Kriptologiya: tədqiqatların müasir vəziyyəti haqqında bəzi qeydlər

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu
yadigar@lan.ab.az

***Xülasə*— Kriptologiya informasiya təhlükəsizliyinin təmin edilməsi üçün baza texnologiyaları təqdim edir. Ölkəmizdə bu sahədə tədqiqatlar başlanğıc səviyyədədir və gənc tədqiqatçıların diqqətinin bu sahədə prioritet istiqamətlərdə tədqiqat mövzularına cəlb edilməsinə ehtiyac vardır. Bu məqsədlə bu məqalə son bir neçə ildə kriptologiyada baş vermiş diqqətəlayiq hadisələrin icmalına həsr olunur. Kriptologiyada həm ənənəvi, həm də yeni meydana çıxan istiqamətlərdə əldə edilmiş əsas nəticələr analiz edilir, kriptologiya üzrə elmi-tədqiqat müsabiqələrinin təcrübəsi təhlil olunur və yeni müsabiqələr barəsində məlumat verilir, bir sıra prioritet tədqiqat istiqamətləri göstərilir.**

Açar sözlər*— *kriptologiya; kriptoqrafiya; kvant kriptoqrafiyası; homomorf şifrləmə; heş funksiya; kriptoqrafiya müsabiqələri; yüngülçəkili kriptoqrafiya.

I. GİRİŞ

Kriptoqrafiya kommunikasiyaların konfidensiallığını, e-sənədlərin həqiqiliyini, elektron tranzaksiyaların təhlükəsizliyini və bir çox digər funksiyanı təmin edərək informasiya təhlükəsizliyinin təmin olunmasında mühüm rol oynayır [1].

Bir zamanlar yalnız dövlət təşkilatlarının sərəncamında olan kriptoqrafiya indi insanların gündəlik həyatına daxil olur: mobil telefonla danışarkən, kompüterə daxil olarkən, bankomatlardan, elektron xidmətlərdən istifadə edərkən, onlayn alış-veriş edərkən kriptoqrafiyadan istifadə edirik. Hazırda kriptologiya sahəsində tədqiqatlar dünyada onlarla aparıcı elmi-tədqiqat institutu, universitetlər, şirkətlər və müvafiq dövlət qurumları tərəfindən aparılır [2].

Son dövrlər informasiya texnologiyalarının inkişaf istiqamətlərini müəyyən edən bir neçə texnologiya – mobil texnologiyalar, Əşyaların İnterneti, bulud texnologiyaları, Big Data texnologiyaları və s. kriptoqrafiyaya xüsusi tələblər qoyur və özünəməxsus kriptoqrafik alqoritmlərin işlənməsini tələb edir. Məsələn, Əşyaların İnterneti yüngülçəkili kriptoqrafiya [3], Big Data və bulud texnologiyaları yüksək sürətli kriptoqrafiya tələb edir [4].

Bu işin məqsədi kriptologiya sahəsində son bir neçə ildə baş vermiş əsas hadisələri sistemləşdirmək və tədqiqatçıların diqqətinə çatdırmaqdır. Kriptoqrafiya sahəsində perspektiv tədqiqat istiqamətləri üzrə işlər təhlil olunur və kriptoqrafik analiz üzrə ən diqqətçəkən hadisələr haqqında məlumat verilir. Kvant kriptoqrafiyasının və post-kvant kriptoqrafiyasının hazırki vəziyyəti analiz edilir. Kriptologiya sahəsində tədqiqatlara stimul verən daha bir mexanizm kriptoqrafik standartların işlənməsi üçün təşkil edilən açıq beynəlxalq müsabiqələrdir. Məqalədə belə müsabiqələrin təcrübəsi də qısaca analiz edilir.

II. KRİPTOLOGİYA SAHƏSİNDƏ TƏDQİQATLARIN AKTUAL İSTİQAMƏTLƏRİ

Kriptologiya sahəsində elmi-tədqiqatların hazırki vəziyyətini qiymətləndirmək üçün Kriptologiya Tədqiqatları üzrə Beynəlxalq Assosiasiyanın (The International Association for Cryptologic Research, IACR) təşkil etdiyi EuroCrypt, Crypto, AsiaCrypt kimi konfransların və bir çox seminarların təcrübəsini izləmək faydalıdır. Assosiasiyanın www.iacr.org veb-saytından konfransların və seminarların əsərlərinə çıxış imkanı vardır.

Müasir kriptoqrafiyada bir neçə böyük tədqiqat istiqaməti formalaşıb: (1) simmetrik kriptosistemlər; (2) açıq açarlı (asimmetrik) kriptosistemlər; (3) elektron imza sistemləri; (4) kriptoqrafik protokollar.

Simmetrik kriptosistemlər. Bu sahədə tədqiqatların əsas istiqamətləri blok şifri primitivləri, axın şifri primitivləri, məlumatı autentifikasiya kodu primitivləri, heş funksiya primitivləri, əməliyyat rejimləri və simmetrik kriptoqrafik primitivlərin istifadəsi, simmetrik üsullar və psevdo-təsadüfi funksiyalar daxil olmaqla, onların nəzəri əsaslarının işlənməsidir [5].

Açıq açarlı kriptoqrafiya sahəsində homomorf şifrləmə və identifikator əsasında şifrləmə sistemləri diqqəti cəlb edir.

Homomorf şifrləmə sistemi şifrlənmiş məlumatlar üzərində məlumatları deşifrləmədən riyazi əməliyyatlar (məsələn, toplama, çıxma, birləşmə, kəsişmə) aparmağa imkan verir. Bu şifrləmə sistemi fərdi məlumatların qorunması, elektron səsvermə, maliyyə məlumatlarının emalı, tövsiyə sistemlərində tətbiq edilə bilər. Homomorf şifrləmə sistemlərindən ən uğurlusu hesab edilən sistem 2009-cu ildə IBM şirkətinin kriptoqrafı tərəfindən təklif edilib və IBM tərəfindən patentləşdirilib [6].

İdentifikator əsasında şifrləmə (ing. İdentity-based encryption, IBE) rəqəmsal informasiyanın şifrlənməsi üçün çevik mexanizmlər təklif edir [7]. Ənənəvi şifrləmə üsulları təsadüfi generasiya edilmiş uzun kriptoqrafik açarlar tələb edir, açarları konkret şəxslə əlaqələndirmək üçün rəqəmsal

sertifikatlardan istifadə edilir. Onların hazırlanması və idarə edilməsi isə mürəkkəb və xərc tələb edən infrastruktur tələb edir.

IBE istənilən sətri – hətta e-poçt ünvanını da açıq açar kimi istifadə etməyə imkan verməklə bu çətinlikdən qurtarmağa xidmət edir. Deşifrləmə açarı isə etibarlı serverdən alınır, bu server açarları generasiya edir və siyasətin həyata keçirilməsini idarə edir.

Kvant kriptoqrafiyasında ilk cığır 1984-cü ildə *açarların kvant paylanması* sistemi ilə açılıb [8]. Hazırda açarların kvant paylanması (QKD) ilə yanaşı təhlükəsiz birbaşa kvant rabitəsi (QSDC), kvant axın şifrləməsi (QSC), kvant steqanoqrafiyası (QS), kvant açarlar infrastrukturu (QKI), – kvant rəqəmsal imzası (QDC) mövzularında da tədqiqatlar aparılır [9]. Açarların kvant paylanması sahəsində aparat kompleksləri təklif edən bir neçə şirkət vardır. Məsələn, ID Quantique İsveçrə firması açarların kvant paylanması üçün Cerberis kommersiya sistemini təklif edir. Şüalandırıcı-qəbuledici cütü təxminən 97 min dollardır. Onun təsir məsafəsi 100 km-i aşmır, lakin ID Quantique mütəxəssisləri eksperimentlərdə ötürmə məsafəsini 250 km-ə çatdıra bilirlər. Nəzəri maksimum isə 400 km-dir.

Qeyd edək ki, 2009-2011-ci illərdə bəzi kommersiya sistemlərində texniki nöqsanlarından istifadə etməklə açarların kvant paylanması sistemlərinə ilk uğurlu hücumlar da təklif edilmişdir [9].

III. POST-KVANT KRİPTOQRAFİYASI

Kriptoqrafiyanı "ölümlə hədələyən" problemlərdən biri kvant kompüterləri və onlarda icra olunacaq kvant alqoritmləridir. Burada yalnız kvant kompüterlərinin inkişaf mərhələlərini qısaca qeyd etməklə kifayətlənək.

Kvant kompüterlərinin ilk modeli 1981-ci ildə verilmiş və qurulmasının nəzəri əsasları işlənmişdi. 2000-ci ildə 1 kubitdən, 2001-ci ildə 2 kubitdən, 2003-cü ildə 7 kubitdən, 2005-ci ildə 10 kubitdən ibarət kvant kompüterləri yaradılmışdı.

Kvant kompüterləri sahəsində son dövrlər xeyli inkişaf əldə olunub. Kanada firması D-Wave Systems 2007-ci ilin fevralında 16 kubitdən ibarət kvant kompüterinin yaradılmasını bəyan etmiş, həmin ilin noyabrında 28-kubitlik kompüteri nümayiş etdirmişdi. 2011-ci iln mayında 128-kubitlik prosessor bazasında yaradılmış D-Wave One kvant kompüteri təqdim olunmuşdu. 2012-ci ilin dekabrında artıq 512 kubit əsasında yaradılmış Vesuvius prosessoru nümayiş etdirilmişdi.

Kvant alqoritmlərinə gəlincə, hələ 1990-cı illərdə klassik analoqları olmayan ilk kvant alqoritmləri təklif edilmiş və onların istənilən klassik alqoritmdən effektiv olmaları isbat edilmişdi. Kriptoqrafiya üçün xüsusi əhəmiyyət kəsb edən kvant alqoritmlərindən axtarış üçün Qrover alqoritmini [10] və ədədin vuruqlara ayrılması üçün Şor alqoritmini göstərmək olar [11].

Simmetrik kriptosistemlərdə bütün variantları yoxlamaqla məxfi açarın tapılmasının zaman mürəkkəbliyi $O(2^n)$-dir, Qrover alqoritmi bu məsələni $O(2^{n/2})$ zaman müddətində həll etməyə imkan verir. Cədvəl 1-də simmetrik kriptosistemlərdə açarın axtarışı məsələsinin kvant və klassik həllərinin zaman mürəkkəbliyi göstərilir.

CƏDVƏL 1. Simmetrik kriptosistemlərdə açarın axtarışı məsələsinin zaman mürəkkəbliyi

Açarın uzunluğu, bit	Kubitlərin sayı	Kvant alqoritmləri	Klassik alqoritmlər
56	56	$2{,}1\cdot10^{8}$	$7{,}2\cdot10^{16}$
80	80	$8{,}6\cdot10^{11}$	$1{,}2\cdot10^{24}$
112	112	$5{,}7\cdot10^{16}$	$5{,}2\cdot10^{33}$
128	128	$1{,}4\cdot10^{19}$	$3{,}4\cdot10^{38}$
168	168	$1{,}5\cdot10^{25}$	$3{,}7\cdot10^{50}$
256	256	$2{,}7\cdot10^{38}$	$1{,}2\cdot10^{77}$

Şor alqoritmi natural N ədədinin sadə vuruqlara ayrılması məsələsini $n = \log(N)$-dən polinomial asılı $O(n^2 \log n \log\log n)$ zaman müddətində həll etməyə imkan verir. Cədvəl 2-də ədədin sadə vuruqlara ayrılması məsələsinin kvant və klassik həllərinin [22] zaman mürəkkəbliyi göstərilir.

CƏDVƏL 2. Ədədin sadə vuruqlara ayrılması məsələsinin zaman mürəkkəbliyi

Açarın uzunluğu, bit	Kubitlərin sayı	Kvant alqoritmləri	Klassik alqoritmlər
512	1024	$0{,}54\cdot10^{9}$	$6{,}4\cdot10^{16}$
1024	2048	$4{,}3\cdot10^{9}$	$3{,}0\cdot10^{24}$
2048	4096	$34\cdot10^{9}$	$9{,}2\cdot10^{33}$
3072	6114	$120\cdot10^{9}$	$6{,}0\cdot10^{38}$
15360	30720	$1{,}5\cdot10^{13}$	$2{,}1\cdot10^{77}$

Qeyd etmək lazımdır ki, kvant hesablamalarına dayanıqlı olan açıq açarlı kriptoqrafik sistemlər də mövcuddur:

Heş funksiaya əsasında kriptosistemlər

- Merkle imza sxemi (MSS, 1979)
- Lamport–Diffi birdəfəlik imza sxemi (LD-OTS, 1979)
- Winternitz birdəfəlik imza sxemi (W-OTS, 1989)

Kodlaşdırma nəzəriyyəsi əsasında kriptoqrafiya

- McEliece açıq açarlı kriptosistemi (1978)
- Niederreiter şifrləmə sxemi (1986)
- McEliece açıq açarlı kriptosisteminin modifikasiyaları

Qəfəslərə əsaslanan kriptosistemlər

- NTRU (Hoffstein, Pipher və Silverman,1998)
- LWE-əsaslı kriptosistem (Regev, 2005)

Çoxparametrli kvadratik tənliklərə əsaslanan kriptosistemlər

- HFEv− açıq açarlı imza sistemi (Patarin, 1996)

- Çoxparametrli imza (Ong, Schnorr, Shamir, 1984)
- Diffi və Fell açıq açarlı kriptosistemi (1985)

2-3 aprel 2015-ci ildə keçirilən "NIST Workshop On Cybersecurity in a Post-Quantum World" seminarında bir sıra məsələlərə baxılırdı [12]:

- Kvant kompüterlərinin inkişafı açıq açarlı alqoritmlərin təhlükəsizliyinə və açıq açarlı infrastruktura əsaslanan digər sistemlərə necə təsir edə bilər?
- Post-kvant kriptoqrafiyasına nə dərəcədə ehtiyac var və post-kvant kriptoqrafiyasının şifrləmə, rəqəmsal imza, açar mübadiləsi və məlumatların autentifikasiyası ilə bağlı arzu olunan xüsusiyyətləri hansılardır?
- Təklif olunan müxtəlif post-kvant kriptoqrafiyası sxemlərinin üstün və zəif cəhətləri hansılardır? Kvant və klassik hucumlara qarşı bu kriptoqrafik sxemlərin təhlükəsizliyindən necə əmin olmaq olar?

IV. KRİPTOANALİZ ÜZRƏ BƏZİ QEYDLƏR

Məlumdur ki, açıq açarlı kriptoqrafiya müəyyən riyazi məsələlərin həllinin zaman və yaddaş mürəkkəbliyinin indiki hesablama resurlarının praktiki imkanları xaricində olmasına əsaslanır. Lakin daha effektiv həllərin tapıla biləcəyi ehtimalını mütləq nəzərə almaq lazımdır. Fransadan olan dörd kriptoqraf diskret loqarifm məsələsinin həlli üçün evristik kvazi-polinomial alqoritm təklif etmişdir, onların nəticəsi 2014-cü ildə nəşr olunmuşdur [13]. Bunun nəticəsində bir çox kriptoqrafik alqoritmin əsaslandığı diskret loqarifm məsələsinin mürəkkəbliyi əhəmiyyətli dərəcədə aşağı düşür. Bu iş hələlik nəzəriyyə mərhələsindədir, onun praktikada nümayiş etdirilməsi üçün müəyyən işlər görülməlidir. Buna baxmayaraq, bu nəticə kriptoqrafik alqoritmlərin təhlükəsizliyində boşluqların olmasını bir daha gündəmə gətirir və əlavə tədqiqatlara yol açır.

İkinci hadisə NİST tərəfindən elliptik əyrilər üzərində təsadüfi ədədlər generatoru Dual_EC_DRBG-nin (Dual Elliptic Curve Deterministic Random Bit Generator) istifadədən çıxarılmasıdır [14].

Üçüncü hadisə SSL/TLS standartında istifadə edilən RC4 axın şifrinin analizində irəliləyişin əldə edilməsidir [15].

V. KRİPTOQRAFİYA ÜZRƏ BEYNƏLXALQ MÜSABİQƏLƏR

İnkişaf etmiş ölkələrin əksəriyyətində kriptoqrafiya üzrə müxtəlif standartlar mövcuddur və bu standartlar vaxtaşırı yenilənir. ABŞ və Avropada kriptoqrafik standartların işlənməsi açıq beynəlxalq müsabiqələr yolu ilə aparılır və standartların təsdiqi mexanizmi aşağıdakı kimidir.

Təşkilatçılar kriptoqrafik standartın seçilməsi üzrə müsabiqə elan edirlər və namizəd-alqoritmlərə tələbləri bildirirlər. Kriptoqraflar müsabiqədə iştirak etmək üçün öz alqoritmlərini müəyyən müddət ərzində göndərirlər.

Göndərilən bütün alqoritmlər veb-saytlarda yerləşdirilir, kifayət qədər uzun müddət ərzində dünyanın müxtəlif ölkələrindən olan kriptoanalitiklər tərəfindən tədqiq olunur.

Nəticədə yüksək kriptoqrafik təhlükəsizliyə malik bir neçə alqoritm seçilir və sonrakı mərhələdə müxtəlif əlavə tələblər – alqoritmin işləmə sürəti, reallaşdırılmasının sadəliyi və s. nəzərə alınmaqla onlardan ən yaxşısı seçilir.

Kriptoqrafiya sahəsində keçirilən açıq müsabiqələr tədqiqatların inkişafına xüsusi stimul verir. Məxfi açarlı kriptoqrafiyada müsabiqələrin müəyyən ənənəsi artıq formalaşıb. 1997-ci ildə ABŞ Milli Standartlar və Texnologiyalar İnstitutu (National Institute of Standards and Technology, NIST) yeni şifrləmə standartını (Advanced Encryption Standard, AES) müəyyən etmək üçün açıq müsabiqə elan etmişdi. Müsabiqəyə dünyanın müxtəlif ölkələrindən olan 50 kriptoqraf tərəfindən 15 blok şifri təqdim olunmuşdu. Müsabiqə bir neçə mərhələdə keçirilmiş, müsabiqəyə təqdim olunmuş blok şifrlərin təhlükəsizliyi və məhsuldarlığı çox sayda kriptoqraf tərəfindən qiymətləndirilmişdi.

AES-in uğurları nəzərə alınaraq, Avropa İttifaqı 2000-2003-cü illərdə NESSIE (New European Schemes for Signatures, Integrity and Encryption) müsabiqəsini keçirdi, Yaponiya isə 2003-cü ildə CRYPTREC (Cryptography Research and Evaluation Committees) komitəsini yaratdı.

ECRYPT şəbəkəsi 2004-cü ilin fevralında başladılmış 4-illik Avropa tədqiqat təşəbbüsü idi, məqsədi informasiya təhlükəsizliyi, xüsusən də kriptologiya və rəqəmsal su nişanları sahəsində Avropa tədqiqatçıları arasında əməkdaşlığı inkişaf etdirmək idi. 2008-ci ildə növbəti 4-illik mərhələ ECRYPT II adı ilə davam etdirildi. ECRYPT virtual laboratoriya adlandırılan beş əsas tədqiqat sahəsi müəyyən edir – simmetrik açarlı alqoritmlər (STVL), açıq açarlı alqoritmlər, protokollar (PROVILAB), təhlükəsiz və effektiv realizələr (VAMPIRE) və su nişanları (WAVILA).

ECRYPT çərçivəsində həyata keçirilmiş ən uğurlu layihələrdən biri axın şifr standartlarının müəyyən edilməsini hədəfləyən eSTREAM layihəsi idi (2004-2008-ci illər).

Kriptoqrafik müsabiqələrdən ABŞ-ın SHA-3 kriptoqrafik heş funksiya standartının seçilməsi üzrə layihəni (NIST, 2007-2012-ci illər) və CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) layihəsini qeyd etmək olar (2012-ci ildən, NIST qrantı ilə maliyyələşir).

SHA-3 müsabiqəsi. 2004-2006-cı illərdə bir sıra heş-funksiyaların sındırılmasından sonra ABŞ Milli Standartlar və Texnologiyalar İnstitutu (National Institute of Standards and Technology, NIST) SHA-1 и SHA-2 alqoritmlərini əvəzləyəcək yeni kriptoqrafik heş-funksiya standartının işlənilməsi üzrə müsabiqə keçirdi (2007-2012-ci illər). Müsabiqəyə təqdim olunmuş 64 alqoritmdən beşi: BLAKE, Grøstl, JH, Keccak, Skein finala çıxmışdı.

Müsabiqənin qalibi Keccak alqoritmi ("catch-ack" kimi tələffüz edilir) elan olundu, Keccak alqoritmi Merkl-Damqard strukturuna əsaslanan SHA-1, SHA-2 və MD5-dən

əhəmiyyətli dərəcədə fərqlənir. Alqoritmlərin fərqli prinsiplər əsasında yaradılmasına görə SHA-2-yə qarşı olan hücumların Keccak üçün işləməyəcəyi söylənilir.

Daha bir müsabiqə hər hansı təşkilat tərəfindən deyil, kriptoqrafların təşəbbüs qrupu tərəfindən keçirilən *Password Hashing Competition* (mart, 2014) idi. Finalçılarda sıxma operatorları (Argon-v2, battcrypt, Lyra2-v3,Parallel-v1, Pufferfish -v1), qraflar nəzəriyyəsi (Catena-v3), avtomatlar nəzəriyyəsi (Pomelo-v2), ədədlər nəzəriyyəsi (mürəkkəb ədədin modulu üzrə kvadrata yüksəltmə, Blum generatoru) (Makwa) kimi qurulma prinsipləri istifadə edilirdi.

Rusiya standartlaşdırma üzrə texniki komitəsi «İnformasiyanın kriptoqrafik mühafizəsi» (TK 26) tərəfindən ГОСТ Р 34.11-2012 heş-funksiyasının kriptoqrafik analizi üzrə elmi işlərin açıq beynəlxalq müsabiqəsi keçirilmişdir (1-ci mərhələ 21.11.2013-30.04.2014, ikinci mərhələ 01.05.2014-13.02.2015). Müsabiqənin qalibləri Sinqapur və Kanadadan olan tədqiqatçılar qrupları və Rusiyadan olan bir gənc tədqiqatçı (Г. Седов) elan olunmuşdu [16-19]. Çindən olan tədqiqatşılar qrupunun işi həvəsləndirici mükafata layiq görülmüşdü (http://www.streebog.info). (1-ci mükafat − 500 min rubl, 2-ci mükafat − hər biri 300 min rubl olmaqla iki mükafat, həvəsləndirici mükafat −150 min rubl idi.)

Avropa İttifaqının Horizon 2020 layihəsi çərçivəsində ICT 2014 – Information and Communications Technologies (H2020-ICT-2014-1) aşağıdakı aktual tədqiqat problemləri müəyyən edilir [20]:

- aparat əsasında real zamanda işləyən kriptoqrafiya üçün resurs baxımından səmərəli, yüksək səviyyədə təhlükəsiz texnologiyalar;
- resurs baxımından səmərəli, real zamanda işləyən, yüksək səviyyədə təhlükəsiz tam homomorf kriptoqrafiya;
- paylanmış kriptoqrafiya, o cümlədən funksional kriptoqrafiya;
- istifadə olunan kriptoqrafik primitivlərin uyğunlaşmaq imkanı olmaqla və ya olmadan proqram və aparat mühitlərinə təhlükəsiz qoşulması üçün kriptoqrafik alətlər;
- uzunmüddətli təhlükəsizlik üçün post-kvant kriptoqrafiyası;
- uzunmüddətli təhlükəsizlik üçün kvant açar paylaşımı sistemləri və şəbəkələri, o cümlədən:
- qısa məsafəli, aşağı bit sürətli kvant açar paylaşımı üçün ucuz komponentlər;
- küy və itkilərə dayanıqlı yüksək bit sürətli kvant açar paylaşımı sistemləri.

NƏTİCƏ

Kriptoqrafiyanın tətbiq sahələrinin genişlənməsi ilə əlaqədar olaraq (rəqəmsal imza, autentikasiya, elektron sənədlərin həqiqiliyinin və tamlığının təsdiqi, elektron kommersiyanın təhlükəsizliyi və s.) müasir cəmiyyətin həyatında kriptoqrafiyanın rolu artır. Vətəndaşların və biznes sektorunun, beynəlxalq tərəfdaşların e-dövlətin informasiya təhlükəsizliyinə etimadını təmin etmək üçün müasir kriptoqrafiya sahəsində düzgün, balanslaşdırılmış siyasətin işlənilməsi və həyata keçirilməsi olduqca vacibdir.

ƏDƏBİYYAT

[1] Əliquliyev R. M., İmamverdiyev Y. N., Kriptoqrafiyanın əsasları. Bakı: İnformasiya Texnologiyaları, 2006, 698 s.

[2] Y. N. İmamverdiyev, "İnformasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması problemləri," Elektron dövlət quruculuğu problemləri üzrə I respublika konfransının əsərləri, 2014, s. 152-155.

[3] Y. N. İmamverdiyev, "Əşyaların İnterneti və yüngülçəkili kriptoqrafiya," İnformasiya təhlükəsizliyi problemləri üzrə I respublika konfransının əsərləri, 2013, s. 137-140.

[4] S. Kamara, K. Lauter, "Cryptographic cloud storage," Financial Cryptography Workshops, vol. 6054 of Lecture Notes in Computer Science, pp. 136–149. Springer, 2010.

[5] C. Gentry, "Fully homomorphic encryption using ideal lattices," STOC, pp. 169-178, 2009.

[6] D. Boneh, M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM J. of Computing, vol. 32, no. 3, pp. 586-615, 2003.

[7] European Union Agency for Network and Information Security (ENISA): Study on cryptographic protocols, Nigel P. Smart (editor), November, 2014.

[8] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, 1984, pp. 175–179.

[9] D. J. Bernstein, J. Buchmann, E. Dahmen. Post-quantum cryptography. Springer Science & Business Media, 2009.

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proc. of 28th STOC, pp. 212-219, 1996.

[11] P. W. Shor,"Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer," Proc. 35th Ann. Symp. on Foundations of Computer Science, pp. 124-134, 1994.

[12] NIST Workshop On Cybersecurity in a Post-Quantum World April 2 – April 3, 2015

[13] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, "A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic," Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, Vol. 8441, pp. 1-16, 2014.

[14] N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, J. C. N. Schuldt, "On the Security of RC4 in TLS and WPA," Proc. of the USENIX Security Symposium, 2013.

[15] Pironti, A., Strub, P., and K. Bhargavan, "Identifying Website Users by TLS Traffic Analysis: New Attacks and Effective Countermeasures.", INRIA Research Report 8067 , 2012.

[16] J. Guo, J. Jean, G. Leurent, T. Peyrin и L. Wang, "The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function," Proc. 21st International Conference Selected Areas in Cryptography (SAC), 2014, pp. 195-211.

[17] R. AlTawy, A.M.Youssef, "Integral Distinguishers for Reduced-Round Stribog," http://eprint.iacr.org/2013/648.pdf

[18] R. AlTawy, A.M.Youssef, "Differential Fault Analysis of Streebog ," Proc. 11th International Conference Information Security Practice and Experience (ISPEC), 2015, pp35-49.

[19] B. Ma, B. Li, X. Li, and R. Hao "Improved Cryptanalysis on Reduced-Round GOST and Whirlpool Hash Function," Proc. 12th International Conference Applied Cryptography and Network Security (ACNS), 2014, pp 289-307.

[20] Information and Communications Technologies (H2020-ICT-2014-1). Topic: Cybersecurity, Trustworthy ICT (ICT-32-2014) http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/96-ict-32-2014.html