XABARLARNI XAVFSIZ UZATISH UCHUN YANGI K-ANONIM PROTOKOLINI ISHLAB CHIQISH

Isayev R.I.
Muhammad al-Alxorazmiy nomidagi
Toshkent Axborot Texnologiyalari Universiteti, prof.

Suyunov Muzaffarjon Nurmurot o‘g‘li
Muhammad al-Alxorazmiy nomidagi
Toshkent Axborot Texnologiyalari Universiteti, magistrant
muzaffarsuyunov1997@gmail.com

ANNOTATSIYA

Ushbu tadqiqot ishida yangi k-anonim uzatish protokolini taklif etamiz. Protokol assimetrik shifrlash algoritmiga asoslangan. Protokolning barcha a’zolari kichikroq guruhlarga bo‘linadi va agar guruhdagi barcha a’zolar protokolni to‘g‘ri bajarsa, protokol jo‘natuvchi k - anonim va qabul qiluvchi k - anonim hisoblanadi. Tadqiqotimizning maqsadi Internetda foydalanuvchilarning anonimligini himoya qilishdir. Bu yerda ikkita muhim masalani tahlil qilingan: samaradorlik va xavfsizlik, taklif qilingan protokolni baholash.

Kalit so‘zlar: *Anonimlik, k-anonim, Dining-Cryptographer, guruh indekslari, a’zolar indekslari, xabar maydoni.*

ABSTRACT

In this research paper, we propose a new k-anonymous transmission protocol. The protocol is based on an asymmetric encryption algorithm. All members of the protocol are divided into smaller groups, and if all members in the group execute the protocol correctly, the protocol is considered to be sender k-anonymous and receiver k-anonymous. The purpose of our research is to protect the anonymity of users on the Internet. Two important issues are analyzed here: efficacy and safety, to evaluate the proposed protocol.

Keywords: *Anonymity, k-anonymity, Dining-Cryptographer, group indexes, member indexes, message space.*

KIRISH

Anonimlik va ma’lumotlar maxfiyligi ko‘plab tarmoq ilovalari uchun juda muhimdir. Anonimlik foydalanuvchi identifikatorini veb-serverlar, tarmoq provayderlari va krakerlar kabi obyektlardan himoya qiladi. Ma’lumotlarning maxfiyligi esa foydalanuvchilarning shaxsiy ma’lumotlarini tashqi manbalar hujumidan himoya qiladi. Internetdan foydalanganda haqiqiy shaxsingizni yashirish uchun juda ko‘p sabablar mavjud. Ba’zan siz o‘zingizning haqiqiy ismingiz qo‘shilmagan holda biror narsa yuborishni xohlaysiz. Ushbu protokollar, maxfiy muxlisning xatlarida bo‘lgani kabi, kim kim bilan muloqot qilishini yashirish muammosini hal qiladi. ¬Anonim protokollarda raqibga tarmoqdagi barcha aloqalarni ko‘rishga ruxsat beriladi, lekin u hali ham xabarni jo‘natuvchi yoki qabul qiluvchini aniqlay olmaydi.

Taklif etilayotgan protokolda ishlatiladigan belgilarni quyidagilar:

M - xabar maydoni
n - protokoldagi a’zolar soni
i, j - a’zolar indekslari (diapazon [1, n])
m - protokoldagi guruhlar soni
g - guruh indekslari (diapazon [1, n/k])
P_i - i-a’zo
G_i - i-guruh
l_i - Pi uzatmoqchi bo‘lgan xabar uzunligi
e_P - a’zo P ning ochiq kaliti
d_P - a’zosi P shaxsiy kaliti
k - simmetrik kalit algoritmi uchun kalit

Yashirin kalitga nisbatan simmetrik shifrlash va shifrni ochishni mos ravishda Ek (·) va Dk (·) bilan belgilang va ochiq kalit yordamida assimetrik shifrlashni e va shaxsiy kalit d yordamida mos ravishda (·)e va (·)d bilan mos keladigan assimetrik shifrni ochishni belgilang. Agar tarmoq a’zosi tasodifiy qatorni shifrlab, uni boshqa a’zoga yuborsa, biz bu xabarni niqoblangan xabar deb ataymiz.

MUHOKAMA VA NATIJALAR

Bizning k-anonim xabarlarni uzatish muammosiga yechimimiz assimetrik kalit algoritmidan foydalanadi. Aytaylik, barcha a’zolar ochiq kalit algoritmi, masalan, RSA va nosimmetrik kalit algoritmi, masalan, Kengaytirilgan shifrlash standarti (AES) bo‘lishi mumkin.

Xabarni uzatish uchun protokoldan foydalanadigan n ta a’zo bor deylik.

K-anonim xabarlarni uzatish protokoli amalga oshirilishidan oldin, barcha a'zolar bir qancha maqsadlarda ishlatilishi mumkin bo'lgan uzoq muddatli ochiq/maxfiy kalit juftligini olishlari kerak. Darhaqiqat, bu elektron to'lov, elektron pochta va boshqalar kabi turli maqsadlarda ishlatilishi mumkin bo'lgan odatiy umumiy/xususiy kalit juftligi bo'lishi mumkin.

Yuridik a'zoga ochiq/maxfiy kalit juftligini ulash uchun biz sertifikat tizimidan foydalanishimiz mumkin. Sertifikatning bunday ochiq/maxfiy kalitini olish xavfsiz onlayn-kanal yoki ishonchli sertifikatlash organiga jismoniy kirish kabi oflayn usul orqali amalga oshirilishi mumkin. (e_P, d_P) P a'zosining umumiy/maxfiy kalit juftligi bo'lsin.

Ochiq/maxfiy kalitlar juftligini yaratishda a'zo RSA ochiq/maxfiy kaliti juftligi $\{e, d\}$ va ikkita katta tub sonni yaratishi kerak; tub sonlar ko'paytmasi n modulini hosil qiladi, bu yerda $de = 1 \bmod \varphi(n)$.

Protokol samaradorligini oshirish uchun protokoldagi n ta a'zoni $O(k)$ o'lchamdagi kichikroq guruhlarga ajratamiz. Quyidagi protokol har bir guruh tomonidan alohida bajarilishi mumkin [1].

Yig'ish bosqichi. Guruhda a'zolardan biri xabarni anonim ravishda tarmoqdagi boshqa a'zoga o'tkazmoqchi bo'lsin. Guruhdagi har bir P_i a'zosi g_i ni, qabul qiluvchiga tegishli bo'lgan guruh indeksini va l_i ni o'tkazmoqchi bo'lgan xabar uzunligini tanlaydi. Agar P_i xabar yuborishni istamasa, u g dan kattaroq g_i ni tanlashi mumkin.

1. Har bir a'zo P_i tanlaydi g_i va l_i ni, keyin u $x_i = (g_i||l_i)^{e_0}$ ni hisoblaydi, bu yerda e_0 guruh rahbarining ochiq kalitidir.

2. P_i tasodifiy $j \in [1, k]$ ni tanlaydi va x_i ni P_j ga yuboradi.

3. Qabul qilingan x_i, P_j uni guruh rahbariga yuboradi.

4. Qabul qilingan x_i, guruh sardori g_i va l_i ni olish uchun $y_i = x_i^{d_0}$ ni hisoblaydi, bu yerda d_0 guruh rahbarining shaxsiy kalitidir.

5. Agar $n/k \leq g_i$ bo'lsa, guruh rahbari bu xabarni bekor qiladi; agar $1 \leq g_i \leq n/k$ bo'lsa, guruh rahbari g_i ni tasdiqlaydi. l $1 \leq g_i \leq n/k$ ni qanoatlantiradigan barcha l_i lar ichida eng katta l_i ni bildirsin. Guruh rahbari l ni ham tasdiqlaydi.

Guruh rahbari l va barcha indekslarni e'lon qilgandan so'ng, har bir P_i a'zosi guruh indeksi g_i e'lon qilingan indekslar to'plamida mavjudligini va l_i uzunligi l dan kichikligini tekshiradi. Agar ikkala shart ham bajarilsa, a'zo P_i "ha" xabarini yuboradi, aks holda u "yo'q" xabarini uzatadi.

Agar guruhning barcha a'zolari "ha" xabarini tarqatsa, protokol keyingi bosqichga o'tadi, aks holda protokol to'xtaydi [2].

Uzatish bosqichi. Oxirgi bosqichda guruhning har bir a'zosi, aytaylik, A guruhi, g_i ni, xabar o'tkaziladigan guruh indeksini va l, uzatilishi mumkin bo'lgan xabar

uzunligini biladi. Endi, xabar g_i guruhidagi a'zoga uzatiladi, deylik, B guruhi, keyin guruhdagi barcha a'zolar quyidagi protokolni bajarishi mumkin.

1. P_i, A guruhidagi i-chi a'zo, B guruhidagi barcha a'zolarning ochiq kalitlarini oladi. P_i tasodifiy ravishda $k_{i,j}$, $1 \le j \le n_B$ maxfiy kalitini tanlaydi, bu yerda n_B B -guruh a'zolari soni.

2. Agar P_i $msg_{i,j}$ xabarini Q_j ga o'tkazmoqchi bo'lsa, B guruhidagi j-chi a'zo $k'_{i,j} = (k_{i,j})^{e_{B,j}}$ va $msg'_{i,j} = E_{k_{i,j}}(msg_{i,j})$, bu yerda $e_{B,j}$ - B guruhidagi j-chi a'zoning ochiq kaliti. Agar $meg_{i,j}$ xabar uzunligi l dan kichik bo'lsa, P_i xabar oxirida 0 raqamini qo'yishi mumkin.

3. Agar P_i xabarni Q_j ga uzatishni istamasa, u $msg_{i,j}$ xabari sifatida tasodifiy qatorni tanlaydi. Keyin u $k'_{i,j} = (k_{i,j})^{e_{B,j}}$ va $msg'_{i,j} = E_{k_{i,j}}(msg_{i,j})$ ni hisoblaydi.

4. P_i guruh rahbariga $k'_{i,1}||msg'_{i,1}|| \dots ||k'_{i,n_B}||msg'_{i,n_B}$ xabarini yuboradi.

5. Guruh rahbari barcha xabarlarni qabul qilib, M_j xabarni tuzadi va uni B guruhining j-chi azosiga yuboradi, bunda $1 \le j \le n_B$. Bu yerga,

$$M_j = k'_{i_1,j}||msg'_{i_1,j}|| \dots ||k'_{i_{n_A},j}||msg'_{i_{n_A},j},$$

bu yerda $\{i_1, \dots, i_{n_A}\}$ ni $\{1, \dots, n_A\}$ ning bilan almashtiriladi.

M xabarini qabul qilgan Q_j, $k_{i,j}$ ni $(k'_{i,j})^{d_{B,j}}$, hisoblash orqali, $msg_{i,j}$ esa $D_{k_{i,j}}(msg'_{i,j})$ orqali olishi mumkin.

Tahlil. Tadqiqotimizning maqsadi Internetda foydalanuvchilarning anonimligini himoya qilishdir. Bu yerda biz norasmiy ravishda ikkita muhim masalani tahlil qilingan: samaradorlik va xavfsizlik, taklif qilingan protokolni baholash uchun.

Aytaylik, P_i, A guruhi a'zosi, B guruhi a'zosi Q_j ga xabarini uzatmoqchi [3].

Ishlash. Protokolning xavfsizligi assimetrik shifrlash algoritmiga asoslangan. Protokolning barcha a'zolari umumiy/maxfiy kalit juftligini olishlari kerak. A'zolar kichik guruhlarga bo'linganda, bir-biriga ishonadigan ba'zi a'zolar guruh tuzishi mumkin yoki tizim tomonidan guruhga a'zo tayinlanishi mumkin.

To'plash bosqichida, agar guruh a'zosi bir nechta a'zolarga xabar jo'natmoqchi bo'lsa, u har bir indeksni shifrlashi va har bir shifrlangan xabarni bir vaqtning o'zida guruhdagi turli a'zolarga yuborishi mumkin. Keyin barcha shifrlangan xabarlar guruh rahbariga yo'naltiriladi va barcha indekslar guruh rahbari tomonidan e'lon qilinadi. Protokolda guruh rahbari o'tkazmoqchi bo'lgan eng uzun xabarning uzunligini e'lon qiladi. Uzatish bitlarini kamaytirish uchun har bir guruh indeksi uchun guruh rahbari ushbu guruhga uzatiladigan eng uzun xabar uzunligini e'lon qilishi mumkin.

Uzatish bosqichida a'zo B guruhidagi turli a'zoga turli xabarlarni yuborishi mumkin. U har bir xabarni tegishli a'zoning ochiq kaliti bilan shifrlaydi, so'ngra xabarlarni niqoblangan xabarlar bilan guruh rahbariga yuboradi. Guruh rahbari

tomonidan qayta tiklangan xabarlar tegishli xabarlarga yuboriladi. Bundan tashqari, *B* guruhi a'zosi bir vaqtning o'zida *A* guruhining turli a'zolaridan bir nechta xabarlarni qabul qilishi mumkin [5].

Mustahkamlik. Yig'ish bosqichida P_i *B* guruhi indeksini shifrlaydi va uni guruhning boshqa a'zosiga yuboradi. Ushbu a'zo ushbu xabarni guruh rahbariga yuboradi. Guruh rahbari xabarning shifrini ochish orqali *B* guruhining indeksini olishi mumkin, keyin esa bu indeksni e'lon qilishi mumkin.

Uzatish bosqichida P_i *msg* xabarini shifrlaydi va uni guruh rahbariga bir necha niqoblangan xabarlar bilan yuboradi. Guruh rahbari yangi M_j xabarini, shu jumladan *msg′* va boshqa niqoblangan xabarlarni tuzadi va keyin M_j ni Q_j ga yuboradi. M_j xabarini qabul qilib, Q_j M_j xabarining shifrini ochish orqali xabarni olishi mumkin.

Shunday qilib, agar guruhdagi barcha a'zolar protokolni to'g'ri bajarsa, protokol P_i xabarini Q_j a'zosiga yuborishi mumkin.

Anonimlik. Ushbu bo'limda anonimlikni ko'rib o'tamiz. Birinchidan, jo'natuvchining anonimligi ko'rib chiqiladi [4].

Ushbu protokolda *A* guruhida uzatilgan xabarlar ham, *A* va *B* guruhlari o'rtasida uzatilgan xabarlar ham shifrlanganligi sababli va *A* guruhidagi barcha a'zolar xabarni guruh rahbariga yuboradilar, guruhdan tashqaridagi raqib qaysi biri xabar uzatilgan xabar va qaysi xabar shunchaki shifrlangan tasodifiy qatordir tanlashni hal qila olmaydi. Shunday qilib, guruhdan tashqaridagi raqib guruhning qaysi a'zosi xabar yuborayotganini bila olmaydi.

Guruh rahbari qaysi guruh a'zosi xabar yuborishini hal qila olmaydi. Sabablari quyidagicha: yig'ish bosqichida guruh rahbari oldinga yuborilgan xabarni oladi, u asl jo'natuvchi kimligini bila olmaydi. Uzatish bosqichida guruh rahbari guruhdagi har bir a'zodan shifrlangan xabarlarni oladi va u qaysi xabar uzatilgan xabar ekanligini hal qila olmaydi.

Yig'ish bosqichida guruh a'zosi xabarni guruh rahbariga yuboradi, lekin u xabar indeks yoki shunchaki tasodifiy raqamdan shifrlanganligini bilmaydi. Uzatish bosqichida u xabarni kim o'tkazishini ham hal qila olmaydi. Shunday qilib, guruh a'zosi guruhning qaysi a'zosi xabar yuborishini hal qila olmaydi.

A'zo *B* guruhi uchun, agar u haqiqiy xabar olsa, u faqat xabarni guruh rahbari yoki *A* guruhi yo'naltirishini biladi, lekin A guruhidagi qaysi a'zo xabarni yuborishini hal qila olmaydi.

Xulosa qilib aytadigan bo'lsak, agar guruhdagi barcha a'zolar protokolni to'g'ri bajarsa, protokol barcha guruh uchun jo'natuvchi k-anonim hisoblanadi.

Ikkinchidan, biz qabul qiluvchining anonimligini ko'rib chiqamiz.

Bizning protokolimizda *A* guruhi va *B* guruhi o‘rtasida uzatiladigan xabarlar shifrlanganligi va *B* guruhining barcha a’zolari xabarni *A* guruhining guruh rahbaridan olganligi sababli, guruhdan tashqaridagi raqib qaysi xabar uzatilgan xabar va qaysi xabar faqat shifrlangan tasodifiy qator ekanligini hal qila olmaydi. Shunday qilib, guruhdan tashqaridagi raqib *B* guruhidagi qaysi a’zo xabarni qabul qilishini bila olmaydi.

Guruh rahbari *B* guruhining qaysi a’zosi xabar olishini hal qila olmaydi. Buning sababi shundaki, guruh rahbari guruhdagi har bir a’zodan shifrlangan xabarlarni oladi va u qaysi xabarni uzatgan xabarni o‘z ichiga olishini hal qila olmaydi. Xuddi shunday, guruh a’zosi *B* guruhining qaysi a’zosi xabar olishini hal qila olmaydi [4].

Xulosa qilib aytadigan bo‘lsak, agar guruhdagi barcha a’zolar protokolni to‘g‘ri bajarsa, protokol qabul qiluvchi k-anonim hisoblanadi.

Maxfiylik. Ushbu protokolda barcha uzatilgan xabarlar shifrlangan. Agar P_i a’zosi Q_j a’zosiga *msg* xabarini yuborsa, bu xabar $k_{i,j}$ maxfiy kaliti bilan shifrlanadi. Bu maxfiy kalit Q_j ning ochiq kaliti bilan shifrlanadi va Q_j ga yuboriladi. Shunday qilib, xabarni faqat Q_j o‘qishi mumkin. Boshqalar esa Q_j shaxsiy kalitini bilishmagani uchun xabarni ololmaydilar.

Samaradorlik. Birinchidan, protokolning xabar murakkabligini baholaymiz. Yig‘ish bosqichida guruhning har bir a’zosi boshqa a’zolarga bir yoki bir nechta xabarlarni yuborishi mumkin, shuning uchun a’zo tomonidan yaratilgan xabar $O(1)$. Shunday qilib, ushbu bosqichdagi umumiy xabarlar $O(k)$ ga teng, chunki guruhda $O(k)$ a’zolar mavjud. Keyin, barcha xabarlar guruh a’zosi tomonidan yo‘naltiriladi, shuning uchun bu bosqichdagi jami xabarlar ham $O(k)$ ga teng. Shuning uchun yig‘ish bosqichidagi umumiy xabarlar $O(k)$ ga teng. O‘tkazish bosqichida har bir a’zo guruh rahbariga xabar yuboradi. Keyin guruh rahbari *B* guruhidagi har bir a’zoga tuzilgan xabarni yuboradi. *A* guruhi ham, *B* guruhi ham $O(k)$ a’zolarga ega bo‘lgani uchun uzatish bosqichidagi umumiy xabarlar $O(k)$ ga teng. Yuqorida aytilganlarning barchasidan bitta turda uzatilgan umumiy xabar $O(k)$ ga teng.

Ikkinchidan, protokolning bit murakkabligini baholaymiz. Yig‘ish bosqichida yig‘ish bosqichidagi jami xabarlar $O(k)$ ga teng. Protokoldan biz ushbu bosqichdagi har bir xabar faqat raqamni shifrlash uchun ekanligini ko‘ramiz, shuning uchun RSA shifrlash tizimidagi modul uzunligi l bo‘lsa, bu fazadagi har bir xabarning uzunligi l ga teng. Shunday qilib, yig‘ish bosqichida umumiy yuborilgan bitlar $O(kl)$ ga teng. Uzatish bosqichida har bir a’zo guruh rahbariga xabar yuboradi. Protokoldan biz har bir xabarni $O(k)$ qismlarga bo‘lish mumkinligini ko‘rishimiz mumkin va har bir qismning uzunligi $l+L$, bu yerda L - uzatiladigan xabarning eng katta uzunligi. Shunday qilib, har bir xabarning umumiy bitlari $O(k(l+L))$ va bu bosqichda jami uzatilgan bitlar

$O(k^2(l+L))$, chunki guruhda $O(k)$ a'zo bor. Keyin guruh rahbari B guruhidagi har bir a'zoga tuzilgan xabarni yuboradi. Bu xabarlar faqat guruhga yuborilgan xabarlarni qayta qurishdir, shuning uchun uzatish bosqichidagi jami uzatilgan bitlar $O(k^2(l+L))$, ham. Ya'ni, bu bosqichda jami uzatilgan bitlar $O(k^2(l+L))$ ga teng. Yuqoridagilarning barchasidan bitta turda o'tkazilgan jami bitlar $O(k^2(l+L)) + O(kl) = O(k^2(l+L))$ dir.

Uchinchidan, protokolning hisoblash murakkabligini baholaymiz. Yig'ish bosqichida har bir a'zo boshqa a'zolarga bir yoki bir nechta shifrlangan xabarlarni yuboradi, so'ngra boshqa a'zo xabarni yo'naltiradi, shuning uchun bu bosqichda har bir a'zo $O(1)$ assimetrik shifrlash operatsiyasini va umumiy $O(k)$ assimetrik shifrlash operatsiyasini bajaradi. Uzatish bosqichida har bir a'zo $O(k)$ assimetrik shifrlash operatsiyasini va $O(k)$ simmetrik shifrlash operatsiyasini bajarishi kerak. Shunday qilib, umumiy assimetrik shifrlash operatsiyasi $O(k^2)$, umumiy simmetrik shifrlash operatsiyasi ham $O(k^2)$ ga teng. Xabarni qabul qilib, B guruhi a'zosi Q_j $O(k)$ assimetrik shifrni ochish operatsiyasini va $O(k)$ simmetrik shifrni ochish operatsiyasini bajarishi kerak. Shunday qilib, umumiy assimetrik shifrni ochish operatsiyasi $O(k^2)$, umumiy simmetrik shifrni ochish operatsiyasi ham $O(k^2)$ ga teng.

XULOSA

Ushbu tadqiqot ishida assimetrik shifrlash algoritmiga asoslangan k-anonim uzatish protokoli taklif etilgan. Protokolning barcha a'zolari kichikroq guruhlarga bo'linadi $O(k)$ va agar guruhdagi barcha a'zolar protokolni to'g'ri bajarsa, protokol jo'natuvchi k-anonim va qabul qiluvchi k-anonim hisoblanadi. Ushbu protokolning yangi xususiyatlari:

- Protokol xabarning maxfiyligini ta'minlaydi. Asimmetrik shifrlash algoritmi xavfsiz bo'lsa, protokol ham xavfsizdir.

- Protokolda guruh a'zosi bir vaqtning o'zida boshqa guruhdagi boshqa a'zoga turli xil xabarlarni yuborishi mumkin.

- Protokolda guruh a'zosi bir vaqtning o'zida boshqa guruhdagi turli a'zolardan bir nechta xabarlarni qabul qilishi mumkin.

– Bir turda uzatilgan jami xabar $O(k)$ va bitta turda uzatilgan jami bitlar $O(k^2(l+L)) + O(kl) = O(k^2(l+L))$.

Ushbu protokolda, agar guruhdagi barcha a'zolar protokolni to'g'ri bajarsa, protokol guruh a'zosining *msg* xabarini boshqa guruh a'zosiga uzatishi mumkin.

ADABIYOTLAR RO‘YXATI

[1] L. von Ahn, A. Bortz and N. J. Hopper. “k-Anonymous Message Transmission”. the 10th ACM Conference on Computer and Communication Security. pages 122-130, 2003.
[2] D. Chaum. “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”. Communications of the ACM. 24(2), pages 84-88, 1981.
[3] D. Chaum. “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. Journal of Cryptology. 1(1), pages 65-75, 1988.
[4] Gang Yao and Dengguo Feng, “A New k-Anonymous Message Transmission Protocol”. WISA 2004, LNCS 3325, pp. 388–399, 2004.
[5] D. Denning, P. Denning, and M. Schwartz. “The tracker: A threat to statistical database security”. ACM Trans. on Database Systems. 4(1), pages 76-96, 1979.