Kvant Hesablama Sistemlərinə Kibertəhlükələr və Onların Reallaşdırılması Mexanizmlərinin Araşdırılması

Məmməd Həşimov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
mamedhashimov@gmail.com

***Xülasə*— Kvant texnologiyalarının sürətli inkişafı kibertəhlükəsizlik üçün yeni problemlər yaradır və bu sahədə mövcud risklərin daha dərindən tədqiq edilməsini zəruri edir. Məqalədə kvant hesablama mühitlərində mövcud kibertəhlükələr və onların reallaşdırılma mexanizmləri təhlil edilir. Xüsusilə klassik kriptoqrafik alqoritmlərin zəifliklərı, kvant rabitə kanalları və bulud əsaslı kvant xidmətlərinin təhlükəsizlik problemləri araşdırılır. Tədqiqat işində kvant hesablama sistemlərinə qarşı yönəlmiş əsas kibertəhlükələr və onların reallaşdırılması mexanizmləri araşdırılır. Eyni zamanda, kvant hesablama infrastrukturlarında təhlükəsizliyin təmin olunmasının əhəmiyyəti vurğulanır.**

Açar sözlər— kvant texnologiyaları; kibertəhlükəsizlik; kvant bulud təhlükəsizliyi; kvant hücumları.

I. GİRİŞ

Müasir dövrdə informasiya texnologiyalarının sürətli inkişafı rəqəmsal sistemlərin həyatın bütün sahələrində geniş tətbiq olunmasına səbəb olmuşdur. Dövlət idarəçiliyi, maliyyə sistemləri, səhiyyə, sənaye, nəqliyyat və bulud texnologiyaları kimi kritik sahələrdə məlumatların elektron formada emalı və saxlanılması kibertəhlükəsizlik məsələlərinin əhəmiyyətini daha da artırmışdır. Rəqəmsallaşmanın genişlənməsi ilə paralel olaraq kibertəhdidlərin miqyası və mürəkkəbliyi də artmağa başlamışdır. Xüsusilə məlumatların məxfiliyinin qorunması, təhlükəsiz ötürülməsi və kritik infrastrukturların müdafiəsi müasir informasiya təhlükəsizliyinin əsas problemlərindən biri hesab olunur.

Hazırda qlobal informasiya təhlükəsizliyi sistemlərinin böyük hissəsi klassik kriptoqrafik alqoritmlərə əsaslanır. Bu alqoritmlər bəzi riyazi problemlərin klassik kompüterlər tərəfindən həll edilməsinin çox vaxt və böyük hesablama gücü tələb etməsinə əsaslanır. Lakin yeni nəsil hesablama texnologiyalarının inkişafı mövcud təhlükəsizlik sistemlərinin gələcəkdə nə qədər etibarlı olacağı ilə bağlı ciddi müzakirələr yaratmışdır.

Son illərdə kvant texnologiyaları informasiya texnologiyaları sahəsində ən perspektivli istiqamətlərdən birinə çevrilmişdir. Klassik kompüterlərdən fərqli olaraq kvant kompüterləri məlumatların emalını qubitlər vasitəsilə həyata keçirir və superpozisiya, dolaşıqlıq kimi kvant mexanikası prinsiplərindən istifadə edir [1]. Bu xüsusiyyətlər kvant sistemlərinə bəzi mürəkkəb hesablama məsələlərini daha qısa müddətdə həll etmək imkanı yaradır. Kvant texnologiyalarının inkişafı süni intellekt, optimallaşdırma, böyük verilənlərin emalı və elmi modelləşdirmə kimi sahələrdə yeni imkanlar yaratsa da, eyni zamanda kibertəhlükəsizlik baxımından yeni risklərin yaranmasına səbəb olur.

Müasir rəqəmsal təhlükəsizlik infrastrukturunda geniş istifadə olunan RSA, Elliptic Curve Cryptography və Diffie–Hellman açar mübadiləsi kimi açıq açarlı şifrələmə metodlarının təhlükəsizliyi müəyyən riyazi problemlərin mürəkkəbliyinə əsaslanır. Lakin kvant kompüterlərində işləyən Shor alqoritmi kimi alqoritmlər həmin problemləri daha qısa müddətdə həll etməyə imkan verir [2]. Bundan əlavə, Grover alqoritmi simmetrik şifrələmə sistemlərinə qarşı kobud güc (brute-force) hücumlarının effektivliyini artırmaq potensialına malikdir.

Bununla yanaşı, gələcəkdə yalnız klassik informasiya sistemlərinin deyil, birbaşa kvant hesablama sistemlərinin özünün də kibertəhlükələrin hədəfinə çevrilməsi ehtimalı mövcuddur. Kvant bulud platformaları, kvant proqram təminatı, kvant şəbəkələri və qubit idarəetmə infrastrukturu potensial hücum səthləri kimi qiymətləndirilir. Xüsusilə Quantum Computing as a Service (QCaaS) yanaşmasının inkişafı kvant resurslarının internet üzərindən istifadəsini mümkün etmiş və bununla da yeni təhlükəsizlik problemlərinin yaranmasına səbəb olmuşdur [3].

Bu baxımdan kvant hesablama sistemlərinə qarşı yönəlmiş kibertəhlükələrin, onların reallaşdırılması mexanizmlərinin və mümkün müdafiə yanaşmalarının araşdırılması müasir kibertəhlükəsizlik sahəsində aktual tədqiqat istiqamətlərindən biri hesab olunur. Məqalənin əsas məqsədi kvant hesablama sistemlərində mövcud və potensial kibertəhlükələrin, onların reallaşdırılması mexanizmlərinin və təhlükəsizlik problemlərinin təhlil edilməsidir.

II. KVANT HESABLAMA SİSTEMLƏRİNİN ƏSASLARI

Kvant texnologiyalarının əsası XX əsrin əvvəllərində kvant mexanikasının formalaşması ilə qoyulmuşdur. Max Planck və Albert Einstein kimi alimlərin tədqiqatları bu sahənin inkişafında mühüm rol oynamışdır. 1980-ci illərdə kvant hesablama sistemlərinin nəzəri modeli Richard Feynman tərəfindən irəli sürülmüşdür. Daha sonra 1990-cı illərdə kvant alqoritmlərinin hazırlanması bu sahəyə marağı daha da artırmışdır [4]. Son onilliklərdə isə kvant texnologiyaları nəzəri mərhələdən çıxaraq praktiki tətbiq mərhələsinə keçməyə başlamışdır. Kvant hesablama sistemlərinin əsas xüsusiyyətləri, arxitekturası və texnoloji problemləri aşağıda göstərilmişdir:

DOI: 10.25045/forensic.gov.2026.09

2.1 Qubit və kvant hesablama prinsipləri. Klassik kompüterlərdə istifadə olunan bit yalnız iki vəziyyətdə, 0 və ya 1, ola bilir. Lakin kvant kompüterlərində istifadə olunan qubit eyni anda bir neçə vəziyyətdə mövcud ola bilir. Bu xüsusiyyət superpozisiya adlanır və kvant sistemlərinin paralel hesablama qabiliyyətini artırır [2].

Kvant hesablama sistemlərinin digər mühüm xüsusiyyəti dolaşıqlıq (entanglement) prinsipidir. Dolaşıqlıq zamanı iki və ya daha çox qubit bir-biri ilə əlaqəli vəziyyətə keçir və qubitlərdən birində baş verən dəyişiklik digərinə də təsir göstərir. Bu xüsusiyyət kvant rabitəsi və kvant hesablama proseslərinin sürətləndirilməsində mühüm rol oynayır. Bundan əlavə, kvant sistemlərində interferensiya prinsipi də mühüm rol oynayır. Bu prinsip vasitəsilə düzgün hesablama nəticələrinin ehtimalı artırılır, səhv nəticələrin isə təsiri azaldılır [2].

2.2 Kvant hesablama sistemlərinin arxitekturası [5]. Kvant hesablama sistemləri həm proqram, həm də aparat səviyyəsində mürəkkəb arxitekturaya malikdir. Kvant prosessorları qubitlər üzərində hesablama əməliyyatlarını həyata keçirən əsas hesablama komponentidir. Müasir kvant kompüterlərində superkeçirici qubitlər, tələyə salınmış ion əsaslı (trapped-ion) sistemlər və foton əsaslı texnologiyalar geniş istifadə olunur. Qubit idarəetmə modulları kvant əməliyyatlarının idarə olunmasını və qubitlərin vəziyyətinə nəzarəti həyata keçirir. Klassik idarəetmə kompüterləri isə kvant sistemlərinin koordinasiyası, əmrlərin icrası və hesablama nəticələrinin emalı üçün istifadə olunur.

Kvant proqram təminatı kvant alqoritmlərinin hazırlanmasını, simulyasiyasını və icrasını təmin edən proqram mühitindən ibarətdir. Bundan əlavə, kvant rabitə infrastrukturu kvant sistemləri arasında məlumat mübadiləsini və təhlükəsiz rabitəni təmin etmək məqsədilə istifadə edilir. Qubitlər xarici mühit təsirlərinə qarşı olduqca həssas olduğundan kvant sistemlərində xüsusi kriogen soyutma infrastrukturu tətbiq edilir. Bir çox kvant kompüterləri mütləq sıfıra yaxın temperatur şəraitində fəaliyyət göstərir. Bu səbəbdən kvant sistemlərinin fiziki təhlükəsizliyi və sabitliyi kibertəhlükəsizlik baxımından da mühüm əhəmiyyət daşıyır.

2.3 Quantum cloud və QCAAS platformaları. Son illərdə kvant hesablama texnologiyalarının bulud mühitində təqdim olunması geniş yayılmışdır. QCaaS internet üzərindən kvant resurslarından istifadə imkanı yaradır. QCaaS platformaları istifadəçilərə kvant alqoritmlərinin hazırlanması, kvant dövrələrinin test edilməsi və eksperimental hesablama aparılması imkanlarını təqdim edir. IBM Quantum Experience və Google Quantum AI kimi platformaları nümunə göstərmək olar [6, 7].

Lakin kvant resurslarının bulud mühitində istifadəsi yeni təhlükəsizlik problemləri də formalaşdırır. İstifadəçi autentifikasiyası, API təhlükəsizliyi, multi-tenant mühitdə resurs paylaşımı və kvant məlumatlarının qorunması kimi məsələlər kvant bulud sistemlərinin əsas təhlükəsizlik problemləri hesab olunur.

2.4 Kvant prosessorlarının fiziki reallaşdırılması və xəta korreksiyası problemləri [8]. Kvant hesablama sistemlərinin praktiki reallaşdırılması ən mürəkkəb texnoloji problemlərdən biri hesab olunur. Klassik kompüterlərdən fərqli olaraq kvant sistemlərində istifadə olunan qubitlər xarici mühit təsirlərinə qarşı olduqca həssasdır. Elektromaqnit səs-küyü, temperatur dəyişiklikləri və vibrasiya kimi faktorlar qubitlərin kvant vəziyyətinin pozulmasına səbəb ola bilər. Bu proses decoherence adlanır və kvant hesablama sistemlərinin əsas problemlərindən biri hesab olunur. Müasir kvant kompüterlərində qubitlərin sabit vəziyyətdə saxlanılması məqsədilə superkeçirici qubitlər, tələyə salınmış ion əsaslı (trapped-ion) sistemlər və foton əsaslı texnologiyalardan istifadə edilir. Bu sistemlərin əksəriyyəti mütləq sıfıra yaxın temperatur şəraitində fəaliyyət göstərir və xüsusi kriogen soyutma infrastrukturu tələb edir.

Kvant sistemlərində yaranan hesablama səhvlərinin azaldılması üçün müxtəlif səhv düzəltmə yanaşmalarından istifadə olunur. Bu məqsədlə məntiqi qubit bir neçə fiziki qubit üzərində paylanmış şəkildə saxlanılır ki, bu da yaranan səhvlərin aşkarlanmasına və müəyyən hallarda düzəldilməsinə imkan yaradır. Lakin əlavə fiziki qubitlərin istifadəsi kvant sistemlərinin resurs tələblərini və texniki mürəkkəbliyini artırır.

Kvant prosessorlarının fiziki zəifliklərı və xəta korreksiyası mexanizmləri kibertəhlükəsizlik baxımından da xüsusi əhəmiyyət daşıyır. Çünki hücumçular elektromaqnit müdaxilə, səs-küy müdaxiləsi və fiziki təsir metodlarından istifadə etməklə qubitlərin vəziyyətini dəyişdirə və kvant hesablama nəticələrinin etibarlılığına təsir göstərə bilərlər.

Beləliklə, kvant hesablama sistemləri klassik kompüterlərdən fərqli olaraq kvant mexanikasının prinsiplərinə əsaslanan mürəkkəb hesablama infrastrukturu formalaşdırır. Qubitlər, superpozisiya və dolaşıqlıq kimi xüsusiyyətlər bu sistemlərə yüksək hesablama imkanları qazandırsa da, eyni zamanda yeni təhlükəsizlik risklərinin yaranmasına səbəb olur. Kvant prosessorlarının fiziki həssaslığı, bulud əsaslı kvant xidmətlərinin yayılması və kvant proqram təminatının mürəkkəbliyi bu sistemlərin həm texniki, həm də kibertəhlükəsizlik baxımından xüsusi yanaşma tələb etdiyini göstərir. Bu baxımdan kvant hesablama infrastrukturlarının iş prinsiplərinin öyrənilməsi gələcəkdə yarana biləcək kibertəhlükələrin və hücum üsullarının daha yaxşı başa düşülməsi üçün vacib hesab olunur.

III. KVANT HESABLAMA SİSTEMLƏRİNƏ QARŞI KİBERTƏHLÜKƏLƏR

Kvant hesablama texnologiyalarının inkişafı informasiya texnologiyaları sahəsində yeni imkanlar yaratmaqla yanaşı, kibertəhlükəsizlik baxımından da yeni risklərin formalaşmasına səbəb olmuşdur. Klassik informasiya sistemlərindən fərqli olaraq kvant hesablama infrastrukturları həm proqram, həm də fiziki səviyyədə mürəkkəb quruluşa malikdir. Bu mürəkkəblik kvant sistemlərini müxtəlif hücum vektorları üçün potensial hədəfə çevirir. Xüsusilə kvant bulud platformalarının inkişafı, kvant resurslarının uzaqdan idarə olunması və kvant proqram təminatının genişlənməsi yeni kibertəhlükələrin yaranmasına şərait yaradır.

Kvant sistemlərinə yönəlmiş kibertəhlükələr yalnız klassik şifrələmə sistemlərinin sındırılması ilə məhdudlaşmır. Müasir tədqiqatlar göstərir ki, kvant hesablama infrastrukturlarının özü də autentifikasiya zəifliklərı, yan kanal hücumları, resurs oğurluğu, fiziki müdaxilə və proqram təminatı manipulyasiyası

kimi təhlükələrə məruz qala bilər. Bu kibertəhlükələrdən bəziləri aşağıda təqdim edilmişdir:

3.1 Alqoritmlər səviyyəsində təhdidlər. Kvant hesablama sistemlərində alqoritmik səviyyəli təhlükələr kvant alqoritmlərinin və hesablama proseslərinin manipulyasiyası nəticəsində yaranan kibertəhlükələri ifadə edir. Müasir kvant infrastrukturlarında kvant alqoritmləri, optimallaşdırma modelləri və hesablama tapşırıqları proqram mühitləri vasitəsilə idarə olunduğundan bu səviyyədə yaranan zəifliklər hesablama nəticələrinin etibarlılığına birbaşa təsir göstərə bilər.

Bu sahədə əsas təhlükələrdən biri kvant alqoritmlərinin manipulyasiyasıdır. Hücumçular kvant hesablama prosesində istifadə olunan alqoritmlərə və ya giriş parametrlərinə müdaxilə etməklə nəticələrin dəyişdirilməsinə və ya saxtalaşdırılmasına səbəb ola bilərlər. Xüsusilə bulud əsaslı kvant xidmətlərində istifadəçilər tərəfindən göndərilən kvant tapşırıqlarının dəyişdirilməsi və ya yönləndirilməsi məlumat bütövlüyü baxımından ciddi risk hesab olunur. Digər mühüm təhlükə səhv inyeksiyası (fault injection) hücumlarıdır. Bu tip hücumlarda kvant hesablama prosesinə müdaxilə edilərək alqoritmlərin düzgün işləməsi pozula və səhv hesablama nəticələri formalaşdırıla bilər [9].

Alqoritmik səviyyədə həyata keçirilən hücumlar xüsusilə kvant optimallaşdırma, maşın öyrənməsi və modelləşdirmə tətbiqlərində təhlükəli nəticələr yarada bilər. Bu tip hücumların reallaşdırılması zamanı hücumçular kvant hesablama prosesində istifadə olunan alqoritmlərə, giriş parametrlərinə və ya kvant tapşırıqlarına müdaxilə etməyə çalışırlar. Müdaxilə nəticəsində alqoritmlərin düzgün işləməsi pozula bilər.

Müasir tədqiqatlarda HHL (Harrow–Hassidim–Lloyd) kvant alqoritmi üzərində aparılan araşdırmalarda Improper Initialization Attack (IIA) və Higher Energy Attack (HEA) kimi hücumların kvant hesablama nəticələrinin düzgünlüyünə təsir göstərə bildiyi göstərilmişdir [10]. Bu səbəbdən kvant sistemlərində təhlükəsizlik yalnız şifrələmə ilə deyil, həm də alqoritmlərin düzgün işləməsinin yoxlanılması, hesablama nəticələrinin izlənməsi və yaranan səhvlərin aşkarlanması ilə təmin olunmalıdır. Beləliklə kvant sistemlərində təhlükəsizlik yalnız şifrələmə ilə deyil, həm də alqoritmlərin düzgün işləməsinin və hesablama nəticələrinin etibarlılığının təmin olunması ilə əlaqəlidir.

3.2 Kvant bulud sistemlərinə hücumlar. QCaaS platformalarının inkişafı kvant resurslarının internet üzərindən istifadəsini mümkün etmişdir. Lakin bu yanaşma yeni təhlükəsizlik problemlərinin yaranmasına da səbəb olmuşdur. Kvant bulud sistemlərinə qarşı hücumların reallaşdırılması zamanı hücumçular ilk növbədə istifadəçi autentifikasiya məlumatlarını hədəfə alırlar. İcazəsiz giriş əldə edildikdən sonra kvant resurslarından qanunsuz istifadə, istifadəçilərin kvant tapşırıqlarına müdaxilə və ya hesablama nəticələrinin dəyişdirilməsi həyata keçirilə bilər.

Xüsusilə multi-tenant arxitekturalarda bir istifadəçinin istifadə etdiyi resursların digər istifadəçilərlə paylaşılması təhlükəsizlik risklərini artırır. Belə mühitlərdə resursların kifayət qədər izolyasiya olunmaması digər istifadəçilərin məlumatlarına dolayı çıxış, məlumat sızması və icazəsiz müdaxilə ehtimalını yüksəldə bilər. Bundan əlavə, xidmətin dayandırılması hücumları vasitəsilə kvant sistemlərinin işləməsi zəiflədilə və ya tamamilə dayandırıla bilər [3].

Quantum bulud platformalarının geniş yayılması kvant sistemlərini klassik bulud təhlükəsizlik problemlərinə də açıq edir. Bu baxımdan kvant resurslarının uzaqdan idarə olunması gələcəkdə daha mürəkkəb kibertəhlükələrin formalaşmasına səbəb ola bilər.

3.3 Kvant proqram təminatına qarşı hücumlar. Kvant hesablama sistemlərində istifadə olunan proqram təminatı da potensial hücum hədəfi hesab olunur. Kvant hesablama sistemlərində istifadə olunan proqram mühitləri, kvant alqoritmləri və idarəetmə modulları ilə əlaqəli təhlükələri əhatə edir. Müasir tədqiqatlar göstərir ki, xüsusilə bulud əsaslı kvant platformalarında proqram səviyyəli zəifliklər və idarəetmə sistemlərinə qarşı hücum riskləri mövcuddurKvant proqram kitabxanalarında və idarəetmə modullarında yaranan zəifliklər hesablama nəticələrinin dəyişdirilməsinə, sistem sabitliyinin pozulmasına və təhlükəsizlik problemlərinin yaranmasına səbəb ola bilər. Xüsusilə bulud əsaslı kvant platformalarında istifadəçilərin göndərdiyi kvant tapşırıqlarının uzaq serverlərdə icra olunması proqram səviyyəli hücum risklərini artırır [11].

Kvant sistemlərinin idarə olunmasında klassik proqram təminatından istifadə edilməsi onların ənənəvi kibertəhlükələrə də açıq olmasına səbəb olur. Bu baxımdan kvant proqram mühitlərinin təhlükəsizliyi müasir kvant infrastrukturlarının əsas problemlərindən biri hesab edilir.

3.4 Fiziki səviyyəli hücumlar və yan kanal təhlükələri. Kvant hesablama sistemləri fiziki mühit faktorlarına qarşı yüksək həssaslığa malik olduğundan aparat səviyyəsində müxtəlif hücumlara məruz qala bilər. Klassik kompüterlərdə olduğu kimi kvant sistemlərində də yan kanal hücumları (Side-Channel Attacks) mühüm təhlükə hesab olunur [12].

Fiziki səviyyəli hücumlar və yan kanal təhlükələrinin reallaşdırılması zamanı hücumçular sistemin proqram hissəsinə birbaşa müdaxilə etmədən kvant cihazlarının fiziki xüsusiyyətlərindən istifadə etməyə çalışırlar. Bu tip hücumlar enerji sərfiyyatı, elektromaqnit təsirləri və digər fiziki göstəricilər vasitəsilə kvant hesablama prosesinə təsir göstərilməsi ilə əlaqəlidir [10]. Bəzi hallarda fiziki müdaxilə nəticəsində qubitlərin vəziyyəti dəyişdirilərək hesablama prosesində səhvlərin yaranmasına və sistem sabitliyinin pozulmasına səbəb olmaq mümkündür.

Qubitlərin xarici mühitə yüksək həssaslığı bu tip hücumların effektivliyini artırır. Xüsusilə kvant vəziyyətinin pozulması (decoherence) prosesi kvant hesablama nəticələrinin etibarlılığına təsir göstərə bilər. Bundan əlavə, kvant sistemlərinin kriogen soyutma infrastrukturu və aparat komponentləri də potensial fiziki hücum hədəfləri hesab olunur. Bu baxımdan kvant hesablama sistemlərinin fiziki təhlükəsizliyi müasir kibertəhlükəsizlik yanaşmalarının mühüm istiqamətlərindən biri hesab edilir [10].

3.5 Kvant idarəetmə sistemlərinə hücumlar - Kvant hesablama sistemləri yalnız kvant aparatlarından ibarət deyil. Bu sistemlərin idarə olunması üçün klassik proqram təminatı, idarəetmə modulları, API interfeysləri (Application Programming Interfaces) və bulud əsaslı proqram platformaları istifadə olunur. Kvant idarəetmə sistemlərinə qarşı hücumlar kvant kompüterlərini idarə edən proqram interfeysləri və aşağı

səviyyəli idarəetmə mexanizmlərində yaranan zəifliklərlə əlaqəli kibertəhlükələri əhatə edir [13].

Kvant idarəetmə sistemlərinə qarşı hücumların reallaşdırılması zamanı hücumçular əsasən autentifikasiya sistemlərini və idarəetmə proqramlarını hədəfə alırlar. İcazəsiz giriş əldə edildikdən sonra kvant resurslarının idarə olunması, istifadəçi məlumatlarının əldə edilməsi və ya hesablama proseslərinin dəyişdirilməsi mümkün ola bilər. Bundan əlavə, idarəetmə proqramlarında yaranan zəifliklər və proqram səviyyəli müdaxilələr kvant sistemlərinin təhlükəsizliyinə təsir göstərə bilər. Xüsusilə QCaaS platformalarında istifadəçilərin uzaqdan kvant resurslarına çıxış əldə etməsi hücum səthini genişləndirir. Hücumçu idarəetmə sisteminə nəzarəti ələ keçirdiyi halda kvant resurslarından icazəsiz istifadə edə, hesablama nəticələrini dəyişdirə və ya digər istifadəçilərin məlumatlarına çıxış əldə edə bilər.

Kvant idarəetmə infrastrukturlarının klassik proqram təminatına əsaslanması onların ənənəvi kibertəhlükələrə də açıq olmasına səbəb olur. Bu baxımdan kvant sistemlərinin təhlükəsizliyi yalnız kvant aparatlarının deyil, həm də onları idarə edən proqram və şəbəkə infrastrukturlarının qorunmasını tələb edir.

3.6 Kvant şəbəkələri və rabitə təhlükələri - Gələcəkdə kvant internet və kvant rabitə sistemlərinin inkişafı ilə kvant şəbəkələrinin təhlükəsizliyi daha aktual məsələyə çevriləcəkdir. Kvant açar paylanması (QKD, Quantum Key Distribution) sistemləri nəzəri baxımdan yüksək təhlükəsizlik təmin etsə də, real şəbəkə mühitində müxtəlif təhlükəsizlik problemləri ilə qarşılaşa bilər [14].

Kvant şəbəkələri və kvant rabitə sistemləri gələcək kvant internet infrastrukturlarının əsas komponentlərindən biri hesab olunur. Bu sistemlərdə məlumatların təhlükəsiz ötürülməsi üçün müxtəlif kvant rabitə texnologiyalarından istifadə edilir. Xüsusilə Quantum Key Distribution (QKD) protokolları kvant rabitə sistemlərində geniş tətbiq olunan təhlükəsizlik mexanizmlərindən biridir. QKD sistemləri yüksək təhlükəsizlik səviyyəsi təqdim etsə də, bu infrastrukturlar tam təhlükəsiz hesab olunmur

Kvant şəbəkələri və rabitə təhlükələrinin reallaşdırılması zamanı hücumçular əsasən kvant rabitə kanallarına və açar mübadiləsi prosesinə müdaxilə etməyə çalışırlar. QKD protokollarına qarşı ortada adam hücumları (man-in-the-middle attacks) və kvant kanalına müdaxilə kimi hücumların mümkün olduğu göstərilmişdir [15]. Bu tip hücumlar nəticəsində açar mübadiləsi prosesinin təhlükəsizliyi zəifləyə və məlumat ötürülməsinin etibarlılığı pozula bilər.

Kvant şəbəkələrinin klassik şəbəkə infrastrukturu ilə birlikdə işləməsi əlavə təhlükəsizlik riskləri yaradır. Klassik sistemlərdə yaranan zəifliklər kvant rabitə proseslərinə də təsir göstərə bilər. Eyni zamanda şəbəkə trafikinin analizi, siqnal itkisi, cihaz nasazlıqları və xarici elektromaqnit təsirlər istifadəçi fəaliyyəti haqqında dolayı məlumat əldə olunmasına və kvant açar mübadiləsinin etibarlılığının zəifləməsinə səbəb ola bilər. Bu səbəbdən kvant şəbəkələrinin təhlükəsizliyinin təmin olunması üçün həm kvant rabitə kanallarının, həm də klassik şəbəkə infrastrukturunun kompleks şəkildə qorunması vacib hesab olunur.

Aparılan təhlillərin nəticəsi olaraq kvant hesablama sistemlərinə qarşı əsas hücum vektorlarının müqayisəli xarakteristikası Cədvəl 1-də göstərilmişdir.

CƏDVƏL I. HÜCUM VEKTORLARININ MÜQAYISƏLI ANALIZI

Hücum vektoru	**Hücumların hədəfi**	**Reallaşdırılma üsulu**	**Potensial təsir**
Alqoritm səviyyəsində hücumlar	Kvant alqoritmləri və hesablama prosesləri	Parametrlərin manipulyasiyası, HHL hücumları	Yanlış hesablama nəticələri, məlumat bütövlüyünün pozulması
Kvant bulud hücumları	QCaaS platformaları, istifadəçi hesabları	Autentifikasiya zəifliklərı, resurs oğurluğu, DoS hücumları	İcazəsiz giriş, xidmətin dayanması, məlumat sızması
Kvant proqram təminatına hücumlar	Kvant proqram kitabxanaları və idarəetmə modulları	Zərərli kod, proqram zəifliklərı, kod manipulyasiyası	Hesablama nəticələrinin dəyişdirilməsi, sistem sabitliyinin pozulması
Fiziki və yan kanal hücumları	Qubitlər və aparat infrastrukturu	Elektromaqnit təsirlər, enerji sərfiyyatının təhlili	Qubit vəziyyətinin dəyişdirilməsi
Kvant idarəetmə sistemlərinə hücumlar	İdarəetmə proqramları	İcazəsiz giriş, İstifadəçi səlahiyyətlərinin artırılması	Resursların idarə olunmasının ələ keçirilməsi
Kvant şəbəkələri və rabitə hücumları	QKD sistemləri və kvant rabitə kanalları	Ortada adam (Man-in-the-Middle) hücumu, kanal müdaxiləsi, trafik analizi	Açar mübadiləsi prosesinə müdaxilə

Beləliklə, yuxarıda qeyd olunan təhlükələri nəzərə alaraq, kvant sistemləri yalnız yüksək hesablama imkanları təqdim edən yeni texnologiya deyil, eyni zamanda mürəkkəb kibertəhlükəsizlik problemləri formalaşdıran kritik infrastruktur hesab olunur. Kvant sistemlərinin proqram, aparat, şəbəkə və bulud səviyyəsində mövcud zəifliklərı gələcəkdə yeni hücum modellərinin yaranmasına səbəb ola bilər. Bu baxımdan kvant hesablama infrastrukturlarına qarşı yönəlmiş kibertəhlükələrin və onların reallaşdırılması mexanizmlərinin araşdırılması müasir informasiya təhlükəsizliyi sahəsinin mühüm istiqamətlərindən biri hesab olunur.

NƏTİCƏ

Kvant texnologiyalarının sürətli inkişafı informasiya texnologiyaları sahəsində yeni imkanlar yaratmaqla yanaşı, kibertəhlükəsizlik baxımından da yeni risklərin formalaşmasına səbəb olur. Kvant sistemləri klassik informasiya sistemlərindən fərqli olaraq mürəkkəb proqram, aparat, şəbəkə və idarəetmə infrastrukturlarına malik olduğundan müxtəlif səviyyələrdə kibertəhlükələrə məruz qala bilər.

Kvant sistemlərinin təhlükəsizliyinin təmin olunması üçün yalnız kriptoqrafik müdafiə mexanizmləri kifayət deyil. Bununla yanaşı proqram təminatı, idarəetmə sistemləri, fiziki infrastruktur və rabitə kanallarının da kompleks şəkildə qorunması vacibdir. Gələcəkdə kvant texnologiyalarının daha geniş yayılması ilə bu sahədə yeni hücum modellərinin və təhlükəsizlik problemlərinin yaranacağı gözlənilir. Bu səbəbdən kvant hesablama sistemlərinə qarşı kibertəhlükələrin və onların reallaşdırılması mexanizmlərinin araşdırılması müasir informasiya təhlükəsizliyi sahəsinin mühüm tədqiqat istiqamətlərindən biri hesab olunur.

ƏDƏBİYYAT

[1] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, 2010.

[2] What Are Shor's and Grover's Algorithms?. https://www.fortinet.com/uk/resources/cyberglossary/shors-grovers-algorithms

[3] A. Dash, B. Naik and S. Pati, "Security Vulnerabilities in Quantum Cloud Systems: A Survey on Emerging Threats," 2024. doi: 10.48550/arXiv.2504.19064

[4] S. S. Gill et al., "Quantum Computing: A Taxonomy, Systematic Review and Future Directions," Software: Practice and Experience 52(1):66-114, 2021. doi: 10.1002/SPE.3039

[5] S. Sarkar, "The Computer Architecture of Quantum Computing," 2018.

[6] IBM Quantum, "Quantum Computing as a Service", https://www.ibm.com/quantum

[7] Google Quantum AI. https://quantumai.google

[8] J. Roffe, "Quantum Error Correction: An Introductory Guide," Contemporary Physics, 60 (3). pp. 226-245. doi.org/10.1080/00107514.2019.1667078

[9] C. Xu, F. Erata, and J. Szefer, "Classification of Quantum Computer Fault Injection Attacks," arXiv preprint arXiv:2309.05478, 2023. https://doi.org/10.48550/arXiv.2309.05478

[10] Y. Tan, H. Kukina, and J. Szefer, "Study of Attacks on the HHL Quantum Algorithm," arXiv preprint arXiv:2410.08010, 2024, doi: 10.48550/arXiv.2410.08010.

[11] S. Ovaskainen et al., "Quantum Software Security Challenges within Shared Quantum Computing Environments," arXiv preprint arXiv:2507.17712, 2025

[12] S. Das, J. Jiang, S. Ghosh, and M. Tehranipoor, "Side-channel Attacks Targeting Classical-Quantum Interface in Quantum Computers," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2020. doi: 10.1109/HOST45689.2020.9300253.

[13] C. Xu and J. Szefer, "Security Attacks Abusing Pulse-level Quantum Circuits," in Proc. IEEE Symposium on Security and Privacy (SP), 2025, pp. 222–239, doi: 10.1109/SP61157.2025.00083.

[14] M. Peev et al., "On the Security of Quantum Key Distribution Networks," Entropy, vol. 24, no. 10, 2022.

[15] H. Amellal, S. El Hajjami, K. Kaushik and G. Chhabra, "Quantum Man-in-the-Middle Attacks on QKD Protocols: Proposal of a Novel Attack Strategy," 2024. doi: 10.1109/ic3i59117.2023.10397711

Cyber Threats to Quantum Computing Systems and Investigation of Their Implementation Mechanisms

Mammad Hashimov
Institute of Information Technology, Baku, Azerbaijan
mamedhashimov@gmail.com

Abstract- The rapid development of quantum technologies creates new challenges for cybersecurity and necessitates a deeper investigation of existing risks in this field. This paper examines cyber threats in quantum computing environments and their implementation mechanisms. In particular, the security weaknesses of classical cryptographic algorithms, quantum communication channels, and cloud-based quantum services are analyzed. The study investigates the major cyber threats targeting quantum computing systems and the methods through which these threats can be realized. Furthermore, the importance of ensuring security within quantum computing infrastructures is emphasized.

Keywords- quantum technologies; cybersecurity; quantum cloud security; quantum attacks.