UOT 519.7

TÜRKİYƏ RESPUBLİKASINDA KRİPTOQRAFİK MÜHAFİZƏ SAHƏSİNDƏ TƏDQİQATLAR VƏ YERİNƏ YETİRİLMİŞ İŞLƏR HAQQINDA

mayor Fərman Məmmədov
Silahlı Qüvvələrin Hərbi Akademiyası
E-mail: fermanmemmedov@gmail.com

Xülasə. Məqalədə Türkiyə Respublikasında kriptologiyanın yaranması və inkişaf tarixi, bu sahədə çalışan qurumlar və onların fəaliyyət istiqamətləri, eləcə də yerinə yetirilən təşkilati və elmi işlərin geniş təhlili aparılır. Bundan əlavə, ölkəmizdə kriptoqrafiya elminin inkişaf etdirilməsi məqsədilə qardaş ölkənin təcrübəsi öyrənilir, ondan faydalanmanın yolları araşdırılır və əməkdaşlıq perspektivləri müəyyənləşdirilir.

Açar sözlər: kriptoqrafiya, alqoritm, şifrləmə, Türkiyə Respublikasında kriptoqrafiya, TUBİTAK, UEKAE.

Giriş

İnformasiya kommunikasiya texnologiyaları (İKT) sənayesi informasiya təhlükəsizliyinin, əsasən də informasiyanın qorunması üçün həm dövlət, həm də özəl sektorun maraqlarından çıxış edərək müxtəlif yanaşmalar təklif edir. Müasir İKT-yə inteqrasiya şəraitində dövlət, cəmiyyət, biznes strukturları və fərdlər kiberfəzada informasiya və onun mənbəyinin həqiqiliyi, elektron xidmətlərdən təhlükəsiz istifadə, fərdi məlumatların qorunması, verilənlərin tamlığı və konfidensiallığı sahəsində kritik problemlərlə qarşılaşır. Yeni kibertəhdidlərin meydana çıxdığı və təkamül etdiyi bir vaxtda ölkələrin qlobal kibertəhdidlərə qarşı çevik, operativ kibertəhlükəsizlik strategiyalarına malik olması mühüm əhəmiyyət kəsb edir [1].

Bu gün dünyada İKT-nin, xüsusən, internetin təsiri ilə qlobal rəqəmsal mühitin, virtual münasibətlərin formalaşması və inkişafı prosesi gedir. Dövlət idarəçiliyi, iqtisadi fəaliyyət sferaları, elm-təhsil sistemi, informasiya-kommunikasiya mühiti şəxsi və məişət həyatını əhatə edən bütün sahələr üzrə münasibətlər ənənəvi mühitdən virtual mühitə transformasiya olunur. Son bir neçə onillikdə internetin geniş istifadəsi sayəsində insanları, təşkilatları və dövlətləri birləşdirən, onları bir-birindən asılı edən qlobal kiberfəza formalaşmışdır [2]. Hətta bəzi mütəxəssislər tərəfindən III Dünya müharibəsinin kibermüharibə olacağı belə qeyd edilməkdədir. Bir çox ölkə və şirkətlər artıq kibertəhlükəsizlik üzrə yüksəkdərəcəli mütəxəssislərin hazırlanması prosesinə start vermişdir. Bəzi şirkətlər isə müvafiq işlər görür və hər gün artan yeni kibertəhdidlərə qarşı "kibertəhlükəsizlik" üzrə yeni sertifikatların verilməsinə başlamışdır [3]. Zaman keçdikcə kiberfəzada təhlükəsizliyin təmin edilməsi məqsədilə dövlətlər arasında beynəlxalq koordinasiyaya da ehtiyac artır.

Dünyada cərəyan edən proseslər bir daha göstərir ki, hazırda informasiya məkanına nəzarəti gücləndirməklə informasiya resurslarının mühafizəsi uğrunda mübarizənin aparılması aktual məsələlərdəndir. Bir çox dövlətlər öz vətəndaşları və iqtisadi maraqlarının təhlükəsizliyi ilə yanaşı, mədəni və mənəvi dəyərlərini qoruyub saxlamaq məqsədilə xüsusi tədbirlər görmək məcburiyyətindədir [4]. Dünyada informasiya təhlükəsizliyinin etibarlı təmin edilməsi dövlətlərin sıx əməkdaşlığını tələb edir [2]. Lakin bu sahədə dövlətlərin səmərəli əməkdaşlığı üçün strateji maraqlarını da nəzərə almaqla, onların hazırkı vəziyyətinin öyrənilməsi mühüm əhəmiyyət kəsb edir.

İnformasiya resurslarına qarşı yönəlmiş təhdidlərin qarşısını almaq üçün informasiyanın gizliliyinin təmin edilməsi vacibdir. Dövlət informasiya sistemləri və ehtiyatlarının yaradılması, idarə olunması, qarşılıqlı əlaqələndirilməsi, inteqrasiyası və təhlükəsizliyinin effektiv qorunmasının təmin edilməsi məqsədilə milli kriptoqrafiya siyasəti formalaşdırılmalıdır. Kriptoqrafiya, əsasən, dövlət sirlərinin qorunması zamanı istifadə olunduğundan dövlətlərarası rəqabət və münaqişələrdə əhəmiyyətli rola malikdir. Bəzi müəlliflərin yanaşmalarında kriptoqrafiya nüvə silahı və raket texnologiyaları ilə

birgə güclü dövlətin simvolu hesab edilir [5]. 1996-cı ildən fəaliyyət göstərən Vaasenaar sazişi ilə kriptoqrafik mühafizə vasitələri silah sistemlərinə aid edilmişdir (hazırda sazişdə 42 ölkə iştirakı edir və onlar ixrac edilən malların icazəsiz dövriyyəsinin qarşısının alınması məqsədilə "Vasitə, texnologiya və silahların ikili istifadəsi siyahısı"nı müəyyənləşdirirlər) [6]. Qloballaşan dünyada güclü kriptoqrafiya da bir neçə dövlətin inhisarındadır. Müstəqilliyini yeni qazanmış və inkişaf etməkdə olan ölkələrdə kriptoqrafiya sahəsində yetərli təcrübə və kadr potensialı yoxdur, müvafiq elmi-tədqiqatlar aparılmır və bu sahədə aparat-proqram vasitələrinin istehsalı müasir tələblərə uyğun deyil [5]. Ölkəmizdə bu sahə üzrə xüsusi təcrübəyə və fəaliyyətləri geniş təhliletmə bacarığına malik kadrların hazırlanmasına ehtiyac vardır.

Müstəqilliyimizin ilk illərindən etibarən Türkiyə Respublikası ilə bütün sahələrdə, eləcə də elm sahəsində hərtərəfli əməkdaşlıq edilmiş və böyük uğurlar qazanılmışdır. Qardaş ölkənin kriptoqrafiya sahəsində təcrübəsini öyrənmək, görülmüş işlərlə tanış olmaq, ondan faydalanmanın yollarını araşdırmaq və əməkdaşlıq perspektivlərini müəyyənləşdirmək məqalənin əsas məqsədini təşkil edir.

Türkiyə Respublikasında kriptoqrafiya sahəsinə töhfə verən qurumlar

Kriptoqrafiya qədim elm olsa da, XX əsrin 60-cı illərinin sonlarında onun bank sistemində tətbiqi ilə ictimaiyyət tərəfindən açıq şəkildə istifadəsinə başlanılmışdır [5]. Qardaş Türkiyə Respublikasında mütəxəssislər, demək olar ki, kriptoqrafiyanın meydana çıxması ilə eyni vaxtda araşdırmalara başlayıblar. Hazırda Türkiyədə kriptoqrafiya ilə bağlı araşdırmalar rəsmi səviyyədə aparılır və Türkiyə Respublikası Müdafiə Sənayesi Komitəsi (*Savunma Sanayii Başkanlığı – SSB*) ilə əməkdaşlıq çərçivəsində 10-a yaxın müəssisə kriptoqrafik cihazların hazırlanması və tədqiqatı ilə məşğul olur. SSB-nin 1000-dən artıq şirkət, tədqiqat müəssisələri və universitetlərin cəlb olunduğu böyük bir tədqiqat potensialı vardır. Eyni zamanda, Türkiyənin müdafiə sənayesi ölkə miqyasında məhsul və texnologiya istehsalı, eləcə də təkmilləşdirilməsi istiqamətində ən böyük sərmayə qoyan sektordur [7].

Türkiyə Elmi və Texnoloji Araşdırma Qurumunun (*Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – TUBİTAK*) tərkibində fəaliyyət göstərən İnformasiya və Məlumat Təhlükəsizliyi İnnovasiya Texnologiyaları Araşdırma Mərkəzinin (*Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi – BİLGEM*) Milli Elektronika və Kriptoqrafiya Tədqiqatları İnstitutu (*Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü – UEKAE) SSB* ilə əməkdaşlıq edən müəssisələrdəndir [8]. Türkiyə Respublikasında kriptologiya elminin yaranması və inkişafı, demək olar ki, bu qurumun adı ilə bağlı olmuşdur. İnstitutun ilkin təməli 1968-ci ildən Orta Şərq Texniki Universitetində (*Orta Doğu Teknik Üniversitesi*) fəaliyyət göstərən Elektronika Tədqiqatları Bölməsində beş tədqiqatçıdan ibarət qrupun 1972-ci ildə Qabzedə yerləşən Marmara Elm və Sənaye Araşdırma İnstitutunun tərkibinə verilməsi ilə qoyulmuşdur. Qurumun fəaliyyət sahəsinin genişliyi nəzərə alınaraq, 1991-ci ildən Elektronika və Yarımkeçirici Teknologiyaları Bölməsi adlandırılmışdır. Bölmə tərkibində görülən işlər 1995-ci ildən Milli Elektronika və Kriptoqrafiya Tədqiqatları İnstitutu (*UEKAE*) adı altında həyata keçirilir. 1997-ci ildən İnstitutun tərkibində Kriptoanaliz Mərkəzi təsis olunub və o, Türkiyə Silahlı Qüvvələrinin (*TSK*) şəbəkə təhlükəsizliyi və açarların idarə olunması məsələlərinə cavabdehdir. 1998-ci ildən *UEKAE TUBİTAK*-ın tərkibinə keçmişdir [9].

UEKAE Türkiyədəki strateji qurumların ehtiyacı olan informasiya təhlükəsizliyi və elektronik sistemlərin layihələndirilməsi istiqamətində fəaliyyət göstərir. 40 ildən artıq təcrübəsi olan İnstitut informasiya təhlükəsizliyi sahəsində texnoloji asılılığı azaltmaq məqsədilə dövlətin kritik infrastrukturlarının ehtiyac duyduğu cihazların işlənməsini həyata keçirir, müasir laboratoriyalar, test sistemləri, elmi üsullar və son texnologiyalardan istifadə etməklə beynəlxalq standartlara uyğun yüksəkkeyfiyyətli məhsullar təklif edir [10].

BİLGEM kriptoqrafiya, eləcə də İKT sahəsində Türkiyə miqyasında bir çox ilklərə imza atmışdır. Bunların bəziləri aşağıda göstərilmişdir [11]:

- mikroçip və kriptoçip istehsalı;
- hərbi və mülki səs və mətn şifrləmə provayderi;
- təhlükəsiz hərbi mesajlaşma provayderi;

– peyk şifrləmə modulu provayderi;
– ümumi açıq açar infrastrukturu;
– elektron imza sistemi provayderi və s.

Ümumiyyətlə, *TUBİTAK* layihələri əsasında kriptoqrafiya istiqamətində görülən işlərin nəticəsi olaraq məxfi rabitə vasitələri, kriptoqrafik açar idarəetmə sistemləri, ağıllı kart və şəxsiyyət təsdiqləmə sistemləri, elektron sertifikatların idarə edilməsi sistemləri sahələrində müxtəlif cihazlar, qurğular və həllər Türkiyə və dünyanın fərqli ölkələrinin, o cümlədən NATO-nun kritik infrastrukturlarında istifadə olunur [9, 11].

Kriptologiya ilə yanaşı, bütövlükdə informasiya təhlükəsizliyi sahəsinə böyük töhfə verən təşkilatlardan biri də İnformasiya Təhlükəsizliyi Dərnəyidir (*Bilgi Güvenliği Derneği*). Dərnək 2007-ci ildən fəaliyyət göstərir və məqsədi informasiya təhlükəsizliyi sahəsində cəmiyyətin bütün təbəqələrini fərdi, təşkilati və milli səviyyədə gözlənilən risklər barədə məlumatlandırmaq, onların bilgi səviyyəsini artırmaq, dünyada baş verən texnoloji inkişaf barədə ölkə ictimaiyyətini və akademik dairələri vaxtında xəbərdar etmək, eləcə də milli texnologiyaların yaradılması və inkişafına töhfə verməkdir. Təşkilatın hədəfi isə informasiya təhlükəsizliyi sahəsində dünya və yerli səviyyədə tərəfsiz, etibarlı və fəal bir milli qeyri-hökumət təşkilatı olmaqdır. Hazırda təşkilatın 120 fərdi, 19 hüquqi üzvü vardır və dərnəyin büdcəsi onların illik üzvlük haqqı, eləcə də digər ianələr hesabına formalaşır. Buna baxmayaraq, dərnək, təşkil etdiyi tədbirləri pulsuz və bütün ictimaiyyətə açıq şəkildə həyata keçirir. Dərnəyin əsas fəaliyyət sahələri konfrans, simpozium, işçi görüşlər, təlimlər keçirmək, hesabat və elmi təhlillər dərc etməkdir. İnformasiya Təhlükəsizliyi Dərnəyi Beynəlxalq informasiya təhlükəsizliyi və kriptologiya konfransının (*ISCTurkey*) əsas təşkilatçısı hesab olunur [12].

ISCTurkey 2006-cı ildən başlayaraq hər il keçirilən və ümumilikdə informasiya təhlükəsizliyi sahəsi ilə maraqlanan tələbə və tədqiqatçıları, eləcə də sənaye şirkətləri və ictimaiyyət nümayəndələrini bir araya gətirən böyük bir tədbirdir [13]. Yarandığı gündən konfransın əsas təşkilatçıları Türkiyənin İnformasiya Təhlükəsizliyi Dərnəyi (*Bilgi Güvenliği Derneği*), Qazi Universiteti, Orta Şərq Texniki Universiteti (*Orta Doğu Teknik Üniversitesi*), İnformasiya Texnologiyaları və Kommunikasiya Qurumu (*Bilgi Teknolojileri ve İletişim Kurumu*) olmuşdur. Vaxt keçdikcə İstanbul Texniki Universiteti və Nəqliyyat, Dənizçilik və Rabitə Nazirliyi (*Ulaştırma, Denizcilik ve Haberleşme Bakanlığı*) də təşkilatçı və dəstəkçilər arasına qatılmışdır. *ISCTurkey* konfransı beynəlxalq səviyyədə Avropa Birliyi Kibertəhlükəsizlik Agentliyi (*ENISA*) tərəfindən də dəstəklənir və hər ilin oktyabr ayında yayımlanması nəzərdə tutulan Avropa Kibertəhlükəsizlik Aylığı (*European Cybersecurity Month*) platformasında yer alır [14].

Koç Universitetinin nəzdində fəaliyyət göstərən Kriptoqrafiya, Təhlükəsizlik və Gizlilik Tədqiqatları Qrupu (*KTGTQ*) Alptekin Küpçü tərəfindən 2010-cu ildə qurulmuşdur. Məqsəd müasir texnologiyaların inkişafına fayda vermək, xalqları, özəl təşəbbüsçüləri və səlahiyyətli idarəçiləri bu sahədə olan texnologiyalarla məlumatlandırmaqdır. Qrup bulud texnologiyası, bulud hesablama və saxlama (*depolama*) sistemləri, kooperativ məlumat bazaları, şifrləmə, blokçeyn (*blokchain*) texnologiyası, kripto ödəniş vasitələri, açıq açar sistemləri, sosial şəbəkələr, gizliliyi qoruyan şəxsiləşdirmə və reklam sistemleri, Türkiyə Respublikasının fərdi məlumatların qorunması haqqında qanununa (*Kişisel Verilerin Korunması Kanunu – KVKK*) uyğunluq üçün kriptoqrafiya, P2P (*peer-2-peer* – tərəflər arasında birbaşa – vasitəsiz) şəbəkələrdə təhlükəsizlik, maşın öyrənməsi və s. sahələrdə araşdırmalarla məşğul olur [15]. A.Küpçünün birgə iştirakçılığı ilə hazırlanan layihələr sırasında: şəbəkə əsaslı autentikasiya (yoxlanılma); sosial şəbəkələrdə məxfiliyin qorunması; dinamik axtarışa və düzəlişlərə imkan verən şifrləmə alqoritmi; buludda genetik autentikasiya, eləcə də hesablama və saxlama (*depolama*) sistemləri; daxili serverdən kənarda (məsələn, buludda) yerləşən məlumat bazasının təhlükəsizliyinin təmin edilməsi; ikitərəfli paylaşım və müxtəlif kriptoqrafik hücumlar kimi işlərə müvafiq patentlərin əldə edilməsini göstərmək olar. Patenti alınmış layihələrin bir neçəsi *TÜBİTAK* tərəfindən də dəstəklənmişdir [16]. Qrup tərəfindən beynəlxalq konfranslar, seminarlar və müxtəlif görüşlərin təşkili, keçirilməsi və ya dəstəklənməsi də həyata keçirilir [17].

Kriptoqrafiya sahəsinə görülmüş bəzi işlərin təhlili

Türkiyəli mütəxəssislər tərəfindən yerinə yetirilmiş bəzi işlərin təhlili aşağıda verilmişdir.

M.Etemad və A.Küpçü [18]-də açıq açarlı infrastrukturlarda yeni və effektiv açar autentikasiya xidməti (*key authentication service – KAS*) təklif edirlər. Bu zaman server tərəfi güvənli xəbərləşmə mənbəyi kimi istifadə olunur və fərz edilir ki, serverlər arasında toqquşma baş vermir. *KAS* bütün istifadəçi açarlarını ayrı-ayrılıqda "heş zənciri" şəklində saxlayır və hər zaman zəncirin son halqasını serverlər arasında paylaşır. Xidmət, istifadəçiləri inandırır ki, ikimənalılıq baş vermir, serverlər onlar üçün eyni görünüşü təmin edir. İstifadəçi açarlarının ayrı-ayrılıqda saxlanılması server və kliyent arasında hesablamaların miqdarını və komunikasiya müddətini ciddi şəkildə aşağı salır ki, bu da *KAS*-ın çox effektiv açıq açarlı autentikasiya üsulu olduğunu ifadə edir.

M.Etemad və A.Küpçü [19]-də bədniyyətlilərin hücumlarına qarşı təhlükəsizlik sistemini uyğunlaşdıran, yoxlanıla bilən, dinamik axtarış imkanına malik simmetrik şifrləmə sxemi təklif edirlər. Təklif edilən sxem irihəcmli fayllarla iş zamanı həm effektivdir, həm faylların əlavə edilmə və silinmə imkanı var, həm də fayl modifikasiyalarını dəstəkləyir. İşin əsas konstruksiyasının təhlükəsizlik parametrlərinə müsbət cavab verməsi ixtiyari orakl (*random oracle model – ROM*) və standart təhlükəsizlik modelində isbat edilmişdir. Sxemin yoxlanışları göstərmişdir ki, şifrlənmiş kontentin içərisində axtarış, nəticələrin yoxlanılması çox sürətlə yerinə yetirilir, istifadəçi tərəfindən tətbiqi zamanı çox kiçik yaddaş tələb edilir və praktiki istifadəsi əlverişlidir.

L.Yuan, D.McNally, A.Küpçü [20]-də apardıqları tədqiqatda fotoların göndərilməsi zamanı fərdi məlumatların qorunmasına əsaslanan açıq açar infrastrukturunda şəkil qarışdırma sxemi təklif edirlər. Sxem JPEG kodlaşdırmasına malik şəkillərin şifrlənməsini nəzərdə tutur və JPEG fayllarının qarışdırılmasına əsaslanır. JPEG faylların təhlükəsiz qarışdırılması zamanı şəklin bir neçə əhəmiyyətli hesab olunan hissəsi (məsələn, şəxsi fotolarda əhəmiyyətli hissə kimi baş nahiyəsi) götürülür. Götürülən hissənin kvantlaşdırılmış diskret kosinus çevirməsinin işarəsi bir və daha çox açardan istifadə etməklə dəyişdirilərək qorunur. Qorunması təmin olunan şifrlənmiş şəkil digər bütün istifadəçilər tərəfindən baxıla bilər. Lakin şəkilin ilkin formada açılması yalnız lazımi məxfi açar olan tərəfdə mümkündür. Açarların tərəflərə çatdırılması asimmetrik şifrləmə qaydalarına yeni yanaşma olan atribut əsaslı şifrləmə ilə həyata keçirilir. Atribut əsaslı şifrləmə sxemlərində tərəflərin məxfi açarı yaş, vəzifə, münasibət və s. kimi atributlarla əlaqələndirilir. Təklif edilən arxitektura "*ProShare*" adlı *iOS* platformalı mobil tətbiqin istifadəsi ilə tədqiq olunur. Araşdırma nəticəsində sosial şəbəkələrdə və digər rəqəmsal mühitlərdə şəkil paylaşılan zaman qorunma təmin edilir.

S.Akleylek və M.Soysaldı [21]-də heç bir məlumat paylaşılmadan üçmərhələli, qəfəs əsaslı yeni şəxsiyyətin təsdiqlənməsi sxemini təqdim edirlər. Layihə *TUBİTAK* tərəfindən dəstəklənmişdir. Məqalədə təhlükəsizliyin fərqli qəfəs problemlərinə əsaslanan şəxsiyyətin təsdiqlənməsi sxemləri tədqiq edilir. Bununla yanaşı, təhlükəsiz təsdiqləmə sxemlərinə (*secure identification scheme – SIS*) əsaslanan yeni bir şəxsiyyətin təsdiqlənməsi sxemi və onun davamlılığının isbatı verilir. Gələcəkdə tədqiqatın genişləndirilərək daha faydalı şəxsiyyət təsdiqlənməsi sxemlərini əldə etmək üçün fərqli qəfəs problemlərinin digər tətbiq istiqamətlərinin müəyyənləşdirilməsində, eləcə də real vaxt rejimində işləyən tətbiqlərin qurulmasında və imzalama sxemlərinə çevrilməsində istifadəsi nəzərdə tutulur. Müəlliflərin digər tədqiqatlarında kvant hesablamalara dayanıqlı və çoxvariantlı kvadrat çoxhədlilərə əsaslanan sxem və ona əsasən yeni imzalama sxemi də təklif edilir [22].

S.Akleylek və M.Soysaldı [23]-də rəqəmsal məlumatların nüsxələnməsi, dəyişdirilməsi və başqa formata salınmasının/çevrilməsinin qarşısını alaraq müəllif hüquqlarının qorunması (*digital rights management – DRM*) məqsədilə şəxsiyyətin təsdiqlənməsi protokolunu təklif edirlər. Bu layihə də *TUBİTAK* tərəfindən dəstəklənmişdir. Protokol post-kvant kriptoqrafiyası üçün ikincidərəcəli çoxdəyişənli çoxhədli sistemlərinə əsaslanır. Əvvəllər mövcud olan sistemlərdə, məsələn, satın alınmış lisenziya nömrəsinin başqaları tərəfindən istifadə edilib-edilməməsinin öyrənmək mümkün deyildi. Bu baxımdan təklif olunan protokol digərlərindən fərqlənir.

M.K.Pehlivanoğlu, S.Akleylek, M.T.Sakallı və N.Duru [24]-də "*CURUPIRA*" ailəsi ("*CURUPIRA-1*", "*CURUPIRA-2*"), "*PRESENT*", "*Piccolo*", "*LED*", "*PRINCE*", "*KLEIN*", "*PRIDE*",

"*Rectangle*", "*SKINNY*", "*MANTIS*" yüngül (*lightweight*) bloklarla şifrləmə alqoritmlərini, onların işləməsi zamanı yayılma mərhələsinin konstruksiyasını, həmçinin effektivliyini təfsilatlı şəkildə təhlil edirlər. Əlavə olaraq, "*KLEIN*" və "*PRESENT*" alqoritmlərinin açar generasiyası prosedurları kəskin uçurum kriteriyasına (*strict avalanche criterion – SAC*) görə müqayisəli analiz olunur. Alqoritmlərin SAC testi göstərir ki, onların zəif açar generasiyası proseduru və "bitlərin itkisi problemi" mövcuddur. Eyni zamanda, tədqiqatda bloklarla şifrləmə zamanı yayılma mərhələsinin təhlükəsizlik səviyyəsini müəyyən etmək üçün maksimum məsafəyə yayılma (*Maximum Distance Separable – MDS*) matrisinin multiplikativ ardıcıllığının sonlu meydanda hesablanmasına əsaslanan metrik (*metric*) təklif olunur və eksperimental nəticələri verilir.

S.Akleylek və K.Seyhan [25]-də post-kvant kriptoqrafiyasına aid bircinsli olmayan kiçik ədəd həllinin ikitərəfli ümumiləşdirilməsi (*bilateral generalization inhomogeneous short integer solution – Bi-GISIS*) ilə yeni autentikasiya edilmiş açıq açarın tərəflərə göndərilməsi (*key exchange*) sxemini təklif edirlər. Layihə *TÜBİTAK* tərəfindən dəstəklənmişdir. Təklif edilən sxemin kriptodavamlılığı *Bi-GISIS*-in çətinliyinə əsaslanır. Bu sxemdə açarın təkrar istifadə edilməsi xassəsi təsadüfi təyinetmə modelində ikitərəfli pasterizasiya metoduna (pasterizasiya metodu əldə olan informasiya ilə açarın tapılmasının qeyri-mümkünlüyünə əsaslanır) görə təmin olunur. Autentikasiya edilmiş açıq açarın tərəflərə göndərilməsi sxemini əldə etmək üçün fərz edilən autentikasiya addımlarından (*implicit authentication steps*) istifadə olunur. Sxemin kriptodavamlılıq analizi, yüksək məxfiliyin təmin edildiyi *Bellare-Rogaway* təhlükəsizlik modelinə əsasən aparılmışdır. Tədqiqatda *Bi-GISIS*-ə əsaslanan autentikasiya edilmiş açıq açar paylaşımı probleminə yeni perspektivdən yanaşılır.

B.B.Kırlar, S.Ergün, S.Z.Alparslan Gök və G.-W.Weber [26]-də kriptoqrafiya, bulud hesablama və oyun nəzəriyyəsinin sintezindən ibarət, semantik təhlükəsizlik xassəsinə malik, effektiv və kompakt altqrup izləmə ifadəsi (*effective and compact subgroup trace representation – XTR*) istifadə etməklə yeni, səmərəli şifrləmə alqoritmi ilə kripto-bulud hesablama nəzəriyyəsi təklif edirlər. Yanaşmanın tətbiqi ilə maliyyə xidmətləri göstərən şirkətlər bulud hesablamanın texniki çətinliklərindən yaxa qurtarmaqla birlikdə, hərtərəfli, genişmiqyaslı və effektiv bulud strategiyasından istifadə edə bilərlər. Sistemin qurulmasında məqsəd oyun nəzəriyyəsi və maliyyə iqtisadiyyatı sahələrində kriptoqrafik vasitələrdən istifadə etməklə natural optimallaşdırma probleminin həllinə töhfə verməkdir. Hesab olunur ki, oyun nəzəriyyəsi və onun optimallaşdırılması ilə kripto-bulud hesablama sisteminin işlənilməsi bulud texnologiyası istifadəçiləri üçün əlverişli mühit yaradacaq.

Ü.Ülker [27]-də apardığı tədqiqatda türk əlifbasına uyğun yeni mətn şifrlənməsi alqoritmini işləmiş və hərflərin işlənmə tezliyi metoduna görə onun kriptoanalizini vermişdir. Şifrləmə zamanı əvvəlcə daxil olunan mətndəki boşluqlar götürülərək bütün mətnə bir söz kimi baxılır. Sonra hərflərin əlifba indeksinə müvafiq olaraq inversiya, əlifbanın gücünə nəzərən modula görə toplama əməliyyatı yerinə yetirilir. Nəticədə, ilkin mətndə olan müxtəlif hərflərin şifrlənmiş mətndə eyni simvollarla ifadə edilməsi baş verir. Tək bir hərfin birdən çox hərfi şifrləyə bilməsi təklif olunan alqoritmin əsas ideyasını təşkil edir və hərflərin işlənilmə tezliyi metoduna görə onun kriptoanalizini çətinləşdirir. Bu səbəbdən alqoritm ümumilikdə simmetrik açarlı alqoritmlər sinfinə aid edilmir. Eyni zamanda, deşifrləmə əməliyyatı da ənənəvi şifrləmənin əks ardıcıllığı qaydası ilə deyil, fərqli şəkildə icra edilir. Tədqiqat işində deşifrləmə əməliyyatı üçün səs komandalarının istifadəsi nəzərdə tutulur.

N.Suçsuz, D.Taşkın, C.Taşkının [28]-də təklif etdikləri metodda MPEG formatlı video faylların qismi şifrlənməsi ideyası təqdim edilir. Axınla şifrləmə alqoritminə əsaslanan üsul, videogörüntünün tamamının deyil, yalnız müəyyən olunmuş hissələrinin tərəflər arasında razılaşdırılmış açardan istifadə etməklə iki moduluna görə toplama əməliyyatı vasitəsilə kodlaşdırılmasını həyata keçirir. Videofaylların həcmi mətn informasiyalara nəzərən çox böyük olduğundan onların şifrlənməsi üçün yüksək hesablama sürətinə malik kompüterlər tələb olunur. Bu səbəbdən də videonun şifrlənmə alqoritmləri qurularkən şifrləmənin sürəti və vaxtı minimuma endirilir. Təklif olunan alqoritm bu tələbə əsaslanaraq videoaxında görüntünün müəyyən hissələrinin şifrlənməsi üçün istinad nömrələri təyin etməklə qismi şifrləməni təmin edir. Üsul şifrləmə və deşifrləmənin həm vaxtını, həm sürətini, həm də şifrlənmiş kontentin həcmini xeyli aşağı salır.

N.Topaloğlu, M.H.Calp, B.Türk [29]-də Sezar şifri, çoxəlifbalı əvəzetmə şifri və Eniqma maşınında tətbiq olunan ideologiyaların sintezindən istifadə edərək mətn tipli məlumatın şifrlənməsi üsulunu təklif edirlər. Əvvəlcə proqrama birincisi əsas olmaqla səkkiz ədəd əlifba daxil edilir. Əlifbaların bir-birindən fərqləndirilməsi əsas əlifbadakı hərflər və simvollar ardıcıllığının öz aralarında qarışdırılması ilə əldə edilir. Alqoritmdə daxil edilən əlifbalar açar rolunu oynayır. Şifrləmə zamanı əlifbalar hər birində üç ədəd olmaqla iki qrupa bölünür. Daxil olunmuş ilkin mətn massivə yığılır və massivin indekslərinin tək və ya cüt mövqelərinə müvafiq olaraq, birinci və ya ikinci qrup əlifbaların simvolları ilə dəyişdirilir. Dəyişdirilmə zamanı ilkin mətnin əsas əlifbadakı indeksi tapılır və növbəti əlifbada həmin indeksdə olan simvolla yerdəyişmə aparılır. Şifrləmənin sonuncu mərhələsində üç dəfə dəyişiklik nəticəsində əldə olunan simvol dördüncü yerdəyişmədə növbəti əlifbanın müvafiq indeksindən bir əvvəlki simvolla əvəz edilir. Proses mətnin sonuna qədər aparılaraq şifrmətn əldə olunur. Deşifrləmə standart qaydada şifrləmənin əksi ardıcıllıqla yerinə yetirilir. Təklif edilən metod dördmərhələli və yeddiəlifbalı qarışdırma və əvəzetmə üsullarının sintezi də hesab oluna bilər.

Ö.Sever [30]-də rəqəmsal imzalama və şifrləmə (*Signcryption*) sxemi ilə yoxlanılan şifrlənmiş imzalama sxemlərinin kombinasiyasından istifadə edərək yeni sintez olunmuş sxem təklif edir (müəllif yeni sxemi *VESigncrypt* adlandırmışdır). Məxfi kontraktların imzalanmasında istifadə edilməsi üsulun əsas üstünlüyüdür.

S.Öztoprak, M.A.Aydın və A.Sertbaş [31]-də RSA – açıq açarlı şifrləmə sistemində açıq açarın barmaq izi vasitəsilə generasiya olunmasına əsaslanan üsul təklif edirlər. Alqoritmə əsasən, barmaq izindəki məlumatlar matris şəklinə salınaraq unikal açar əldə edilir. Şifrləmədə istifadə edilən açıq açar isə həmin unikal açar vasitəsilə generasiya olunur. Təklif edilən metodla açıq açar bir növ gizlədilmiş və ya şəxsdən asılı vəziyyətə salınaraq şifrləmənin davamlılığını artırmış olur.

Nəticə

Tədqiqat nəticəsində aydın olur ki, kriptoqrafiya Türkiyədə dövlət səviyyəsində daima nəzarətdə saxlanılan, eləcə də milli və dövlət maraqları üçün istifadə olunan bir sahədir. İllər ərzində sistemli fəaliyyətlər nəticəsində rəsmi orqanlar, universitetlər, institutlar və tədqiqat mərkəzləri, eləcə də qeyri-hökumət təşkilatlarının qarşılıqlı əməkdaşlığı ilə istər proqram, istərsə də aparat səviyyəsində böyük işlər görülmüşdür. Hazırda Türkiyə şirkətləri tərəfindən istehsal olunan müxtəlif məhsullar beynəlxalq qurumlar, dövlət və kommersiya təşkilatları tərəfindən istifadə edilir. Eyni zamanda, qeyd edilməlidir ki, aparılan təşkilatlı və sistemli fəaliyyətlərlə kriptologiya elmi şaxələnərək müxtəlif istiqamətlər üzrə dərin inkişaf yolu izləmiş və dövlət orqanları, əsasən də silahlı qüvvələr tərəfindən tətbiq olunaraq praktiki əhəmiyyətini isbat etmişdir. Hazırda qardaş ölkənin mütəxəssisləri tərəfindən qlobal səviyyədə kriptoqrafiyanın trenddə olan istiqamətləri üzrə araşdırmalar artan sürətlə davam etdirilir və dünya miqyasında töhfələr verilir. Ümumiləşdirirək deyə bilərik ki, Türkiyə Respublikası qeyd olunan sahə üzrə dünyanın qabaqcıl təcrübəyə, eləcə də geniş imkanlara malik ölkələrindəndir və ölkəmizin onun bu potensialından istifadəsi üçün geniş perspektivləri mövcuddur.

İstifadə edilmiş ədəbiyyat siyahısı

1. Tanrıverdiyev, E. Müasir kibertəhlükəsizlik strategiyalarının tədqiqi // Hərbi bilik, – 2018. №1, – s. 45-51.

2. İmamverdiyev, Y.N. İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiya modeli // İnformasiya cəmiyyəti problemləri, – 2019. №1, – s. 14-20.

3. Həsənov, A.H. Azərbaycan Respublikasının Silahlı Qüvvələrində kiber ordunun yaradılmasının vacibliyini şərtləndirən amillər // – Bakı: Milli təhlükəsizlik və hərbi elmlər, – 2016. Cild 2, №2, – s. 112-115.

4. Tanrıverdiyev, E. İnformasiya müharibəsinin inkişaf mərhələləri, istiqamətləri və hədəfləri // Hərbi bilik, – 2018. №3, – s. 92-99.

5. İmamverdiyev, Y.N. İnformasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması problemləri // İnformasiya cəmiyyəti problemləri, – 2015. №1, – s. 12-23.

6. About us: [Elektron resurs] / Official web site of Wassenaar Arrangement. – 2019. URL: https://www.wassenaar.org/about-us/

7. Türk savunma sanayii ürün kataloğu / V.Pekuz, U.Ütük, B.Erginer [ve b.]. – Ankara: MİLDATA Prodüksiyon, – 2019. – 634 s.

8. TUBİTAK BİLGEM Teknoloji ve ürün kataloğu: [Elektronik resurs]. – 2019. URL: https://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tanitim-materyalleri.

9. UEKAE, Tarihçe: [Electronic resource]. URL: https://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce.

10. UEKAE, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü: [Elektronik resurs]. URL: https://uekae. bilgem.tubitak.gov.tr/tr/kurumsal/uekae.

11. TUBİTAK BİLGEM Sunum Dosyası: [Elektronik resurs]. – 2019. URL: https://uekae.bilgem.tubitak. gov.tr/tr/kurumsal/tanitim-materyalleri.

12. BGD Genç: [Elektronik resurs]. – 2020. URL: https://www.bilgiguvenligi.org.tr/bgd-genc/.

13. Önceki Konferanslar: [Elektronik resurs]. – 2020. URL: https://www.iscturkey.org/past_conf.html.

14. ISCTurkey2018, Sonuç Bildirgesi: [Elektronik resurs]. – 2020. URL: https://www.iscturkey.org/assets/files/ISCTurkey2018Sonu%C3%A7Bildirgesi_7.pdf.

15. Kriptoloji, Güvenlik ve Gizlilik Araştırmaları Grubu: [Electronic resource]. – 2020. URL: https://crypto.ku.edu.tr/tr/.

16. Projects: [Electronic resource]. – 2020. URL:https://crypto.ku.edu.tr/projects/.

17. Events and Announcements: [Electronic resource]. – 2020. URL:https://crypto.ku.edu.tr/events-and-announcements/.

18. Etemad, M., Küpçü, A. Efficient Key Authentication Service for Secure End-to-End Communications // International Conference on Provable Security, ProvSec 2015: Provable Security, LNCS 9451, – 2015, – p. 183-197. URL: https://crypto.ku.edu.tr/wp-content/uploads/2019/05/certificate-transparency.pdf.

19. Etemad, M., Küpçü, A. Verifiable dynamic searchable encryption // Turkish Journal of Electrical Engineering & Computer Sciences, – 2019. Volume 27, Number 4, – p. 2606-2623.

20. Yuan, L. Privacy-preserving photo sharing based on a public key infrastructure / L.Yuan, D.McNally, A.Küpçü [et al.] // Proc. SPIE 9599, Applications of Digital Image Processing, – 2015. XXXVIII, 95991I. URL: https://doi.org/10. 1117/12.2190458.

21. Akleylek, S., Soysaldı, M. 3-aşamalı Sıfır Bilgi Paylaşımlı Kafes Tabanlı Yeni Kimlik Doğrulama Şeması // The 4th International Conference on Computer Science and Engineering (UBMK19), – Samsun, Turkey: – September 11-15, – 2019, – s. 409-413.

22. Akleylek, S., Soysaldı, M. A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials // Turk J Math, – 2019. 43, – p. 241 – 257. doi:10.3906/mat-1803-92.

23. Akleylek, S., Soysaldı, M. Kuantum sonrası güvenilir dijital hak yönetim için yeni kimlik doğrulama protokolü // The 2th International Conference on Computer Science and Engineering (UBMK17), – Samsun, Turkey: – September 11-15, – 2017, – s. 322-327.

24. Pehlivanoğlu, M.K., Akleylek, S., Sakallı, M.T., Duru, N. On the design strategies of diffusion layers and key schedule in leightweight block ciphers // The 2th International Conference on Computer Science and Engineering (UBMK17), – Samsun, Turkey: – September 11-15, – 2017, – s. 322-327.

25. Akleylek, S., A Probably Secure Bi-GISIS Based Modified AKE Scheme With Reusable Keys // K.Seyhan, IEEE Access, – 2020. Vol.8, – p. 26210-26222. DOI:10.1109/ACCESS.2020. 2970537.

26. Kırlar, B.B. A gametheoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects / B.B.Kırlar, S.Ergün, S.Z.Alparslan Gök [et al.] // Annals of Operations Research, – 2016. 260 (1-2), – p. 217–231. doi:10.1007/s10479-016-2139-y.

27. Ülker, Ü. Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti // Bilişim Teknolojileri Dergisi, – 2013. cilt 6, sayı 2, – s. 31-39.

28. Suçsuz, N., Taşkın, D., Taşkın, C. Kısmi MPEG akımının XOR işlemi ile şifrelenmesi // II. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, ABG'08, – Kuzey Kıbrıs Türk Cumhuriyeti, Girne: TMMOB ELEKTRİK MÜHENDİSLERİ ODASI, – 16-18 Mayıs, – 2008. URL: http://www.emo.org.tr/ekler/540451347c2c0da_ek.pdf

29. Topaloğlu, N., Calp, M.H., Türk, B. Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi // Bilişim Teknolojileri Dergisi, – 2016. Cilt 9, Sayı 3, – s. 291-301.

30. Sever, Ö. Verifiably Encrypted Signcryption Scheme Based on Pairings // International Journal of Information Security Science, – 2017. Vol.6, No.1, – p.1-10.

31. Öztoprak, S., Aydın, M.A., Sertbaş, A. Biometric Based Cryptographic Key Generation For Secure Applications // 10. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı (ISCTurkey 2017), – Ankara: Bilgi Güvenliği Derneği, – 20-21 October, – 2017, – p. 23-28.

Аннотация
О исследованиях и проведённых работ в области криптографии в Турецкой Республике
Фарман Мамедов

В статье представлен широкий анализ создания и истории развития криптографии, органов, работающих в этой сфере, и направления их деятельности, а также организационной и научной работы, проводимой в Турецкой Республике. Кроме того, в целях развития науки криптографии в нашей стране изучается опыт братской страны, исследуются способы его использования, определяются перспективы сотрудничества.

Ключевые слова: криптография, алгоритм, шифрование, криптография в Турецкой Республике, TUBITAK, UEKAE.

Abstract
About the researches and the work carried out in the field of cryptography in the Republic of Turkiye
Farman Mammadov

The article provides a broad analysis of the creation and history of the development of cryptography, bodies working in this area and the direction of their activities, as well as the organizational and scientific work performed in the Republic of Turkey. In addition, in order to develop the science of cryptography in our country, the experience of the fraternal country is being studied, ways of using it are being investigated, and prospects for cooperation are determined.

Keywords: cryptography, algorithm, encryption, cryptography in the Republic of Turkey, TUBITAK, UEKAE.

Məqalə redaksiyaya daxil olmuşdur: 22.08.2020
Təkrar işlənməyə göndərilmişdir: 12.09.2020
Çapa qəbul edilmişdir: 26.09.2020