UOT 519.7

MÜASİR ZAMANDA QƏRB ÖLKƏLƏRİNDƏ KRİPTOQRAFİYA SAHƏSİNDƏ GÖRÜLMÜŞ İŞLƏR HAQQINDA

mayor Fərman Məmmədov[1]
Vüsalə Həsənova[2]
[1]Silahlı Qüvvələrin Hərbi Akademiyası
[2] Odlar Yurdu Universiteti
E-mail: fermanmemmedov@gmail.com

Xülasə. Məqalədə Avropada kriptoloqiya sahəsində çalışan müxtəlif təyinatlı təşkilatlar və onların fəaliyyət istiqamətləri, eləcə də yerinə yetirilən təşkilati və elmi işlərin geniş təhlili verilir.

Açar sözlər: kriptoqrafiya, alqoritm, şifrləmə, IACR, ENİSA, ECRYPT.

Giriş

Qloballaşan dünyada kompüter, şəbəkə və internet texnologiyalarının meydana çıxması ilə həssas məlumatlar bir çox yerlərdə müxtəlif formalarda (mətn, şəkil, səs, video və s.) yayılmağa başlamışdır [1]. Hər gün internet üzərindən hərbi, tibbi, kredit kartı, maliyyə, vergi, fərdi və s. kimi saysız-hesabsız sayda əhəmiyyətli məlumatların mübadiləsi həyata keçirilir [2]. Sayı bilinməyən müxtəlif kommunikasiyalarda informasiya təhlükəsizliyinin təmin edilməsi sistematik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlər aparılmalıdır. Cəmiyyətin informasiya təhlükəsizliyinin təmin olunması üçün beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin işlənilməsi və reallaşdırılması, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı, əhalinin maarifləndirilməsi və vətəndaşlarda informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması zəruridir [3]. Bunlarla yanaşı, informasiya təhlükəsizliyinin təmin olunması istiqamətində onun tərkib hissələrinin ayrı-ayrılıqda tədqiqi vacibdir. Zəruri tədbirlərin həyata keçirilməsi üçün ayrı-ayrı ölkələrin, eləcə də beynəlxalq təşkilatların təcrübəsinə istinad edilə bilər.

İnformasiya mübadiləsi zamanı informasiyanın təhlükəsiz ötürülməsi, saxlanılması, emalı, bir sözlə, qorunmasında kriptoqrafiyadan geniş istifadə olunur. Müasir dövrdə qərb, əsasən də Avropa ölkələri bir çox sahələrdə olduğu kimi, kriptologiya elmi istiqamətində də istər təşkilati, istərsə də aparılan tədqiqatlar baxımından mühüm nailiyyətlər əldə etmişdir.

Məqalədə məqsəd müasir dövrdə kriptoqrafiyanın inkişaf tarixini, cari vəziyyətini və perspektivlərini Avropa təcrübəsi əsasında araşdırmaqdır. Tədqiqat işində qərb ölkələrində beynəlxalq koalisiyalar daxilində fəaliyyət göstərən bəzi təşkilatların, həmin qurumlar nəzdində yerinə yetirilmiş işlərin və təklif olunan alqoritmlərin analizi təqdim edilir.

Qərbdə kriptoqrafiya sahəsində fəaliyyət göstərən bəzi təşkilatlar

Kriptologiya Tədqiqatları üzrə Beynəlxalq Assosiasiya (*International Association for Cryptologic Research – IACR*) kriptoqrafiya və ona yaxın sahələrdə tədqiqatların inkişaf etdirilməsi məqsədi daşıyan qeyri-kommersiya təşkilatıdır [4]. Assosiasiyanın yaradılması 1981-ci ildən başlayaraq Kaliforniya Universitetində (ABŞ, Santa Barbara) ildə bir dəfə keçirilən ikinci konfransda (*Crypto*) Devid Çaum (*David Chaum*) tərəfindən irəli sürülmüş, 1983-cü ilin iyun ayının 16-da isə rəsmi olaraq təsis edilmişdir. *IACR* iki əsas funksiyanı yerinə yetirir [5]:

- kriptologiya ilə bağlı görüşləri koordinasiya edir və keçirir;
- konfransların təşkilati məsələlərini həll edir.

IACR prezident və Direktorlar Şurası tərəfindən müxtəlif komitələr vasitəsilə idarə olunur. Qaydalara əsasən, Assosiasiyanın Direktorlar Şurası üç il müddətinə üzvlər arasından seçilir və ya şura tərəfindən təyin edilir [6]. *IACR* tərəfindən hər il kriptoqrafiya sahəsində üç ümumi və dörd ixtisaslaşmış konfrans, həmçinin bir simpozium və təlim məktəbləri (*training schools*) təşkil olunur. Simpozium Real Dünya Kriptoqrafiyası (*Real World Cryptography – RWC*) adlanır. Ümumi konfranslar isə aşağıdakılardır [5; 7]:

– Beynəlxalq kriptologiya konfransı (*International Cryptology Conference – Crypto*) 1981-ci ildən ABŞ-ın Santa Barbara şəhərində keçirilir. Assosiasiyanın yaradılması da yuxarıda göstərildiyi kimi bu konfransın adı ilə bağlıdır.

– Kriptoqrafik tətbiq və nəzəriyyələrin texnikaları üzrə beynəlxalq konfrans (*International Conference on the Theory and Applications of Cryptographic Techniques – Eurocrypt*) 1982-ci ildən Avropada keçirilir. Lakin 1983-cü ildən başlayaraq *Eurocrypt* olaraq adlandırılmış və *IACR* tərəfindən qismən sponsorluq edilmişdir. Assosiasiya sonrakı illərdən etibarən *Eurocrypt* konfransının təşkilatçılığı və sponsorluğunu tam şəkildə yerinə yetirmişdir.

– Kriptologiya və informasiya təhlükəsizliyi sahəsində tətbiq və nəzəriyyələr üzrə beynəlxalq konfrans (*International Conference on the Theory and Application of Cryptology and Information Security – Asiacrypt)* 1990-cı ildən etibarən hər dəfə Asiya ölkələrinin birində keçrilir. 2000-ci ildən başlayaraq *Asiacrypt*-ə *IACR* təşkilatçılıq və sponsorluq etmişdir;

IACR tərəfindən təşkil olunan ixtisaslaşmış konfranslar aşağıdakılardır [7]:

– Kriptoqrafik aparat sistemləri (*Cryptographic Hardware and Embedded Systems – CHES*);
– Sürətli proqram şifrləməsi (*Fast Software Encryption – FSE*);
– Açıqaçarlı kriptoqrafiya (*Public Key Cryptography – PKC*);
– Nəzəri kriptoqrafiya konfransı (Theoretical Cryptography Conference – TCC).

Hazırda Assosiasiyanın təsis etdiyi üç jurnal fəaliyyət göstərir. Kriptologiya jurnalı 1988-ci ildən dərc olunmağa başlanıb və baş redaktor IACR Direktorlar Şurasının üzvü kimi fəaliyyət göstərir. Digər iki jurnal isə Simmetrik Kriptologiya Tranzaksiyaları (IACR Transactions on Symmetric Cryptology – ToSC) və Kriptoqrafik Aparat Sistemləri Tranzaksiyaları (IACR Transactions on Cryptographic Hardware and Embedded Systems – TCHES) adlanır [8]. Jurnallar Almaniyanın Boxum Ruhr Universiteti tərəfindən dərc olunur. Kriptoqrafik Aparat Sistemləri Tranzaksiyaları (IACR Transactions on Cryptographic Hardware and Embedded Systems – TCHES) jurnalı yeni dərc edilməyə başladığına görə (2018) hələlik nüfuzlu bazalara düşməsə də, digər iki jurnal "Scopus" bazasında indeksləşmişdir.

Kriptologiya üzrə Avropa Mükəmməlik Şəbəkəsi (European Network of Excellence for Cryptology – ECRYPT) layihəsi Avropa Komissiyasının (European Commission) proqramları çərçivəsində maliyyələşdirilərək, iki müxtəlif layihə şəklində icra edilmiş və səkkiz il ərzində (2004–2012) həyata keçirilmişdir. ECRYPT layihələrinin əsas fəaliyyəti tərəfdaş qurumlara qarşılıqlı səfərlər, işçi görüşlər, yay məktəblərinin keçirilməsi, virtual laboratoriyalar vasitəsilə qarşılıqlı əməkdaşlıq, eləcə də alqoritmlər və açar uzunluqları barədə illik hesabatlar dərc etməkdən ibarət olmuşdur.

ECRYPT 2004–2008-ci illərdə həyata keçirilmiş və onun məqsədi informasiya təhlükəsizliyi, əsasən də kriptologiya və rəqəmsal su nişanları sahəsində fəaliyyət göstərən avropalı tədqiqatçıların əməkdaşlığını intensivləşdirmək, eləcə də qeyd edilən sahələrdə araşdırmaların elm və sənayedə davamlı şəkildə inteqrasiyasını təmin edərək mükəmməlliyə çatmaqdan ibarət olmuşdur. Bunun üçün Avropanın müxtəlif ölkələrinin elm və təhsil müəssisələrindən ibarət 32 aparıcı oyunçu (oyunçular əsasən Avropanın aparıcı universitetləri və tədqiqat institutları idi) aşağıda qeyd olunan beş virtual laboratoriya vasitəsilə öz tədqiqatlarını əlaqələndirmiş və qarşılıqlı inteqrasiya etdirmişdir: simmetrik açarlı alqoritmlər (symmetric key algorithms – STVL), açıqaçarlı alqoritmlər (public key algorithms – AZTEC), protokollar (protocols – PROVILAB), təhlükəsiz və effektiv vasitələr (secure and efficient implementations – VAMPIRE) və su nişanları (watermarking – WAVILA) [9].

ECRYPT II isə 2008–2012-ci illərdə həyata keçirilmiş və məqsədi birinci layihə olan ECRYPT-də icra edilmiş fəaliyyətləri sahəsində avropalı tədqiqatçıların əməkdaşlığını intensivləşdirmək olmuşdur. ECRYPT II-də aparıcı oyunçuların sayı 11, virtual laboratoriyaların sayı isə 3 ədəd idi. Virtual

laboratoriyalarda simmetrik açarlı alqoritmlər (symmetric key algorithms – SymLab), açıqaçarlı alqoritmlər və protokollar (public key algorithms and protocols – MAYA), aparat və proqram vasitələri (hardware and software implementations – VAMPIRE) sahəsində tədqiqatlar əlaqələndirilmişdir [10]. Göründüyü kimi, ikinci layihədə oyunçu və laboratoriyaların ümumi sayının azalmasına baxmayaraq, tədqiqat istiqamətləri genişləndirilmişdir.

Avropa Birliyi Kibertəhlükəsizlik Agentliyi (European Union Agency for Cybersecurity – ENISA) 2004-cü ildən fəaliyyət göstərir [11] və Avropa Birliyi (AB) ölkələri üçün kibertəhlükəsizlik siyasətinə töhfə vermək, dövlət sərhədlərindən kənarda (dövlət xaricində) baş vermiş genişmiqyaslı kiber insidentlər nəticəsində iki və daha artıq AB ölkəsinin və ya şirkətinin ziyan çəkməsi halında üzv dövlətləri dəstəkləmək məqsədi daşıyır. Agentlik Yunanıstanın Afina şəhərində yerləşir, Heklion şəhərində isə ikinci ofisi mövcuddur [12].

ENISA AB-nin siyasət və qanunlarının şəbəkə və informasiya təhlükəsizliyi (*network and information security – NIS*) sahəsində inkişafını və tətbiqini dəstəkləyir, eləcə də üzv dövlətlərə, AB institutları, qrupları (*bodies*) və digər agentliklərinə könüllülük əsasında kiber boşluqların aşkara çıxarılması siyasətinin qurulması və tətbiqi istiqamətində yardımçı olur [13].

Nümunə olaraq bildirək ki, 2019-cu ildə Vahid Rəqəmsal Bazara (*Digital Single Market*) keçidi dəstəkləmək üçün "Kibertəhlükəsizlik Aktı"nın (*Cybersecurity Act*) tərkib hissəsi olan, məhsulların, proses və xidmətlərin sertifikatlaşdırılmasının əsasını təşkil edən "Avropa kibertəhlükəsizliyinin sertifikatlaşdırma sxemi"nin hazırlanması *ENISA*-ya tapşırılmışdır. Avropa "Kibertəhlükəsizlik Aktı" informasiya kommunikasiya texnologiyaları (İKT) sahəsində iş, məhsul və xidmətlərin kibertəhlükəsizlik səviyyəsinin sertifikatlaşdırılmasını dəstəkləyən prosesləri təqdim edir [14].

ENISA-nın maliyyələşməsi AB büdcəsi, Yunanıstan hökumətinin dotasiyaları, eləcə də Agentliyin fəaliyyətində iştirak edən dövlətlərin yardımları ilə həyata keçirilir. 2019-cu il üçün Agentliyin büdcəsi 17 milyon avro təşkil etmişdir [15].

Agentlik AB ölkələri və özəl sektorla yaxından əməkdaşlıq edir, aşağıdakı bəzi birlikarası fəaliyyətlərdə məsləhət və həllər təklif edir [14; 16]:

– AB ölkələri üçün kibertəhlükəsizlik təlimləri;
– Milli Kibertəhlükəsizlik Strategiyalarının inkişafı və qiymətləndirilməsi;
– kompüter insidentlərinə qarşı mübarizə qruplarının (*computer security incident response teams – CSIRTS*) inkişafı və iş həcminin artırılması;
– kibertəhlükəsizlik sahəsində məsləhətlərin verilməsi;
– siyasət quruculuğu (*policy making*) və tətbiqi sahəsində fəaliyyətlərin icrası;
– AB tərkibində fəaliyyət göstərən əməliyyat qrupları ilə birbaşa əməkdaşlıq;
– genişmiqyaslı kiber insidentlər zamanı onlara qarşı mübarizədə AB icmalarını bir araya gətirərək onların koordinasiya edilməsi;
– kibertəhlükəsizlik sxemlərinin tərtib edilməsi;
– əşyaların interneti (*IoT*) və ağıllı (*smart*) infrastrukturların öyrənilməsi, məlumatların qorunması işləri, fərdiliyin genişləndirilməsi və meydana gələn texnologiyaların fərdiliyi, *eID* (elektron kimlik) və şəxsiyyətin təsdiqlənməsi xidmətləri, kibertəhdid mühitinin müəyyənləşdirilməsi (*identifying*) və s.

ENISA yuxarıda sadalanan fəaliyyətlərlə yanaşı informasiyanın qorunması, kriptoqrafiya və informasiya təhlükəsizliyinin müxtəlif sahələrində hesabatlar (*reports*) da hazırlayır. Aşağıda Agentliyin hazırladığı bir neçə hesabat haqqında ümumi məlumatlar verilmişdir [17].

AB üzvü dövlətlərində kriptoqrafiyaya olan tələbin minimal səviyyəsini müəyyənləşdirən və informasiya təhlükəsizliyi sahəsində təməl bilgilərə sahib kompüter istifadəçilərinin şəxsi, o cümlədən əhəmiyyətli məlumatlarının qorunması üçün kriptoqrafiyanın tətbiqi texnikaları haqqında ümumi məlumatlar verilir. Vəsait rəqəmsal və elektron mühitdə fərdi məlumatların saxlanılması və işlənilməsi zamanı qeyri-peşəkar şəxslərə informasiya təhlükəsizliyi haqqında əsas anlayışları açıqlayır.

Növbəti [18] "məsləhətlər çoxluğu" (*recommendations set*) əvvəl çap olunan hesabatın [17] davamı olaraq idarəçilər, eləcə də mütəxəssislər üçün kriptoqrafik məhsulların/həllərin işlənilməsi və

tətbiqi ilə bağlı texniki xarakterli sənəddir. 2004–2012-ci illərdə dərc olunmuş alqoritmlər və açar uzunluqları barədə illik hesabatları (*Yearly Report on Algorithms and Key Lengths*), o cümlədən *ECRYPT II* və *ECRYPT*-i əvəz edir. Sənədə əsasən alqoritmlər, açar uzunluqları və parametrlərinin müqayisəsi verilir, məsləhət bilinməyən protokol və sxemlərdən çəkinmə, İKT-nin sürətli inkişafını və nəticədə kriptoqrafik məhsulun köhnələcəyi ehtimalını nəzərə alaraq 5–10 il ərzində onun dəyişdirilməsi planı və mexanizmini işləməklə yeni üsulların tətbiqi istiqamətində işlər görməyin əhəmiyyəti vurğulanır.

[19]-dakı hesabatın hazırlanmasında məqsəd idarəçi və mütəxəssislərə real vaxt rejimində kommunikasiya zamanı həssas məlumatların qorunması ilə bağlı qərar verilməsində protokol seçiminə yardımçı olmaqdır. Çünki etibarlı görünən sxemlərin protokol tərkibində istifadə zamanı zəifliyi meydana çıxa və vacib məlumatların təhlükəyə məruz qalması ilə nəticələnə bilər. Hesabatın digər bir məqsədi davamlı təhlükəsizliyə xidmət edən standart protokollar sahəsində kifayət qədər işlərin olmamasıdır. Kriptoqrafiyanın digər sahələrində fundamental və geniş araşdırmaların aparılmasına baxmayaraq protokollar sahəsində tədqiqatların sayının azlığı hazırlanan hesabatla mütəxəssislərin bu istiqamətdəki işlərini bir növ stimullaşdırılmışdır. Hesabatda istifadədə olan əsas protokolların texniki detalları, onların məhdudiyyətləri və ümumi təsviri haqqında məlumatlar verilmiş, standartlaşdırma sahəsində görülmüş işlər təhlil edilmişdir. Bundan başqa, tədqiqatçılara və protokolların işlənilməsi ilə məşğul olan təşkilatlara yeni protokolların işlənilməsi, mövcud olanların təkmilləşdirilməsi barədə istiqamət və məsləhətlər ümumiləşdirilmişdir.

Avropalı tədqiqatçılar tərəfindən yerinə yetirilmiş bəzi işlərin təhlili

Avropalı mütəxəssislər tərəfindən yerinə yetirilmiş bəzi alqoritmlərin təhlili aşağıda verilmişdir. C.Hazay, G.L.Mikkelsen, T.Rabin və b. [20]-də iki tərəf arasında açıqaçarlı kriptoqrafiyadan (*Rivest, Shamir, Adleman – RSA*) istifadə etməklə kommunikasiya zamanı effektiv açar generasiyası və başlanğıc ədədlərin seçilməsi üçün protokol təklif etmişdir. Protokolun mahiyyəti ondan ibarətdir ki, *RSA* şifrləməsi zamanı açarların təyin edilməsi məqsədilə sadə ədədlərin seçilməsi prosesi, eləcə də yekunda açıq və məxfi açarların özləri hər iki tərəf üçün gizli saxlanılır. Metod zərərli davranışlara və hücumlara qarşı dözümlüdür, açarların tərəflər arasında razılaşdırılması müddətində generasiya olunan, *RSA* alqoritminin başlanğıc ədədləri üçün ilk ümumi olmayan və tamamilə simulyasiya edilə bilən protokol rolunu oynayır. Eyni zamanda tədqiqatda protokolun çoxtərəfli kommunikasiyada istifadə imkanları təsvir olunur. Təqdim olunan *RSA* açar generasiyası protokolu, *RSA* qarışığının (*composite*) (qarışıq dedikdə açar generasiyası zamanı qarşılıqlı sadə ədədlərin hasili nəzərdə tutulur) generasiyası zamanı tərəflərə göndərilməsi və generasiya olunmuş qarışığın uyğunluğunun yoxlanılması üçün qarşılıqlı sadəlik testi (*biprimality test*) altprotokollarını əhatə edir.

M.Hajiabadi və B.M.Kapron [21]-də fundamental kriptoqrafik primitivlərin ümumi konstruksiyası əsasında, yenidən hasil etmə (*reproducibility*) xassəsinə malik, bit səviyyəsində şifrləmə üçün dövri təhlükəsizliyi (*circular security*) özündə birləşdirən yeni şifrləmə primitivi təqdim edirlər. Kriptoqrafik primitivlər informasiyanın şifrlənməsi zamanı onların çevrilməsinin girişlər çoxluğundan çıxışlar çoxluğuna inikasının təsvir edilməsini ifadə edir [22]. Yenidən hasil etmə xassəsi – açıqaçarlı şifrləmə zamanı eyni təsadüfi ədəddən (*random string*) istifadə olunaraq polinomial vaxt ərzində yenidən hasil etmə alqoritminin mövcudluğuna əsaslanır [23]. Dövri təhlükəsizlik – açarların idarə edilməsi zamanı məxfi açarın yerdəyişməsi hallarında onun qorunmasını nəzərdə tutur [24]. Konstruksiyanın özəyini təkrarən təsadüfi seçilmə imkanına malik, yenidən hasil edilən (*reproducible*), açıqaçarlı, bit səviyyəsində şifrləmə sxemləri və əsas şifrləmə sxeminin dövri təhlükəsizliyi üçün əvvəllər təklif olunmuş "baca funksiyası" ailəsinin ("baca funksiyası" – açar generasiyası, qiymətləndirmə və inversiya əməliyatlarından ibarət funksiyadır) biristiqamətli vəziyyətlərini məhdudlaşdıran yeni üsul təşkil edir. Təklif olunan şifrləmə primitivi vasitəsilə qurulmuş əsas primitivlər bunları əhatə edir: biristiqamətli, *k*-dərəcəli (*k-wise*) "baca funksiyası" ailələri; seçilmiş şifrmətnlə hücuma dözümlü şifrləmə; deterministik şifrləmə. Tədqiqatın nəticələri homomorf şifrləmə (homomorf şifrləmə – şifrmətn üzərində müxtəlif əməliyyatların aparılmasına əsaslanır) və simvolik dözümlülükdən (*symbolic soundness*) tamamilə uzaq

dövri təhlükəsiz şifrləmənin yeni tətbiqlər çoxluğunu nümayiş etdirir. Tədqiqatın yekununda *Crypto 2008*-də D.Boneh, S.Halevi, M.Hamburg və b.-nin [24]-də təklif etdiyi "Qərarlı Diffie-Hellman" əsaslı, (*decisional Diffie-Hellman-based*) ("Qərarlı Diffie-Hellman" fərziyyəsi – diskret loqarifma və dövri qruplardan istifadə etməklə mürəkkəb hesablama fərziyyəsidir) dövri təhlükəsiz sxemində, eləcə də *Crypto 2010*-da Brakerski və Qoldvasser (*Goldwasser*) tərəfindən [25]-də irəli sürülmüş fərq edilməyən əsaslı (*indistinguishability-based*) sxemində (fərq edilməyən anlayışı bir riyazi qrupdakı təsadüfi elementin digər qrupdakı təsadüfi elementdən istifadə edərək hesablanmasının mümkün olmamasını ifadə edir) müəlliflərin fərziyyələrinin mümkünlüyü və yenidən hasil edilən (*reproducible*) olduğu göstərilir.

I.Chillotti, N.Gama, M.Georgieva və b. [26]-da amerikalı tədqiqatçılar Centri, Sahai və Votersin təklif etdiyi *GSW* (*Gentry, Sahai, and Waters* – şifrmətnin hər bir homomorf əməliyyatdan sonra matris şəklində toplama və vurma əməliyyatlarının aparılması ilə (*matrix addition and multiplication*) yenilənməsinə əsaslanır [27]) və onun halqa variantları əsaslı *(RingGSW)*, tam homomorf şifrləməni (*fully homomorphic encryption – FHE*) yenidən müzakirə, ümumiləşdirmə və təsvir etməklə "torus" vəziyyətində (torus – həqiqi ədədlərin vahidə bölünməsindən alınan qalığı və ya bir moduluna görə toplama əməliyyatını ifadə edir) tam homomorf sürətli şifrləmə (*fast fully homomorphic encryption scheme over the torus – TFHE*) sxemini təqdim edirlər. Ən sadə *FHE* sxemləri, şifrləmə zamanı alqoritmdə şifrmətnin bir hissəsi və ya hamısından yenidən açar kimi istifadə etməklə şifrləmənin təkrarlanması hesabına qurulan ikilik keçidlərdən (*bootstrapped binary gates*) asılı olur. Dukas və Missiansionun (*Ducas and Micciancio*) *Eurocrypt 2015*-də təklif etdiyi şifrmətnin təkrar istifadəsi ilə qurulan və keçid rejimində (*gate bootstrapping mode*) olan *FHEW* sxemi (*FHEW* sxemi – şifrmətnin hər bir homomorf əməliyyatdan sonra vektorial toplanması ilə (*ciphertext vector additions*) yenilənməsinə əsaslanır) yalnız yekun nəticəyə, *GSW* və səhvlərlə öyrənmə (*Learning With Errors – LWE)* şifrmətnlərinə görə ifadə edilə bilər. *LWE* – sonlu sayda verilmiş və bəziləri səhv olan $y_i = f(x_i)$ nümunələrindən yaradılan halqa üzərində n pozisiyalı xətti f funksiyasının hesablanması problemidir. [26]-da aparılan tədqiqatla bu nəticənin və bəzi optimallaşdırmaların yekununa əsasən, təhlükəsizlik parametrlərini saxlama və şifrmətnin istifadəsi (*bootstrapping*) ilə həmin açarın həcmini 1GB-dan 16MB-a qədər azaldaraq şifrmətnin təkrar istifadə (*bootstrapping*) vaxtını 690 millisaniyədən (ms) 13 ms-ə endirməyə nail olunmuşdur. Mərhələli homomorf vəziyyətində (*leveled homomorphic mode*) şifrmətnin uzunluğunu (*expansion*) azaltmaq, eləcə də *RingGSW* əsaslı homomorf sxemlərində müraciət olunan cədvəllərdə və qərarvermə funksiyalarında qiymətləndirməni optimallaşdırmaq üçün paket verilənləri ilə manipulyasiya etmək məqsədilə iki metod təklif olunur. Eyni zamanda, I.Chillotti, N.Gama, M.Georgieva və b.-nin *Eurocrypt 2016*-da təklif etdikləri çəkili avtomatın (*weighted automata*) (çəkili avtomat dedikdə mətn, səs və ya bioloji proseslərin kompüterdə emalı zamanı istifadə olunan funksiyalar nəzərdə tutulur) effektiv mərhələli qiymətləndirilməsinin "avtomat məntiqi" genişləndirilir, bundan əlavə vurma əməliyyatında meydana çıxan bütün elementar hesablamaları dəstəkləyən yeni homomorf sayğac (*Bit Sequence Representation – TBSR*) təqdim olunur. Bu təkmilləşdirmələr paket səviyyəsi rejimində (*packed leveled mode*) əksər hesablama funksiyalarının qiymətləndirilmə sürətini artırır. Yekunda, *LWE* şifrmətnini 137 ms ərzində aşağı küy səviyyəli *RingGSW* şifrmətninə çevirən, şifrmətnin təkrar istifadəsi ilə qurulan keçid yanaşmasına (*gate bootstrapping approach*) nəzərən hesablama funksiyalarının sürətini kifayət qədər artıraraq, *TFHE*-nin nizamlana bilən səviyyə vəziyyətini (*leveled mode*) meydana gətirən, şifrmətnin təkrar istifadəsi (*bootstrapping*) ilə yeni dövrə təqdim olunur. Ümumiləşdirərək qeyd etmək olar ki, tədqiqat işi açıqaçarlı kriptoqrafiya sxemlərinə aiddir və eyni zamanda *LWE* əsaslı sxemlər üçün məxfi açarın entropiyası (açarın dözümünün nəzəri ölçüsü) və xəta dərəcəsinin təhlükəsizlik parametri ilə birbaşa əlaqəli alternativ praktiki analizini, həmçinin konkret parametr dəstləri və təklif olunan konstruksiyanın vaxta görə müqayisəsini təmin edir.

P.Ekdahl və T.Johansson [28]-də *SNOW* adlandırdıqları iki bayt əsaslı (*word-oriented*) axınla şifrləmə generatoru təklif edirlər. Generator xətti əks-əlaqəli sürüşdürmə registri (*liner feedback shift register – LFSR*) və sonlu vəziyyət maşınından (*finite state machine – FSM*) ibarətdir. Axın şifrlərində bir qayda olaraq generatorun başlanğıc dəyişənlərini müəyyən edən açar, *SNOW* şifrində iki variantda,

128 və 256 bit formasında ola bilər. Şifrlənəcək məlumat iki ədəd 16 bitdən ibarət *LSFR*-ə daxil olur və çıxışda *FSM*-in iki ədəd 32 bitlik, R1 və R2 adlanan registerlərində müxtəlif çevirmələrə məruz qalır. *FSM*-in R1 və R2 registerlərində 2^{32} moduluna görə toplama, bitlərlə *XOR* əməliyyatı, dövri olaraq sola doğru 7 vahid sürüşdürmə və *S-box* çevirməsi həyata keçirilir. Şifrin başlanğıc fazası qısadır və 32 bit prosessorlu sistemlərdə, eləcə də aparat vasitəsilə reallaşdırıldığı zaman yaxşı nəticə göstərir. *SNOW AES* (*Advanced Encryption Standard*) şifrindən sürətli olmasına baxmayaraq, kriptodavamlılığı ona bərabərdir.

C.Beierle, G.Leander, A.Moradi və b. [29]-də *CRAFT* (*effi**C**ient p**R**otection **A**gainst differential **F**ault analysis a**T**tacks*) adlı diferensial xəta analizinə (*Differential Fault Analysis – DFA*) qarşı effektiv qorumalı, simmetrik, yüngül (*lightweight*), artırma (*tweakable*) xassəsi olan, bloklarla şifrləmənin yeni metodunu təklif edirlər. *CRAFT*-ın blokları və artırması 64 bit, açar uzunluğu isə 128 bitdən ibarət olur. Daxil olan parametrlər $4x4$ ölçülü ikilik massiv şəklində ifadə olunur. Şifrləmə zamanı 128 bitlik açar K0 və K1 olmaqla iki yerə bölünür. 64 bitlik artırmalar (T) ilə 4 ədəd TK0, TK1, TK2 və TK3 şəklində artırma açarı generasiya olunur. Artırma açarları da, həmçinin $4x4$ ölçülü iki ölçülü massiv şəklində ifadə olunur. İlkin vəziyyət göstərilən şəkildə müəyyən olunduqdan sonra şifrmətnin əldə edilməsi üçün məxfi məlumat 31 ədəd dövri funksiya ilə çevrilir və bir ədəd xətti dövrlə toplanılır. Deşifrləmə əməliyyatı şifrləmənin əks ardıcıllığı ilə yerinə yetirilir. Təklif olunan alqoritmin bəzi hissələri *AES* şifrləmə standartı ilə oxşarlıq təşkil edir.

Nəticə

Beləliklə, aydın olur ki, kriptoqrafiya sahəsinin inkişafına töhfə verən təşkilatların əsas dəstəkçiləri Avropa universitetləridir. Təhsil müəssisələrinin həm professor-müəllim heyəti, həm də tələbələri sənayedəki problemlərin aradan qaldırılması istiqamətində fəal çalışırlar. Ölkəmizdə kriptoqrafiya istiqamətinin inkişaf perspektivlərinin və milli kriptoqrafiya siyasətinin reallaşdırılması üçün ali təhsil müəssisələrində bu sahədə xüsusi bölmələrin (fakültə, kafedra və ixtisasların) fəaliyyətinin təşkil olunması vacibdir. Respublikamızda kriptologiya elminin inkişafının dünya standartları səviyyəsinə çatdırılması üçün Qərbdə bu istiqamətdə görülən işlərin nəzərə alınması xüsusi əhəmiyyət kəsb edir.
Alqoritmlərin təhlili göstərir ki, tətbiq olunan yanaşmalar sürətlə yenilənir və təkmilləşdirilir. Görülən işlərə və aparılan hərtərəfli tədqiqatlara baxmayaraq kriptoqrafik üsulların ən həssas tərəfi – açarın tərəflərə çatdırılması məsələsi əsas problem kimi öz aktuallığını qorumaqdadır.

İstifadə edilmiş ədəbiyyat siyahısı

1. Adekanmbi, O.O. Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System / O.O.Adekanmbi, O.O.Omitola, T.R.Oyedare [et al.] // Journal of Advancement in Engineering and Technology, – 2015. Voume 3, Issue1, – p. 1-8.
2. Soradge, N., Thakare, K.S. A Review on Various Visual Cryptography Schemes // International Journal of Computer Science and Business Informatics, – 2014. Vol. 12, No. 1. – p. 45-54.
3. Mövlamov, F. Veb hücumların intensivlik tipologiyasının təsnif prinsipləri və onlardan mühafizənin təmini // Hərbi bilik, – 2018. № 6, – s. 57-62.
4. About the IACR: [Electronic resource] / IACR website. – 05.04.2020. URL:https://www.iacr.org/about/
5. McCurley, K. History of the IACR: [Electronic resource] / IACR website. – 05.04.2020. URL: https://iacr.org/docs/history/
6. IACR Board of Directors: [Electronic resource] / IACR website. – 05.04.2020. URL: https://www.iacr.org/bod.html
7. Committees and Special Roles: [Electronic resource] / IACR website. – 05.04.2020. URL: https://www.iacr.org/committees.html
8. IACR Publications: [Electronic resource] / IACR website. – 05.04.2020. URL: https://www.iacr.org

9. Network of Excellence in Cryptology: [Electronic resource] / ECRYPT website. – 31.07.2008. URL: https://www.ecrypt.eu.org/ecrypt1/index.html

10. European Network of Excellence in Cryptology II: [Electronic resource] / ECRYPT website. – 30.09.2012. URL: https://www.ecrypt.eu.org/ecrypt2/

11. ENISA Mandate and Regulatory Framework: [Electronic resource] / ENISA website. – 05.04.2020. URL:https://www.enisa.europa.eu/about-enisa/regulatory-framework

12. Looking into the crystal ball, A report on emerging technologies and security challenges, – Heraklion, Greece: European Union Agency for Network and Information Security (ENISA), – 2018. – 32 p. URL: https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

13. Mission and Objectives: [Electronic resource] / ENISA website. – 05.04.2020. URL: https://www.enisa.europa.eu/about-enisa/mission-and-objectives

14. About ENISA: [Electronic resource] / ENISA website. – 05.04.2020. URL: https://www.enisa.europa.eu/about-enisa

15. Accounting & Finance: [Electronic resource] / ENISA website. – 05.04.2020. URL: https://www.enisa.europa.eu/about-enisa/accounting-finance

16. Policies and Procedures: [Electronic resource] / ENISA website. – 05.04.2020. URL: https://www.enisa.europa.eu/about-enisa/procedures-and-policies

17. ENISA. Recommended cryptographic measures. Securing personal data, – Heraklion, Greece: European Union Agency for Network and Information Security (ENISA), – 2013. – 34 p. URL: https://www.enisa.europa.eu/ publications/recommended-cryptographic-measures-securing-personal-data

18. ENISA. Algorithms, Key Sizes and Parameters Report. 2013 recommendations, – Heraklion, Greece: European Union Agency for Network and Information Security (ENISA), – 2013. – 96 p. URL: https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report

19. ENISA. Study on cryptographic protocols, – Heraklion, Greece: European Union Agency for Network and Information Security (ENISA), – 2014. – 52 p. URL: https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

20. Hazay, C. Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting / C.Hazay, G.L.Mikkelsen, T.Rabin [et al.] // Journal of Cryptology (J Cryptol), – 2019. 32, – p. 265-323. URL: https://doi.org/10.1007/s00145-017-9275-7

21. Hajiabadi, M., Kapron, B.M. Reproducible Circularly Secure Bit Encryption: Applications and Realizations // Journal of Cryptology (J Cryptol), – 2017. 30, – p. 1187-1237. DOI: 10.1007/s00145-016-9246-4

22. Əliquliyev, R.M. Kriptoqrafiyanın əsasları / R.M.Əliquliyev, Y.N.İmamverdiyev. – Bakı: "İnformasiya texnologiyaları" nəşriyyatı, – 2006. – 688 s.

23. Bellare, M., Boldyreva, A., Staddon, J. Randomness re-use in multi-recipient encryption schemeas // Proceedings of the Public Key Cryptography –PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, – Miami, FL, USA, – January 6–8, – 2003, Lecture Notes in Computer Science, vol. 2567 (Springer, 2003), – p. 85–99

24. Boneh, D. Circular-Secure Encryption from Decision Diffie-Hellman / D.Boneh, S.Halevi, M.Hamburg [et. al] // Proceedings of the Advances in Cryptology – CRYPTO 2008, 28th Annual International Cryptology Conference, – Santa Barbara, CA, USA, – August 17–21, – 2008, Lecture Notes in Computer Science, vol. 5157 (Springer, 2008), – p. 108–125.

25. Brakerski, Z., Goldwasser, S. Circular and leakage resilient public-key encryption under subgroup indistinguishability (or: Quadratic residuosity strikes back) // Proceedings of the Advances in Cryptology –CRYPTO 2010, 30th Annual Cryptology Conference, – Santa Barbara, CA, USA, – August 15–19, – 2010, Lecture Notes in Computer Science, vol. 6223 (Springer, 2010), – p. 1-20.

26. Chillotti, I. TFHE: Fast Fully Homomorphic Encryption Over the Torus / I.Chillotti, N.Gama, M.Georgieva [et al.] // Journal of Cryptology (J Cryptol), – 2019. 33, – p. 34-91. URL: https://doi.org/10.1007/s00145-019-09319-x

27. Gentry, C., Sahai, A., Waters, B. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based // Proceedings of Advances in Cryptology – Crypto-2013. DOI: 10.1007/978-3-642-40041-4_5, URL: https://eprint.iacr.org/2013/340.pdf

28. Ekdahl, P., Johansson, T. SNOW - a new stream cipher // Proc. of the first open Nessie Workshop, – Heverlee, Belgium, – November 13-14, – 2000. URL: https://pdfs.semanticscholar.org/900e/081fa7ba0d0b45e36185e327e1081bf55d28.pdf

29. Beierle, C. CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks / C.Beierle, G.Leander, A.Moradi [et al.] // IACR Transactions on Symmetric Cryptology, – 2019. No. 1, – p. 5-45. DOI:10.13154/tosc.v2019.i1.5-45

Аннотация

Анализ проведённых работ в области криптографии в современное время в западных странах

Фарман Мамедов, Вусала Гасанова

В статье дается всесторонний анализ различных организаций, работающих в сфере криптологии в Европе, их деятельности, а также организационной и научной работы.

Ключевые слова: криптография, алгоритм, шифрование, криптография в западных странах, IACR, ENİSA, ECRYPT.

Abstract

Analysis of the work carried out in the field of cryptography in modern times in Western countries

Farman Mammadov, Vusala Hasanova

The article provides a comprehensive analysis of various organizations working in the field of cryptology in Europe and their activities, as well as organizational and scientific work.

Keywords: cryptography, algorithm, encryption, cryptography in Western countries, IACR, ENİSA, ECRYPT.

Məqalə redaksiyaya daxil olmuşdur: 12.11.2020
Təkrar işlənməyə göndərilmişdir: 19.11.2020
Çapa qəbul edilmişdir: 23.11.2020