589x^{535} + 188x^{534} + 381x^{533} + 849x^{532} + 43x^{531} + 741x^{530} +$
 $61x^{529} + 457x^{528} + 831x^{527} + 57x^{526} + 779x^{525} + 286x^{524} + 631x^{523} + 360x^{522} +$
 $634x^{521} + 605x^{520} + 879x^{519} + 158x^{518} + 387x^{517} + 380x^{516} + 551x^{515} + 376x^{514} +$
 $22x^{513} + 333x^{512} + 343x^{511} + 379x^{510} + 343x^{509} + 729x^{508} + 501x^{507} + 450x^{506} +$
 $488x^{505} + 723x^{504} + 715x^{503} + 61x^{502} + 909x^{501} + 144x^{500} + 228x^{499} + 79x^{498} +$
 $225x^{497} + 465x^{496} + 783x^{495} + 310x^{494} + 936x^{493} + 153x^{492} + 965x^{491} + 540x^{490} +$
 $936x^{489} + 477x^{488} + 128x^{487} + 31x^{486} + 414x^{485} + 599x^{484} + 937x^{483} + 662x^{482} +$
 $732x^{481} + 621x^{480} + 554x^{479} + 534x^{478} + 210x^{477} + 302x^{476} + 357x^{475} + 893x^{474} +$
 $364x^{473} + 815x^{472} + 342x^{471} + 294x^{470} + 466x^{469} + 759x^{468} + 9x^{467} + 34x^{466} +$
 $231x^{465} + 389x^{464} + 739x^{463} + 419x^{462} + 488x^{461} + 439x^{460} + 453x^{459} + 560x^{458} +$
 $741x^{457} + 453x^{456} + 153x^{455} + 28x^{454} + 412x^{453} + 111x^{452} + 173x^{451} + 201x^{450} +$
 $135x^{449} + 110x^{448} + 339x^{447} + 421x^{446} + 871x^{445} + 895x^{444} + 523x^{443} + 693x^{442} +$
 $240x^{441} + 460x^{440} + 449x^{439} + 558x^{438} + 932x^{437} + 255x^{436} + 481x^{435} + 311x^{434} +$
 $305x^{433} + 615x^{432} + 432x^{431} + 325x^{430} + 869x^{429} + 816x^{428} + 430x^{427} + 948x^{426} +$
 $374x^{425} + 416x^{424} + 843x^{423} + 777x^{422} + 194x^{421} + 721x^{420} + 79x^{419} + 132x^{418} +$
 $387x^{417} + 182x^{416} + 676x^{415} + 362x^{414} + 501x^{413} + 574x^{412} + 595x^{411} + 815x^{410} +$
 $281x^{409} + 491x^{408} + 443x^{407} + 561x^{406} + 840x^{405} + 266x^{404} + 150x^{403} + 850x^{402} +$
 $299x^{401} + 166x^{400} + 698x^{399} + 538x^{398} + 672x^{397} + 949x^{396} + 726x^{395} + 524x^{394} +$
 $335x^{393} + 784x^{392} + 294x^{391} + 906x^{390} + 281x^{389} + 653x^{388} + 510x^{387} + 351x^{386} +$
 $159x^{385} + 381x^{384} + 109x^{383} + 657x^{382} + 764x^{381} + 298x^{380} + 756x^{379} + 918x^{378} +$
 $659x^{377} + 686x^{376} + 764x^{375} + 858x^{374} + 961x^{373} + 630x^{372} + 746x^{371} + 903x^{370} +$
 $186x^{369} + 790x^{368} + 129x^{367} + 804x^{366} + 148x^{365} + 988x^{364} + 277x^{363} + 335x^{362} +$
 $489x^{361} + 633x^{360} + 913x^{359} + 698x^{358} + 111x^{357} + 1008x^{356} + 361x^{355} +$
 $871x^{354} + 735x^{353} + 651x^{352} + 994x^{351} + 992x^{350} + 734x^{349} + 314x^{348} + 566x^{347} +$
 $697x^{346} + 399x^{345} + 463x^{344} + 250x^{343} + 711x^{342} + 956x^{341} + 350x^{340} + 438x^{339} +$
 $803x^{338} + 932x^{337} + 275x^{336} + 731x^{335} + 390x^{334} + 951x^{333} + 793x^{332} + 116x^{331} +$
 $966x^{330} + 659x^{329} + 876x^{328} + 360x^{327} + 476x^{326} + 177x^{325} + 552x^{324} + 84x^{323} +$
 $663x^{322} + 610x^{321} + 356x^{320} + 997x^{319} + 1001x^{318} + 230x^{317} + 735x^{316} +$
 $783x^{315} + 814x^{314} + 736x^{313} + 225x^{312} + 767x^{311} + 239x^{310} + 658x^{309} + 784x^{308} +$
 $464x^{307} + 732x^{306} + 507x^{305} + 764x^{304} + 233x^{303} + 1005x^{302} + 782x^{301} +$
 $152x^{300} + 28x^{299} + 226x^{298} + 84x^{297} + 811x^{296} + 523x^{295} + 775x^{294} + 525x^{293} +$
 $305x^{292} + 800x^{291} + 642x^{290} + 204x^{289} + 625x^{288} + 521x^{287} + 217x^{286} + 193x^{285} +$
 $893x^{284} + 982x^{283} + 590x^{282} + 73x^{281} + 307x^{280} + 966x^{279} + 711x^{278} + 959x^{277} +$
 $823x^{276} + 619x^{275} + 923x^{274} + 902x^{273} + 728x^{272} + 695x^{271} + 256x^{270} + 441x^{269} +$
 $277x^{268} + 16x^{267} + 665x^{266} + 298x^{265} + 812x^{264} + 852x^{263} + 562x^{262} + 185x^{261} +$
 $93x^{260} + 1004x^{259} + 265x^{258} + 822x^{257} + 819x^{256} + 775x^{255} + 375x^{254} + 112x^{253} +$
 $974x^{252} + 200x^{251} + 44x^{250} + 976x^{249} + 83x^{248} + 501x^{247} + 983x^{246} + 94x^{245} +$
 $322x^{244} + 75x^{243} + 538x^{242} + 839x^{241} + 167x^{240} + 138x^{239} + 199x^{238} + 418x^{237} +$
 $553x^{236} + 535x^{235} + 997x^{234} + 336x^{233} + 31x^{232} + 872x^{231} + 32x^{230} + 879x^{229} +$
 $163x^{228} + 677x^{227} + 989x^{226} + 808x^{225} + 552x^{224} + 77x^{223} + 341x^{222} + 956x^{221} +$
 $140x^{220} + 756x^{219} + 914x^{218} + 814x^{217} + 986x^{216} + 480x^{215} + 250x^{214} + 976x^{213} +$
 $122x^{212} + 23x^{211} + 779x^{210} + 546x^{209} + 994x^{208} + 284x^{207} + 380x^{206} + 589x^{205} +$
 $541x^{204} + 458x^{203} + 592x^{202} + 512x^{201} + 52x^{200} + 612x^{199} + 442x^{198} + 590x^{197} +$

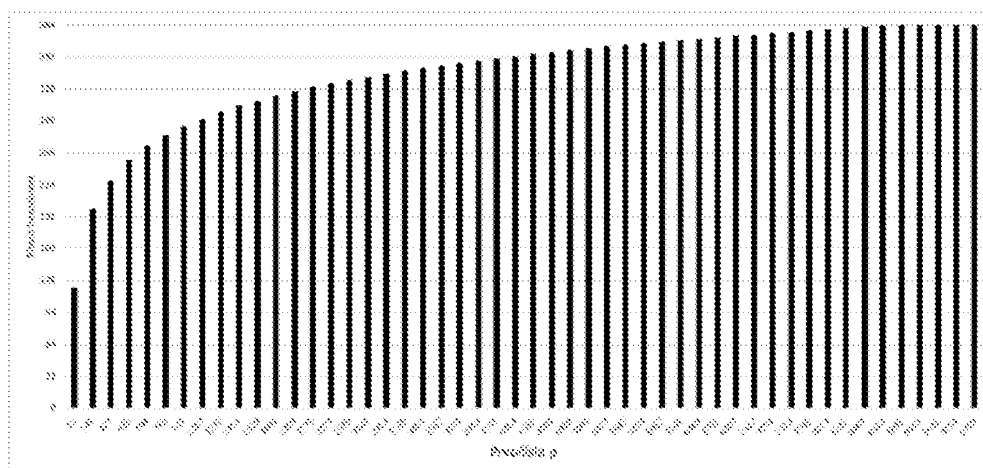
Obr. 4 pokračování

$$\begin{aligned}
& 4x^{186} + 522x^{185} + 64x^{184} + 685x^{183} + 833x^{182} + 110x^{181} + 935x^{180} + 940x^{179} + \\
& 159x^{188} + 1005x^{187} + 561x^{186} + 15x^{185} + 581x^{184} + 899x^{183} + 732x^{182} + 681x^{181} + \\
& 254x^{180} + 770x^{179} + 16x^{178} + 568x^{177} + 250x^{176} + 563x^{175} + 848x^{174} + 423x^{173} + \\
& 22x^{172} + 919x^{171} + 674x^{170} + 14x^{169} + 296x^{168} + 412x^{167} + 880x^{166} + 18x^{165} + \\
& 560x^{164} + 765x^{163} + 502x^{162} + 372x^{161} + 428x^{160} + 247x^{159} + 413x^{158} + 471x^{157} + \\
& 333x^{156} + 577x^{155} + 160x^{154} + 190x^{153} + 676x^{152} + 951x^{151} + 804x^{150} + 426x^{149} + \\
& 96x^{148} + 846x^{147} + 877x^{146} + 388x^{145} + 511x^{144} + 399x^{143} + 837x^{142} + 509x^{141} + \\
& 82x^{140} + 39x^{139} + 676x^{138} + 763x^{137} + 798x^{136} + 291x^{135} + 928x^{134} + 690x^{133} + \\
& 303x^{132} + 634x^{131} + 69x^{130} + 3x^{129} + 664x^{128} + 402x^{127} + 14x^{126} + 590x^{125} + \\
& 522x^{124} + 658x^{123} + 253x^{122} + 688x^{121} + 294x^{120} + 725x^{119} + 102x^{118} + 711x^{117} + \\
& 339x^{116} + 420x^{115} + 669x^{114} + 38x^{113} + 41x^{112} + 285x^{111} + 631x^{110} + 960x^{109} + \\
& 9x^{108} + 771x^{107} + 286x^{106} + 89x^{105} + 232x^{104} + 73x^{103} + 783x^{102} + 653x^{101} + \\
& 222x^{100} + 722x^{99} + 753x^{98} + 273x^{97} + 418x^{96} + 882x^{95} + 39x^{94} + 926x^{93} + \\
& 333x^{92} + 660x^{91} + 644x^{90} + 318x^{89} + 83x^{88} + 443x^{87} + 556x^{86} + 610x^{85} + \\
& 976x^{84} + 492x^{83} + 881x^{82} + 668x^{81} + 719x^{80} + 947x^{79} + 854x^{78} + 753x^{77} + \\
& 610x^{76} + 721x^{75} + 949x^{74} + 412x^{73} + 289x^{72} + 237x^{71} + 832x^{70} + 659x^{69} + \\
& 497x^{68} + 562x^{67} + 566x^{66} + 972x^{65} + 298x^{64} + 697x^{63} + 988x^{62} + 445x^{61} + 8x^{60} + \\
& 403x^{59} + 870x^{58} + 356x^{57} + 660x^{56} + 514x^{55} + 822x^{54} + 38x^{53} + 278x^{52} + \\
& 991x^{51} + 742x^{50} + 437x^{49} + 208x^{48} + 759x^{47} + 209x^{46} + 174x^{45} + 606x^{44} + \\
& 404x^{43} + 922x^{42} + 275x^{41} + 1002x^{40} + 463x^{39} + 833x^{38} + 979x^{37} + 508x^{36} + \\
& 981x^{35} + 274x^{34} + 271x^{33} + 335x^{32} + 999x^{31} + 366x^{30} + 319x^{29} + 62x^{28} + \\
& 399x^{27} + 932x^{26} + 700x^{25} + 221x^{24} + 771x^{23} + 142x^{22} + 594x^{21} + 317x^{20} + \\
& 672x^{19} + 397x^{18} + 896x^{17} + 113x^{16} + 476x^{15} + 281x^{14} + 640x^{13} + 535x^{12} + \\
& 482x^{11} + 930x^{10} + 488x^9 + 931x^8 + 511x^7 + 159x^6 + 147x^5 + 936x^4 + 313x^3 + \\
& 609x^2 + 898x + 498
\end{aligned}$$

Obr. 4 pokračování



Obr. 5



Obr. 6