Əşyaların İnterneti üçün yüngülçəkili kriptoqrafiya

Yadigar İmamverdiyev[1], Tae Woon Kang[2]

[1]*AMEA İnformasiya Texnologiyaları İnstitutu*

[2]*National Research Foundation, Seoul, Korea*

[1]yadigar@lan.ab.az, [2]kungurum.kang@gmail.com

***Xülasə*— Əşyaların İnterneti yalnız insanları birləşdirən hazırki İnternetin növbəti inkişaf mərhələsidir və insanları əhatə edən bütün faydalı əşyaların qlobal şəbəkəyə qoşulmasını nəzərdə tutur. Əşyaların İnternetində təhlükəsizlik və gizlilik problemləri olduqca aktualdır və bu problemlərin həllində yüngülçəkili kriptoqrafiyanın əhəmiyyətli rol oynayacağı gözlənilir. Bu işdə kriptoqrafiyanın yeni istiqaməti olan yüngülçəkili kriptoqrafiyaya yürüdülən tələblər və bu sahədə tədqiqatların müasir vəziyyəti analiz edilir, perspektiv tədqiqat istiqamətləri müəyyən edilir.**

Açar sözlər*— *Əşyaların İnterneti; RFID texnologiyası; yüngülçəkili kriptoqrafiya; blok şifrləri; yan kanal hücumları.

I. GİRİŞ

Bugünkü İnternet insanların istifadəsində olan kompüterlərin qlobal şəbəkəsindən ibarətdir. İnternetin növbəti inkişaf mərhələsində isə bizi əhatə edən bütün faydalı əşyaların (məişət avadanlıqlarının, elektrik cihazlarının, gündəlik istehlak mallarının, nəqliyyat vasitələrinin, istehsal qurğularının, əmək alətlərinin, informasiya daşıyıcılarının, tibbi ləvazimatların, mühafizə və nəzarət sistemlərinin, bitki və heyvanat aləminin) bu qlobal şəbəkəyə qoşulması, Əşyaların İnternetinin (Əİ, ing. Internet of Things – IoT) yaranması gözlənilir. "Əşyaların İnterneti" termini ilk dəfə 1999-cu ildə Massaçusets Texnologiya İnstitutunun Auto-ID laboratoriyası tərəfindən RFID (Radio Frequency IDentification, radio tezlik identifikasiyası) texnologiyaları vasitəsi ilə İnternetə qoşulan obyektlərin şəbəkəsini ifadə etmək üçün işlədilib [1].

Əİ ideyasının reallaşdırılması ilə bağlı bir sıra milli, regional və beynəlxalq təşəbbüslər irəli sürülüb. Avropa Birliyi hesab edir ki, Əİ əlverişli siyasət, texniki inkişaf və işgüzar əməkdaşlıq şəraitində uğurla reallaşa bilər [2].

İnternetin təhlükəsizliyi ilə bağlı bütün problemlər Əİ üçün də aktualdır. İnformasiya təhlükəsizliyinin, fərdi məlumatların, intellektual mülkiyyət hüquqlarının qorunması kimi məsələlər həll edilmədən bu şəbəkənin uğurlu fəaliyyəti mümkün deyil [3,4]. İnternet mühitində bu problemlərin həllində müxtəlif kriptoqrafik alqoritmlər geniş istifadə edilir. Lakin onların Əİ üçün tətbiqində bir sıra problemlər mövcuddur. Son dövrlər məhdud resurslu mühitlərdə kriptoqrafiyanın tətbiqi cəhdləri kriptoqrafiyada yeni istiqamətin – yüngülçəkili kriptoqrafiyanın yaranmasına təkan vermişdir [5]. Bu tədqiqat işində yüngülçəkili kriptoqrafiyanın xüsusiyyətləri, müasir vəziyyəti və perspektiv inkişaf istiqamətləri araşdırılır.

II. RFID TEXNOLOGİYASI

Əİ texnoloji mahiyyətinə görə RFID texnolgiyasına əsaslanır. RFID obyektlərin avtomatik identifikasiyası metodudur, burada radiosiqnallar vasitəsi ilə RFID-teqlərdən məlumat oxunur və ya yazılır. RFID-sistemin tərkibinə aşağıdakı elementlər daxildir [5]:

Teq (ing. tag) və ya transponder – verilənləri saxlamağa və ötürməyə qabil mikrocip. Teqin enerjidən asılı olmayan yaddaşında unikal identifikasiya kodu və istifadə sahəsindən asılı olaraq başqa informasiya saxlanır. Bəzi növ teqlərdə yenidən yazılan yaddaş da olur.

Antena – elektromaqnit sahəsinin tuşlanması və bu sahəyə düşən teqlərdən informasiyanın alınması üçün istifadə edilir.

Oxucu (ing. reader) – antenaların köməyi ilə teqlərdən informasiyanı oxuyan və teqlərə informasiyanı yazan cihaz.

Oxucunu idarəetmə sistemi (ing. middleware) – proqram təminatıdır, teqlərin oxunması və ya yazılması sorğularını formalaşdırır, oxucuları qruplarda birləşdirərək onları idarə edir, teqlərdən alınan informasiyanı toplayır və analiz edir, bu informasiyanı uçot sistemlərinə ötürür.

RFID-sistemlər dörd tezlik diapazonundan istifadə edir: 125-150 kHs, 13,56 MHs, 862-950 MHs və 2,4-5 QHs (2,45 QHs diapazonu – Bluetooth və Wi-Fi standartı naqilsiz qurğularının işlədiyi tezliklərdir). Göstərilən tezlik diapazonlarının hər biri üçün öz standartı qüvvədədir.

RFID-sistemlərin istənilən mühitdə effektiv işləməsi üçün müxtəlif cür realizə edilmiş bir sıra teqlər işlənmişdir. Onları şərti olaraq enerji təchizatına görə (aktiv, passiv, yarıpassiv), oxuma-yazma əməliyyatlarına görə («yalnız oxuma», «bir dəfə yazma və bir neçə dəfə oxuma», «oxuma və yazma»), teqlərin realizə olunmasına görə (yapışqanlı qat olmadan, yapışqan qatlı, standart plastik kartlar, breloklar, xüsusi korpuslarda və s.) növlərə bölmək olar.

Passiv RFID-teqlərdə daxili enerji mənbəyi olmur, oxucudan gələn elektromaqnit siqnalının antenada induksiya etdiyi cərəyan teqdəki çipin işləməsi və cavab siqnalının göndərilməsi üçün kifayət edir. Aktiv RFID-teqlərin daxili enerji mənbəyi var və verilənlərin ötürülməsi üçün bu mənbədən istifadə edir. Bu teqlər oxucudan gələn enerjidən asılı deyil, nəticədə onlar daha uzaq məsafədən oxunur. Yarıpassiv (yarıaktiv) teqlər passiv teqlərə çox oxşardır, belə teqlərdə qidalanma elementi olur. Element oxucu ilə rabitə üçün deyil, yalnız mikrosxemlərin işini təmin etmək üçün istifadə edilir.

Prof. Tae Woon Kang is a visiting scientist assigned to Institute of Information Technology of ANAS from National Research Foundation (NRF) of S. Korea.

III. ƏŞYALARIN İNTERNETİNDƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

Əİ-də mövcud olan informasiya təhlükəsizliyi problemlərinin çoxu indiki İnternetdə də var. Məsələn, yanlış marşrutlama, məlumatın ələ keçirilməsi, icazəsiz istifadə, xidmətdən imtina (ing. Denial of Service, DoS) hücumları və s. Fərq ondadır ki, spesifik hücumlar kifayət qədər fərqli ola bilər. Məsələn, DoS-hücumlar qovşaqları mürgüləməyə qoymayan siqnallar göndərilməklə edilə bilər [6]. Bəzi məsələlər indiki İnternetdə problem yaratmasa da, Əİ-də böyük problem ola bilər. Məsələn, Əİ-də qurğuların fiziki əlyetənliyi asan olduğundan onların məhv edilməsi, onlardan məxfi informasiyanın çıxarılması və s. riskləri daha yüksəkdir.

RFID-oxucu ilə teqlər arasında mühafizəsiz naqilsiz rabitə istifadə edildiyindən bir çox təhlükəsizlik və gizlilik (ing. privacy) problemləri meydana çıxır [3,4,6-8]:

İnformasiyanın sızması: bədniyyətli teqdən faydalı məlumat əldə edə bilər. Hücum metodu hədəf teqə sorğu göndərmək və ya teq ilə oxucu arasındakı kommunikasiyaya gizli qulaq asmaqdır.

Gizliliyin pozulması: bədniyyətli teqli obyektin hərəkətini (və onunla əlaqəli insanı) izləyə bilər. Hücum metodunda bədniyyətli hədəf teqə sorğu göndərir və bir neçə RFID-oxucunun məlumatlarını əlaqələndirir (korrelyasiya edir).

Teqin saxtalaşdırılması: bədniyyətli özünü həqiqi teq kimi qələmə verməyə çalışır. Hücum zamanı hədəf teqə sorğu göndərir və ya teqlə oxucular arasındakı kommunikasiyanı dinləyir. Sonra hədəf teqin cavablarından istifadə edərək qanuni oxucunu aldatmağa cəhd edir.

Təkrarlama hücumu – bədniyyətli teq ilə oxucu arasında uğurlu autentifikasiya etmək üçün əvvəlki seansların məlumatlarından təkrar istifadə etməyə cəhd edir. Hücum metodunda bədniyyətli keçmiş tranzaksiyalardan həqiqi autentifikatorları ələ keçirir və onlardan istifadə edərək autentifikasiya olunur.

Xidmətdən imtina hücumu – bədniyyətli teq ilə oxucu arasında qarşılıqlı əlaqələri pozur. Hücum zamanı bədniyyətli ötürülən məlumatların qarşısını kəsir, bu teq ilə oxucu arasında ortaq açarın sinxronluğunun pozulmasına gətirib çıxara bilər.

İrəli və geri izləmə – bədniyyətli hətta teq sındırıldıqdan sonra da teqdə keçmişdə və gələcəkdə yerinə yetiriləcək hərəkətlərlə teqi əlaqələndirə bilər. Bu hücum zamanı bədniyyətli teqi sındıraraq hədəfin keçmiş və gələcək tranzaksiyalarını izlətməyə cəhd edir.

Oxucu adından istifadə hücumu – bədniyyətli özünü teqə qanuni oxucu kimi təqdim edir. Hücum metodunda bədniyyətli həqiqi seansı gizli dinləyir və bəzi məlumatların teqə çatmasının qarşısını alır. Sonra özünü qanuni oxucu kimi təqdim edərək başqa bir seans başladır.

Yuxarıda sadalanan təhlükəsizlik problemləri RFID-sistemlər üçün təhlükəsizlik mexanizmlərinin yaradılmasını kəskin problem kimi qarşıya qoyur []. Yüngülçəkili kriptoqrafik alqoritmlər və protokollar RFID-sistemlərin təhlükəsizliyi üçün həlledici əhəmiyyət daşıyır. Məsələn, autentifikasiya protokolu oxucuya sorğulanan teqin həqiqiliyinə əmin olmağa imkan verir. Eyni zamanda, bu protokol teqə sorğu verən oxucunun həqiqiliyinə əmin olmağa imkan verə bilər. (Əgər hər iki tərəf autentifikasiya olunursa, bu qarşılıqlı autentifikasiya adlanır.)

IV. YÜNGÜLÇƏKİLİ KRİPTOQRAFİYA

Yüngülçəkili kriptoqrafiya RFID-teqlər, sensorlar, kontaktsız smart-kartlar, tibb qurğuları daxil olmaqla, məhdud resurslu mühitlərdə reallaşdırmaq üçün nəzərdə tutulmuş kriptoqrafik alqoritmlər və protokollardır [9,10]. Yüngülçəkililik parametrləri platformadan asılıdır. Aparat realizəsində çipin ölçüləri və sərf edilən enerji vacib parametrlərdir. Proqram təminatı realizələrində isə proqram kodunun uzunluğu və RAM-ın həcmi vacibdir.

Yüngülçəkili kriptoqrafik alqoritmlərin işlənilməsində əsas problem təhlükəsizlik, sürət və qiymət arasında balansın təmin edilməsidir. Sərt qiymət məhdudiyyətlərinə görə kriptoqrafik alqoritm yalnız etibarlı və sürətli deyil, həm də reallaşdırmada ucuz olmalıdır. Hər üç tələbin eyni zamanda ödənilməsi olduqca çətin məsələdir. Məsələn, təhlükəsizliklə sürət arasında yaxşı balansın təmin edilməsi üçün çipdə böyük sahə tələb edilir, bu isə qiymətin artmasına səbəb olur. Digər tərəfdən, etibarlı və ucuz sistem yaratmaq olar, lakin onun sürəti məhdud olacaq.

Passiv RFID-teqlər daha çox yayılıb və onlarda istifadə edilən kriptoqrafik alqoritmlərin yaradılması daha aktualdır. Passiv RFİD-teqlər kimi olduqca yüngülçəkili tətbiqlər üçün kriptoqrafik primitivlərin yaradılmasına üç yanaşma var [9,10]:

1) standartlaşdırılmış kriptoqrafik alqoritmlərin az xərc tələb edən optimal realizələri;

2) Yaxşı araşdırılmış və aparat realizələri optimal olan şifrlərdə kiçik modifikasiyalar etmək;

3) Aparat təminatında realizə xərcləri aşağı olan yeni şifrlər işləmək.

Birinci yanaşmada problem ondan ibarətdir ki, müasir blok şifrlərinin bir çoxu proqram realizələrinin səmərəli olması məqsədi ilə yaradılıb. Onların aparat realizələri artıq xərc tələb edir, çipin ölçülərini artırmaqla bunu aradan qaldırmaq olar, lakin məhdud resurslu qurğularda bu mümkün deyil və buna görə bir çox blok şifrini belə mühitdə tətbiq etmək olmur.

İkinci yanaşmada yaxşı tədqiq olunmuş şifrlərin ehtiyatsız modifikasiyası ciddi arzuolunmaz nəticələrə gətirib çıxara bilər. Buna görə də, alqoritmin bəzi elementlərini modifikasiya edən zaman əlavə zəifliklərin meydana çıxması ehtimalını əsaslı surətdə qiymətləndirmək lazımdır.

Yüngülçəkili kriptoqrafiya sahəsində həllərin əksəriyyəti üçüncü yanaşmaya əsaslanır. Aydındır ki, kriptoqrafik dözüm nöqsanları olmayan yeni şifrlərin yaradılması olduqca çətin məsələdir. Mövcud alqoritmlərdən bəziləri yaxşı nəticələr göstərirlər və gələcəkdə RFID-sistemlərin təhlükəsizliyini təmin edən kriptosistemlərdə öz tətbiqlərini tapa bilərlər.

RFID-teqlərdə əsasən simmetrik kriptoalqoritmlər tətbiq edilir. Asimmetrik alqoritmlərlə müqayisədə onların sürəti daha yüksəkdir, bu da baxılan qurğular üçün kritikdir.

Yüngülçəkili blok və axın şifrləri mövcuddur [11]. Hazırda nisbətən yaxşı xarakteristikalara malik üç axın şifri var. Bunlar MICKEY, Trivium və GRAIN alqoritmləridir. Lakin fərdi

xüsusiyyətlərinə görə bu şifrlərin passiv RFID-sistemlərdə tətbiqi mümkün deyil. Məsələn, Trivium çipdə yolveriləndən 1,5 dəfə çox sahə tələb edir (3488 GE, məhdudiyyət 2000 GE-dir. GE (ing. Gate Equivalent) – rəqəmsal elektron dövrələrin mürəkkəbliyinin ölçü vahidir, çipin sahəsi ilə əlaqələndirilir). GRAIN alqoritminə əlaqəli açarlarla uğurlu hücum mümkündür. MICKEY alqoritminin isə dözümü yalnız bəzi hücumlara qarşı yoxlanılıb, bu ona inamı təmin etmək üçün yetərli deyil.

Yüngülçəkili blok şifrləri sahəsində vəziyyət bir qədər yaxşıdır. Belə şifrlərə misal olaraq DESL, PRESENT, KATAN, KTANTAN, HIGHT, mGrypton, MIBS və TWIS göstərilə bilər. PRESENT-in müxtəlif realizələri var və ən optimal variantda cəmi 1000 GE tələb edilir, bu yüngülçəkili şifrlərdə ən yaxşı nəticələrdən biridir [12].

Yüngülçəkili kriptoqrafik heş-funksiyalar sahəsində tədqiqatlar yeni başlayır [13]. Ümumməqsədli heş-funksiyalar (məsələn, SHA-1, SHA-2, SHA-3) yüngülçəkililik xassələrini ödəmir. Yüngülçəkili kriptoqrafik heş-funksiyaları yüngülçəkili blok şifrləri əsasında qurmaq mümkündür.

Yüngülçəkili açıq açar primitivləri ağıllı obyektlərin şəbəkələrində açarların idarə edilməsi protokolları üçün çox vacibdir, lakin açıq açarlı primitivlər üçün tələb edilən resurslar simmetrik açarlı primitivlərlə müqayisədə olduqca çoxdur. Hazırda RSA və ECC ilə müqayisədə yetərli təhlükəsizlik və yüngülçəkililik xassələri olan ümidverici primitivlər yoxdur.

V. YÜNGÜLÇƏKİLİ KRİPTOQRAFİYA ÜZRƏ STANDARTLAR

ISO/IEC 29192 standartı məhdud resurslu mühitlərdə tətbiq edilmək üçün şifrləmə alqoritmlərini müəyyən edir. Standart 4 hissədən ibarətdir: 1) Ümumi müddəalar, 2) Blok şifrləri, 3) Axın şifrləri və 4) Açıq açarlı kriptoqrafiya əsasında mexanizmlər. 1-ci, 2-ci və 3-cü hissələr uyğun olaraq 29 may 2012-ci il, 10 yanvar 2012-ci il və 28 sentyabr 2012-ci ildə qəbul edilmişdir, 4-cü hissə isə hələlik ilkin variantda işlənmişdir.

ISO/IEC 29192-2:2012 standartı yüngülçəkili kriptoqrafiya üçün yararlı iki blok şifri müəyyən edir:

a) PRESENT: yüngülçəkili blok şifri, blokun uzunluğu 64 bit və açarın uzunluğu 80 və ya 128 bit;

b) CLEFIA: yüngülçəkili blok şifri, blokun uzunluğu 128 bit və açarın uzunluğu 128, 192 və ya 256 bit.

PRESENT sürətli və yığcam aparat realizəsi üçün SPN əsaslı blok şifri kimi layihələndirilib və CHES 2007-də elan edilib [12]. Şifrin müəllifləri onun xətti və diferensial analizə, cəbri hücumlara və bəzi digər hücumlara qarşı dözümünü tədqiq ediblər. PRESENT 64-bitlik bloklarla 31 raund işləyir, açarın uzunluğu 80 və ya 128 bitdir. PRESENT-in hər bir tam raundu aşağıdakı ardıcıllıqda işləyir: raund altaçarı ilə bit XOR qatı; S-blok qatı – 4 ədəd sabit 4-bitlik S-blok aralıq şifr vəziyyətinə 16 dəfə paralel tətbiq edilir; xətti çevirmə - sabit bit permutasiyasından ibarətdir. 31-ci raunddan sonra çıxış çevirməsi var – axırıncı raund altaçarı XOR edilir.

RFID-sistemlərdə ötürülən məlumatların şifrlənməsi ilə yanaşı, PRESENT-in bəzi modifikasiyaları digər kriptoqrafik primitivlərin reallaşdırılması üçün də istifadə edilir. Məsələn, H-PRESENT-128 məlum heş-funksiyalardan ən yığcamıdır. Bundan başqa, onu cryptoGPS sxemində psevdotəsadüfi ədədlər generatoru kimi də istifadə etmək mümkündür.

CLEFIA şifri Sony və Naqoya Universiteti birlikdə yaratmışlar [14]. AES kimi onun da blokunun uzunluğu 128 bitdir və üç müxtəlif açar uzunluğu var: 128, 192 və 256 bit. CLEFIA 4-qollu və 8-qollu 2-ci növ ümumiləşmiş Feystel şəbəkəsindən istifadə edir və bir bloku açar uzunluğundan asılı olaraq 18(128 bit), 22 (192 bit) və ya 26 (256 bit) raund ərzində şifrləyir.

ISO/IEC 29192-3:2012 standartı yüngülçəkili kriptoqrafiya üçün iki axın şifri müəyyən edir:

a) Enocoro-80: açarın uzunluğu 80 bit;

b) Enocoro-128v2: açarın uzunluğu 128 bit;

c) Trivium: açarın uzunluğu 80 bit.

Enocoro yüksəksürətli axın şifri MUGI-nin əsasında yaradılıb [15], daxili vəziyyətin saxlanması üçün istifadə edilən registrlərin sayının kəskin azaldılması yolu ilə aparat sxeminin ölçüsü kiçildilib. Əlavə olaraq, əvəzləmə-permutasiya şəbəkəsinin (ing. Substitution-Permutation Network, SPN) iki iterasiyalı strukturunda qarışdırma funksiyası tətbiq etməklə registrdə verilənləri daha effektiv qarışdıra bilir və bununla təhlükəsizliyi yüksəldir və eyni zamanda istifadə edilən enerjini azaldır.

Trivium aparat təminatında realizə üçün nəzərdə tutulmuş sinxron axın şifridir, şifrləmə sürəti ilə elementlərin sayı arasında balans saxlanır, yetərincə effektiv proqram realizəsi də mümkündür. Şifr Avropa İttifaqının axın şifrlərinin müəyyən edilməsi üzrə təşkil etdiyi eSTREAM layihəsinə [16] təqdim edilmişdi, şifrin müəllifləri Kristof De Kannyer və Bart Preneldir [17].

Trivium şifri 80 bitlik açardan və 80 bitlik IV başlanğıc vektorundan 2^{64} bit uzunluğa kimi çıxış axını generasiya edir. Bu şifr eSTREAM layihəsinin ən sadə şifridir və kriptoanaliz üzrə əla nəticələr göstərir [17]. Kobud güc hücumunun çətinliyi məlumatın uzunluğundan asılıdır və 2^{120} tərtibindədir.

Triviumun başlanğıc vəziyyəti toplam uzunluğu 288 bit olan müxtəlif uzunluqlu 3 sürüşmə registrində saxlanır. Hər taktda düz və əks əlaqənin qeyri-xətti kombinasiyası yolu ilə sürüşmə registrlərində bitlər dəyişir. İlkin yüklənmə zamanı K açarı və IV başlanğıc vektoru 3 registrdən ikisinə yazılır və alqoritm 4x288 = 1152 dəfə yerinə yetirilir, bu ilkin vəziyyətin hər bir bitinin açarın və başlanğıc vektorun hər bir bitindən asılılığını təmin edir.

İlkin yüklənmə mərhələsi keçildikdən sonra şifrləmə üçün hər taktda açar axınının yeni elementi generasiya edilir və mətnin növbəti elementi ilə XOR ediliir. Deşifrləmə əks istiqamətdə gedir – şifrmətnin yeni elementi açar axınının növbəti elementi ilə XOR ediliir.

ISO/IEC DIS 29192-4 standartına aşağıdakı kriptoqrafik alqoritmlər daxildir:

- cryptoGPS identifikasiya sxemi – elliptik əyrilər üzərində diskret loqarifm məsələsi əsasında birtərəfli autentifikasiya mexanizmidir [18];

- ALIKE autentifikasiya və açar mübadiləsi sxemi (Authenticated Lightweight Key Exchange) – birtərəfli autentifikasiya və seans açarını müəyyənləşdirilməsi üçün mexanizmidir;
- IBS identifikasiya məlumatları əsasında (ing. ID-based) imza sxemidir.

VI. YÜNGÜLÇƏKİLİ KRİPTOQRAFİYANIN PROBLEMLƏRİ

Yüngülçəkili kriptoqrafiya alqoritmlərinin layihələndirilmə məqsədi kiçik resurs tələbləri, sürət və kriptoqrafik alqoritmin dözümü arasında balansın təmin edilməsidir. Resurs məhdudiyyətləri kriptoqrafları yüngülçəkili alqoritmləri kiçik blok və açar uzunluğu ilə layihələndirməyə məcbur edir. Bu düşmənə yüngülçəkili alqoritmə üst-üstə düşən şirfmətnlə hücum etməyə imkan verə bilər: m-bitlik blok şifrləri üçün eyni şifrmətn bloklarının tapılacağını $2m/2$ sayda bloku şifrlədikdən sonra gözləmək olar (ad günü paradoksuna görə). Üst-üstə düşən şiftmətn hücumu 16-, 32-, 48-bitlik blok şifrlərinə qarşı effektivdir. Buna görə, blok uzunluğu kiçik olan şifrləri ECB kimi rejimlərdə istifadə etmək çox təhlükəlidir [19].

Yüngülçəkili alqoritmlərin daxili vəziyyəti də mümkün qədər kiçik layihələndirilir. Klassik alqoritmlərlə müqayisədə daha sadə qarışdırma və diffuziya çevirmələri istifadə edilir.

Digər problem yüngülçəkili alqoritmlərin realizələrinə qarşı yan kanal hücumlarının mümkünlüyüdür. Yan kanal hücumlarının RFID-yə qarşı mümkünlüyü bir neçə işdə göstərilmişdir. Beləliklə, bu hücumlara qarşı yüngülçəkili kriptoqrafiyanın realizə olunduğu qurğularda da tədbirlər görülməsi zəruridir, bu isə həmin qurğulara əlavə yük deməkdir.

Fərz etmək olar ki, yaxın gələcəkdə yüngülçəkili kriptoqrafiyanın inkişafı fəal olacaq, çünki sənayenin və praktikanın ona tələbatı böyükdür. Yüngülçəkili kriptoqrafiyanın inkişafında aşağıdakı meylləri seçmək olar: 1) ultra-yüngülçəkili alqoritmləri yüngülçəkili kriptoqrafiyanın xüsusi bir bölməsi kimi ayrılması; 2) yüngülçəkili kriptoqrafiyanın aparat və proqram təminatı realizələrinin bir-birindən ayrılması.

NƏTİCƏ

Əşyaların İnterneti gələcək texnoloji inkişafı müəyyən edən çox ümidverici paradiqmalardan biridir. Əşyaların İnterneti insan-insan, maşın-maşın, insan-əşya, əşya-əşya, əşya-əşyalar kommunikasiyaları üçün böyük imkanlar açır, kompyutinq və şəbəkə təsəvvürlərini kökündən dəyişdirir. Eyni zamanda, bu evolyusiyada təhlükəsizlik və gizlilik problemləri də diqqətlə nəzərə alınmalıdır. Ənənəvi kriptoqrafiya bu yeni mühitə uyğunlaşa bilmir, lakin yüngülçəkili kriptoqrafiya şəbəkələşmiş ağıllı obyektlər arasında təhlükəsiz kommunikasiyaya imkan verməklə Əşyaların İnternetinin təhlükəsizliyi və gizliliyi üçün mühüm həllər təklif edir. Kriptoqrafik alqoritmləri yüngülçəkili kimi klassifikasiya etmək üçün dəqiq meyarlar yoxdur, lakin yüngülçəkili kriptoqrafik alqoritmlərin geniş yayılmış əlamətləri hədəf qurğularda əsas resursların olduqca məhdud olması şərtləridir. Yüngülçəkili kriptoqrafiya üzrə elmi tədqiqatlar nisbətən yeni başlayır, passiv RFİD-teqlər üçün kriptoqrafik alqoritmlərin və protokolların yaradılması olduqca aktualdır və öz həllərini gözləyir.

ƏDƏBİYYAT

[1] R.Əliquliyev və R. Mahmudov, "Əşyaların İnterneti: mahiyyəti, imkanları və problemləri," İnformasiya cəmiyyəti problemləri, №2(4), 2011, s.29-40.

[2] A. H. Sundmaeker et al., eds., "Vision and Challenges for Realizing the Internet of Things," IoT European Research Cluster, March 2010. www.internet-of-things-research.eu.

[3] Gan Gang, Lu Zeyong, Jiang Jun, "Internet of Things Security Analysis," International Conference on Internet Technology and Applications (iTAP), 2011, pp.1-4.

[4] I.Gudymenko, K.Borcea-Pfitzmann, and K. Tietze, "Privacy Implications of the Internet of Things," AmI 2011 Workshops - Constructing Ambient Intelligence, Communications in Computer and Information Science Vol. 277, 2012, pp. 280-286.

[5] S. Lahiri, RFID sourcebook. IBM Press, 2006. 276 p.

[6] Y.Fu, C.Zhang, and J.Wang, "A research on Denial of Service attack in passive RFID system," International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID), 2010, pp.24-28.

[7] M. R. Rieback. Security and Privacy of Radio Frequency Identification. PhD thesis, Vrije Universiteit, Amsterdam, The Netherlands, 2008.

[8] A.Juels, "RFID security and privacy: a research survey," IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp.381-394.

[9] A.Poschmann, M.Robshaw, F.Vater, C.Paar, "Lightweight Cryptography and RFID: Tackling the Hidden Overheads," Proc. of the 12th International Conference Information, Security and Cryptology – ICISC 2009, Vol. 5984 of LNCS, 2010, pp. 129-145.

[10] D.Maimut, K.Ouafi, "Lightweight Cryptography for RFID Tags," IEEE Security & Privacy, 2012, Vol. 10 , Issue 2, pp. 76-79.

[11] T. Eisenbarth, S. Kumar, L. Uhsadel, C. Paar, A. Poschmann, "A Survey of Lightweight-Cryptography Implementations," IEEE Design & Test, Vol.24, Issue 6, 2007, pp.522-533.

[12] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. "PRESENT: An ultra-lightweight block cipher," Proc. of CHES'07, Vol. 4727 of LNCS, pp. 450–466. Springer, 2007.

[13] J.-P. Aumasson, L. Henzen,W. Meier, and M. Naya-Plasencia, "Quark: A Lightweight Hash." Proc. of CHES 2010, Vol. 6225 of LNCS, pp. 1-15, Springer-Verlag, 2010.

[14] T.Shirai, K.JShibutani, T.Akishita, S.Moriai, and T.Iwata, "The 128-Bitblockcipher CLEFIA," Proc. of FSE 2007, Vol. 4593 of LNCS, pp. 181–195. Springer, 2007.

[15] D. Watanabe, S. Furuya, K. Takaragi, B. Preneel, "A New Keystream Generator MUGI," Proc. of 9th International Workshop on Fast Software Encryption (FSE 2002). Springer-Verlag. 2002, pp. 179-194.

[16] "The eSTREAM project." 2004–2008. http://www.ecrypt.eu.org/stream/

[17] C. De Canniere & B.Preneel, "TRIVIUM Specifications," eSTREAM. ECRYPT Stream Cipher Project, Report 2005/001, 2005. http://www.ecrypt.eu.org/stream/

[18] M. Girault, G. Poupard, and J. Stern. "On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order," Journal of Cryptology, vol. 19, pp. 463-487, Springer, 2006.

[19] S. Panasenko, and S. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches," International Journal of Computer Theory and Engineering, 2011, Vol. 3, No. 4, pp. 516-520.