ELLIPTIK EGRI CHIZIQLARGA ASOSLANGAN SAMARALI DIFFI-XELLMAN IKKI TOMONLAMA KALIT TAQSIMLASH PROTOKOLLARI TAHLILI

Arziyeva Jamila Tileubayevna
Berdaq nomidagi Qoraqalpoq davlat universiteti,
Amaliy matematika kafedrasi professori v.b.
Jabbarov Nuriddin Akbarovich
Muhammad al-Xorazmiy nomidagi TATU, assistenti
Umarov Shohzod Zafar o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU, magistranti

ANNOTATSIYA

Kalit taqsimlash protokollari ikki (yoki undan ko‘p) tomon o‘rtasida xavfsiz bo‘lmagan tarmoq orqali aloqa maxfiyligini ta’minlash uchun asosiy ahamiyatga ega. Ushbu maqolada biz elliptik egri chiziq guruhlari ustida Diffi-Xellman va diskret logarifmlash muammolarining murakkabligiga asoslangan mavjud ikki tomonlama protokollarni ko‘rib chiqamiz. Shuningdek, yangi ikki tomonlama o‘zaro autentifikatsiyalangan kalit taqsimlash protokolini taklif qilamiz va barcha ko‘rib chiqilgan sxemalarning xavfsizligi va samaradorligini birgalikda baholaymiz. Elliptik egri chiziq texnikalari resurslari cheklangan qurilmalarda hisoblash ishlarini minimallashtirish va kamroq bit bilan xavfsizlik darajalarini ta’minlash uchun qo‘llaniladi.

Kalit so‘zlar: Elliptik egri chiziqlar, kriptografiya, kalit taqsimlash, protokollar.

ABSTRACT

Key distribution protocols are essential for ensuring the confidentiality of communications between two (or more) parties over an insecure network. In this paper, we review existing two-way protocols based on the complexity of the Diffie-Hellman and discrete logarithm problems over elliptic curve groups. We also propose a new two-way mutually authenticated key distribution protocol and jointly evaluate the security and efficiency of all considered schemes. Elliptic curve techniques are used to minimize computational effort on resource-constrained devices and to provide security levels with fewer bits.

Keywords: Elliptic curves, cryptography, key distribution, protocols.

KIRISH

Xavfsiz bo‘lmagan tarmoq (masalan, Internet) orqali ikki tomon o‘rtasida xabar almashish jarayonida ularning maxfiyligi va/yoki yaxlitligini ta’minlash uchun asosiy xavfsizlik talabi - umumiy maxfiy kalitni o‘rnatishdir. To‘g‘ri bajarilgan kalit taqsimlash protokollari quyidagi minimal xavfsizlik talablariga javob berishi kerak: bir xil sessiya kalitlari bilan yakunlanishi, bir tomonning (o‘zaro) ikkinchi tomonga autentifikatsiyadan o‘tishi, yaxshi sifatli (tasodifiy) kriptografik kalitlarning yaratilishi, uchinchi tomonlardan sessiya kalitining maxfiyligini himoya qilish.

Sessiya kalitining haqiqiyligi faqatgina noyob muloqot sessiyasi davomida amal qilishi talab etiladi, chunki bu kalit buzilgan taqdirda xavfni cheklashi, turli sessiyalar o‘rtasidagi mustaqillikni ta’minlashi, boshqaruvni soddalashtirishi va ko‘p maqsadlarda bir vaqtning o‘zida ko‘plab kalitlardan foydalanish natijasida yuzaga kelishi mumkin bo‘lgan zaifliklarni oldini olishi mumkin.

Umuman olganda, bunday protokollar foydalanuvchilardan dastlabki sozlash bosqichida xavfsiz tarzda tarqatilgan yoki o‘rnatilgan (simmetrik yoki assimetrik) autentifikatsiyalangan kriptografik kalitlarga ega bo‘lishni talab qiladi. Ushbu kalitlarning to‘g‘ri boshqarilishi muhim masala bo‘lib, u inson tomonidan boshqariladigan jarayonlarga, ishonchli uchinchi tomonlarning mavjudligiga yoki ba’zi hollarda qimmat tamper-dalillarga ega qurilmalardan foydalanishga bog‘liq bo‘lishi mumkin.

Ommaviy tarmoqda (masalan, Internetda) xolis tomonlar tomonidan bajariladigan istalgan protokol davomida almashiladigan xabarlar tajovuzkor tomonidan eshitib qolinish xavfiga ega ekanligi taxmin qilinadi. Amalda bunday hujumni amalga oshirish nisbatan oson bo‘lishi mumkin. Bunday holatda, odatda, passiv hujum sodir bo‘ladi, bunda tajovuzkorlar haqiqiy protokol yozuvlaridan olingan ma’lumotlarni oflayn tahlil qilish imkoniyatiga ega bo‘ladi.

Kalit taqsimlash protokollarari uchun xavfsizlik talablari

Umumiy ikki tomonlama protokollarda ishtirokchilar (asosiy tomonlar) A va B har biri o‘ziga xos identifikatorlarga (id_A, id_B) ega bo‘lib, ular NAMESPACE $\subseteq \Sigma^{\ell}$ to‘plamidan tanlanadi (masalan, $\ell \geq 64$). Soddalashtirish uchun NAMESPACE to‘plami Sertifikatlash Organining (CA) boshqaruvidagi domenni anglatadi, bu CA sertifikatlarni chiqarish bilan shug‘ullanadi (sertifikatlar identifikatsiya ma’lumotlarini o‘z ichiga oladi).

[2] da kalit kelishuv protokollari uchun ikki asosiy kalit autentifikatsiya modeli ta’riflangan: Autentifikatsiya qilingan kalit (AK - Authenticated Key) kelishuvi va Kalitni tasdiqlash bilan AK (AKC - AK with Key Confirmation).

AK protokoli asosan foydalanuvchi yo‘naltirilgan maqsadni ta’riflaydi va zaif kalit autentifikatsiyasi yoki Implikatsion Kalit Autentifikatsiyasini (IKA) taqdim etadi, shu bilan birga kalit tasdiqlash bosqichining qo‘shilishi (hech qanday kalitga oid ma’lumot oshkor qilinmasligi kerak) kuchli kalit autentifikatsiyasiga olib keladi, bu esa Aniq Kalit Autentifikatsiyasi (EKA) deb ataladi:

Authenticated Key (AK). AK protokoli halol bajarilganda, A tomoni B tomonidan tashqari hech kim sessiya kaliti sk qiymatini bilishi mumkin emasligiga ishonch hosil qiladi. A tomoni B ning sessiya kaliti sk ni hisoblab chiqqanligini aniq isbotlay olmaydi, lekin protokolga ishtirok etgan boshqa tomonni samarali autentifikatsiya qilish uchun mexanizm mavjud bo‘lishi kerak.

AK with Key Confirmation (AKC). AK protokoliga kalit tasdiqlashni qo‘shish orqali kuchliroq maqsadga erishiladi, ya’ni AKC protokoli halol bajarilganda, A tomoni B (yoki aksincha) sessiya kalitini haqiqatan ham hisoblab chiqqanligini (yoki uni hisoblash usulini bilishini) tasdiqlaydi. Bu holatda, tomon sessiya kalitining autentifikatsiyalangan protokol ishtirokchisi bilan bog‘lanishini tasdiqlovchi kafolat oladi.

Asosiy tomon A B bilan har qanday sonli protokol suhbatlarini boshlashi mumkin, va A tomonidan boshlangan i-chi protokol misoli (instansiyasi) $\Pi^{i}_{A,B}$ simvoli bilan ifodalanadi. Dushmanlar aloqa kanali ustidan to‘liq nazoratga ega, shuning uchun ular har bir protokol instansiyasi bilan o‘zaro aloqada bo‘lishi, xabar oqimlarini qo‘shish, o‘zgartirish, o‘chirish va qayta o‘ynash (va boshqalar) imkoniyatiga ega.

$SK \subseteq \Sigma^{\ell}$ to‘plami, bu yerda $\ell \geq 128$, sessiya kalitlari sk ning aniqlanish domenini ifodalaydi, yaxshi kalit kelishuv protokoli (ideal holda, passiv dushman mavjud bo‘lsa) SK bo‘yicha tasvirlangan 0-birlik tasodifiy o‘zgaruvchisini chiqarishi kerak. [5] ishiga asoslanib, umumiy kalit almashinuvi protokoli uchun kerakli bo‘lgan asosiy xavfsizlik xususiyatlari quyidagicha ta’riflanadi:

1. Ma’lum kalit xavfsizligi (KK-S - Known-Key Security). Ikki halol tomon A va B kalit kelishuv protokolining har qanday bajarilishida ishtirok etayotgan bo‘lsa, tegishli instansiyalar $\Pi^{i}_{A,B}$ va $\Pi^{j}_{B,A}$ faqat bitta va mos keladigan sessiya kaliti sk bilan yakunlanishi kerak. Bundan tashqari, yuqoridagi shart, sessiyalar dushmanga oshkor bo‘lsa ham (protokol xatolari tufayli yuz berishi mumkin), saqlanishi kerak.

2. Oldinga maxfiylik (FS - Forward Secrecy). Agar A va/yoki B ning uzoq muddatli maxfiy kaliti dushmanga oshkor bo‘lsa, avvalgi o‘rnatilgan sessiya kalitlari sk ning maxfiyligi halol protokol bajarilishlarida ta’sirlanmasligi kerak.

3. Kalit-kompromisga taqlid qilish chidamliligi (KCI-R - Key-Compromise Impersonation Resilience). Agar $\Pi^{i}_{A,B}$ instansiyasi A ning uzoq muddatli maxfiy kaliti bilan buzilsa, dushman A ni har qanday boshqa tomonga taqlid qilishi mumkin. Dushman A ni boshqa bir tomon sifatida taqlid qila olmasligi kerak.

4. Noma’lum kalit almashish chidamliligi (UKS-R - Unknown Key-Share Resilience). A ning ma’lumotidan holi bo‘lgan holda B bilan kalitni almashishga majbur qilinmasligi kerak, ya’ni A o‘zini B bilan kalitni almashgan deb bilsa, va B (to‘g‘ri) o‘zini A bilan kalitni almashgan deb bilsa. Dushman maqsadi sessiya kalitini olishdan iborat bo‘lmasligi kerak. Ochiq kalitga asoslangan protokollarda, dushman E faqatgina $W_E = W_A$ ni tanlab, amalga oshirilgan sertifikatni olishni maqsad qilgan bo‘lsa, sertifikatlash organi E ning maxfiy kalitini bilishini tekshirishi kerak.

5. Kalitni boshqarish (KC - Key Control). Hech bir tomon, na A, na B, o‘rnatilayotgan sessiya kaliti sk ning hech qanday qismini oldindan belgilay olmasligi kerak.

6. Shaxsni tasdiqlash (IA - Identity Assurance). Har bir tomon protokol bajarilishida ishtirok etayotgan boshqa tomonni autentifikatsiya qilishi kerak. Bu uzoq muddatli statik kalit va tomonning identifikatorini bog‘lash orqali amalga oshirilishi mumkin.

AK protokollari

MTI/A0 Protokoli. MTI/A0 kalit taqsimlash protokoli, 1-rasmda tasvirlangan, Matsumoto va boshqalar [6] tomonidan taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S va KCI-R hisoblanadi.

Kalit quyidagi ifodadan olinadi: $h(r_A w_B + r_B w_A)P$. Protokolda FS atributi mavjud emas, chunki sessiya kaliti ekvivalent ifodadan olinishi mumkin: $h(w_B Q_A + w_A Q_B)$, va bu holda faqat w_A, w_B oshkor qilinishi kifoya, chunki Q_A, Q_B umumiy ma’lumotdir. Shuningdek, UKS-R atributi ham bu protokolda mavjud emas [16].

UM Protokoli. Unified Model (UM) kalit taqsimlash protokoli, 2-rasmda tasvirlangan, Ankney va boshqalar tomonidan [4] taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S, FS, va UKS-R hisoblanadi. Kalit quyidagi ifodadan olinadi: $(w_A w_B)P||k(r_A r_B)P$. Protokol KCI-R atributini ta’minlamaydi, chunki w_A yoki w_B uzoq muddatli statik kalitlaridan biri haqidagi bilim ZS_A/ZS_B ni hisoblash uchun yetarli bo‘ladi.

MQV Protokoli. MQV kalit taqsimlash protokoli, 3-rasmda tasvirlangan, Law va boshqalar tomonidan [5] taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S, FS, va KCI-R hisoblanadi.

Ushbu protokolda $f = \lfloor \log_2 n \rfloor + 1$, agar Q cheklangan elliptik egri chiziq nuqtasi bo‘lsa va $\bar{x}$ esa Q.x ning ikkilamchi ko‘rsatilishidan olingan butun sonni bildirsa, unda $\bar{Q}$ quyidagicha aniqlanadi: $(\bar{x} \bmod 2^{\lceil f/2 \rceil}) + 2^{\lceil f/2 \rceil}$. Kalit quyidagi ifodadan olinadi: $h(r_A r_B + r_A w_B \bar{Q}_B + r_B w_A \bar{Q}_A + w_A w_B \bar{Q}_A \bar{Q}_B)P$, bu esa (A tomonidan) $hs_A(Q_B + \bar{Q}_B W_B)$ orqali olinadi.

Ushbu protokolning maxsus xususiyati shundaki, $Q_B + \bar{Q}_B W_B$ omili samarali skalyar ko‘paytirishlarni ta’minlaydi, ammo, bu omil jamoatga ma’lum bo‘lgan ma’lumotlardan (Q_B, W_B) hisoblanadi va bu holat muvaffaqiyatli noma’lum kalit ulashish hujumlarini amalga oshirish uchun ekspluatatsiya qilindi [7].

LLK Protokoli. LLK kalit taqsimlash protokoli, 4-rasmda tasvirlangan, Lee va boshqalar tomonidan [8] taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S, FS, KCI-R, va UKS-R hisoblanadi.

Kalit quyidagi ifodadan olinadi: $h(r_A w_B + r_B w_A)P$.

SK Protokoli. SK kalit kelishuv protokoli, 5-rasmda tasvirlangan, Song va boshqalar tomonidan [9] taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S, FS, KCI-R, va UKS-R hisoblanadi.

Kalit quyidagi ifodadan olinadi: $h(r_A w_B + r_B w_A + r_A r_B)P$.

SSEB Protokoli. SSEB kalit taqsimlash protokoli, 6-rasmda tasvirlangan, Al-Sultan va boshqalar tomonidan [10] taklif qilingan. Ushbu protokolning taxmin qilingan xavfsizlik atributlari KK-S, FS, KCI-R, va UKS-R hisoblanadi.

Kalit quyidagi ifodadan olinadi: $h(r_A r_B + w_A w_B)P$.

Agar sk (masalan, A uchun) hisoblash quyidagicha o‘zgartirilsa: $h(r_A Q_B + w_A W_B)$ va $Q_B = r_A P$ bo‘lsa, maydon elementlarining teskari qiymatini hisoblashdan qochish mumkin.

Ushbu protokol (va boshqa protokollar) bilan ehtiyot bo‘lish kerak, chunki qisqa muddatli maxfiy kalitlarning degenerate qiymatlari bilan hujumlar xavfi mavjud. Buni ko‘rsatish uchun, w_B ni bilgan bir dushman Q_A ga javoban $Q_E = P$ (E $r_E = 1$ o‘rnatadi) deb javob beradi va shunday qilib, KCI-R atributini osonlik bilan yengib o‘tadi. U to‘g‘ri sessiya kalitini $T_A = r_A Q_E + w_A W_B = Q_A + w_E W_A$ ($=T_E$) hisoblab topadi, chunki Q_A va W_A ommaviy ravishda mavjud.

Bunday hujumlarga qarshi choralar sifatida, A $Q_E \neq P$ ekanligini tekshirishi kerak (yoki $nQ_E = P_\infty$).

ECKE-1 Protokoli. Elliptik egri chiziq AK taqsimlash protokoli ECKE-1 ning yuqori darajadagi tavsifi 7-rasmda ko‘rsatilgan. Protokol ikkita o‘tish (1-raund) asosida ishlaydi. Bu yerda domen parametrlarini EC _D tekshirish usullari quyidagi tarzda amalga oshirilishi mumkin:

- Aniq tasdiqlash jarayoni orqali;
- Sertifikatlar yordamida, dastlabki bir martalik o‘rnatish fazasida;
- Yoki ishonchli kalit tarqatish markazi tomonidan chiqarilgan kriptografik qurilmalar (masalan, aqlli karta) orqali.

A		B
$r_A \xleftarrow{R} [1, n-1]$		$r_B \xleftarrow{R} [1, n-1]$
$Q_A \leftarrow r_A P$	Q_A →	$Q_B \leftarrow r_B P$
	Q_B ←	
$T_A \leftarrow h(r_A W_B + w_A Q_B)$		$T_B \leftarrow h(r_B W_A + w_B Q_A)$
$sk \leftarrow G(T_A.x)$		$sk \leftarrow G(T_B.x)$

1-rasm. MTI/A0 protokoli

A		B
$r_A \xleftarrow{R} [1, n-1]$		$r_B \xleftarrow{R} [1, n-1]$
$Q_A \leftarrow r_A P$		$Q_B \leftarrow r_B P$
	Q_A →	
$ZS_A \leftarrow w_A W_B$	Q_B	$ZS_B \leftarrow w_B W_A$
$ZE_A \leftarrow r_A Q_B$	←	$ZE_B \leftarrow r_B Q_A$
$sk \leftarrow G(ZS_A \| ZE_A)$		$sk \leftarrow G(ZS_B \| ZE_B)$

2-rasm. UM protokoli

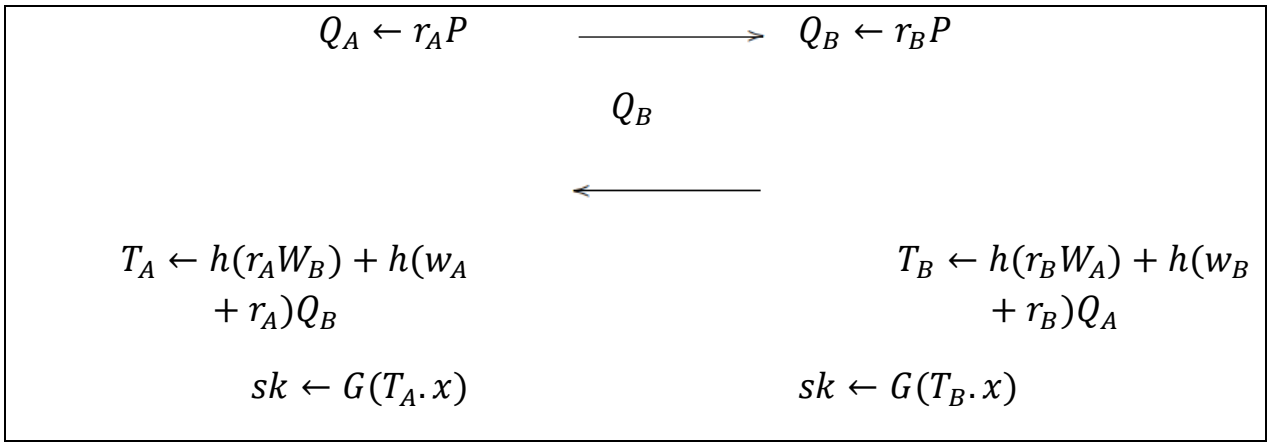
A		B
$r_A \overset{R}{\leftarrow} [1, n-1]$		$r_B \overset{R}{\leftarrow} [1, n-1]$
$Q_A \leftarrow r_A P$	Q_A →	$Q_B \leftarrow r_B P$
$s_A \leftarrow r_A + \overline{Q_A} w_A$	Q_B ←	$s_B \leftarrow r_B + \overline{Q_B} w_B$
$T_A \leftarrow hs_A(Q_B + \overline{Q_B} W_B)$		$T_B \leftarrow hs_B(Q_A + \overline{Q_A} W_A)$
$sk \leftarrow G(T_A.x)$		$sk \leftarrow G(T_B.x)$

3-rasm. MQV protokoli

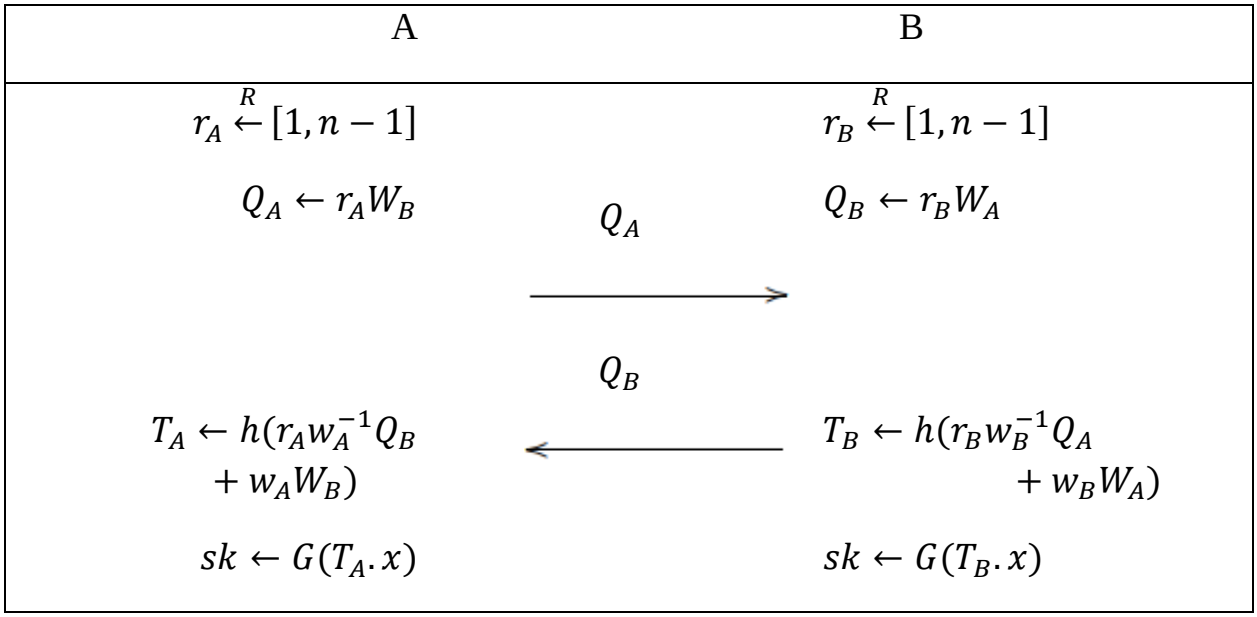
A		B
$r_A \overset{R}{\leftarrow} [1, n-1]$	Q_A →	$r_B \overset{R}{\leftarrow} [1, n-1]$
$Q_A \leftarrow hr_A W_B$		
		$R_B \leftarrow hr_B W_A$
		$T_B \leftarrow Q_A + R_B$
		$Q_B \leftarrow R_B + r_B w_B^{-1} Q_A$
$T_A \leftarrow Q_A + (w_A(w_A + r_A)^{-1})Q_B$	Q_B ←	$sk \leftarrow G(T_B.x)$
$sk \leftarrow G(T_A.x)$		

4-rasm. LLK protokoli

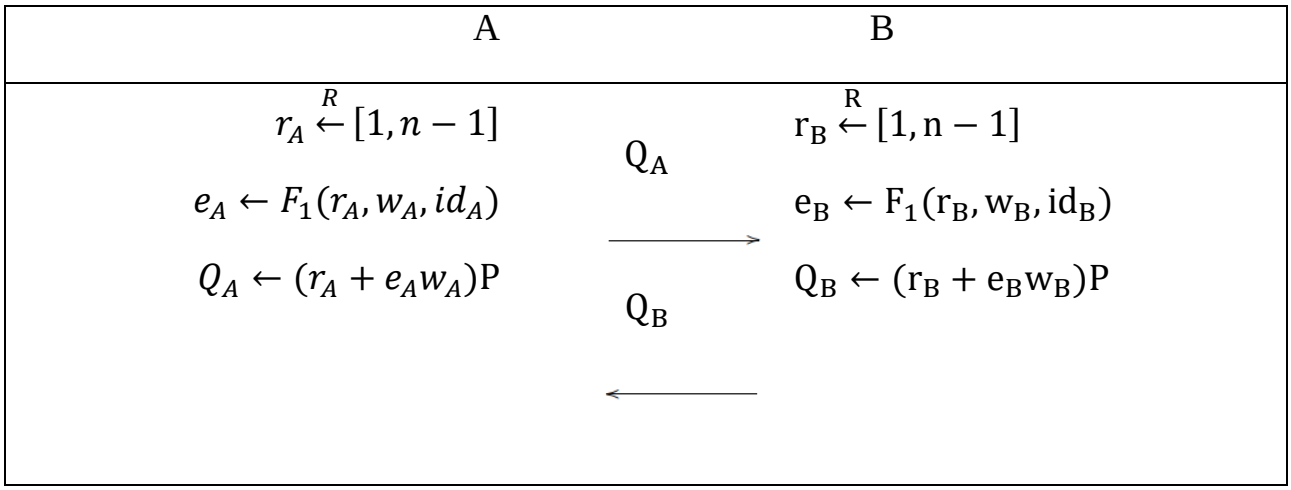
A		B
$r_A \overset{R}{\leftarrow} [1, n-1]$	Q_A	$r_B \overset{R}{\leftarrow} [1, n-1]$



5-rasm. SK protokoli



6-rasm. SSEB protokoli



d_A	d_B
$\leftarrow w_A F_2(Q_A.x, Q_B.x, id_A, id_B)$	$\leftarrow w_B F_2(Q_A.x, Q_B.x, id_A, id_B)$
$T_A \leftarrow h((r_A + e_A w_A)Q_B + d_A W_B)$	$T_B \leftarrow h((r_B + e_B w_B)Q_A + d_B W_A)$
$sk \leftarrow G(T_A.x)$	$sk \leftarrow G(T_B.x)$

7-rasm. ECKE-1 protokoli

ECKE-1 protokoli quyidagi asosiy harakatlarni amalga oshiradi:

1. A tasodifiy r_A ni [1, n - 1] oralig‘idan tanlaydi va e_A ni 3-to‘plamdan (r_A,w_A,id_A) hisoblaydi. B tasodifiy r_B [1, n - 1] oralig‘idan tanlaydi va e_B ni 3-to‘plamdan (r_B,w_B,id_B) hisoblaydi.
2. A ning yoki B ning $Q_A \equiv P_\infty$ (yoki $Q_B \equiv P_\infty$) bo‘lsa, A (yoki B) 1-qadamni takrorlaydi. Aks holda, A boshlovchi sifatida Q_A ni B ga yuboradi.
3. B Q_A ning jamoat kalitini tasdiqlash protsedurasini ishga tushiradi va agar tasdiqlash muvaffaqiyatsiz bo‘lsa, protokolni to‘xtatadi.
4. B javob beruvchi sifatida Q_B ni A ga yuboradi.
5. A Q_B ning jamoat kalitini tasdiqlash protsedurasini ishga tushiradi va agar tasdiqlash muvaffaqiyatsiz bo‘lsa, protokolni to‘xtatadi.
6. A va B mos ravishda T_A va T_B nuqtalarini hisoblaydi.
7. Har ikkala A va B protokolni yakunlab, umumiy sessiya kaliti $sk \in SK$ ni olishadi.

Bu jarayon A va B o‘rtasida umumiy kalitni xavfsiz tarzda o‘rnatishga imkon beradi, agar har ikki tomon protokolni to‘g‘ri bajarishsa va jamoat kalitini tasdiqlashda hech qanday zaiflik yuzaga kelmasa.

Agar 3-to‘plam (r_A,e_A,Q_A) va (r_B,e_B,Q_B) oldindan hisoblanadigan bo‘lsa, har bir subyekt uchun onlayn ishni faqat ikkita skalyar ko‘paytirish va bitta xesh funksiyasini hisoblashdan iborat qilish mumkin.

Kalit hosil qilish funksiyasi G(·) sessiya kaliti sk ni $T_A.x$ (yoki $T_B.x$) dan hosil qilish uchun ishlatiladi, shuningdek, bu funksiyaning zaif bitlarni bashorat qilishdan himoya qiluvchi roli ham mavjud. Standart kalit hosil qilish funksiyalari [4] da belgilangan.

Protokolning to‘g‘ri bajarilishi quyidagi faktga asoslanadi: har qanday to‘g‘ri bajarilgan holatda $T_A \equiv T_B$, shuning uchun A va B ikkisi ham bir xil maxfiy kalit sk

ni hisoblashadi, bu esa $h(r_Ar_B+r_Be_Aw_B+r_Ae_Bw_A+e_Ae_Bw_Aw_B+d_Ad_Bw_Aw_B)P$ formulasi orqali amalga oshiriladi.

ECKE-1 protokolining xavfsizlik tahlili

Endi ECKE-1 protokoli yuqoridagi xavfsizlik atributlariga nisbatan tahlil qilinadi:

KK-S. Har bir sessiya kaliti sk tasodifiy vaqtincha kalitlar r_A, r_B va statik xususiy kalitlar w_A, w_B (e_A, e_B, d_Ad_B qurilishi orqali) yordamida yagona tarzda hosil bo‘ladi. Shuning uchun, faqat sessiya kalitlariga ega bo‘lgan, ammo r_A, r_B, w_A, w_B haqida hech qanday ma’lumotga ega bo‘lmagan dushman, protokolning har qanday bajarilishiga qarshi muvaffaqiyatli hujum qilish ehtimoli juda pastdir, chunki bu ma’lumotlarni olish uchun (kamida) Elliptik egri chiziqlarda diskret logarifmlash masalasining hal qilinishi (ECDLP) kerak bo‘ladi.

FS. Agar dushman A ning uzoq muddatli xususiy kaliti w_A (va/yoki w_B) haqida bilsa, sessiya kalitini hosil qilish uchun r_A va r_B talab qilinadi. Bundan tashqari, d_A, d_B, e_A, e_B tasodifiy qiymatlar bo‘lib (tasodifiy orakl farazida), sessiya kaliti shuningdek Diffie-Hellman maxfiy r_Ar_BP ga bog‘liq. Elliptik egri chiziqlarda Diffie-Hellman masalalarining yechishning qiyinligi farazida, bu qiymatlarni tiklash kompyuter resurslari bilan imkonsizdir.

KCI-R. Agar dushman A ning statik xususiy kaliti w_A ga ega bo‘lsa, protokolga impersonatsiya (A o‘rnida yolg‘on ishtirokchi bo‘lish) orqali hujum qilish imkoniyati mavjud. Dushman (E sifatida impersonatsiya qilgan holda) A bilan o‘rtoqlashgan haqiqiy sessiya kalitini hisoblash uchun quyidagi r_A da no-chiziqli tenglamani hal qilishi kerak: $(r_A+e_Aw_A)Q_E+d_AW_E=T_E$, bunda $T_E=(r_E+e_Ew_E)Q_A+d_EW_A$ va $Q_E=(r_E+e_Ew_E)P$. Bu yerda dushman (w_E,W_E) haqiqiy kalit juftligini biladi deb faraz qilinadi (bu ma’lumotga ega bo‘lmagan dushman uchun muammo qiyinroq).

UKS-R. E qiyofasida niqoblangan raqib A ni E dan olingan xabarlar B dan kelgan deb aldashi mumkin emas. Haqiqatan ham, raqib $cert_E = cert_B$ dan id_E bilan har qanday protokolda foydalana olmaydi, chunki A $id_E \in cert_E$ yoki yo‘qligini osongina tekshira oladi (Sertifikat berishdan oldin CA shaxsiy kalitlarga egaligini tekshiradi). Bundan tashqari, agar raqib haqiqiy sertifikat sertifikatiga ega bo‘lsa ham, ba’zilar uchun (w_E, W_E), hujum muvaffaqiyatsiz bo‘ladi, chunki seans kalitlari haqiqiy sertifikatlardan olingan identifikatorlarni (id_A) almashilgan (Q_A) xabarlarga bog‘laydigan qiymatlardan (d_A) hosil bo‘ladi. Protokolga kalit tasdiqlashni qo‘shish orqali hujumning oldini olish mumkin.

KC. Diffie-Hellman asosidagi kalit kelishuv protokollarida, javob beruvchi (masalan B) ishtirokchisi uchun vaqtincha xususiy kalitni (r_B) tanlashda oldindan bashorat qilinishi mumkin bo‘lgan imkoniyat mavjud. Ammo, ishtirokchilar tomonidan almashilgan vaqtincha jamoa kalitlari (Q_A, Q_B) r_A, r_B, e_A, e_B, w_A, w_B ning no-chiziqli ifodalariga qurilgan, bu yerda e_A, e_B tasodifiy (F2 tasodifiy orakl deb faraz qilinsa), shuning uchun har qanday javob beruvchi amalda qisman yoki noaniq kalit nazoratini (IKC) amalga oshirishi mumkin [4].

Protokol bajarishida bitta foydalanuvchi uchun amaliyotlar sonining samaradorligi 1-jadvalda umumlashtirilgan. Birinchi ikkita ustun nuqta ko‘paytmalari sonini ko‘rsatadi, mos ravishda (SM) va oldindan hisoblashlar bilan (SM-pre). Uchinchi ustun xesh-funksiyalarni ko‘rsatadi. Kalit hosil qilish funksiyalari barcha protokollarga taalluqli, chunki ular barcha protokollarda qo‘llaniladi. To‘rtinchi ustun maydon inversiyalarini hisoblaydi.

1-jadval

Hisoblash samaradorligi taqqoslanishi

Protokol/Amal	**SM**	**SM-pre**	**Xesh**	**Maydon-inv**
MTI/A0	3	2	0	0
UM	3	2	0	0
MQV	2.5	1.5	0	0
LLK	2	1	0	1
SK	3	2	0	0
SSEB	3	2	0	1
ECKE-1	3	2	2	0

Standart hujjatlar [4] yaxshi tanilgan an’anaviy kriptografik xesh funksiyalarini, masalan, SHA-1, RIPEMD-160 va boshqalarni qo‘llashni tavsiya qiladi. Umuman olganda, xavfsiz amaliy xesh funksiyalarini yaratish qiyin. Ular yaxshi tanilgan texnikalar yordamida formallashgan xavfsizlik modellari bilan to‘liq tavsiflangan bo‘lsa-da [1], bu natijalarni real hayotda to‘liq samarali deyish qiyin.

Barcha protokollarning taxmin qilingan xavfsizlik atributlari 2-jadvalda umumlashtirilgan. Osonlikcha tekshirish mumkin, ular hamma IKA (Identifikatsiya

kalitini taqsimlash) atributiga ega, lekin hech biri EKA (Aniq kalitni taqsimlash) atributiga ega emas.

2-jadval

Taxmin qilingan xavfsizlik atributlari

Prot./Atribut	KK-S	FS	KCI-R	UKS-R	IKC
MTI/A0	Ha	Yo‘q	Ha	Yo‘q	Yo‘q
UM	Ha	Ha	Yo‘q	Ha	Ha
MQV	Ha	Ha	Ha	Yo‘q	Yo‘q
LLK	Ha	Ha	Ha	Ha	Ha
SK	Ha	Ha	Ha	Ha	Yo‘q
SSEB	Ha	Ha	Ha	Ha	Yo‘q
ECKE-1	Ha	Ha	Ha	Ha	Ha

XULOSA VA KELGUSI ISHLAR

Biz yangi AK protokoli ECKE-1 ni taklif qildik va uni boshqa ma’lum elliptik egri chiziq asosidagi ochiq kalitli protokollar bilan taqqosladik. Elliptik egri chiziq texnikalari kichikroq tizim parametrlarini, past quvvat talablarini, kenglik samaradorligini va tezroq bajarilishni ta’minlashi mumkin. Barcha protokollar samaradorlik jihatidan taqqoslanadigan darajada.

Xavfsizlik talablari elliptik egri chiziq asosidagi Diffie-Hellman taxminlariga asoslangan. ECKE-1 protokoli asosiy qurilish elementi sifatida xesh funksiyalarini ishlatadi, bu esa muhim xavfsizlik atributlarini ta’minlash imkonini beradi (garchi ular tasodifiy orakl modeli asosida bo‘lsa ham).

Kelgusidagi ishlar ECKE-1 protokolining ishchi prototipini amalga oshirishni o‘z ichiga oladi, bu esa samaradorlik ko‘rsatkichlarini taqdim etish va ushbu ishda taxmin qilingan haqiqiy (haqiqiy dunyo) xavfsizlik xususiyatlarini baholashga yordam beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. M. Bellare and P. Rogaway. Entity authentication and key distribution. In Proceedings of CRYPTO 1993, LNCS 773:232–249, 1994.
2. S. Blake-Wilson, D. Johnson, and A. Menezes. Key agreement protocols and their security analysis. In Proceedings of the 6th IMA Int.l Conf on
3. ANSI-X9.62-1998. Public key cryptography for the financial services: The elliptic curve digital signature algorithm (ECDSA). American National Standards Institute, 1999.
4. IEEE-P1363-2000. Standard specifications for public key cryptography. Institute of Electrical and Electronics Engineers, 2000.
5. L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, pages 28:119–134, 2003.
6. T. Matsumoto, Y. Takashima, and H. Imai. On seeking smart public-key distribution systems. Transactions of IEICE, VolE69:99–106, 1986.
7. B. Kaliski. An unknown key share attack on the MQV key agreement protocol. ACM Transactions on Information and System Security, pages 36–49, 2001.
8. C. Lee, J. Lim, and J. Kim. An efficient and secure key agreement. IEEE p1363a draft, 1998.
9. B. Song and K. Kim. Two-pass authenticated key agreement protocol with key confirmation. Progress in Cryptology - Indocrypt 2000, LNCS 1977:237–249, 2000.
10. K. Al-Sultan, M. Saeb, M. Elmessiery, and U.A.Badawi. A new two-pass key agreement protocol. Proceedings of the IEEE Midwest 2003 Symp. On Circuits, Systems and Computers, 2003.