UNIVERSITATEA TEHNICĂ A MOLDOVEI

Cu titlu de manuscris
C.Z.U.: 004.056.53/512.54

CUNEV VEACESLAV

TEHNOLOGII INFORMAȚIONALE INTEROPERABILE MODERNE ÎN SISTEMELE DE PLATĂ ELECTRONICE PROTEJATE, BAZATE PE ALGORITMI DE ANALIZĂ A FORMANȚILOR

232.02 –TEHNOLOGII, PRODUSE ŞI SISTEME INFORMAŢIONALE

Rezumatul tezei de doctor în informatică

CHIŞINĂU, 2023

Teza a fost elaborată în cadrul departamentului Ingineria Software și Automatică, Universitatea Tehnică a Moldovei.

Conducător ştiinţific:

BEȘLIU Victor, doctor în științe tehnice, profesor universitar.

Referenţi oficiali:

PERJU Veaceslav, doctor habilitat în științe tehnice, conferențiar universitar, Academician A.I.I.

OHRIMENCO Serghei, doctor habilitat în științe economice, profesor universitar.

Componenţa Consiliului Ştiinţific Specializat:

BOSTAN Viorel, **președinte**, doctor habilitat în științe tehnice, profesor universitar.

FIODOROV Ion, **secretar științific**, doctor în informatică, conferențiar universitar.

GAINDRIC Constantin, doctor habilitat în informatică, profesor universitar, membru corespondent al Academiei de Științe a Moldovei.

BOLUN Ion, doctor habilitat în informatică, profesor universitar.

COSTAȘ Ilie, doctor habilitat în informatică, profesor universitar.

ZGUREANU Aureliu, doctor în științe fizico-matematice, conferențiar universitar.

MORARU Victor, doctor în științe tehnice, conferențiar universitar.

Susţinerea va avea loc la **"30" iunie 2023**, ora **15.00** în şedinţa Consiliului Ştiinţific Specializat D 232.02-23-4, din cadrul Universităţii Tehnice a Moldovei pe adresa: MD-2045, Republica Moldova, Chişinău, str. Studenţilor 9/7, bl. 3, sala 3-208.

Teza de doctor şi rezumatul pot fi consultate la Biblioteca tehnico-științifică a Universităţii Tehnice a Moldovei şi pe pagina web a Agenției Naționale de Asigurare a Calității în Educație și Cercetare (www.cnaa.md/www.anacec.md).

Autoreferatul a fost expediat la "27" mai 2023.

Secretar ştiinţific
al Consiliului Ştiinţific Specializat
Dr. în informatică, conf. univ — **FIODOROV Ion**

Conducător ştiinţific
Dr. în informatică, conf. univ — **BEȘLIU Victor**

Autor — **CUNEV Veaceslav**

CUPRINSUL

I. REPERE CONCEPTUALE ALE CERCETĂRII

Actualitatea temei de cercetare. Toate sistemele financiare și de plăți (PS) existente, s-au dezvoltat dintr-o varietate de sisteme bazate pe hârtie, ce aveau diferite caracteristici ale contabilizării tranzacțiilor financiare, pentru fiecare țară a lumii. În prezent, în ciuda unificării semnificative ale acestui tip de sisteme, încă există diferențe majore în construcția și logica de afaceri a unor astfel de sisteme din diferite țări ale lumii. În același timp, deși sistemele de plăți sunt forțate să interacționeze între ele pentru a efectua tranzacții financiare, interfețele de interacțiune corespunzătoare sunt unice pentru fiecare sistem individual și, prin urmare, procesul de integrare este întotdeauna extrem de complex și consumator de timp, iar în exploatare apar probleme particulare referitoare la funcționarea neîntreruptă, dar și probleme de securitate a tranzacțiilor financiare, în general [1].

În teză termenul de "interoperabilitate" în contextul sistemelor de plăți este înțeles ca fiind compatibilitatea funcțională și informațională a acestor sisteme. Acesta reprezintă capacitatea unui număr mare de sisteme de plăți cu interfețe deschise de a interacționa și de a funcționa între ele fără restricții privind accesul și execuția, inclusiv schimbul și utilizarea informațiilor privind tranzacțiile, obținute ca urmare a schimbului. Cu alte cuvinte, sistemele de plăți ar trebui să funcționeze pe principiul "plata prin Internet" - ca o mulțime de sisteme independente, care utilizează un set standardizat de reguli, proceduri și protocoale [3, 4, 6, 7].

Necesitatea de a garanta securitatea informațiilor provine din cerința de a asigura protecția și integritatea tranzacțiilor, fiabilitatea și secretul informațiilor stocate sau transmise, indiferent de efectele distructive accidentale sau deliberate ale utilizatorilor sau generate de defecțiunile echipamentelor.

În prezent, criptografia este o parte integrantă a sistemelor de plăți și, pentru a realiza interoperabilitatea și securitatea acestora, este necesar să se utilizeze astfel de instrumente de criptografie care sunt compatibile, scalabile în ceea ce privește puterea criptografică și care au o viteză mare de funcționare [9, 10, 11, 12, 13]. Supremația cuantică poate anula toate

sistemele de plată actuale și, pe de altă parte, poate înlocui criptografia actuală cu ceva fundamental diferit, ceea ce va duce la costuri colosale. Astfel, este necesar să se consolideze fundamental criptografia existentă, fără a fi schimbate principiile de funcționare. În consecință, una dintre tendințele actuale în criptografie este dezvoltarea de noi metode care să asigure securitatea informațiilor și puterea criptografică, inclusiv utilizarea metodelor de analiză comparativă - ramură a teoriei numerelor, ce permite sporirea puterii criptografice a sistemelor existente, inclusiv pentru sistemul criptografic RSA [14, 16]. Puterea criptografică ridicată a sistemului RSA se bazează pe utilizarea dificultăților în determinarea funcțiilor inverse unidirecționale, în special atunci când este vorba despre descompunerea în factori a numerelor mari. Complexitatea temporală a algoritmilor de rezolvare a acestei probleme este extrem de mare, chiar dacă sunt utilizate cele mai performante echipamente de calcul.

În teză este propusă o tehnologie de criptare a datelor, bazată pe expedierea în timp real a unor date de volum scăzut despre informații, nu a informațiilor propriu zise cum are loc de obicei. Ca și rezultat, este asigurată puterea criptografică necesară pentru sistemul criptografic și eliminate întârzierile temporale.

Domeniul de cercetare include aspecte teoretice și practice ale protecției datelor, principalele idei ale organizării, construcției și utilizării instrumentelor criptografice în sistemele interoperabile, în contextul amenințării supremației cuantice, precum și dependența de dispozitivele tehnice disponibile persoanelor rău intenționate.

Obiectul cercetării este reprezentat de tehnologii bazate pe modele, metode și algoritmi de criptare/decriptare a datelor, pe analiza formantă în contextul aplicației lor, pentru utilizarea în sisteme de plată interoperabile și verificarea performanței acestor algoritmi în timp real, în limita unor constrângeri semnificative de timp.

Scopul și obiectivele cercetării. Scopul tezei este de a cerceta și dezvolta metode și algoritmi de protecție a datelor în sistemele de plăți interoperabile, atât în fața unei creșteri multiple a numărului de tranzacții, cât și a amenințării supremației cuantice.

Din scopul propus reiese următoarele obiective:

1. Analiza arhitecturilor și metodelor de interoperabilitate ale sistemelor de plăți pentru asigurarea protecției datelor în timp real.
2. Identificarea proprietăților și proceselor obligatorii ale sistemelor de plată interoperabile necesare, pentru a asigura proprietățile interoperabilității.
3. Dezvoltarea, pe baza metodelor de analiză formantă și a teoriei moderne a numerelor, a unor algoritmi eficienți de protecție criptografică, oferind o anumită rezistență criptografică temporară a sistemelor în timp real, pentru a asigura interoperabilitatea sistemelor de plăți și nivelul necesar de securitate.
4. Dezvoltarea unui algoritm, care oferă o creștere controlabilă a complexității computaționale a algoritmilor criptografici, fără reducerea performanței generale și debitul sistemului.
5. Dezvoltarea unui algoritm extins de criptare/decriptare în funcție de parametrii variabili ai algoritmului, care oferă o fiabilitate înaltă algoritmului RSA cu lungime mică a cheii.
6. Testarea eficacității algoritmilor propuși prin proiectarea unui sistem de protecție vocală în care mesajele criptate sunt transmise în timp real la o rată de transmisie de aproximativ 64 kb/s. Astfel se va verifica eficiența algoritmilor în timp real în sisteme în care viteza de procesare a datelor este mai mare decât în sistemele de plată.

Ipoteza cercetării. Realizările supremației cuantice pot anula toate rezultatele actuale din sistemele clasice de criptografie și, în consecință, necesitatea de a înlocui criptografia actuală cu ceva fundamental diferit va duce la costuri enorme. Una din soluții constă în consolidarea sistemelor criptografice existente fără a modifica principiile de funcționare.

În consecință, viteza relativ scăzută a criptosistemului RSA, dar puterea sa criptografică ridicată îi obligă pe dezvoltatori să caute modalități de a rafina acest sistem în condiții de posibilă supremație cuantică.

Suportul metodologic şi teoretico-ştiinţific al cercetărilor. La rezolvarea problemelor stabilite în lucrare, au fost utilizate metode de analiză formantă și analiză comparativă a teoriei numerelor, proiectarea obiectelor, metodele teoriei mulțimilor, teoria grafurilor și teoria rafinării specificațiilor.

Suportul metodologic al studiului se bazează pe teoria sistemelor, analiza matematică, teoria algoritmilor, metodele de modelare matematică și tehnologiile orientate pe obiecte.

Noutatea ştiinţifică. Noutatea științifică și semnificația teoretică a rezultatelor obținute rezidă în propunerea unor algoritmi RSA modernizați pe baza algebrei formanților și a aritmeticii șirurilor de analiză comparativă și formantă, ceea ce face posibilă utilizarea acestei abordări pentru a proteja sistemele moderne de plăți.

Originalitatea soluțiilor propuse constă în utilizarea analizei formante în criptografie, și anume pentru implementarea algoritmilor de criptare/decriptare care oferă o anumită putere criptografică temporară a sistemului în timp real și în propunerea metodei pentru creșterea controlată a complexității computaționale a algoritmilor criptografici, fără a reduce performanța generală și debitul sistemului.

Problema ştiinţifică soluționată este dezvoltarea de algoritmi de protecție a datelor pe baza algebrei formanților și aritmetica șirului de analiză comparativă și formantă, care oferă posibilitatea unei creșteri controlate a complexității computaționale a algoritmilor criptografici.

Semnificaţia teoretică a tezei constă în dezvoltarea unor metode și algoritmi originali, bazați pe analiza formantă, pentru a asigura securitatea sistemelor de plăți interoperabile care pot fi utilizate cu succes pentru protejarea datelor în timp real, ceea ce este deosebit de important pentru criptografia post-cuantică**.**

Valoarea aplicativă a lucrării constă în propunerea modernizării unor algoritmi de criptare cunoscuți, modernizare care constă în înlocuirea informațiilor transmise cu date protejate indirecte despre aceste informații. Algoritmii propuși sporesc puterea criptografică și complexitatea algoritmilor de criptare existenți fără a genera costuri suplimentare semnificative pentru modernizarea sistemelor curente.

Rezultatele practice obținute au fost brevetate în patentul RM Nr. 4511 (13) B1, „Dispozitiv și procedeu de protecție criptografică a

informației binare (variante)". A fost depusă o cerere de brevet „Metoda de criptare a informațiilor binare în spațiul spectral și unui dispozitiv de transmisie în baza lui".

Rezultatele ştiinţifice înaintate spre susţinere:

- O tehnologie bazată pe algoritmi de transmitere a informațiilor criptate prin crearea de date indirecte sub formă de formanți bazate pe analiza formantă.
- Algoritmi de criptare /decriptare - RSA-mAB (AB1, AB2, AB3), care oferă o anumită putere criptografică temporară a sistemelor în timp real.
- Algoritm extins de criptare/decriptare RSA-mAB, care oferă o creștere controlată a complexității computaționale în funcție de parametrii variabili.

Aprobarea rezultatelor lucrării. Conceptul principal, metodele și rezultatele au fost prezentate la 2 forumuri științifice:

- Conferinţă Internaţională "Telecomunicaţii, Electronică şi Informatică", ICTEI 2018, Mai 24-27, 2018, Chişinău, Moldova.
- Conferința "Teoria controlului matematic și aplicațiile sale" (MTUP-2020), 6-8 octombrie 2020, Sankt-Petersburg, Rusia.

Publicaţii ştiinţifice. Principalele rezultate ale cercetării teoretice sunt reflectate în 6 publicații, dintre care 3 sunt în reviste științifice, 2 rezumate ale discursurilor la conferințe științifice internaționale și o carte a fost publicată pe baza materialului prezentat. Rezultatele practice ale cercetării au fost brevetate în 2017, iar în 2021 a fost depusă o cerere de brevet.

Structura şi volumul lucrării. Lucrarea cuprinde: 110 pagini textul de bază, constând din introducere, patru capitole, concluzii și recomandări, bibliografie de 162 de surse.

II. CONȚINUTUL TEZEI

În **Introducere**, este prezentată argumentarea relevanței temei de cercetare. Se formulează scopul și obiectivele studiului, se prezintă domeniul și obiectul cercetării, sunt prezentate elementele noutății științifice a rezultatelor obținute, semnificația teoretică și valoarea

aplicativă a domeniului de cercetare, precum și un scurt rezumat al rezultatelor cercetării.

În primul capitol - **Cerințe moderne pentru interoperabilitatea sistemelor informatice**, a fost descrisă o imagine de ansamblu a caracteristicilor și categoriilor de sisteme interoperabile, a fost prezentat un model conceptual și o arhitectură generalizată a unui sistem interoperabil. Au fost analizate standardele pentru asigurarea interoperabilității și securității sistemelor informatice, s-a realizat o prezentare generală a problemelor de interoperabilitate a sistemelor moderne de plăți și au fost propuse principiile construirii unor sisteme de plată interoperabile.

Pentru a asigura interoperabilitatea și nivelul necesar de securitate al sistemelor moderne de plăți, trebuie să fie asigurate următoarele proprietăți importante:

- Garantarea integrității și a nerepudierii tranzacțiilor printr-un mecanism de semnătură digitală.
- Asigurarea nerepudierii oricărei acțiuni din sistem, atât a utilizatorului, cât și a administratorului sistemului.
- Fiecare utilizator și administrator trebuie să aibă propriul ID digital unic.
- Infrastructura informațională nu ar trebui să aibă un singur punct de defecțiune - acest lucru se aplică atât echipamentelor serverului, cât și sistemului informatic. De fapt, se vorbește despre o clasă descentralizată de sisteme.
- Proprietățile nerepudierii, integrității și protecției tranzacțiilor financiare și condițiile acestora ar trebui să se bazeze pe principii matematice și nu pe încrederea reciprocă a părților ce iau parte la tranzacție sau, față de intermediar.

Cel puțin, următoarele procese ar trebui să fie descentralizate în sistemele de plați interoperabile:

- confirmarea integrității tranzacțiilor;
- verificarea tranzacțiilor;
- păstrarea datelor;
- auditul de sistem (audit criptografic automat);
- luarea deciziilor cu privire la actualizare.

În capitolul doi - **Descrierea și modelarea proceselor criptografice** – se prezintă principalele domenii de aplicare a protecției criptografice, principiile puterii sistemelor criptografice și principalele metode de criptare - bazate pe lucrul cu date: criptarea blocurilor și a fluxurilor și bazate pe principiul de lucru cu chei: criptare simetrică și asimetrică. S-au prezentat avantajele și dezavantajele pentru fiecare metodă și algoritm analizat.

Astăzi, cel mai cunoscut și mai răspândit sistem criptografic este sistemul asimetric RSA [14, 15, 16]. Însă, există o problemă cu viitorul acestui algoritm, problemă care a apărut ca urmare a dezvoltării rapide a puterii de calcul și a apariției calculatoarelor cuantice: se presupune că aceste calculatoare vor rezolva problema descompunerii unui număr mare în factori primi în timp acceptabil.

Realitatea amenințării utilizării criptografiei clasice în sectorul financiar a fost analizată de compania americană ASC X9, care dezvoltă standarde financiare globale, inclusiv în domeniul protecției datelor criptate. În anul 2019 ASC X9 în raportul informativ "Riscurile calculului cuantic pentru industria serviciilor financiare" [5] oferă o prognoză a creșterii numărului de qubiți ai computerelor cuantice și încearcă să răspundă la întrebarea “pentru ce lungime de cheie a criptomonedelor clasice creșterea numărului de qubiți reprezintă un risc de compromitere?” În raport se afirmă că, dacă numărul de qubiți atinge valoarea 2500, criptografia clasică cu o lungime a cheii de 2048 de biți riscă să fie compromisă. Conform prognozei ASC X9 aceasta se poate întâmpla înainte de sfârșitul acestui deceniu.

Pe baza acestui fapt, una dintre tendințele actuale în criptografie este dezvoltarea de noi metode care asigură securitatea informațiilor și puterea criptografică, folosind metode de analiză comparativă.

Astfel, ținând cont de cerințele standardelor de interoperabilitate și securitate ale sistemelor de plată în comerțul electronic, se propune o tehnologie bazată nu pe transferul de informații în sine pe un canal deschis, ci pe transferul de date indirecte despre aceste informații, date care pot fi transmise în formă criptată cu gradul necesar de putere criptografică folosind RSA, fără întârzieri [15, 17].

În capitolul trei - **Protecția informațiilor folosind algoritmi RSA-mAB pe baza analizei formante**, sunt prezentați algoritmii RSA modernizați dezvoltați pe baza algebrei formante și aritmetica de analiză comparativă și formantă a șirurilor.

Se propune o metodă pentru o creștere controlată a complexității computaționale a algoritmilor criptografici, fără a reduce performanța generală și debitul sistemului. Este prezentat un algoritm extins de criptare/decriptare RSA-mAB, în funcție de parametrii variabili ai algoritmului, care oferă o fiabilitate ridicată a RSA cu o lungime mică a cheii.

Algoritmul AB1. Orice număr din analiza formantă poate fi reprezentat ca o construcție binomială [15];

$$N=pk+q, \tag{1}$$

unde p – este baza formantei; k - nucleul; q - restul. Cunoașterea tuturor celor trei parametri va permite cu ușurință de restabilit rapid numărul original.

Figura 1 prezintă o schemă bloc a algoritmului AB1 [4].

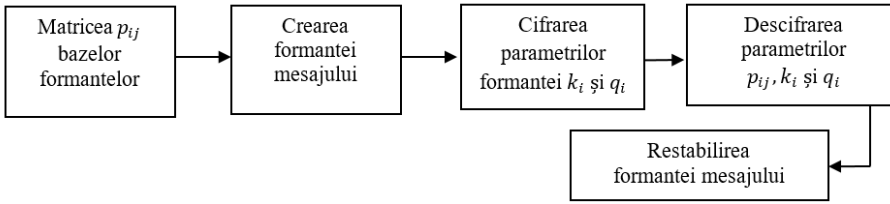

Fig. 1. Schema bloc a algoritmului AB1.

Pe baza (1), nu trebuie să se cripteze un număr N, ci doar trei numere mici. Diferența este că N este un număr întreg mare (de ordinul 10^{20} ... 10^{500} sau mai mult) și p, k și q sunt numere întregi ale căror valori sunt semnificativ mai mici și a căror lungime în biți este determinată numai de viteza necesară de transmitere a informațiilor printr-un canal deschis.

Se recomandă ca baza p să fie un număr mare, de ordinul lungimii cheii RSA (de exemplu, un număr corespunzător unui cifru bloc), astfel încât reziduurile de formantă să fie într-un set de numere suficient de

mari, ceea ce crește puterea criptografică finală. Pentru a crește viteza algoritmului, se creează o bază de date dinamică, de exemplu, sub forma unei matrice, în celulele cărora sunt stocate numere de bază formante pre-generate. În funcție de cerințele privind gradul de putere criptografică a algoritmului de criptare, acestea pot fi matrice pre-create cu tranziție rigidă sau flexibilă, automată sau manuală, de la o matrice la alta. Sau poate fi aceeași matrice în care celulele de bază își schimbă indicii. De exemplu, în conformitate cu regula $p_{ij}=p_{ji}$, $i=j=0,1\ldots n$, sau modificarea procedurii de indexare în conformitate cu o lege arbitrară diferită.

Descrierea algoritmului:

1. Din matricea bazelor, este selectat aleatoriu un număr de celulă, al cărui conținut va fi egal cu baza $p_{ij}=d_1$.
2. Blocul-numeric (mesaj deschis) este reprezentat ca formantă cu baza p_{ij} și se determină nucleul $k_i=d_2$ și restul $q_i=d_3$ conform formulei $F_p[N]=pk+q$.
3. Se generează un mesaj deschis $d_1d_2d_3$ despre formanta mesajului deschis.
4. Mesajul formant $d_1d_2d_3$ este criptat cu algoritmul RSA-m.
5. Datele criptate sunt transmise către un canal deschis.
6. Este primit un bloc de 64 de biți.
7. Din blocul primit, coordonatele celulei sunt extrase din matricea de bază p_{ij}.
8. Se restabilește baza p_i.
9. Numere k_i și q_i sunt extrase din bloc.
10. Mesajul formant este restabilit utilizând formula:

$$F=p_{ij}\cdot k_i+q_i=p_i\cdot d_2+d_3. \qquad (2)$$

Algoritmul AB2. Spre deosebire de algoritmul AB1, aici există două matrice - matricea de bază a formantei și matricea cheii RSA. Pentru fiecare sesiune de comunicare, indiferent de celula selectată a matricei de bază, cheile de sesiune RSA sunt selectate aleatoriu din matricea cheie RSA. Sunt transmise următoarele:

1. În mod deschis:

– Adresa celulei cheie a sesiunii RSA.

2. În mod criptat:
   – Adresa celulei matricei cu bazele formantei.
   – Nucleul formantei.
   – Restul formantei.

Într-o matrice de 10.000 de celule (100 de rânduri pe 100 de coloane), celulele sunt numerotate în ordine naturală:

00 De la 0 … până la 099
01 De la 100…. până la199
02 De la 200 … până la 299
…….
98 De la 8000… până la 8999
99 De la 9000 … până la 9999.

Aceleași celule pot fi reprezentate ca o variabilă cu două indici p_{ij} unde $i, j = 00, 01, ... 99$. De exemplu, numărul de celulă 457 are o adresă (index) P_{045}, iar numărul de celulă 4057 are P_{4057}. Fiecare celulă a matricei $p_{ij}(e, d, n)$ conține un index numeric criptat RSA, unde e este cheia publică, d este cheia privată și $n=p \cdot q$. Pentru a crește gradul de putere criptografică a RSA-mAB, se recomandă modificarea aleatorie a matricelor corespunzătoare diferitelor mesaje bloc criptografice în procesul de creare a unui bloc criptat de o lungime fixă. Numărul de astfel de matrice și dimensiunea lor depind de secretul pe termen lung al informațiilor, precum și de cantitatea de memorie operațională cât și capacitatea memoriei a microcontrolerului pe care este implementat criptosistemul RSA-mAB [15].

Algoritmul AB3. Spre deosebire de algoritmul AB2, există un set finit de matrice cu bazele formanților și matrici de chei RSA. Pentru fiecare sesiune de comunicare, este selectată o pereche aleatorie de matrice cu bazele formanților și matrice de chei RSA. Sunt transmise următoarele:

1. În mod deschis:
   – Numerele curente a matricelor cu bazele formantelor și cheile RSA.
   – Adresa celulei cheie RSA.
2. În mod criptat:

– Adresa celului matriciei cu bazele formantelor.
– Nucleul formantei.
– Restul formantului.

Acest algoritm constă din pașii corespunzători [15]:

1. Se formează un mesaj bloc. Din matricea cu bazele fromantelor, baza p_{ij} a formantei este selectată aleatoriu și numărul său este scris ca mesaj d_1 (celula d_1 stochează baza formantei create).
2. Numărul inițial, al blocului de informații generat, este reprezentat sub forma unei formante, toți ceilalți parametri fiind nucleul $k_i = d_2$, restul $q_i = d_3$ sunt determinați în dependența de baza selectată și sunt înregistrați în mesajele d_2 și d_3.
3. Se generează un mesaj $d_1\ d_2\ d_3$.
4. Cheile criptografice sunt generate pentru k_i și q_i.
5. Mesajul formant $d_1\ d_2\ d_3$ este criptat.
6. Mesajul criptat este transmis canalului de comunicare.
7. Este recepționat un bloc de 64 de biți.
8. Adresa de coordonate p_{ij} este extrasă din blocul recepționat.
9. Valoarea bazei formantei este restabilită.
10. Din blocul corespunzător, se extrag k_i și q_i ;
11. Formanta este restabilită din mesajul criptat pe baza formulei standard.

Pe partea de transmitere, programul are un tabel cu chei pe 64 de biți deja generate (conține valori pentru $p,\ q,\ n,\ e,\ d\ ,\ \varphi(n)$ unde p și q sunt de 64 de biți), unde $n = p \cdot q$; e – cheie publică; d – cheie privată; $\varphi(n) = (p-1)(q-1)$ - valoarea funcției Euler. Se introduce textul, care este convertit în numere, fiecare literă este codificată cu un număr zecimal de trei cifre. Apoi, pentru fiecare literă, se generează un index cheie (adresa celulei matricei de chei), iar cheile din tabel sunt citite utilizând acest index, apoi textul este criptat folosind algoritmul RSA clasic. Blocurile criptate sunt separate de patru zerouri plus indexul cheie din tabel și sunt afișate pe ecran (Figura 2) [15]. Pe partea de recepție, se analizează cifrul și locul (biții) unde, de exemplu, se află patru zerouri, ceea ce înseamnă pentru algoritm că acesta este începutul blocului și după 4 zerouri există un bloc de informații, de exemplu, o adresă sau un index cheie.

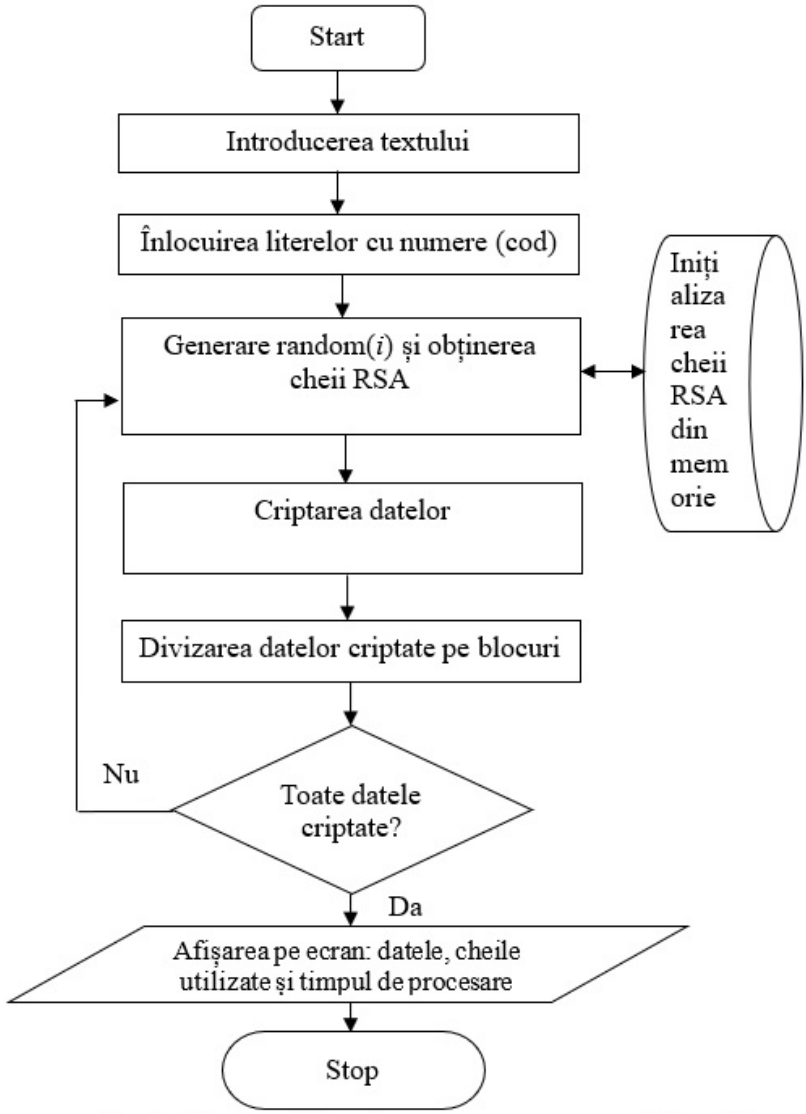

Fig. 2. Algoritmul de criptare pentru partea emițătorului.

La acest index, cheile RSA sunt selectate din zona de memorie corespunzătoare, după care se lansează procedura de decriptare a următorului bloc de date analizat. În continuare, acest număr este

convertit într-o literă, caracterul original sau un număr (secvență de biți) (Figura 3) și continuă din nou să caute zerouri în textul cifrat.

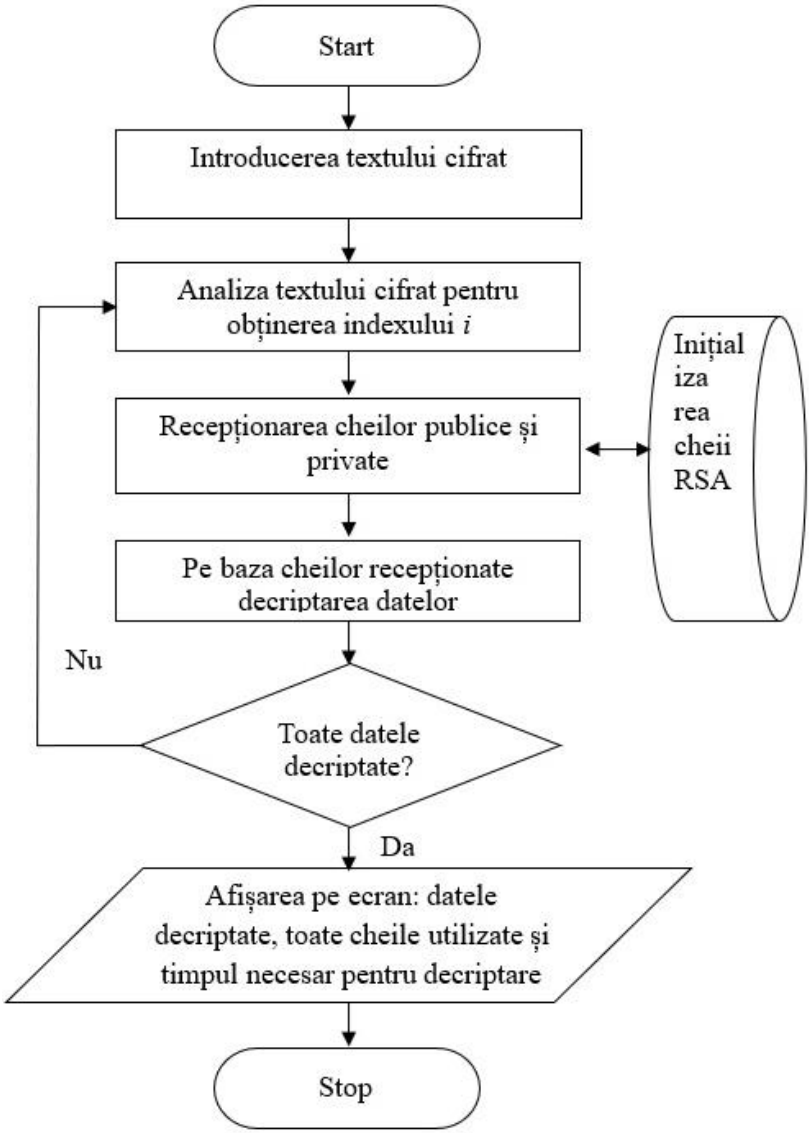

Fig. 3. Algoritmul de decriptare pe parte a receptorului.

Algoritmul extins RSA-m. Analiza puterii criptografice a RSA-mAB în funcție de parametrii variabili ai algoritmului.

Analiza formantei permite introducerea de incertitudini suplimentare în timpul criptării/decriptării dacă parametrul „*a*" este introdus suplimentar în ecuația de blocare criptografică RSA (3). După cum se știe, sistemul RSA asimetric utilizează proprietățile funcțiilor unidirecționale pentru un argument întreg care îndeplinește condițiile de existență a unei soluții a unuia dintre tipurile de ecuație diofantică cu parametrul a=1 [14-15].

$$e \cdot d = \varphi(n) \cdot k + 1. \qquad (3)$$

Pentru a=1 expresia (3) prezintă cheia de criptare obișnuită a sistemului clasic RSA.

Algoritmul extins („criptoblocare" modernizat, sau algoritmul RSA-mAB) înseamnă următoarea ecuație diofantică care leagă cheia publică (e, n) și cheia privată (p, q, d) RSA:

$$e \cdot d = k \cdot \varphi(n) + a = k \cdot \varphi(p) \cdot \varphi(q) + a = k \cdot (p-1) \cdot (q-1) + a,\ a \geq 1. \qquad (4)$$

Mai jos este prezentat un grafic comparativ pentru estimarea puterii criptografice a diferiților algoritmi prin compararea complexității rezolvării problemei factorizării unui număr în factori primi (problemă de factorizare) pentru următorii algoritmi:

- Algoritmul lui Shor - algoritm polinomial de factorizare cu timpul $log(n)$, destinat utilizării pe computerele cuantice [10].
- Metoda generală a filtrării unui câmp numeric - mai eficient algoritm de factorizare a algoritmilor clasici la moment.
- Algoritmul RSA-mAB. Complexitatea algoritmului este estimată prin formula:

$$O(\exp\{(\alpha+1)[\ln n]^r \ln[\ln n]^{n-r}\}) + O(A^s),$$

sau $O\left(e^{1,9lg[N]^{\frac{1}{3}}\, lg([logN])^{\frac{2}{3}}}\right) + O(A^S)$.

Pentru a estima complexitatea decodării câmpului de incertitudini introduse de formanți, se poate aplica formula $O(A^s)$, (unde A este lungimea alfabetului, de exemplu, de la 32 până la 560 de caractere), s

este lungimea bazei formantei (de la 15 până la 700 de zecimale sau și mai mulți biți până la 2048, Figura 4).

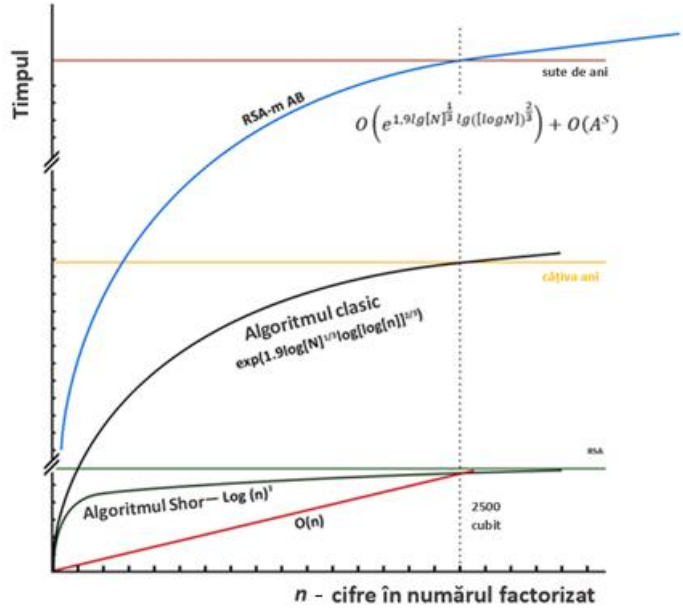

Fig. 4. Grafic comparativ pentru estimarea rezistenței criptografice la un atac de forță brută în perioada post-cuantică (r = 2048 biți).

În capitolul patru - **Sistem de criptare asimetrică pe biți a formantei unui mesaj vocal**, referitor la necesitatea modernizării algoritmului RSA pentru a corecta unele deficiențe bazate pe – analiza formanților. A fost analizată procedura de implementare a algoritmilor RSA modernizați în canalele de comunicații în bandă largă, ca un criptosistem principal pentru criptarea informațiilor, folosind o lungime mică a cheii, cu înlocuirea sa frecventă și rapidă. În acest capitol, a fost descris în detaliu sistemul de criptare asimetrică pe biți a formantei unui mesaj vocal.

Pentru a implementa abordarea în baza algebrei formante în pregătirea unui mesaj inițial pentru criptare, se formează matrice KN de dimensiune $n \times n$ pentru a stoca modulele numerice $N=p'q'$, calculate în conformitate cu algoritmul lui Euler pe baza numerelor prime p' și q' ale transformării criptografice RSA și perechii preselectate de chei

criptografice e_i și d_i cu lungimi diferite de $\mu(s_i)$ biți, precum și o matrice *PF* pentru stocarea bazelor p_i, nucleelor k_i și resturilor q_i a formantei corespunzătoare codului mesajului și o matrice *R*, de dimensiunea $n \times n$ pentru stocarea secvențelor de biți aleatorii de *M*-biți pentru codificarea blocurilor de informații criptate.

În procesul de difuzare a unei conversații pe un canal de comunicare (radio, telefon mobil, Internet etc.), fiecare eșantion la ieșirea ADC cu o amplitudine de biți $A_d(t_i)$ este considerat ca fiind adresa locației cheilor de criptare-plasate în memoria ROM în matrice *PF* de dimensiunea 2^{32}, unde cheile de criptare sunt distribuite aleatoriu între adrese, adică adresa matricei nu coincide cu valoarea eșantionului.

Criptarea se realizează în două etape: 1) găsirea parametrilor formantei - nucleul k_i și restul q_i pentru amplitudine A_d (t_i) a fonemului discret (sau bloc) pe baza p_i; 2) criptarea de către algoritmul RSA-m a parametrilor formantei k_i și q_i mbodulo N_i cu cripto-cheia individuală e_i, (*i* fiind numărul blocului discret sau informațional care urmează să fie criptat/decriptat și, în conformitate cu algoritmul RSA de criptare a sistemului $e_i d_i (\mathrm{mod}\ N)=1$). După fiecare sesiune de comunicare, adresarea cheilor din memoria ROM se schimbă automat în funcție de algoritmul.

Astfel, metoda revendicată este de fapt echivalentă cu criptarea unui mesaj cu o cheie unică cu o lungime aleatorie, în funcție de lungimea mesajului, sub forma unui discret sau bloc (conform algoritmului selectat), ceea ce corespunde îndeplinirii condițiilor teoremei lui Shannon privind imposibilitatea decriptării [8].

Toate discrete sunt criptate cu trei parametri ai formantei *p*, *q, k* și stocate în memorie sub formă de indici ai matricei M_1. Astfel, același discret în memoria ROM va avea 10.000 de indici de adresă diferiți într-o matrice de tip M_1.

Aceeași distribuție în memoria ROM se formează pe partea de recepție [2].

Cum funcționează emițătoul:

1. Sunetul, vorbirea sunt digitizate folosind ADC.
2. Următorul discret este scris în buffer:

a) valoarea eșantionului este convertită într-un număr întreg de biți;

b) formanta este calculată (sau un astfel de număr este căutat în ROM) și adresa sa este scrisă în memoria RAM (la această adresă toate informațiile despre întregul flux vor fi localizate în ROM).

3. Se formează text-semnal al pachetului: se transmit 4 adrese: 3 adrese pentru *p*, *q*, *k* și a 4-a adresă pentru controlul informațiilor transmise în celula de control.

Funcționarea pe partea de recepție:

1. Recepția și analiza semnalului. Adresele *p*, *q*, *k* sunt citite și valorile lor sunt comparate cu datele din celula de control.

2. Semnalul vocal se restabilește în baza adreselor discretelor.

3. Reproducerea semnalului.

Figura 5 prezintă transferul de date care are loc după cum urmează: microfon → ADC → calculul formantei discretei curente (în forma de un număr întreg) → găsirea adresei celulei formante → înscrierea în memorie (buffer) → formarea semnalului-text cifrat a mesajului: → transmiterea adresei criptate a celulei spre receptor → .... → recepția semnalului cifrat al mesajului → decodare → decriptare → descompunere pachetului recepționat → reproducerea semnalului vocal [2].

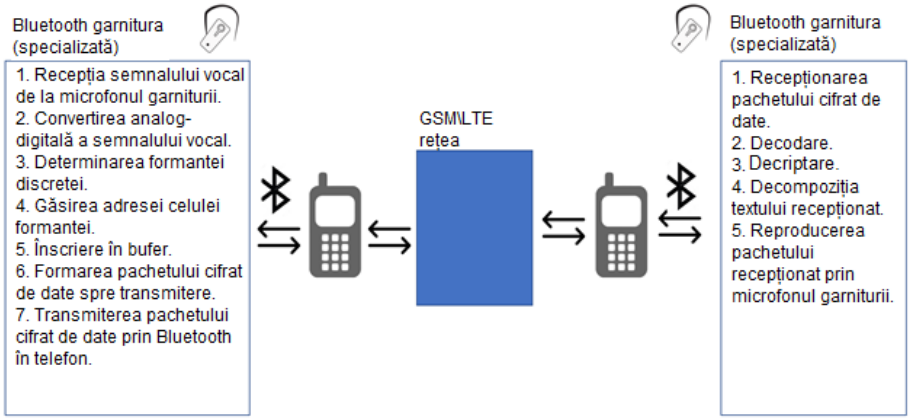

Fig. 5. Infograma dispozitivului de transmisie securizată a datelor mobile.

III. CONCLUZII GENERALE ȘI RECOMANDĂRI

Această lucrare este un studiu care își propune dezvoltarea de noi metode, proceduri și algoritmi originali utilizați pentru a proteja informațiile din sistemele de plăți interoperabile. Metodele dezvoltate în teză pot fi utilizate cu succes pentru a proteja informațiile secrete pe termen scurt și pe termen lung în sistemele de plăți interoperabile, în care prelucrarea și transmiterea datelor se desfășoară online.

Analizând rezultatele obținute în teză, pot fi trase următoarele concluzii:

1. Pentru a asigura interoperabilitatea sistemelor de plăți și nivelul necesar de securitate, este necesar de utilizat instrumente criptografice compatibile, scalabile referitor la puterea criptografică și care au o viteză mare de operare, având în vedere creșterea exponențială a numărului de tranzacții din sistemele de plăți. Progresele în calculul cuantic ar putea compromite securitatea tuturor sistemelor de plăți actuale bazate pe mecanismele criptografice actuale. Înlocuirea criptografiei actuale cu ceva fundamental diferit va duce la costuri și pierderi enorme, astfel încât există o nevoie urgentă de a consolida puterea criptografică existentă fără a-i schimba principiile de funcționare.

2. Reieșind din cerințele standardelor de interoperabilitate și securitate a sistemelor de plăți în comerțul electronic, a fost stabilit că este necesar de dezvoltat tehnologii, ce folosesc algoritmi de transmitere a datelor criptate, bazați pe utilizarea formanților numerici, expediind în timp real în locul informațiilor propriu zise, date indirecte despre aceste informații, date care a căror lungime în biți este mult mai mică. Ca și rezultat, aceste date sunt transmise în format criptat la viteza necesară și putere criptografică suficientă folosind sistemul RSA-m actualizat.

3. Algoritmul RSA a fost modernizat pe baza unei noi direcții a teoriei numerelor – analiza formantă. Astfel, au fost introduși parametri suplimentari nedefiniți pentru a fi determinați în timpul încercărilor de hacking, ceea ce sporește timpul necesar hackingului și, în cazul criptării informațiilor pe termen scurt, pot servi ca mijloc de creștere a puterii criptografice a sistemului (de exemplu, în timpul negocierilor operaționale sau în cazul tranzacțiilor în timp real).

4. Pe baza algoritmilor de analiză formantă, au fost dezvoltați algoritmi de criptare/decriptare - RSA-mAB (AB1, AB2, AB3), care oferă, la viteza necesară, o anumită stabilitate criptografică temporară a sistemelor de plată în timp real, când timpul de descompunere și restabilire a numerelor este cu mai multe ordine de mărime mai mic decât timpul de criptare și decriptare a aceluiași număr folosind criptosistemul clasic RSA.

5. Algoritmul extins RSA-m reduce semnificativ timpul pentru generarea de noi chei criptografice ale următorului pachet de date și, astfel, permite schimbarea rapidă a cheilor criptografice de un număr nelimitat de ori în timpul procesului, ceea ce va complica, de asemenea, în mod semnificativ, sarcina de hacking a mesajelor transmise, ceea ce este un punct slab în sistemul RSA clasic. Stabilitatea criptografică a algoritmului RSA-m poate fi semnificativ mai mare decât toți algoritmii criptografici existenți și poate crește cu ordine de mărime pe măsură ce cerințele pentru nivelul de protecție cresc, numai prin schimbarea parametrului de funcționare a algoritmului, fără o scădere semnificativă a vitezei de funcționare.

6. Algoritmii propuși au fost testați pentru a cripta informații din sistemele de comunicații vocale, unde sunt transmise mesaje vocale criptate, în timp real, la o rată de transmisie de aproximativ 64 kb/s. O caracteristică a sistemului dezvoltat este utilizarea în timp real a criptării asimetrice pe biți (streaming sau block-phonemic, bloc pe 32 de biți) a formantei unui mesaj vocal (adică un analog adecvat sub forma unui model - imagine, convoluție) prin algoritmi RSA-mAB, menținând în același timp nivelul ridicat de securitate criptografică inerent al algoritmului RSA, dar folosindu-l cu o frecvență ridicată de schimbare a cheilor criptografice scurte suficientă pentru a oferi un nivel de protecție pe termen scurt pentru negocieri (3-10 minute), și cu o creștere a nivelului pe termen lung (până la câteva luni și ani), modificarea și lungimea cheilor criptografice la valori care asigură nivelul revendicat de putere criptografică la intervale de timp crescute de secretizare. În acest caz, atunci când se utilizează chei care se schimbă rapid, fiecare dintre acestea având o lungime de 19 zecimale (≈152 biți), sistemul va asigura securitatea unei sesiuni de negociere de 24 de ore pentru o

perioadă de trei ani și cu o lungime cheie de 9 zecimale (≈ 72 de biți) - aproximativ câteva săptămâni.

Ca domenii viitoare de cercetare, se propune:

1. Utilizarea algoritmilor în alte domenii, în diverse scopuri: autentificare, blockchain, sisteme de plată cu cardul etc. adaptându-i (modernizându-i).

2. Implementarea hardware completă a acestor algoritmi pe baza microprocesoarelor, pentru a oferi o viteză de criptare mai mare și, prin urmare, explorarea acestui domeniu de implementare hardware, deoarece sistemele interoperabile includ atât sisteme software cât și hardware implementate pe microprocesoare, unde există limitări ale memoriei utilizate și ale vitezei de procesare a datelor.

3. Implementarea algoritmilor în procesul de autentificare automată pe baza caracteristicilor biologice unice ale unei persoane, unde este necesar să se recunoască în mod clar obiectele în timp real, asigurând sistemului puterea criptografică necesară.

IV. BIBLIOGRAFIE

1. ALHOTHAILY, A., ALRAWAIS, A., CHENG, X. et al. A novel verification method for payment card systems. In: *Pers Ubiquit Comput* 19, 2015, p. 1145–1156. https://doi.org/10.1007/s00779-015-0881-9.
2. BALABANOV, A., AGAFONOV, A., **CUNEV, VEACESLAV**. Dispozitiv și procedeu de protecţie crypto-grafică a informaţiei binare (variante). Brevet de invenție 4511 (13) B1, 31 august 2017.
3. CAI, XQ., WEI, CY. Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature. In: *Quantum Inf Process* 12, 2013, p. 1651–1657. https://doi.org/10.1007/s11128-012-0477-5.
4. CHEN, D., CHUNG, J.Y., OBI&XML standard based business to business electronic business solution. In: *Proceedings of the International Symposium on Government and E-commerce Development*, Ningbo, China, 23-24 April 2001, pp. 35-41.

5. *Informative Report. ASC X9 IR 01-2019. Quantum Computing Risks to the Financial Services Indutry.* By the ASC X9 Quantum Computing Risk Study Group, 1st ediation, 2019, 42 p.
6. LUHACH, ASHISH, DWIVEDI, SANJAY, JHA C. Designing and Implementing the Logical Security Framework for Ecommerce Based on Service Oriented Architecture. In: *International Journal of Advanced Information Technology (IJAIT)* Vol. 4, No. 3, June 2014, pp. 25-34. DOI : 10.5121/ijait.2014.4303
7. MATSUI, M. The First Experimental Cryptanalyst of the Data Encryption Standard. *Proc. CRYPTO'94. Lecture Notes in Comp*, Sci. Springer-Verlag, 1996.
8. PRICE, E., WOODRUFF, D. P. Applications of the Shannon-Hartley theorem to data streams and sparse recovery. In: Proceedings of the *2012 IEEE International Symposium on Information Theory*, 2012, p. 2446-2450. doi: 10.1109/ISIT.2012.6283954.
9. SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science,* 1994, p.124-134. doi:10.1109/sfcs.1994.365700.
10. WESTERMANN, B. Security Analysis of AN.ON's Payment Scheme. In: Jøsang A., Maseng T., Knapskog S.J. (eds) Identity and Privacy in the Internet Age. NordSec 2009. *Lecture Notes in Computer Science*, vol 5838. Springer, Berlin, Heidelberg., 2009, p. 255-270. https://doi.org/10.1007/978-3-642-04766-4_18.
11. XIE, SC., NIU, XF. & ZHANG, JZ. An Improved Quantum E-Payment System. *Int J Theor Phys* 59, 2020, p. 445–453. https://doi.org/10.1007/s10773-019-04338-7.
12. YANG, JH., CHANG, CC. A Low Computational-Cost Electronic Payment Scheme for Mobile Commerce with Large-Scale Mobile Users. *Wireless Pers Commun* 63, 2012, p. 83–99. https://doi.org/10.1007/s11277-010-0109-2.
13. ZGUREANU, A. Information encryption systems based on Boolean functions. In: *Computer Science Journal of Moldova*, vol.18, no.3(54), 2010, pp. 319-335.

14. АГАФОНОВ, А. *Научные труды по математике, физике и социологии истории. Математические начала в исследовании исторических процессов*. Избранное / А.Ф. Агафонов. Научный редактор академик РАЕН – А.А. Балабанов. К. : ТУМ, 2011, 227 с. ISBN 978-9975-45-177-2.
15. БАЛАБАНОВ, А., **КУНЕВ, В. В.** *Защищённые IT-системы на основе алгоритмов формантного анализа: Новые направления и перспективы*. LAP LAMBERT Academic Publishing, 2016, 220 с. ISBN 3659948268, 9783659948268.
16. БАЛАБАНОВ, А. А., АГАФОНОВ, А. Ф. Методы сопоставительного анализа и формантных уравнений теории чисел в задачах криптографии. *Вестник Российской Академии Естественных Наук*,Том 14, № 4, 2014, кат. Б, с. 47-53. ISSN 1682-1696.
17. БАЛАБАНОВ, А.А., АГАФОНОВ, А.А. *Сопоставительный анализ и его приложения. Классические и современные задачи теории чисел и криптографии*. LAP LAMBERT Academic Publishing, 2016, 200 с. ISBN 978-3-659-92621-1.

V. LISTA LUCRĂRILOR PUBLICATE LA TEMA TEZEI

În reviste din străinătate recunoscute:

1. БАЛАБАНОВ, А., **КУНЕВ, В. В.** Современное применение алгоритмов формантного анализа для криптозащиты IT-систем. *Журнал: Вестник Российской Академии Естественных Наук РАЕН*, том 19, № 3, 2019, 25-35 с.

În reviste din Registrul Naţional al revistelor de profil, cu indicarea categoriei:

Categoria B +

2. BALABANOV, A. **KUNEV, V**., COLESNIC V. Spectral Space as a Method for Data Crypto Protection Using the Fast Fourier Transform. In: *Journal of Engineering Science* Vol. XXVIII (1) 2021, pp. 75 – 82. ISSN 2587-3474/ eISSN 2587-3482. https://doi.org/10.52326/jes.utm.2021.28(1).07. https://jes.utm.md/vol-xxviii-1-2021/

3. **KUNEV, V**. Extended RSA-M Algorithm as a Way of Increase Computational Complexity of Cryptosystems. In Journal of Engineering Science Vol. XXV(2) (2018), pp. 45-56. ISSN 2587 3474/ eISSN 2587-3482. DOI: 10.5281/zenodo.2564486. Microsoft Word - JES 2-2018 (utm.md)

Articole în culegeri ştiinţifice:
În lucrările conferinţelor ştiinţifice internaţionale (peste hotare):

4. БАЛАБАНОВ, А., **КУНЕВ, В. В.** Криптографическая защита цифровой информации в частотной и спектральной областях на основе алгоритмов форматного анализа (ч.1. основы теории) В: *Материалах Конференции «Математическая теория управления и ее приложения» (МТУиП-2020)*, Санкт-Петербург, 6–8 октября 2020, с. 228-233.

În lucrările conferinţelor ştiinţifice internaţionale (Republica Moldova)

5. CUNEV, V. Secure Voice Data Transmission Based on the Formant Analysis Algorithms. In: P*roceedings of the 6th International Conference "Telecommunications, Electronics and Informatics" ICTEI 2018*, Chisinau, 24-27 mai 2018, pp. 34-39. ISBN 978-9975-45-540-4.

Brevete de invenţii şi alte obiecte de proprietate inteectuală, materiale la saloanele de invenţii

6. BALABANOV, A., AGAFONOV, A., CUNEV, V. Dispozitiv și procedeu de protecţie crypto-grafică a informaţiei binare (variante). 4511 (13) B1, Int. Cl.: H04L 9/14 (2006.01) H04L 9/28 (2006.01) H04L 9/30 (2006.01) G06F 1/00 (2006.01) G06F 12/16 (2006.01) G11B 20/00 (2006.01); a 2016 0046; 2016.04.20, 31 august 2017.

7. Cerere de înregistrare a brevetului din 15 aprilie 2021, titlu: Metoda de criptare a informațiilor binare în spațiul spectral și unui dispozitiv de transmisie în baza lui; autori BALABANOV, A., KUNEV, V., CERNOMOREȚ, E.

Adnotare

la teza de doctor în informatică cu tema „Tehnologii informaționale interoperabile moderne în sistemele de plată electronice protejate, bazate pe algoritmi de analiză a formanților", Chișinău, 2023

autor: CUNEV Veaceslav

Structura tezei. Teza de doctor cuprinde introducerea, patru capitole, concluzii, bibliografia cu 162 titluri, 110 pagini text de bază, inclusiv 25 figuri. Rezultatele obţinute sunt publicate în 5 - lucrări ştiinţifice, 1 – carte, 1- brevet de invenție, 1 – cerere de înregistrare a brevetului.

Cuvinte cheie: Interoperabilitate sistemelor, securitatea informațională, criptografie, cripto-stabilitate a sistemelor, algoritmii de analiza formantă.

Domeniul de studiu îl constituie aspectele teoretice şi practice ale asigurării securității datelor, ideile de bază ale organizării, formării și utilizării instrumentelor criptografice în sistemele informaționale interoperabile.

Scopul şi obiectivele lucrării constă în dezvoltarea metodelor și algoritmilor de protecție a datelor pentru sistemele interoperabile, cu un nivel ridicat de securitate criptografică, pe baza metodelor de analiza formantă și a teoriei numerelor.

Noutatea şi originalitatea ştiinţifică a rezultatelor obţinute constă în propunerea algoritmilor modernizați-RSA pe baza algebrei formante și a aritmeticii de șiruri a analizei comparative și formante, cu asigurarea stabilității criptografice temporale date a sistemului în timp real și propunerea unei metode de creșterea controlată a complexității de calcul a cripto-algoritmilor.

Semnificaţia teoretică a lucrării constă în propunerea și dezvoltare a metodelor și algoritmilor de protecție a datelor bazate pe analiza formantă, care pot fi utilizate cu succes pentru asigurarea securității datelor în timp real în sisteme interoperabile.

Valoarea aplicativă a lucrării constă în modernizare a unor algoritmi criptografici cunoscuți de cifrare/decifrare, prin înlocuirea informației închise transmise cu niște date protejate indirecte. Algoritmii criptografici dezvoltați au permis de a crește cripto-stabilitate și complexitatea algoritmilor criptografici, fără a fi nevoie de costuri semnificative de modernizare a sistemelor informatice existente.

Implementarea rezultatelor ştiinţifice: rezultatele științifice ale cercetării au fost brevetate, iar algoritmii dezvoltați au fost acceptați pentru testare ca parte a produselor proprii de companii: KVAZAR-MICRO S.R.L., Qsystems S.R.L., Alfasoft S.R.L.

Аннотация

Диссертации на соискание учёной степени доктор в информатике, с темой „Современные интероперабельные информационные технологии в защищенных платежных системах на основе алгоритмов формантного анализа", Кишинёв 2023,

автор: КУНЕВ Вячеслав

Структура работы. Диссертация состоит из введения, четырёх глав, выводов, библиографии из 162 наименований, 110 страниц основного текста, включая 25 рисунков. Полученные результаты опубликованы в 5–и научных работах, 1-й – книги, 1 - патент, 1 – заявка на патент.

Ключевые слова: интероперабельность систем, информационная безопасность, криптография, криптостойкость систем, алгоритмы формантного анализа.

Область исследования включает в себя теоретические и практические аспекты защиты данных, основные идеи организации, построения и использования криптографических средств в интероперабельных информационных систем.

Цель и задачи работы состоят в разработке методов и алгоритмов защиты информации в интероперабельных платежных системах, с повышенным уровнем крипто защищённости, на основе методов формантного анализа и современной теории чисел.

Научная новизна и оригинальность полученных результатов заключается в предложении модернизированных RSA-алгоритмов на основе формантной алгебры и строковой арифметики сопоставительного и формантного анализа, обеспечивающих заданную временную криптостойкость системы в режиме реального времени, и в предложении способа контролируемого повышения вычислительной сложности криптоалгоритма RSA.

Теоретическое значение заключается в разработке и развитие оригинальных методов и алгоритмов на основе формантного анализа для обеспечения безопасности интероперабельных платежных систем, которые могут быть успешно использованы для защиты данных в режиме реального времени.

Практическая ценность работы заключается в предлагаемой модернизации известных крипто-алгоритмов, позволивших заменить передаваемую информацию защищёнными косвенными данными о ней. Разработанные алгоритмы криптозащиты позволяют наращивать криптостойкость и сложность существующих криптоалгоритмов без существенных затрат на модернизацию уже существующих информационных систем.

Научные результаты работы были запатентованы, а разработанные алгоритмы были приняты для тестирования в составе собственных продуктов компаниями: S.R.L. КВАЗАР-МИКРО S.R.L., QSystems S.R.L., генеральный директор Alfasoft S.R.L.

Annotation

Of the Ph. D. Thesis in Informatics with title „ Modern interoperable information technologies in secured payment systems based on formant analysis algorithms", Chisinau, 2023

author: CUNEV Veaceslav

Thesis structure. The Ph.D. thesis consists of the Introduction, four Chapters, Conclusions, Bibliography (162 titles), 110 pages of main text, 25 figures. The obtained results have been published in 5 - scientific articles, 1 – book, 1 – patent, 1 – patent application.

Kew words: interoperability of the systems, information security, cryptography, cryptographic stability of systems, formant analysis algorithms.

The field of research encompasses theoretical and practical aspects of data protection, the main ideas of organization, design and use of cryptographic tools in the interoperable information systems.

The research objectives focus on the development of methods and algorithms for information protection within interoperable systems with high level of crypto - security, based on the methods of formant analysis and modern number theory.

Scientific novelty and originality of the obtained results consists in proposing the modernized RSA – algorithms, which are based on formant algebra and string arithmetic of comparative and formant analysis, which provide a given temporary cryptographic stability of the system in real time and in proposing the method for controlled increase the computational complexity of crypto algorithms.

Theoretical value of the paper consists in elaborating methods and algorithms for cipher/decipher data based on formant analysis that ensure the security of interoperable systems in real time.

Practical value of the paper consists in the procedure modernization of well-known crypto-algorithms, which made possible to replace the transmitted information with protected indirect data about it. The developed cryptographic protection algorithms allow to increase the cryptographic stability and complexity of existing crypto algorithms without significant costs for the modernization of existing information systems

Implementation of the scientific results: the scientific results of the work were patented and the developed algorithms were accepted for testing as a part of products develop by the companies: KVAZAR-MICRO S.R.L., QSystems S.R.L., Alfasoft S.R.L.

CUNEV VEACESLAV

TEHNOLOGII INFORMAȚIONALE INTEROPERABILE MODERNE ÎN SISTEMELE DE PLATĂ ELECTRONICE PROTEJATE, BAZATE PE ALGORITMI DE ANALIZĂ A FORMANȚILOR

232.02 –TEHNOLOGII, PRODUSE ŞI SISTEME INFORMAŢIONALE

Rezumatul tezei de doctor în informatică

Aprobat spre tipar: 25.05.2023
Hârtie ofset. Tipar digital.
Coli de tipar: 1.73

Formatul hârtiei 60×84 1/16
Tirajul 50 exemplare
Comanda Nr. 20

U.T.M. 2023. Chişinău, bd. Ştefan cel Mare şi Sfânt 168.
Secţia Redactare şi Editare a U.T.M.
2045, Chişinău, str. Studenţilor 9/9.