AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun
"Elm-Təhsil İnteqrasiyası" məqsədli qrant müsabiqəsinin
(EİF/MQM/Elm-Təhsil-1-2016-1(26)) qalibi olmuş
layihənin yerinə yetirilməsi üzrə

YEKUN ELMİ-TEXNİKİ HESABAT

Layihənin adı: **Hərbi-müdafiə sistemində ötürülən səsli məlumatların sürüşən inikaslı şifrlənməsi sistemi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Səbziyev Elxan Nəriman oğlu**
Qrantın məbləği: **28 600 manat**
Layihənin nömrəsi: **EİF/MQM/Elm-Təhsil-1-2016-1(26)-71/06/1-M-09**
Müqavilənin imzalanma tarixi: **17 avqust 2020-ci il**
Qrant layihəsinin yerinə yetirilmə müddəti: **6 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 sentyabr 2020-ci il – 01 mart 2021-ci il**
Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulmalıdır
Diqqət! Uyğun məlumat olmadığı təqdirdə müvafiq bölmə boş buraxılır

Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

1	Layihənin həyata keçirilməsi üzrə yerinə yetirilmiş işlər, istifadə olunmuş üsul və yanaşmalar
	Azərbaycan Respublikasının Silahlı Qüvvələrdə radio-danışıq rabitəsinin həyata keçirilməsi zamanı danışığın məzmumumun üçüncü tərəfdən etibarlı şəkildə qorunmaqla ötürülməsi hər zaman önəmli məsələlərdən biri hesab olunur. Ötürülmə prosesində məlumatların şifrlənməsi və deşifrlənməsi onların qorunması üsulları sırasında əsas yeri tutur. Bu məsələ radio-rabitə kanalları ilə ötürülən məlumatlarf da aiddir. Mövcud şəbəkələr üzərindən ötürülən məlumatların rabitə operatorları tərəfindən şifrlənməsi həyata keçirilir. Korporativ radiorabitə sistemlərində isə şifrləmə və deşifrləmə aparat vasitələri ilə həyata keçirilir və onların etibarlılığı yoxlanıla bilmir. Layihə bu tip aparat vasitələri ilə ötürülən səsli məlumatların (danışığın) üçüncü tərəfdən etibarlı qorunması məsəqsədilə şifrləmə-deşifrləmə sisteminin işlənilməsi problemi tədqiq olunmuşdur. Ümumilikdə bir il müddətində yerinə yetirilməsi nəzərdə tutulmuş layihənin ilk 6 ayı ərzində hərbi təyinatlı məlumatların mübadiləsinə qoyulan tələblər formalaşdırılmış, səsli məlumatların (danışığın) şifrlənməsi və deşifrlənməsi üçün nəzəri əsaslar işlənilmiş, şifrlənmə və deşifrlənmə alqoritmləri işlənilmiş və uyğun proqram modulu yaradılmışdır. Belə ki, rəqəmsal sistemlərdə səsli

məlumatların ötürülməsi mexanizmindən çıxış edərək, **sürüşən inikaslı şifrlənmə** adlanan aşağıdakı şifrləmə mexanizmin təklif olunmuşdur:

- Məlumatın ayrılmış hissəsi (chunk) nömrələnir və tərəflərin hər ikisinə (məlumatı ötürən və qəbul edən tərəflər) məlum olan açar sözü (password) ilə şifrələnir. Bir qayda olaraq açar sözün uzunluğu 1 chunk-a aid olan məlumatın uzunluğundan bir-neçə dəfə çox olur.
- Şifrələmə qaydasına görə əvvəlcə açar sözü ASII cədvəli üzrə "0" və "1"-lərlə ifadə olunur.
- Səsli məlumatın "chunk"larla daxil olan və "0" və "1"-lərdən ibarət hər bir hissəsi açar sözün hissələri ilə belə şifrlənir: "birinci chunk" üçün – onun "0" və "1"-lərlə ifadə olunur ifadəsi açar sözün eyni uzunluqda başlanğıc hissəsi ilə toplanır; sonrakı "chunk"ların şifrlənmsi üçün açar sözü təşkil edən növbəti "0" və "1"-lər ardıcıllığı tətbiq olunur; bu proses hər bir növbəti "chunk" üçün eyni qaydada davam etdirilir. Hər hansı addımda açar sözün simvollarının sayı daxil olan "chunk" üçün bəs etmədikdə açar sözün əvvəlinə qayılır və onlar çatışmayan hissəyə tətbiq edilir.
- Şirfələnmiş məlumat (şifrələnmiş chunk-lar) uyğun protokollar tətbiq edilməklə rabitə kanalları vasitəsi ilə ötürülür.
- Qəbul edən tərəf məlumatı açar sözə əsasən deşifrə edir və bundan sönra çıxış qurğusuna (məsələn, mikrofona) ötürür; Deşifrələnmə qaydası şifrələnmə qaydasını əksindən ibarətdir, yəni açar sözün "0" və "1"-lərlə ifadə olunnan hissələrini qəbul edilən chunk-lardan (şifrələnmiş chunk-lardan) çıxmaqla həyata keçirilir.

Təklifr olunan şifrləmə mexanizminə uyğun olaraq səsli məlumatların şifrlənməsi və deşifrlənməsinin üçün alqoritmlər tərtib olunmuşdur. Tərtib olunmuş alqoritmlərə uyğun olaraq proqram təminatının həyata keçirilməsi mərhələsində aşağıdakı bir sıra problemlər aşkar olunmuş və həll olunmuşdur. Belə ki, səsli məlumatı göndərmək istəyən operator əvvəlcə klaviaturadan müəyyən açar sözü daxil edir, bu sözü ilkin açar sözü adlandıraq. Onun uzunluğu, bir qayda olaraq 15-25 simvol olur (15-25 bayt). Sonra məlumat faylını yükləməklə şifrləyib rabirə kanalları ilə tələb olunan ünvana göndərir. Şifrləmə prosesində səs faylının chunk adlanan və ötürülən hər bir hissəsi (wav-faylı üçün bu hissə 1600 bayt təşkil edir) operatorun klaviaturadan daxil etdiyi ilkin açar sözlə müqayisədə həcmcə dəfələrlə böyükdür. Ona görə də sürüşən inikaslı şifrlənmənin tətbiqi zamanı səs məlumatının daşınıldığı ədədi ardıcıllığın elementləri orta hesabla eyni qədər azalmış və ya artmış olur. Nəticədə şifrlənmiş məlumatı səsləndirəndə ilkin səsi başa düşməyə ciddi mane olmayan küy əmələ gəlir.

Digər tərəfdən, insan qulağı səsin (danışığın, musiqinin) tanınmasında robastlıq xüsusiyyətinə malikdir. Başqa sözlə, səsli məlumatın ayrı-ayrı hissələrindəki təhriflərə baxmayaraq ahənginə görə insan eşitmə aparatının robastlığı hesabına onu başa düşə bilir. Sürüşən inikaslı şifrlənmənin tətbiqi zamanı açar sözün hər bir simvolu chunkda yalnız özünə aid olduğu baytı dəyişdirir. Çox zaman operatorlar açar sözün yenilənməsi üçün əvvəlki sözdə bir neçə simvolu dəyişməklə kifayətlənirlər. Lakin bir birinə yaxın olan belə açar sözləri ilə sifrlənən səsli məlumatlar ahənginə görə bir-birindən az fərqlənmiş olur. Kripto-hücumlar zamanı etibarlı qorunmanın təmin edilməsi baxımından, bu yol verilməzdir. Belə ki, sürüşən inikaslı şifrlənmənin birbaşa tətbiqi zamanı, məsələn, "Salamov_Sabir" bə "Salahov_Cabir" açar sözlərindən biri ilə şifrlənmiş səsli məlumat ikinci aşar sözlə deşifrə olunaraq dinlənildikdə rahat başa düşülür. Deməli, bu halda üçüncü tərəfin əlinə düşdüyünə görə açar sözünün dəyişdirilməsi şifrlənərək ötürülən səsli məlumatın məxviliyini təmin etməyəcək. (Qeyd etmək lazımdır ki, bu problemlər mətn tipli məlumatların şifrıənməsi zamanı meydana çıxmır). Adı çəkilən problemlərlə bağlı səsli məlumatın şifrlənməsi zamanı onun gizliliyini təmin etmək üçün ilkin açar sözü əsasında müəyyən törəmə açar sözlərin generasiyası alqorirmləri işlənilmişdir. Bu alqoritm ilkin $\overline{A_1A_2A_3 \dots A_k}$ açar sözündən əvvəlcə böyük üzunluğa malik qeyri trivial $\overline{B_1B_2B_3 \dots B_n}$ ($n \gg k$), sonra $\overline{B_1B_2B_3 \dots B_n}$ əsasında $C_j = \sum_{i=1}^{k}(i+j) \times B_i$ formulu üzrə $\overline{C_1C_2C_3 \dots C_n}$ törəmə açar sözünün generasiyasını təklif edir. (Açar sözün ardına özünün əlavə edilməsi hesabına onun uzadılması trivial uzadılma hesab

edilir və burada tətbiq edilə bilməz!)

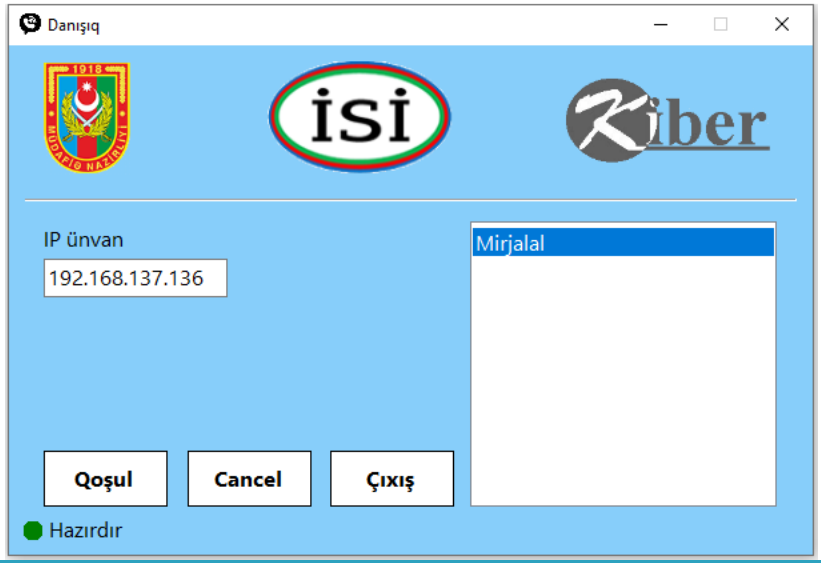
Layihə üzrə növbəti 6 ayı ərzində işlənmiş proqram təminatının texniki quğulara yüklənməsi ilə bağlı işlər nəzərdə tutulurdu. Lakin layihənin yeni variantında növbəti 6 ay ərzində onun ilkin variantından fərqli olaraq mobil ötürüçü qurğuların yaradılması üçün zəruri olan avadanlıq, cihaz və qurğuların əldə olunması nəzərdə tutulmadığından, məlumatın ötürülməsinin məsələsinin həllində texniki quğuları şəbəkədə işləyən kompüterlərdən istifadə etməklə həyata keçirmək qərara alındı.

Beləliklə, layihə üzrə tədqiqatın strukturuna uyğun olaraq iki kompüter arasında rabitə sistemini qurması və mübadilənin təşkili məsələləri həll olunmuşdur. Bu xüsusda xüsusi proqram interfeysi yaradılmışdır. İki iş yeri arasında şifrlənən səsli məlumat mübadiləsini aparmaq üçün proqramın işləmə ssenarisi işlənilmiş və həmin ssenari üzrə işləyən kompüter-proqram sistemi yaradılmışdır. Bu ssenariyə uyğun olaraq kompüter-proqram sistemi eyni şəbəkədə olan və iş yerləri kimi fəaliyyət göstərən iki kompüterdə arasında əlaqənin qurulduğunu yoxlayır, mübadilə protokollarını razılaşdırır, operatorlar tərəfindən daxil edilən parolları qəbul və səsli məlumatın mübadilə rejiminə keçir.

Kompüterlər arasında informasiya mübadiləsi yaratmaq üçün socket proqramlaşdırmadan istifadə olunmuşdur. Socket proqramlaşdırma vasitəsilə informasiya mübadiləsi yaradılarkən hər bir iş yerində server socket və klient socket vasitəsilə sadə klient-server arxitekturası qurulmuşdur. Bu zaman, server kimi istifadə olunan proqram təminatı müəyyən IP ünvanda və müəyyən port nömrəsində olan serveri aktivləşdirir. Klient kimi istifadə olunan proqram təminatları isə serverin IP ünvanını və serverin istifadə etdiyi port nömrəsi daxil edərək serverə qoşulur. Sonra proqram təminatının interfeysi vasitəsilə informasiya mübadiləsi kanalı yaradılır.

Windows əməliyyat sisteminə malik müxtəlif kompüterlər arasında səsli məlumatın şifrlənərək ötürülməsini həyata keçirən proqram modulunun işinin dayanıqlılığını yoxlamaq məqsədi ilə ədədi eksperimentlər layihələndirilmiş və çoxsaylı sınaqlar aparılmışdır. Eksperimentlərin nəticələrinə uyğun olaraq, interfeys təkmilləşdirilmiş, proqram modulunun işi mükəmməlləşdirilmişdir. Təklif olunmuş **məlumatların sürüşən inikaslı şifrlənməsi** üsulunun kriptohücumlara qarşı (üçüncü şəxslər tərəfindən oxunaraq deşifrə olana bilmə cəhdlərinə qarşı) dayanıqlılığı qiymətləndirilmişdir.

Layihədən gözlənilən nəticələr - səsli məlumatların şifrlənməsi və deşifrlənməsin nəzəriyyəsi müasir hesablama texikasının imkanlarının tətbiqi istiqamətində inkşaf etdirilməsi, uyğun elmi məqalələr çap etdirilməsi, həmçinin, səsli məlumatları şifrləyən və deşifrləyən proqram sistemi işlənib hazırlanması və səsli məlumatları şifrləmək və deşifrləməklə iki iş yeri arasında məlimat mübadiləsini təmin edən proqram sistemi işlənib hazırlanması tam şəkildə əldə olunmuşdur. Proqram interfeysinin əsas səhifəsi aşağıdakı şəkildə verilir.



Beləliklə, iş tam yerinə yetirilmişdir.

Layihənin yerinə yetirilməsi zamanı müxtəlif problemlərin həll edilməsi zərurəti meydana çıxmışdı. Problemlərin bir hissəsi səsli məlumatın bilavasitə şifrlənməsi və deşifrələnməsi məsələsi ilə bağlı olmuşdur, onların həlli üşün sistemli analiz və riyazi modeləşdirmə üsullarından, həmşinin qarşılıqlı-birqiymətli inikas üsullarından istifadə olunmuşdur.

İkinci qrup problem - kompüterlərin eyni hüquqlu olmaqla bir-biri arasında arasında informasiya mübadiləsinin həyata keçirilməsi problemi olmuşdur. Onun həlli üçün soket proqramlaşdırmadan istifadə olununmuş, kompüter-proqram sisteminin yaradılması zamanı obyekt yönümlü proqramlaşdırma prinsipi tətbiq olunmuşdur.

2 Layihənin həyata keçirilməsi üzrə planda nəzərdə tutulmuş işlərin yerinə yetirilmə dərəcəsi (faizlə qiymətləndirməli)

Layihədən gözlənilən nəticələr - səsli məlumatların şifrlənməsi və deşifrlənməsin nəzəriyyəsi müasir hesablama texikasının imkanlarının tətbiqi istiqamətində inkşaf etdirilməsi, uyğun elmi məqalələr çap etdirilməsi, həmçinin, səsli məlumatları şifrləyən və deşifrləyən proqram sistemi işlənib hazırlanması və səsli məlumatları şifrləmək və deşifrləməklə iki iş yeri arasında məlimat mübadiləsini təmin edən proqram sistemi işlənib hazırlanması tam şəkildə əldə olunmuşdur.

Beləliklə, iş tam yerinə yetirilmişdir - 100%.

3 Hesabat dövründə alınmış **elmi nəticələr** (onların yenilik dərəcəsi, elmi və təcrübi əhəmiyyəti, nəticələrin istifadəsi və tətbiqi mümkün olan sahələr aydın şəkildə göstərilməlidir)

- Səsli məlumatların şifrlənməsi və deşifrlənməsi üçün “**sürüşən inikaslı şifrlənmə”** üsulu işlənilmişdir. Üsulun yeniliyi ondadır ki, tətbiq olunan açar sözü kifayət qədər uzundur və şifrləmə zamanı ötürüləcək məlumatların hissələri “müxtəlif kodlarla” şifrlənmiş olur. Bu, şifrləndikdən sonra eyni tipli məlumatları bir-birindən fərqləndirir və onların deşifrlənməsi üçün açar sözün tapılmasında tezliklərin analizi üsullarının tətbiqini mənasız edir.
- İnsan qulağının səsin tanınmasında robastlıq xüsusiyyətinə görə səsli məlumatın şifrələnməsi üçün “sürüşən inikaslı şifrlənmə” üsulunun tətbiq olunması “əlavə tədbirlərin” tətbiq edilməsinin zəruri etdi. Bu məsələni həll etmək üçün ilkin açar sözü əsasında müəyyən **törəmə açar sözlərin generasiyası alqorirmləri** işlənmişdir.
- Socket proqramlaşdırma vasitəsilə informasiya mübadiləsi yaradılarkən hər bir iş yerində server **socket və klient socket vasitəsilə sadə klient-server arxitekturası təklif olunmuş** və qurulmuşdur. Beləliklə hər bir iş yeri eyni zamanda server və client olmuşdur. Başqa sözlə, yaradılmış proqram təminatı həm server kimi, həm də klient kimi fəaliyyət göstərir. Bu halda, iş yerləri (kompüterlər) arasında olan məlumat mübadiləsinin yaradılması üçün əlavə heç bir server tələb olunmur. Kompüterlər arasında informasiya mübadiləsinin həyata keçirilməsi üçün təklif olunmuş bu arxitektura alınmış elmi nəzicə hesab oluna bilər.

  Səsli məlumatın çifrlənməsi və ötürülməsi ilə bağlı törəmə açar sözlərin tətbiq olunması ideyası bu layihə tədqiqatları zamanı əsas elmi yeniliklərdən biri hesab oluna bilər. Layihədə, həmçinin bu ideyanın realizasiyası həyata keçirilmiş, törəmə açar sözlərin generasiyası alqorirmi işlənmişdir.

  Layihə çərçivəsində əldə edilmiş elmi nəticələr hərbi təyinatlı rabitə sistemlərində və digər güc strukturlarının idarəetmə sistemləırində səsli məlumatın (danışıqların) ötürülməsi zamanı istifadə oluna bilər. Törəmə açar sözlərin generasiyası alqorirmləri Həmçinin hərbi

	təyinatlı telekommunikasiya və kompüter şəbəkələrində məlumatların rabitə kanalları vasitəsi ilə ötürülməsi zamanı konfidensiallığın təmin edilməsi məqsədilə tətbiq oluna bilər.
4	Layihə üzrə **elmi nəşrlər** (elmi jurnallarda məqalələr, monoqrafiyalar, icmallar, konfrans materiallarında məqalələr, tezislər) (dərc olunmuş, çapa qəbul olunmuş və çapa göndərilmişləri ayrılıqda qeyd etməklə, uyğun məlumat - jurnalın adı, nömrəsi, cildi, səhifələri, nəşriyyat, indeksi, İmpact Factor, həmmüəlliflər və s. bunun kimi məlumatlar - ciddi şəkildə dəqiq olaraq göstərilməlidir) *(surətlərini kağız üzərində və CD şəklində əlavə etməli!)*
	Layihə üzrə 2 məqalə və 2 tezis çap olunub: - **Həsənov A.H., Səbzyiev E.N., Talibov Ə.M., İmanov R.R., Nifrəliyev T.A.** Hərbi təyinatlı idarəetmə sistemində səsli məlumatın sürüşən inikaslı şifrlənməsi // İnformasiya təhlükəsizliyi (elmi-metodiki jurnal), 2019, №2, S.16-19. (*jurnal EİF-na təqdim olunub*). - **Həsənov A.H., Səbzyiev E.N.** Səsli məlumatın şifrlənmə problemlərinin analizi və həlli yolları // Milli təhlükəsizlik və hərbi elmlər, 2019, C.5, №2, S.13-16. (*jurnal EİF-na təqdim olunub*). - **Сабзиев Э.Н., Садыгова Р.И., Мамедова У.М., Амирасланова З.Н.** Шифрование речевой информации с применением метода генерации вторичных ключевых слов // Матерıали дев'ятої мıжнародної науково-технıчної конференцıї "Сучасні напрями розвитку ınформацıйно-комунıкацıйних технологıй та засобıв управлıння", 11-12 апрель 2019, Харьков, Украина. С.94. (1 Səh). (*tezis EİF-na təqdim olunub*). - **Aliyev Y.A.** Position encryptıon accordıng to the key's symbols for data protectıon // 10th International Conference "Modern Directions of Development of the Information and Communication Technologies and Control Systems". 9-10 April 2020, Xarkiv. Vol 2, p.4. (1 Səh). (*tezis EİF-na təqdim olunub*).
5	İxtira və patentlər, səmərələşdirici təkliflər
	Layihə müqaviləsinin qüvvədə olduğu müddətdə ixtira, patent və səmərələşdirici təkliflər olmayb.
6	Layihə üzrə ezamiyyətlər (ezamiyyə baş tutmuş təşkilatın adı, şəhər və ölkə, ezamiyyə tarixləri, həmçinin ezamiyyə vaxtı baş tutmuş müzakirələr, görüşlər, seminarlarda çıxışlar və s. dəqiq göstərilməlidir)
	Layihə müqaviləsinin qüvvədə olduğu müddətdə layihə üzrə ezamiyyətlər olmayb.
7	Layihə üzrə elmi ekspedisiyalarda iştirak (əgər varsa)
8	Layihə üzrə digər tədbirlərdə iştirak (əgər varsa)
	(burada doldurmalı)
9	Layihə mövzusu üzrə elmi məruzələr (seminar, dəyirmi masa, konfrans, qurultay, simpozium və s. çıxışlar) (məlumat tam şəkildə göstərilməlidir: a) məruzənin növü: plenar, dəvətli, şifahi və ya divar məruzəsi; b) tədbirin kateqoriyası: ölkədaxili, regional, beynəlxalq)
	(burada doldurmalı)

	- 2019-cu ilin 11-12 aprelində Xarkov Maşınqayırma Texnologiyaları elmi tədqiqat institutunun təşəbbüsü ilə təşkil edilmiş beynəlxalq "Сучасні напрямки розвитку інформаційних технологій і засобів зв'язку" ("İnformasiya texnologiyalarının və rabitə vasitələrinin müasir inkişaf istiqamətləri") konfransına "Шифрование речевой информации с применением метода генерации вторичных ключевых слов" ("***İkinci açar sözlərinin generasiya olunma üsulunun tətbiqi ilə danışıq məlumatının şifrlənməsi***") adlı məruzə təqdim olunmuşdur. Məruzənin növü: şifahi Tədbirin kateqoriyası: beynəlxalq - 2020-ci ilin 9-10 aprelində Xarkov Maşınqayırma Texnologiyaları elmi tədqiqat institutunun təşəbbüsü ilə təşkil edilmiş beynəlxalq "Сучасні напрямки розвитку інформаційних технологій і засобів зв'язку" ("İnformasiya texnologiyalarının və rabitə vasitələrinin müasir inkişaf istiqamətləri") konfransına "Позиционное шифрование по символам ключа для защиты данных" ("***Ötürülən məlumatların qorunması üçün açar sözün simvolları üzrə mövqeli şifrləmə***") adlı məruzə təqdim olunmuşdur. Məruzənin növü: şifahi Tədbirin kateqoriyası: beynəlxalq
10	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar, komplektləşdirmə məmulatları
	Layihənin ilkin variantına uyğun olaraq onun ilk mərhələləri dövründə avadanlıq, cihaz və qurğuların adları və spesifikasiyası tərtib olunaraq alınmaq üçün Elmin İnkişaf Fonduna təqdim edilmişdi. Lakin bir sıra obyektiv səbəblərdən onlar əldə olunmadı. Sonrakı mərhələdə - Elmin İnkişaf Fondu yenidən fəaliyyətə başladıqdan sonra imzalanmış razılaşmaya uyğun olaraq avadanlıq, cihaz və qurğuların alınmasına maliyyə vəsaiti ayrılmamışdır, ona görə də avadanlıqların alınması məsələsi tamamilə gündəlikdən çıxarılmışdır.
11	Yerli həmkarlarla əlaqələr
	Şifrləmə problemi hələ cari layihə təsdiq olunmadığı dövrdə də Silahlı Qüvvələrin Ali Hərbi Akademiyasının və Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun diqqət mərkəzində olmuşdur. Bu işlərdə aparıcı yerlərdən birini tutan İdarəetmə Sistemləri İnstitutunun laboratoriya rəhbəri Ədalət B.Paşayev və gənc mütəxəssislər kiçik elmi işçi Yadigar Əliyev və Mircalal Talışınski layihə ilə bağlı tədqiqatlara cəlb edilmişdir.
12	Xarici həmkarlarla əlaqələr
	Layihə müqaviləsinin qüvvədə olduğu müddətdə layihə üzrə görülən tədqiqat işləri ilə bağlı xarici həmkarlarla əlaqələr olmayb.
13	Layihə mövzusu üzrə kadr hazırlığı (əgər varsa)
14	Sərgilərdə iştirak (əgər baş tutubsa)
15	Təcrübəartırmada iştirak və təcrübə mübadiləsi (əgər baş tutubsa)

16	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s. (məlumatı tam şəkildə göstərilməlidir)
	Layihə müqaviləsinin qüvvədə olduğu müddətdə layihə üzrə görülən tədqiqat işləri və layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s. olmayb.

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Aparıcı məsləhətçi
Hüseynzadə Leyla İlqar qızı

_____
(imza)
“ __” _____ 2021-ci il

İCRAÇI:

Layihə rəhbəri
Səbziyev Elxan Nəriman oğlu

_____
(imza)
“ __” _____ 2021-ci il

AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

MÜQAVİLƏYƏ ƏLAVƏ

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun "Elm-Təhsil İnteqrasiyası" məqsədli qrant müsabiqəsinin (EİF/MQM/Elm-Təhsil-1-2016-1(26)) qalibi olmuş layihənin yerinə yetirilməsi üzrə

ALINMIŞ NƏTİCƏLƏRİN ƏMƏLİ (TƏCRÜBİ) HƏYATA KEÇİRİLMƏSİ VƏ LAYİHƏNİN NƏTİCƏLƏRİNDƏN GƏLƏCƏK TƏDQİQATLARDA İSTİFADƏ PERSPEKTİVLƏRİ HAQQINDA MƏLUMAT VƏRƏQİ

(Qaydalar üzrə Əlavə 16)

Layihənin adı: **Hərbi-müdafiə sistemində ötürülən səsli məlumatların sürüşən inikaslı şifrlənməsi sistemi**

Layihə rəhbərinin soyadı, adı və atasının adı: **Səbziyev Elxan Nəriman oğlu**

Qrantın məbləği: **28 600 manat**

Layihənin nömrəsi: **EİF/MQM/Elm-Təhsil-1-2016-1(26)-71/06/1-M-09**

Müqavilənin imzalanma tarixi: **17 avqust 2020-ci il**

Qrant layihəsinin yerinə yetirilmə müddəti: **6 ay**

Layihənin icra müddəti (başlama və bitmə tarixi): **01 sentyabr 2020-ci il – 01 mart 2021-ci il**

Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulma

Layihənin nəticələrinin əməli (təcrübi) həyata keçirilməsi

1	Layihənin əsas əməli (təcrübi) nəticələri, bu nəticələrin məlum analoqlar ilə müqayisəli xarakteristikası
	Layihə çərçivəsində işlənilmiş səs siqnalının sürüşən inikaslı şifrlənməsi alqoritmi məlumatların emalı nöqteyi nəzərdən standart açar sözünü tərbiq etməklə mətn tipli məlumatların şifrlənməsi üçün tətbiq olunan şifrləmə alqoritminin təkmilləşdirilmiş analoqu hesab oluna bilər. Bu baxımdan mövcud alqoritmlərdən əsas fərq tətbiq olunan əlifba düzülüşünün müntəzəm olaraq sürüşdürülməsindən ibarətdir. Lakin mətnlərin şifrlənməsi üçün işlənmiş alqoritmi formal olaraq səsli məlumatın şifrlənməsinə tətbiq olunması demək olar ki, heç bir müsbət nəticə vermir. Ona görədə şifrləmə usulunun tərkib hissəsi kimi ikinci açar söz generasiya olunur. Üsulun mahiyyəti ondan ibarətdir ki, kiçik uzunluqlu (3 simvoldan az olmamaq şərti ilə) ilkin açar söz xüsusi qaydada tərtib olunmuş alqoritmlə lazım olan qədər birqiymətli şəkildə uzadılır və şifrləmə zamanı ötürüləcək məlumatların hissələrinin şifrlənməsində istifadə olunur.

	Üsulun üstünlüyü ondan ibarətdir ki, generasiya edilən açar söz kifayət qədər uzadıldığından şifrləmə zamanı ötürüləcək məlumatların hissələri tamamilə dəyişdirilmiş olur. Bu qaydada şifrləndikdən sonra eyni tipli məlumatlar (chunk-lar [çank]) bir-birindən kəskin fərqlənmiş olur və üçüncü tərəfin onların deşifrlənməsi üçün açar sözün tapılmasında tezliklərin analizi üsullarının tətbiqini mənasız edir. Beləliklə, təklif olunan səs siqnallarının şifrləmə üsulu mövcud ənənəvi şifrləmə üsullarından onunla fərqlənir ki, əvvəlcə ilkin qısa açardan istifadə edilərək uzun açar generasiya edirlər, sonra isə uzun açar vasitəsi ilə ötürülən səs siqnalının hər chunck-ı şifrlənərək göndərirlər, qəbul edən tərəfdə də ilkin qısa açardan eyni qaydada uzun açar generasiya edirlər və alınmış şifrli səs chunck-ını deşifre edərək səsləndirici qurğuya ötürürlər. Mahiyyətinə görə ötürülən səs siqnalı şifrləndikdən sonra da məlumat səs siqnalı formatına malik olur, ona görə də onu rəqəmsal rabitə şəbəkələri ilə göndərilməsi əlavə texniki qurğular tələb etmir. Beləliklə, məxfiləşdirilmiş səsli məlumatların açıq rabitə kanalları ilə ötürülməsi zamanı təklif edilən şifrləmə-deşifrləmə alqoritmi tətbiq edilə bilər.
2	Layihənin nəticələrinin əməli (təcrübi) həyata keçirilməsi haqqında məlumat (istehsalatda tətbiq (tətbiqin aktını əlavə etməli); tədris və təhsildə (nəşr olunmuş elmi əsərlər və s. – təhsil sisteminə tətbiqin aktını əlavə etməli); bağlanmış xarici müqavilələr və ya beynəlxalq layihələr (kimlə bağlanıb, müqavilənin və ya layihənin nömrəsi, adı, tarixi və dəyəri); dövlət proqramlarında (dövlət orqanının adı, qərarın nömrəsi və tarixi); ixtira üçün alınmış patentlərdə (patentin nömrəsi, verilmə tarixi, ixtiranın adı); və digərlərində)
	(burada doldurmalı) Hazırlanmış proqram təminatını 2019-cu ilin oktyabrında Silahlı Qüvvələrin Hərbi Akademiyasında sınaqdan keçirilmişdir. Aparılmış sınaqların nəticəsi haqqında aktda bildirilir ki, prorqam təminatı qoşunların idarə edilməsi zamanı məlumat təhlükəsizliyinin təmini üçün dinləyicilərin biliklərinin təkmilləşdirilməsi məqsədilə tədris prosesində tətbiq edilə bilər. *Sınaq aktının surəti əlavə olunur*.

1. **Layihənin nəticələrindən gələcək tədqiqatlarda istifadə perspektivləri**

1	Nəticələrin istifadəsi perspektivləri (fundamental, tətbiqi və axtarış-innovasiya yönlü elmi-tədqiqat layihə və proqramlarında; dövlət proqramlarında; dövlət qurumlarının sahə tədqiqat proqramlarında; ixtira və patent üçün verilmiş ərizələrdə; beynəlxalq layihələrdə; və digərlərində)
	(burada doldurmalı) Layihə çərçivəsində işlənilmiş səs siqnalının sürüşən inikaslı şifrlənməsi alqoritminin Silahlı qüvvələrdə, xüsusi rabitə sistemlərində məxfiləşdirilmiş səsli məlumatların açıq rabitə kanalları ilə ötürülməsi zamanı tətbiq edilə bilər.

SİFARİŞÇİ:

Elmin İnkişafı Fondu

Aparıcı məsləhətçi
Hüseynzadə Leyla İlqar qızı

_____

(imza)
“ __” _____ 2021-ci il

İCRAÇI:

Layihə rəhbəri

Səbziyev Elxan Nəriman oğlu

_____

(imza)
“ __” mart 2021-ci il

AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

MÜQAVİLƏYƏ ƏLAVƏ

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun
"Elm-Təhsil İnteqrasiyası" məqsədli qrant müsabiqəsinin
(EİF/MQM/Elm-Təhsil-1-2016-1(26)) qalibi olmuş
layihənin yerinə yetirilməsi üzrə

ALINMIŞ ELMİ MƏHSUL HAQQINDA MƏLUMAT
(Qaydalar üzrə Əlavə 17)

Layihənin adı: **Hərbi-müdafiə sistemində ötürülən səsli məlumatların sürüşən inikaslı şifrlənməsi sistemi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Səbziyev Elxan Nəriman oğlu**
Qrantın məbləği: **28 600 manat**
Layihənin nömrəsi: **EİF/MQM/Elm-Təhsil-1-2016-1(26)-71/06/1-M-09**
Müqavilənin imzalanma tarixi: **17 avqust 2020-ci il**
Qrant layihəsinin yerinə yetirilmə müddəti: **6 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 sentyabr 2020-ci il – 01 mart 2021-ci il**

Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulmalıdır

1. Elmi əsərlər (sayı)

№	Tamlıq dərəcəsi / Elmi məhsulun növü	Dərc olunmuş	Çapa qəbul olunmuş və ya çapda olan	Çapa göndərilmiş
1.	Monoqrafiyalar			
	həmçinin, xaricdə çap olunmuş			

2.	Məqalələr həmçinin xarici nəşrlərdə	Həsənov A.H., Səbzyiev E.N., Talibov Ə.M., İmanov R.R., Nifrəliyev T.A. Hərbi təyinatlı idarəetmə sistemində səsli məlumatın sürüşən inikaslı şifrlənməsi // İnformasiya təhlükəsizliyi (elmi-metodiki jurnal), 2019, №2, S.16-19. (jurnal *EİF-na təqdim olunub*).		
		Həsənov A.H., Səbzyiev E.N. Səsli məlumatın şifrlənmə problemlərinin analizi və həlli yolları // Milli təhlükəsizlik və hərbi elmlər, 2019, C.5, №2, S.13-16. (*jurnal EİF-na təqdim olunub*).		
3.	Konfrans materiallarında məqalələr O cümlədən, beynəlxalq konfras materiallarında			
4.	Məruzələrin tezisləri həmçinin, beynəlxalq tədbirlərin toplusunda	Сабзиев Э.Н., Садыгова Р.И., Мамедова У.М., Амирасланова З.Н. Шифрование речевой информации с применением метода генерации вторичных ключевых слов. // Матерıали дев'ятої мıжнародної науково-технıчної конференцıї "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 11-12 апрель 2019, Харьков, Украина. С.94. (1 Səh). (*tezis EİF-na təqdim olunub*).		
		Aliyev Y.A. Position encryptıon accordıng to the key’s symbols for data protectıon // 10th International Conference "Modern Directions of Development of the Information and Communication Technologies and Control Systems". 9-10 April 2020, Xarkiv. Vol 2, p.4. (1 Səh). (*tezis EİF-na təqdim olunub*).		
5.	Digər (icmal, atlas, kataloq və s.)			

2. İxtira və patentlər (sayı)

№	Elmi məhsulun növü	Alınmış	Verilmiş	Ərizəsi verilmiş
1.	Patent, patent almaq üçün ərizə			
2.	İxtira			
3.	Səmərələşdirici təklif			

3. Elmi tədbirlərdə məruzələr (sayı)

№	Tədbirin adı (seminar, dəyirmi masa, konfrans, qurultay, simpozium və s.)	Tədbirin kateqoriyası (ölkədaxili, regional, beynəlxalq)	Məruzənin növü (plenar, dəvətli, şifahi, divar)	Sayı
1.	2019-cu ilin 11-12 aprelində Xarkov Maşınqayırma Texnologiyaları elmi tədqiqat institutunun təşəbbüsü ilə təşkil edilmiş beynəlxalq "Сучасні напрямки розвитку інформаційних технологій і засобів зв'язку" ("İnformasiya texnologiyalarının və rabitə vasitələrinin müasir inkişaf istiqamətləri") konfransı	beynəlxalq	şifahi	1
2.	2020-ci ilin 9-10 aprelində Xarkov Maşınqayırma Texnologiyaları elmi tədqiqat institutunun təşəbbüsü ilə təşkil edilmiş beynəlxalq "Сучасні напрямки розвитку інформаційних технологій і засобів зв'язку" ("İnformasiya texnologiyalarının və rabitə vasitələrinin müasir inkişaf istiqamətləri") konfransı	beynəlxalq	şifahi	1
3.				

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Aparıcı məsləhətçi
Hüseynzadə Leyla İlqar qızı

_____
(imza)
“ __” _____ 2021-ci il

İCRAÇI:

Layihə rəhbəri
Səbziyev Elxan Nəriman oğlu

_____
(imza)
“ __” _____ 2021-ci il