AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun və Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin İKT-nin inkişafına yönəlmiş əhəmiyyətli layihələrin dəstəklənməsi məqsədi ilə qrantların verilməsi üzrə 2013-cü il üçün 2-ci məqsədli birgə İKT müsabiqəsinin (EİF-RİTN-MQM-2/İKT-2-2013-7(13)) qalibi olmuş və yerinə yetirilmiş layihə üzrə

YEKUN ELMİ-TEXNİKİ HESABAT

Layihənin adı: **Asimmetrik kriptoqrafiya əsasında məlumatların şifrələnməsi və onun Azərbaycan Respublikasında elektron hökumət xidmətlərində tətbiqi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Mailov Arif Ələsgər oğlu**
Qrantın məbləği: **99 000 manat**
Layihənin nömrəsi: **EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/19/1-M-23**
Müqavilənin imzalanma tarixi: **30 aprel 2014-cü il**
Qrant layihəsinin yerinə yetirilmə müddəti: **12 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 may 2014-cü il – 01 may 2015-ci il**

Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulmalıdır
Diqqət! Uyğun məlumat olmadığı təqdirdə müvafiq bölmə boş buraxılır

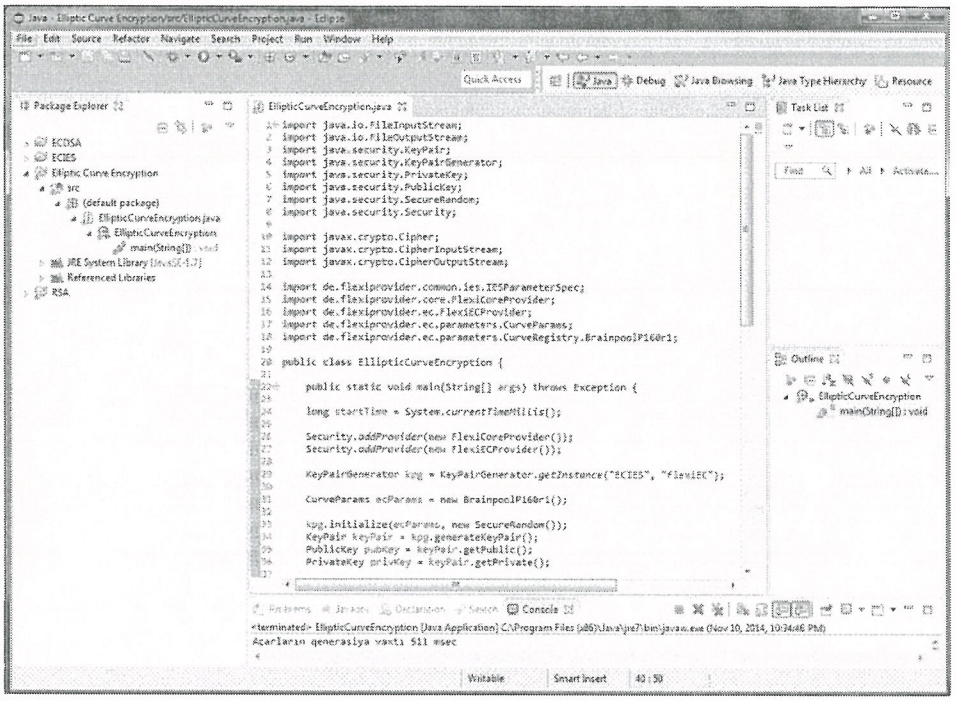
Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

1	Layihənin həyata keçirilməsi üzrə yerinə yetirilmiş işlər, istifadə olunmuş üsul və yanaşmalar
	1. Java Kriptoqrafiya Arxitekturası (JCA/JCE) üçün tətbiq edilən FlexiProvider kitabxanası quraşdırıldı və kriptoqrafik modulların köməyi ilə elliptik əyrilərə əsaslanan şifrələmə və deşifrələmə proqramı yazılmışdır. Sadə ədədlər sahəsinin Z_p üzərində təyin edilmiş elliptik əyrinin standart forması $y^2 = x^3 + ax + b \pmod p$ Weierstrass tənliyi ilə təsvir edilir. Elliptik əyrilərin domeyn parametrləri $a,b \in Zp$, p, n, sadə ədədlərdir və G - kriptioqrafiyada istifadə edilən (x_G, y_G) nöqtəsinin qeneratorudur. Burada singularlığı istisna edən əsas şərt $4a^3 + 27b^2 \neq 0 \pmod p$ olmalıdır. Kriptoqrafiyaya aid ədəbiyyatda adı çekilən tanınmış *secp256r1* NİST ayrisi üçün təklif olunan parametrlər aşağıda kimi istifadə edilmişdir: p = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF =

$2^{224}(2^{32}-1)+2^{192}+2^{96}-1$
a = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC
b = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
G = 03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296

256-bit *brainpoolP256r1* ayrisi üçün isə domeyn parametrlər
p = A9FB57DB A1EEA9BC 3E660A90 9D838D72 6E3BF623 D5262028 2013481D 1F6E5377
a = 7D5A0975 FC2C3057 EEF67530 417AFFE7 FB8055C1 26DC5C6C E94A4B44 F330B5D9
b = 26DC5C6C E94A4B44 F330B5D9 BBD77CBF 95841629 5CF7E1CE 6BCCDC18 FF8C07B6
G = A9FB57DB A1EEA9BC 3E660A90 9D838D71 8C397AA3 B561A6F7 901E0E82 974856A7

Elliptik əyrilərə əsaslanan şifrələmə və deşifrələmə GF(p) sadə ədədlər sahəsində SHA-1 alqoritm ilə aparılmışdır və zəruri proqram təminatı Java Eclipse mühitində yazılmışdır.



FlexiProvider kitabxanasının əhatə etdiyi 70-dən çox elliptik əyri yoxlanılmışdır və şifrələmənin nəticələri RSA şifrləmənin nəticəsi ilə qarşılaşdırılmışdır.
Aşağıda təqdim edilən cədvəldə açarların qenerasiya müddətlərinin açarların uzunluğundan asılı olaraq İntel(R) Core i7-2630QM CPU@ 2.00 GHz və RAM 6.00 GB prosessoru və Windows 7 64-bit əməliyyat sistemi olan kompüterdə hesablanmışdır

Elliptik əyrinin növü	Açarların uzunluğu (bit)	Açarların qenerasiya müddəti (msec)
BrainpoolP160r1	160	411
BrainpoolP192r1	192	410
BrainpoolP224r1	224	417
BrainpoolP256r1	256	419

BrainpoolP320r1	**320**	**429**
BrainpoolP384r1	**384**	**437**
BrainpoolP512r1	**512**	**473**
Secp112r1 (NİST əyrilər)	**112**	**412**
Secp160r1	**160**	**407**
Secp224r1	**224**	**406**
Secp384r1	**384**	**428**
Secp512r1	**512**	**475**
Secp160k1	**160**	**402**
Secp192k1	**192**	**405**
Secp224k1	**224**	**406**
Secp256k1	**256**	**412**
RSA şifrələmə		
RSA512	**512**	**565**
RSA1024	**1024**	**840**
RSA2048	**2048**	**3592**
RSA3072	**3072**	**12534**
RSA4096	**4096**	**29576**

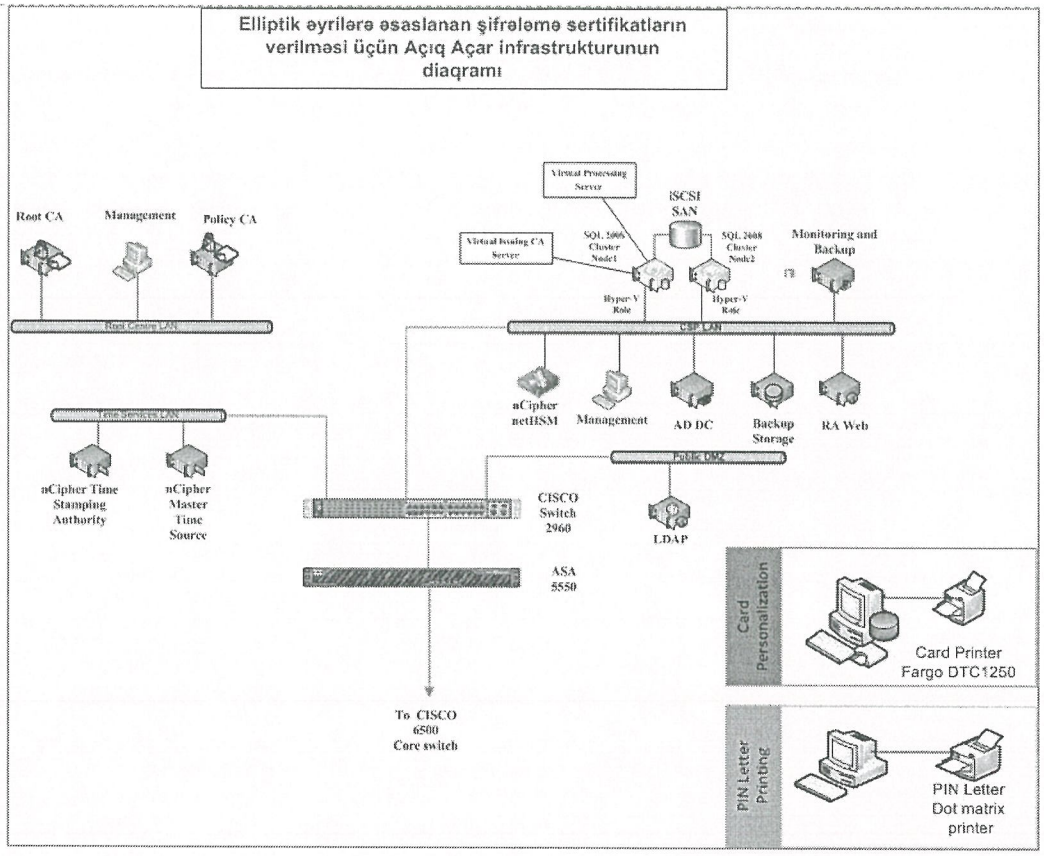
Elliptik əyrilərlə şifrləmədə qenerasiya olan 256 bit uzunluqda açarların təhlükəsizliyi RSA şifrləmədə istifadə olunan 4096-bit açarın təhlükəsizlik səviyyəsinə bərabərdir. Cədvəldən görünür ki, RSA 4096-bit açarların qenerasiya müddəti elliptik əyri ilə 256 bit açarın qenerasiya müddətindən ən azı 50 dəfə daha çoxdur. NİST və Brainpool əyrilər arasında açarların qenerasiya müddətində heç bir fərq müşahidə olunmur.

2. İstifadə edilən smart kart çipinin əməliyyat sisteminin dəstəklədiyi ECC Brainpool standart elliptik əyrilər generasiya edilmişdir və kriptodayanıqlığının təyin edilməsi üçün müvafiq proqram təminatının hazırlanmışdır;

3. Elliptik əyrilər kriptografiyasına əsaslanan şifrələmənin dəstəklənməsi və sertifikatların hazırlanması üçün Sertifikat Xidmətləri Mərkəzində Açıq Açar infrastrukturunun layihələndirilməsi aparılmışdır və HSM, Vaxt möhürü xidmətinin avadanlığı, LDAP serveri quraşdırılmışdır;

4. Sertifikat Xidmətləri Mərkəzində elliptik əyrilər kriptografiyasını dəstəkləyən Açıq Açar infrastrukturunun quraşdırılması üzrə işlər aparılmışdır. Layihə üçün yeni alınmış – Fargo DTC4500e smart kartı fərdiləşdirən printer quraşdırılıb sistemə daxil edilmişdir. İki tip smart kartların (NXP J3A081 dual interfeysli çip, əməliyyat sistemi JCOP 2.4.2 və CardOS 5.0 İnfineon) oxunması üçün aşağı səviyyəli drayverlərin yazılmışdır. Elliptik əyrilər kriptoqrafiyasının infrastrukturunun xarici müdaxilələrdən qorunması üçün layihə çərçivəsində əldə edilmiş Cisco ASA5550 fayrvol avadanlığı konfiqurasiya edilib sistemə qoşulmuşdur.

5. Məlumatların təhlükəsiz mühitdə saxlanılması üçün açıq açar infrastrukturunda verilənlər bazası failover klusteri növündə konfiqurasiya edilmişdir. Bundan əlavə olaraq sertifikatları dərc edən server (İssuing CA) quraşdırılmışdır və hal-hazırda onun sistemə inteqrasiyası üzrə işlər aparılmaqdadır.



6. Smart kart çipinə yazılacaq sertifikatın profili tərtib edilib sistemə inteqrasiya edilmişdir. Şifrələmə sertifikatın qenerasiyası 256-bit NİST və Brainpool elliptik əyrilər əsasında açarlar üçün hazırlanmışdır. Sertifikatlar 512-bit açarlar üçün isə hal-hazırda mütəxəssislərimiz tərəfindən tədqiq edilmişdir.

7. Əyrilərin xüsusiyyətlərinin öyrənilməsi istiqamətində də işlər aparılmışdır.
Kök mərkəzinin açarlarının 512-bit uzunluqda olmasını nəzərə aldıqda aşağıdakı domeyn parametləri ***brainpool 512-bit*** *əyrilər* üçün qəbul edilmişdir:

p = AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA7
03308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

A = 7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863
BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA

B
=3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7
B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723

x = 81AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D009
8EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F822

Aşağıdakı cədvəldə İntel(R) Core i7-2630QM CPU@ 2.00 GHz və RAM 6.00 GB prosessoru və

Windows 7 64-bit əməliyyat sistemi olan kompüterdə hesablanmış elliptik əyrilərin bir neçə növü üçün 100 Kb mətnin şifrələmə və deşifrələmə müddətlərinin açarların uzunluğundan asılı olaraq nəticələri təqdim edilmişdir.

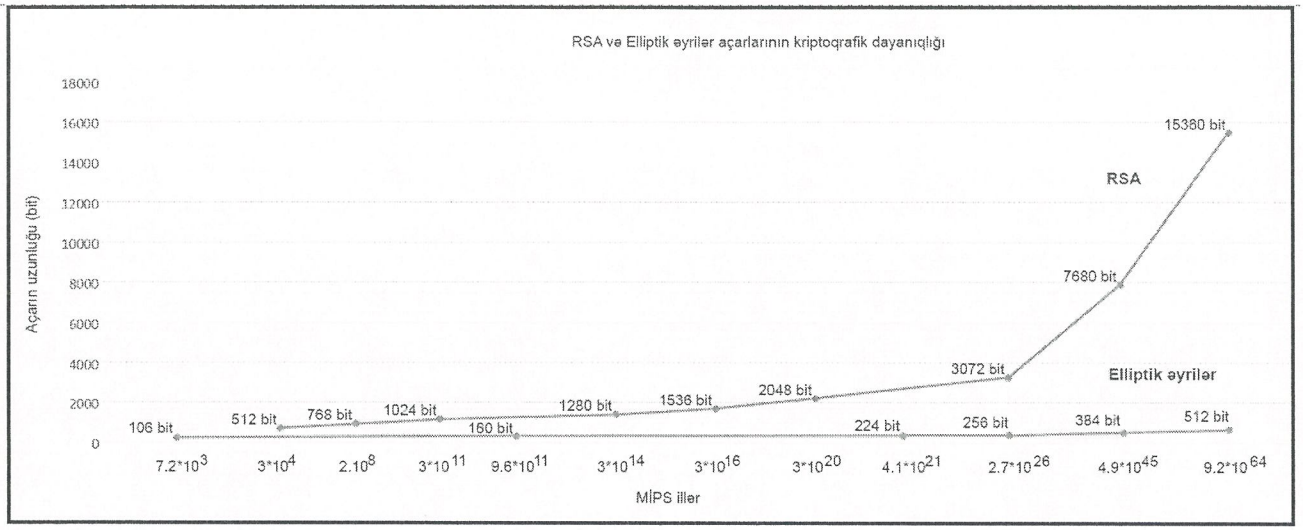
Elliptik əyrinin növü	Açarların uzunluğu (bit)	Açarların qenerasiya müddəti (msec)	Şifrələmə müddəti (100Kb-lıq mətn) (msec)	Deşifrələmə müddəti (100Kb-lıq mətn) (msec)
BrainpoolP160r1	160	5	22	32
BrainpoolP192r1	192	7	28	39
BrainpoolP224r1	224	9	38	49
BrainpoolP256r1	256	12	47	62
BrainpoolP320r1	320	19	72	94
BrainpoolP384r1	384	31	103	140
BrainpoolP512r1	512	66	201	299
Secp112r1 (NİST əyrilər)	112	3	16	26
Secp160r1	160	5	23	32
Secp224r1	224	8	32	53
Secp256r1	256	12	41	68
Secp320r1	320	17	53	83
Secp384r1	384	28	102	125
Secp512r1	512	68	227	279
Certicom əyriləri				
Secp160k1	160	4	19	32
Secp192k1	192	6	24	38
Secp224k1	224	8	30	47
Secp256k1	256	11	37	56
RSA şifrələmə				
RSA512	512	46	52	53
RSA1024	1024	307	312	293
RSA2048	2048	2777	2896	3011
RSA3072	3072	12898	23668	14157
RSA4096	4096	42619	49196	38892

Müəyyən olunmuşdur ki, elliptik əyrilərdə mətnin şifrləmə və deşifrləmə müddətləri bir neçə vahid faktora qədər fərqlənir. RSA şifrləmədə isə qeyd edilən proseslər arasında vaxt fərqi müşaidə edilməmişdir.

8. Kriptodayanıqlıq elliptik əyrilər üzərində diskret loqarifm probleminin həlli ilə əlaqəlidir. River-Şamir-Adleman alqoritmdən fərqli olaraq elliptik əyrilərdə həllin mürəkkəbliyi açarların bit sayından (n) asılıdır və nəzəriyyədə sub-eksponensial (~polinomiala yaxın) formada

$$C_{ECDLP(n)} \approx 2^{n/2}$$

təqdim edilir.



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

100%

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

Kriptosistemin yaradılması üçün əsas üç alqoritmin olması zəruridir:

- Açarların qenerasiya alqoritmi;
- Şifrləmə alqoritmi;
- Deşifrləmə alqoritmi.

Nəzəri və praktiki tədqiqatlar göstərir ki, RSA şifrləməyə əsaslanan kriptosistemlərin kiber hücumlara dayanaqlığı texniki avadanlığın sürətli inkişafı səbəbindən yetərincə yüksək səviyyədə deyil. Digər tərəfdən təhlükəsizlik səviyyəsinin yüksəldilməsi məqsədi ilə sadəcə açarların uzunluğunun artırılmasında RSA şifrləmə və elektron imza sertifikatlarının istehsal vaxtının əhəmiyyətli dərəcədə böyüməsi ilə nəticələnir. Bu səbəbdən Elliptik əyrilərə əsaslanan kriptosistemlər daha çox perspektivlər vəd edir. Şifrələmədə iştirak edən açarların daha kiçik uzunluğunu nəzərə alınarsa, elliptik əyrilər alqoritmləri riyazi ko-prosessorlar olmadan da smart kartlarda tətbiq ola bilər.

Azərbaycan Respublikasında yeni nəsil şəxsiyyət vəsiqəsinin tətbiqi ilə bağlı əlavə tədbirlər haqqında Azərbaycan Respublikası Prezidentinin 2014-cü il 28 noyabr tarixli 893 nömrəli Sərəncamın 2-ci bəndinə əsasən vətəndaşların elektron imza sertifikatlarını yeni nəsil şəxsiyyət vəsiqələrinə daxil edilməsi Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyinə tapşırılmışdır. Sertifikatlar RYTN-in Sertifikat Xidmətləri Mərkəzi tərəfindən hazırlanaraq Daxili İşlər Nazirliyinin fərdiləşdirmə mərkəzlərinə təhlükəsiz şəbəkə üzərindən ötürülməsi nəzərdə tutulmuşdur.

Lakin nəzərdə tutulmuş yeni nəsil şəxsiyyət vəsiqələrinin çipində RSA açarların qenerasiyası icraçı olan İsveçrənin Trüb şirkətinin qoyduğu tələblərə cavab vermirdi (ildə 2 mln. açarın qenerasiyası). Bu məqsədlə yeni və dayanıqlığı yüksək olan alqoritmin istifadəsi üzərində tədqiqatların aparılması razılaşdırılmışdır. Sertifikat Xidmətləri Mərkəzinin mütəxəssisləri grant çərçivəsində əldə etdikləri nəticələrini yeni nəsil şəxsiyyət vəsiqəsi layihəsində tətbiqini təklif etdilər.

Elliptik əyrilər əsasında yaradılacaq alqoritm, RSA alqoritmi ilə müqayisədə daha tez işləyəcək və açarın daha kiçik uzunluğunda müqayisə olunmayan dərəcədə hakerlərin hücumuna yüksək

	dayanıqlığı təmin edəcək.
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!)*
	"Study and İmplementation of Elliptic Curve Encryption Algorithm for Azerbaijan e-İD card" məqaləsi İnternational Journal of İnnovative Research in Computer and Communication Engineering jurnala göndərilmişdir. Scientific Journal İmpact Factor value for 2014 is **5.618**. Məqalənin sürəti kağız üzərində və CD şəklində əlavə olunur.
5	İxtira və patentlər, səmərələşdirici təkliflər
	Yoxdur
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)
	Yoxdur
7	Layihə üzrə elmi ekspedisiyalarda iştirak (əgər varsa)
	Yoxdur
8	Layihə üzrə digər tədbirlərdə iştirak
	Digər nazirliklər və komitələrlə birlikdə Azərbaycan Respublikası vətəndaşının yeni nəsil şəxsiyyət vəsiqəsi üzrə layihənin işçi grupunda iştirak edilmişdir
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)
	a) "Elliptik əyrilərə əsaslanan şifrələmə" adlı ölkədaxili məruzə Rabitə və Yüksək Texnologiyalar Nazirliyinin Məlumat Hesablama Mərkəzi b) Azərbaycan Respublikası vətəndaşlarının yeni nəsil şəxsiyyət vəsiqəsinə elektron imza sertifikatların daxil edilməsi layihəsi üzrə işçi grupu üçün ölkədaxili məruzə "Status of Azerbaijan e-İD chip".
10	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar, komplektləşdirmə məmulatları
	1. 1U Rack Server kompüteri HP Proliant DL360p G8, SixCore Xeon E6-2620v2, 8 GB,SATA/SAS (RAİD 0/1/1 + 0/5/5 + 0), 2x300 GB 10K SAS 2.5 SC HDD, DVD-RÜ, NC331FLR 4-port GigabitEth, 460W Gold PS - 1 ədəd; 2. HP 82Q 8Gb Dual Port PCİ-E FC HBA – 2 ədəd; 3. HP MSA 2040 SAN DC SFF Storage (HP MSA 12x450 GB 6 G SAS 10K 2.5in DP ENT HDD, 2xHP MSA 2040 8GB SW FC SFP 4 Pk HP 3Y 4 Hr 24x7 Proactive Care SVC, 8xHP Premier Flex LC/LC 5 cbl) - 1 ədəd; 4. Dual-sided İD Card Printer – Fargo DTC4500e (Asure İD 7 Exchange + 047709 İSO Magnetic Stripe Encoder + 053724 Dual-Sided Simultaneous Lamination Module) + 045200 ECO YMCKO: Full color ribbon with resin black and clear overlay panel – 500 images; 5. İntelliJ İDEA 13.X Commercial License (JAVA proqramlaşdırma mühiti) - 2 ədəd;

	6. JCOP v 2.4.2 NXP J3A081 Dual İnterface Smart Card - 10 ədəd + JavaCard SDK 3.0.1 (Windows); 7. PVC cards with CardOS 5.0 + CardOS V5.2 API (Windows) - 2 ədəd.
11	Yerli həmkarlarla əlaqələr
	Yoxdur
12	Xarici həmkarlarla əlaqələr
	İsveçrənin Trüb, Almaniyanın Charismatics şirkətləri
13	Layihə mövzusu üzrə kadr hazırlığı (əgər varsa)
	Yoxdur
14	Sərgilərdə iştirak (əgər baş tutubsa)
	Yoxdur
15	Təcrübəartırmada iştirak və təcrübə mübadiləsi (əgər baş tutubsa)
	Yoxdur
16	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s. (məlumatı tam şəkildə göstərilməlidir)
	http://bizimyol.info/news/50925.html http://news.milli.az/society/333793.html http://apa.tv/video/18699 Elliptik əyrilərə əsaslanan şifrləyici proqram aşağıda göstərilən saytdan təqdim edilir- http://e-imza.az/esigner.php?tp=encoder&ide=53&lang=az

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Müşavir
Babayeva Ədilə Əli qızı

_____
(imza)
"26" may 2015-ci il

İCRAÇI:

Layihə rəhbəri
Mailov Arif Ələsgər oğlu

_____
(imza)
"26" May 2015-ci il

Baş məsləhətçi

Daşdəmirova Xanım Faiq qızı

_____

(imza)

" __ " _____ 201_-ci il

AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA

ELMİN İNKİŞAFI FONDU

MÜQAVİLƏYƏ ƏLAVƏ

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun və Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin İKT-nin inkişafına yönəlmiş əhəmiyyətli layihələrin dəstəklənməsi məqsədi ilə qrantların verilməsi üzrə 2013-cü il üçün 2-ci məqsədli birgə İKT müsabiqəsinin (EİF-RİTN-MQM-2/İKT-2-2013-7(13)) qalibi olmuş və yerinə yetirilmiş layihə üzrə

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

(Qaydalar üzrə Əlavə 16)

Layihənin adı: **Asimmetrik kriptoqrafiya əsasında məlumatların şifrələnməsi və onun Azərbaycan Respublikasında elektron hökumət xidmətlərində tətbiqi**

Layihə rəhbərinin soyadı, adı və atasının adı: **Mailov Arif Ələsgər oğlu**

Qrantın məbləği: **99 000 manat**

Layihənin nömrəsi: **EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/19/1-M-23**

Müqavilənin imzalanma tarixi: **30 aprel 2014-cü il**

Qrant layihəsinin yerinə yetirilmə müddəti: **12 ay**

Layihənin icra müddəti (başlama və bitmə tarixi): **01 may 2014-cü il – 01 may 2015-ci il**

1. Layihənin nəticələrinin əməli (təcrübi) həyata keçirilməsi

1	Layihənin əsas əməli (təcrübi) nəticələri, bu nəticələrin məlum analoqlar ilə müqayisəli xarakteristikası
	Hal-hazırda elektron sənədlər Rabitə və Yüksək Texnologiyalar Nazirliyinin Milli Sertifikat Xidmətləri Mərkəzi tərəfindən sertifikatlaşdırılmış elektron imza ilə mühafizə olunurlar. Bu imzanın yaradılmasında böyük ədədlərin faktorizasiyasına (RSA alqoritmi) əsaslanmış açıq açar kriptoqrafik alqoritm istifadə olunur. Layihənin tədqiqatları nəticəsində elliptik əyrilərə əsaslanan alqoritmin xüsusiyyətləri araşdırılıb RSA alqoritmi ilə müqayisə edilmişdir. Hesablamalar göstərdi ki, elliptik əyrilər alqoritmi RSA alqoritmi ilə müqayisədə dəfələrcə tez işləyir və açarın daha kiçik uzunluqlarında qırılmaya daha yüksək dayanıqlığı təmin edir. Layihənin əsas nəticəsi kimi, elliptik əyrilər əsasında kriptoqrafik şifrləmə alqoritminin Azərbaycan Respublikası vətəndaşlarının yeni nəsil şəxsiyyət vəsiqəsində açarların və sertifikatların yaradılmasında istifadə olunacağı göstərilə bilər. Göstərilən alqoritm əsasında sənədlərin şifrələnməsi üçün proqram təminatı hazırlanaraq vətəndaşların, dövlət qurumlarının

	və biznes strukturların istifadəsi üçün təqdim edilmişdir (proqramı bu linkdən əldə etmək olar http://www.e-imza.az).
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)
	Yeni nəsil şəxsiyyət vəsiqəsinin tətbiqi ilə bağlı əlavə tədbirlər haqqında Azərbaycan Respublikası Prezidentinin 2014-cü il 28 noyabr tarixli 893 nömrəli Sərəncamına əsasən yeni nəsil şəxsiyyət vəsiqəsinə elektron imza sertifikatlarının daxil edilməsi dövlət layihəsində RYTN yeni Sertifikat mərkəzinin quraşdırılması tapşırılmışdır.

2. **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)
	Layihənin nəticələri gələcəkdə dövlət qurumlarının sahə tədqiqat proqramlarında istifa edilə bilər.

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Müşavir
Babayeva Ədilə Əli qızı

_____
(imza)
"26" may 2015-ci il

İCRAÇI:

Layihə rəhbəri
Mailov Arif Ələsgər oğlu

_____
(imza)
"26" May 2015-ci il

Baş məsləhətçi
Daşdəmirova Xanım Faiq qızı

_____
(imza)
"__" _____ 201_-ci il

AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

MÜQAVİLƏYƏ ƏLAVƏ

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun və Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin İKT-nin inkişafına yönəlmiş əhəmiyyətli layihələrin dəstəklənməsi məqsədi ilə qrantların verilməsi üzrə 2013-cü il üçün 2-ci məqsədli birgə İKT müsabiqəsinin (EİF-RİTN-MQM-2/İKT-2-2013-7(13)) qalibi olmuş və yerinə yetirilmiş layihə üzrə

ALINMIŞ ELMİ MƏHSUL HAQQINDA MƏLUMAT
(Qaydalar üzrə Əlavə 17)

Layihənin adı: **Asimmetrik kriptoqrafiya əsasında məlumatların şifrələnməsi və onun Azərbaycan Respublikasında elektron hökumət xidmətlərində tətbiqi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Mailov Arif Ələsgər oğlu**
Qrantın məbləği: **99 000 manat**
Layihənin nömrəsi: **EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/19/1-M-23**
Müqavilənin imzalanma tarixi: **30 aprel 2014-cü il**
Qrant layihəsinin yerinə yetirilmə müddəti: **12 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 may 2014-cü il – 01 may 2015-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			"Study and İmplementation of Elliptic Curve Encryption Algorithm for Azerbaijan e-ID card" məqaləsi International Journal of Innovative Research in Computer and Communication Engineering jurnala göndərilmişdir. Scientific Journal İmpact Factor value for 2014 is 5.618.
3.	Konfrans materiallarında məqalələr			
	O cümlədən, beynəlxalq konfras materiallarında			
4.	Məruzələrin tezisləri			
	həmçinin, beynəlxalq tədbirlərin toplusunda			
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.	Azərbaycan Respublikası vətəndaşının yeni nəsil şəxsiyyət vəsiqəsi layihəsi üzrə işçi qrup "Status of e-İD chip"	Ölkədaxili	Plenar	1
2.	RYTN Məlumat Hesablama	Ölkədaxili	Plenar	1

	Mərkəzində "Elliptik əyrilər kriptoqrafiyası"			

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Müşavir
Babayeva Ədilə Əli qızı

_____
(imza)
"26" May 2015-ci il

Baş məsləhətçi
Daşdəmirova Xanım Faiq qızı

_____
(imza)
" __" _____ 201_-ci il

İCRAÇI:

Layihə rəhbəri
Mailov Arif Ələsgər oğlu

_____
(imza)
"26" May 2015-ci il