

پروتکل کارا برای جمع چندسویه امن با قابلیت تکرار

شادیه عزیزی، مائده عاشوری تلوکی* و حمید ملا

گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران

چکیده

در محاسبات چند سویه امن، گروهی از کاربران، نتیجه یک تابع ریاضی را بر روی داده محرمانه خود، با حفظ حریم خصوصی داده‌ها محاسبه می‌کنند. از موارد پرکاربرد محاسبات چندسویه امن، جمع چندسویه امن است که هدف آن انجام عملیات جمع بر روی داده محرمانه کاربران است. در برخی کاربردها ممکن است، هر عضو چندین مقدار محرمانه داشته و هدف، محاسبه مجموع داده‌های متناظر باشد؛ در این صورت لازم است، پروتکل جمع چندسویه امن، چندین بار برای محاسبه مجموع داده‌های گروه تکرار شود. در این پژوهش، مسئله جمع چندسویه امن با قابلیت تکرار، بدون افزایش هزینه محاسباتی و ارتباطی، مورد توجه قرار گرفته است؛ در این مسئله هر کاربر چندین مقدار محرمانه دارد و اعضا قصد دارند مجموع داده‌های محرمانه خود را به صورت نظیر به نظیر محاسبه کنند؛ به طوری که محرمانگی داده‌های هر کاربر حفظ شود. در این مقاله یک پروتکل کارا جهت محاسبه جمع چندسویه امن با قابلیت تکرار در مدل شبه‌درست کار ارائه شده است. راه کار پیشنهادی، بدون نیاز به کانال امن، محرمانگی داده‌های کاربران و نتایج حاصل جمع را تأمین کرده و در مقابل تبانی جزئی کاربران تا سطح $n - 2$ نفر ایمن و نسبت به روش‌های موجود، از نظر هزینه محاسبات و ارتباطات بسیار کاراست.

واژگان کلیدی: جمع چندسویه امن، کانال ناامن، تبانی جزئی، مدل شبه‌درست کار.

An Efficient and Secure Frequent Multiparty Summation protocol

Shadi Azizi, Maede Ashouri-Talouki* & Hamid Mala

Department of IT Engineering, Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran

Abstract

In secure multiparty computation (SMC), a group of users jointly and securely computes a mathematical function on their private inputs, such that the privacy of their private inputs will be preserved. One of the widely used applications of SMC is the secure multiparty summation which securely computes the summation value of the users' private inputs. In this paper, we consider a secure multiparty summation problem where each group member has m private inputs and wants to efficiently and securely computes the summation values of their corresponding inputs; in other words, users compute m summation values where the first value is the summation of users' first private inputs, the second one is the summation of users' second private inputs and so on. We propose an efficient and secure protocol in the semi honest model, called frequent-sum, which computes the desired values while preserving the privacy of users' private inputs as well as the privacy of the summation results.

Let $\{P_1, P_2, \dots, P_n\}$ be a set of n users and the private inputs of user P_i is denoted as $\{d_{i1}, d_{i2}, \dots, d_{im}\}$. The proposed frequent-sum protocol includes three phases:

1. In the first phase, each user P_i selects a random number r_i , computes and publishes the vectors V_i of m components where each component j of V_i is of $d_{ij} + r_i$ form $V_i = \langle d_{i1} + r_i, d_{i2} + r_i, \dots, d_{im} + r_i \rangle$.

* نویسنده عهده‌دار مکاتبات • تاریخ ارسال مقاله: ۱۳۹۶/۶/۱۲ • تاریخ آخرین بازنگری: ۱۳۹۷/۸/۵ • تاریخ پذیرش: ۱۳۹۷/۱۰/۱۹ • Corresponding author

$r_i > .$ After it, P_i computes the vector $V = \langle \sum_{i=1}^n d_{i1} + \sum_{i=1}^n r_i, \sum_{i=1}^n d_{i2} + \sum_{i=1}^n r_i, \dots, \sum_{i=1}^n d_{im} + \sum_{i=1}^n r_i \rangle$, such that each component j is of $\sum_{i=1}^n d_{ij} + \sum_{i=1}^n r_i$ form.

2. In the second phase, users jointly and securely compute their AV-net (Anonymous Veto network) masks and the Burmester-Desmedt (BD) conference key. To do so, each user P_i selects two random numbers a_i and e_i and publishes (g^{a_i}, g^{e_i}) to the group. Then, P_i computes and sends $t_i = (g^{e_{i+1}}/g^{e_{i-1}})^{e_i}$ to the group. Then, each user is able to compute $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^n g^{a_j})$ and $K = K_i = (g^{e_{i-1}})^{n e_i} \cdot t_i^{n-1} \cdot t_{i+1}^{n-2} \dots t_{i-2} \pmod{p^2}$; $g^{a_i b_i}$ is the AV-net mask of P_i and K is the conference key.
3. In the third phase, using the AV-net mask and the conference key, group members securely and collaboratively compute the summation of their random numbers r_i , $(\sum_{i=1}^n r_i)$. To achieve this, each user broadcasts $w_i = (1 + r_i p) g^{a_i b_i} g^{e_{i-1} e_i}$ to the group, where $g^{a_i b_i}$ is the AV-net mask of P_i and $g^{e_{i-1} e_i}$ is the P_i 's portion of the conference key. Multiplying all w_i s results in canceling the AV-net mask and getting the value of $\prod_{i=1}^n w_i = (1 + p \sum_{i=1}^n r_i) K \pmod{p^2}$. Then each member is able to compute $\sum_{i=1}^n r_i$ by the following Eq.:

$$\sum_{i=1}^n r_i = \frac{(\prod_{i=1}^n w_i) K^{-1} - 1}{p}$$

Now each user is able to compute $\sum_{j=1}^n d_i$ by subtracting $\sum_{i=1}^n r_i$ from each component of V :

$$V - \sum_{i=1}^n r_i = \langle \sum_{j=1}^n d_{i1}, \sum_{j=1}^n d_{i2}, \dots, \sum_{j=1}^n d_{im} \rangle$$

It is shown that the proposed protocol is secure against collusion attack of at most $n - 2$ users. In other words, the frequent-sum protocol is secure against partial collusion attack; only a full collusion (collusion of $n - 1$ users) would break the privacy of the victim user, in this situation there is no reason for the victim user to join to such a group. The performance analysis shows that the proposed protocol is efficient in terms of the computation and communication costs, comparing with previous works. Also, the computation cost of the frequent-sum protocol is in-dependent of the number of inputs of each user (m) which makes the protocol more efficient than the previous works. Table 1 compares the proposed protocol with previous works.

Keywords: secure multiparty sum, without secure channel, partial collusion, semi honest model.

۱- مقدمه

در محاسبات چندسویه امن، گروهی از کاربران قصد دارند نتیجه محاسبه تابع f را بر روی مقادیر محرمانه خود به دست آورند؛ به طوری که در نهایت هر کاربر فقط از نتیجه تابع و داده محرمانه خود اطلاع داشته باشد. محاسبات چندسویه امن نخستین بار توسط یائو تحت عنوان مسئله میلیونرها مطرح شد [1]؛ در این مسئله دو میلیونر بدون افشای میزان ثروت خود تعیین می کنند کدام یک ثروتمندتر است. تاکنون توابع مختلفی در قالب محاسبات چندسویه امن ارائه شده است. در این مقاله جمع چندسویه امن در نظر گرفته شده که در آن تابع f برابر مجموع مقادیر محرمانه اعضای گروه است.

جمع چندسویه امن در موارد متعددی مانند استخراج قوانین انجمنی در پایگاه داده [2]، الگوریتم های رأی گیری الکترونیکی [3]، الگوریتم های پالایش گروهی در سامانه های پیشنهاددهنده [4]، یافتن نزدیک ترین همسایه به گروهی از افراد در خدمات مبتنی بر مکان [5-8]، تجمیع داده در شبکه هوشمند برق [9] و بسیاری مسائل دیگر [10-12] کاربرد دارد. یکی از نیازهایی که در استفاده از جمع چندسویه امن به وجود می آید، نیاز به تکرار کردن پروتکل جهت محاسبه حاصل جمع های مقادیر محرمانه مختلف است. به عنوان مثال در

کاربردهای مبتنی بر مکان، گروهی از افراد را در نظر بگیرید که قصد دارند، جلسه ای را در نزدیک ترین مکان به گروه از بین مکان های نامزد برگزار کنند، به طوری که حریم مکانی اعضای گروه محافظت شود. در این صورت لازم است، مجموع فاصله افراد از هر یک از مکان های نامزد به طور امن محاسبه شده و مکان متناظر با کمترین مجموع فاصله به عنوان محل جلسه انتخاب شود. در این مسئله و مسائل مشابه لازم است پروتکل جمع چندسویه امن به ازای تعداد مقادیر محرمانه کاربران تکرار شود. با افزایش تعداد مقادیر محرمانه کاربران، هزینه محاسبات و ارتباطات پروتکل افزایش می یابد و منجر به ناکارآمدی پروتکل می شود. در این مقاله راه کاری کارا برای جمع چندسویه امن با قابلیت تکرار ارائه شده است. این راه کار علاوه بر این که به ازای یکبار اجرا نسبت به راه کارهای پیشین کارا تر است، مسئله تکرار پروتکل را نیز در نظر می گیرد و راه کاری ارائه می دهد که هزینه محاسبات هر کاربر مستقل از تعداد داده های محرمانه کاربران باقی بماند.

راه کارهای جمع چندسویه امن براساس فرض کانال ارتباطی به دو دسته: راه کارهای با فرض کانال امن و ناامن تقسیم می شوند. در راه کارهای با فرض کانال امن، کانال ارتباطی بین اعضای گروه غیر قابل شنود است و در صورت

دسترسی دارند؛ این فرض یک نیاز اولیه و کلی در محاسبات چندسویه امن است [1]. راه کار پیشنهادی نیازهای امنیتی زیر را برآورده می کند:

- ۱- تأمین محرمانگی داده های کاربران از دید دیگر کاربران گروه و نیز مهاجمان خارجی؛
- ۲- تأمین محرمانگی نتایج مجموع داده های کاربران از دید مهاجمان خارجی؛
- ۳- امنیت در برابر تبانی جزئی کاربران تا سطح $n - 2$ نفر

۳- کارهای مرتبط

در این بخش راه کارهای جمع چندسویه امن در دو دسته با فرض وجود کانال امن و ناامن بررسی می شوند.

۳-۱- راه کارهای با فرض وجود کانال امن

کلیفتون و همکاران در راستای داده کاوی راه کاری برای جمع چندسویه امن ارائه دادند که در آن اعضا در چیدمان حلقه قرار می گیرند [2]. عضو نخست چیدمان داده محرمانه خود را با یک عدد تصادفی جمع و برای عضو دوم حلقه می فرستد؛ او نیز مقدار محرمانه خود را با مقدار دریافتی جمع کرده و برای عضو بعدی می فرستد؛ روال تا کامل شدن حلقه ادامه دارد؛ سپس عضو آغازگر با کم کردن مقدار تصادفی اولیه، مجموع مقادیر محرمانه را محاسبه و برای اعضا می فرستد این راه کار در برابر تبانی دو نفر امن نیست. راه کار بعدی توسط شیخ و همکاران ارائه شد [13] که در آن هر عضو داده محرمانه خود را به n بلوک تقسیم و به ازای هر بلوک روال راه کار کلیفتون و همکاران طی می شود؛ اما این راه کار در برابر تبانی جزئی دو نفر امن نیست. بنابراین در راه کار بعدی [14] عضو دوم چیدمان اولیه در هر دور با عضو کناری جابه جا می شود، این راه کار نیز در برابر تبانی جزئی تا سطح $n - 2$ نفر امن نیست. پس در ارتقای بعدی راه کار شیخ و همکاران [15] هر کاربر داده محرمانه خود را به n بلوک تقسیم و بین اعضا توزیع می کند؛ به طوری که هر کاربر n بلوک داشته و یکی از آنها متعلق به اوست. بدین طریق این راه کار در برابر تبانی جزئی تا سطح $n - 2$ نفر امن است.

در ادامه راه کارهای [16] و [17] نیز ارائه شدند که هزینه ارتباطی کمتری دارند؛ اما به طرف سوم مورد اعتماد نیاز دارند؛ سپس یوون و همکاران راه کاری را با دو مرحله ارائه دادند [18] که در مرحله نخست هر عضو اعداد تصادفی را انتخاب و در بین اعضا به طور محرمانه توزیع می کند. گیرنده عدد تصادفی را از داده محرمانه خود کم یا به آن اضافه می کند و فقط به فرستنده اطلاع می دهد تا عکس عمل انجام شده را

ارسال پیام در کانال، فقط گیرنده از محتوای آن مطلع می شود. در راه کارهای با فرض کانال ناامن، کانال ارتباطی بین اعضای گروه، قابل شنود توسط مهاجم و جهت محرمانه ماندن پیام های ارتباطی نیاز به روش های رمزنگاری است، از این رو راه کارهای با فرض کانال ناامن پرهزینه تر و امن تر از راه کارهای با فرض کانال امن هستند. در راه کار پیشنهادی کانال ارتباطی به صورت ناامن در نظر گرفته می شود.

در محاسبات چندسویه امن دو مدل مهاجم وجود دارد: مدل شبه درست کار و مدل بدخواه. در مدل شبه درست کار، اعضای گروه از روال پروتکل تبعیت کرده اما جهت به دست آوردن اطلاعاتی راجع به داده محرمانه سایر اعضای گروه کنجکاوی می کنند؛ اما در مدل بدخواه، اعضا از روال پروتکل تبعیت نمی کنند و به دلخواه رفتار می کنند. در این مقاله مدل مهاجم شبه درست کار در نظر گرفته شده است.

بنابراین در این مقاله راه کاری کارا جهت جمع چندسویه امن با قابلیت تکرار و با فرض کانال ناامن در مدل شبه درست کار ارائه شده است. راه کار ارائه شده در برابر حمله تبانی جزئی تا سطح $n - 2$ نفر امن است. به علاوه در این راه کار به ازای هر چندبار تکرار، محرمانگی نتایج حاصل جمع های محاسبه شده حفظ می شود و فقط اعضای گروه قادر به محاسبه حاصل جمع ها هستند.

ساختار مقاله به صورت زیر است: در بخش دوم مسئله جمع چندسویه امن به صورت فرمال بیان می شود. در بخش سوم، کارهای مرتبط با جمع چندسویه امن با فرض کانال امن و کانال ناامن مرور می شوند. در بخش چهارم روش های استفاده شده در این مقاله به اختصار توضیح داده می شود؛ در بخش پنجم، راه کار پیشنهادی را شرح داده و امنیت و کارایی آن تحلیل می شود؛ به منظور مقایسه، در بخش ششم پروتکل پیشنهادی با راه کارهای پیشین مقایسه می شود. در بخش هفتم مقاله جمع بندی می شود.

۲- تعریف مسئله

فرض کنید n کاربر $\{P_1, P_2, \dots, P_n\}$ وجود دارند و هر کاربر P_i مجموعه داده های محرمانه $\{d_{i1}, d_{i2}, \dots, d_{im}\}$ را در اختیار دارد. اعضای گروه قصد دارند با m مرتبه تکرار جمع چندسویه امن، حاصل جمع مقادیر محرمانه و متناظر خود را محاسبه کنند؛ به عبارت دیگر پروتکل پیشنهادی باید مقدار $(\sum_{i=1}^n d_{ij})$ را به ازای $j = 1, 2, \dots, m$ به طور امن محاسبه کند؛ به طوری که هر کاربر P_i فقط از داده محرمانه خود یعنی d_{ij} و $\sum_{i=1}^n d_{ij}$ اطلاع داشته باشد. در پروتکل پیشنهادی فرض می شود، اعضای گروه به یک کانال عمومی و احراز اصالت شده

روی داده محرمانه خود انجام دهد. در مرحله دوم روال راه کار کلیفتون طی می شود. این راه کار با افزایش هزینه ارتباطی در برابر تبانی جزئی تا سطح $n-2$ نفر امن است.

سپس *راوتاری* و همکاران راه کاری را در چیدمان باس ارائه دادند [19] که هر عضو، داده محرمانه خود را به n بلوک تقسیم و به ازای هر دور روال راه کار کلیفتون طی می شود؛ اما این راه کار در برابر تبانی جزئی دونفر امن نیست. بنابراین در راه کار بعدی *راوتاری* و همکاران [20] کاربر نخست چیدمان اولیه در هردور با سایر اعضا جابه جا می شود؛ این راه کار در برابر تبانی جزئی امن نیست؛ در راه کار بعدی [21] هر کاربر پس از تقسیم داده محرمانه به n بلوک آن را در بین اعضا توزیع می کند و مابقی روال مانند [19] طی می شود. این راه کار در برابر تبانی جزئی تا سطح $n-2$ نفر امن است.

۳-۲- راه کارهای با فرض کانال ناامن

جانگ و همکاران راه کاری برای جمع چندسویه امن بدون نیاز به کانال امن ارائه دادند [22]. در این راه کار عدد نخست بسیار بزرگ p انتخاب و p^2 به عنوان پیمانه محاسباتی انتخاب می شود، اعضا در چیدمان حلقه قرار گرفته و هر عضو با انجام عمل نماسانی، مقداری را برای گروه می فرستد و سپس با کمک مقادیر دریافتی از دو عضو کناری خود در حلقه مقدار محرمانه R_i را محاسبه و با ضرب داده محرمانه خود در R_i آن را مخفی و پخش همگانی می کند. با ضرب مقادیر ارسالی اعضای گروه، مقادیر R_i حذف و مجموع داده های محرمانه محاسبه می شود. این راه کار در برابر تبانی جزئی دو نفر امن نیست و به منظور افزایش امنیت در برابر تبانی جزئی تا سطح $n-2$ نفر هزینه عملیات $O(n^2)$ نماسانی و در صورت m بار تکرار پروتکل هزینه از مرتبه $O(mn^2)$ نماسانی می شود. به علاوه محرمانگی حاصل جمع نیز حفظ نمی شود.

راه کار بعدی توسط *عاشوری* و همکاران بر مبنای شبکه وتوی گمنام و پروتکل توافق کلید *Burmester-Desmedt* (BD) ارائه شد که در آن سه پروتکل ارائه شده است [23]. در این راه کار عدد مرکب $N = p_1 p_2$ انتخاب می شود که تجزیه N برای همه مجهول است. در پروتکل نخست، یعنی *securesum-v1* اعضا شبکه وتوی گمنام راه اندازی می کنند و هر عضو با ضرب داده محرمانه در مقادیر شبکه وتوی گمنام، داده محرمانه خود را مخفی و پخش همگانی می کند؛ با ضرب مقادیر گروه، ماسک شبکه از بین رفته و حاصل جمع آشکارا محاسبه می شود. در پروتکل دوم یعنی *securesum-v2* اعضا علاوه بر راه اندازی شبکه وتوی گمنام، براساس روش BD، کلید جلسه به اشتراک می گذارند و پس

از ضرب داده محرمانه در مقادیر شبکه و سهم هر کاربر از کلید آن را پخش همگانی می کنند. با ضرب مقادیر گروه حاصل جمع رمز شده حاصل می شود. در پروتکل سوم تحت عنوان *securesum-v3* با هزینه محاسباتی پایین تر حاصل جمع به صورت رمز شده محاسبه می شود. دو پروتکل نخست در برابر تبانی جزئی تا سطح $n-2$ نفر امن هستند؛ اما پروتکل سوم در برابر تبانی جزئی تا سطح $n-4$ نفر امن است. در این راه کار عدد مرکب N وجود دارد و در صورت m بار تکرار هزینه $O(nm)$ نماسانی می شود.

مهناز و همکاران با استفاده از زیرساخت کلید عمومی روشی جهت محاسبه مجموع داده های محرمانه به صورت امن ارائه کردند [24]. در این روش هر فرد یک جفت کلید عمومی و خصوصی دارد و $n-1$ داده تصادفی انتخاب کرده و هر یک را به صورت رمز شده با کلید عمومی یکی از اعضای گروه به صورت منفرد ارسال می کند، به طوری که هر عضو تنها یک بخش از داده تصادفی هر عضو دیگر گروه را در اختیار دارد؛ سپس هر عضو گروه مجموع داده های ارسالی خود را محاسبه و (P_{IS}) سپس داده های دریافتی از $n-1$ عضو دیگر گروه را رمزگشایی کرده و مجموع داده های دریافتی را نیز محاسبه می کند (P_{IR}) . آن گاه هر عضو، مجموع داده محرمانه خود، P_{IS} و P_{IR} را محاسبه و برای مدیر گروه ارسال می کند. مدیر مجموع داده های دریافتی را که برابر با مجموع داده های محرمانه است، محاسبه کرده و به اعضا اطلاع می دهد. واضح است که این روش هزینه محاسباتی زیادی را به اعضای گروه تحمیل می کند $(n-1)$ عمل رمزگذاری و $n-1$ عمل رمزگشایی برای هر عضو. این پروتکل در مقابل تبانی $n-2$ نفر ایمن است.

۴- روش های مورد استفاده

در راه کار ارائه شده در این مقاله از پروتکل های شبکه وتوی گمنام [25] و اشتراک کلید جلسه به روش *Burmester-Desmedt* (BD) [26] و از خاصیت پیمانه ای رابطه (۱) [22] استفاده می شود که در آن p عدد اول است:

$$\prod_{i=1}^n (1 + d_i p) = \left(1 + p \sum_{i=1}^n d_i \right) \mod p^2 \quad (1)$$

در ادامه پروتکل شبکه وتوی گمنام و پروتکل توافق کلید BD به اختصار شرح داده می شوند.

مولد $g = g_0^p \bmod p^2$ در نظر گرفته می‌شوند. بنابراین اعضای گروه بر روی گروه حلقوی G از مرتبه q توافق کرده‌اند. پروتکل پیشنهادی با نام Frequent-sum دارای سه مرحله زیر است که در شکل (۱) نشان داده شده است:

- مرحله نخست: ارسال مقادیر توسط اعضای گروه و محاسبه مجموع مقادیر ارسالی
- مرحله دوم: راه‌اندازی شبکه وتوی گمنام و اشتراک جلسه
- مرحله سوم: محاسبه نتایج حاصل جمع‌ها

در مرحله نخست، هر عضو P_i عدد تصادفی $r_i \in_R Z_p$ انتخاب می‌نماید و آن را با هر کدام از مقادیر محرمانه خود جمع و بدین طریق بردار V_i با m مؤلفه را ایجاد و پخش همگانی می‌کند که در رابطه (۲) نشان داده شده است:

$$V_i = \langle d_{i1} + r_i, d_{i2} + r_i, \dots, d_{im} + r_i \rangle \quad (2)$$

حال، هر عضو گروه مقادیر ارسالی کل اعضا را با یکدیگر جمع و بردار حاصل جمع کل مؤلفه‌ها (V) را ایجاد می‌کند که در رابطه (۳) نشان داده شده است. لازم به ذکر است مؤلفه با کمترین مقدار، دارای کمترین مجموع است.

$$V = \langle \sum_{i=1}^n d_{i1} + \sum_{i=1}^n r_i, \sum_{i=1}^n d_{i2} + \sum_{i=1}^n r_i, \dots, \sum_{i=1}^n d_{im} + \sum_{i=1}^n r_i \rangle \quad (3)$$

در مرحله دوم، هر عضو P_i دو مقدار تصادفی $a_i, e_i \in_R Z_q$ انتخاب می‌کند و g^{a_i} را به منظور برقراری شبکه وتوی گمنام و مقدار g^{e_i} را در راستای تشکیل کلید مشترک پخش همگانی می‌کند؛ سپس مقدار $t_i = (g^{e_{i+1}}/g^{e_{i-1}})^{e_i}$ را محاسبه و پخش همگانی می‌نماید.

حال هر عضو گروه به تنهایی قادر به محاسبه مقدار $K = (g^{e_{i-1}})^{n e_i} \cdot t_i^{n-1} \cdot t_{i+1}^{n-2} \cdot \dots \cdot t_{i-2} \pmod{p^2}$ و کلید مشترک K به صورت زیر است:

$$K = K_i = (g^{e_{i-1}})^{(n e_i)} \cdot t_i^{(n-1)} \cdot t_{i+1}^{(n-2)} \cdot \dots \cdot t_{i-2} \pmod{p^2}$$

در مرحله سوم، هر کاربر P_i مقدار w_i را محاسبه و پخش همگانی می‌کند:

$$w_i = (1 + r_i p) g^{a_i b_i} g^{e_{i-1} e_i} \quad (4)$$

۴-۱- پروتکل شبکه وتوی گمنام

پروتکل شبکه وتوی گمنام توسط هائو و همکاران برای حل مسئله وتوی گمنام ارائه شد [25]. در این پروتکل، دو عدد اول بسیار بزرگ p و q انتخاب می‌شوند؛ به طوری که $q | p-1$. گروه حلقوی G از مرتبه q و با مولد g در نظر گرفته می‌شود. n کاربر داریم و مقادیر (G, g, p, q) آشکار هستند. پروتکل شامل دو مرحله است: در مرحله نخست، هر عضو P_i یک عدد تصادفی $a_i \in_R Z_q$ را انتخاب و مقدار g^{a_i} را پخش همگانی می‌کند؛ سپس هر عضو P_i با توجه به مقادیر دریافتی از سایر اعضا مقدار $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^n g^{a_j})$ را محاسبه می‌کند. در مرحله دوم، هر عضو مقدار $g^{c_i b_i}$ را پخش همگانی می‌کند؛ به طوری که مقدار c_i برابر a_i است، اگر کاربر وتو نکند و در غیر این صورت c_i یک عدد تصادفی از گروه G است؛ سپس هر کاربر مقادیر $g^{c_i b_i}$ کل کاربران درهم ضرب می‌کند؛ در صورتی که کل کاربران در وتو شرکت نکنند، حاصل ضرب برابر یک خواهد شد ($\prod_i g^{c_i b_i} = g^{\sum_{i=1}^n a_i b_i} = 1$) و در صورتی که دست کم یک کاربر در وتو شرکت کند، حاصل ضرب مخالف یک خواهد شد ($\prod_i g^{c_i b_i} \neq 1$).

۴-۲- پروتکل توافق کلید Burmester-Desmedt (BD)

هدف پروتکل توافق کلید (BD)، برقراری یک کلید تازه و برروی یک کانال امن در بین گروهی از افراد است؛ به طوری که تنها، اعضای گروه، کلید تشکیل شده را می‌دانند و هیچ کس دیگری امکان ساخت یا کشف کلید را ندارد. در راه کار برمستر و همکاران دو عدد نخست بسیار بزرگ p, q و $g \in Z_p$ انتخاب می‌شوند به طوری که g از مرتبه عدد نخست بسیار بزرگ q باشد [26]. مقادیر p, q, g آشکار هستند. هر کاربر P_i یک عدد تصادفی $e_i \in_R Z_q$ را انتخاب، سپس g^{e_i} و در ادامه مقدار $t_i = (g^{e_{i+1}}/g^{e_{i-1}})^{e_i}$ را محاسبه و پخش همگانی می‌کند. هر کاربر P_i کلید مشترک را طبق رابطه $K_i = (g^{e_{i-1}})^{n e_i} \cdot t_i^{n-1} \cdot t_{i+1}^{n-2} \cdot \dots \cdot t_{i-2}$ محاسبه می‌کند. کلید مشترک محاسبه شده برای کل کاربران برابر $K = g^{e_1 e_2 + e_2 e_3 + \dots + e_n e_1}$ خواهد بود.

۵- راه کار پیشنهادی

دو عدد نخست بسیار بزرگ p و q به عنوان پیمانانه اعداد انتخاب می‌شوند؛ به طوری که $q | p-1$ و گروه حلقوی G_0 از مرتبه q و با مولد g_0 انتخاب می‌شود و گروه حلقوی دیگری (G) با

Frequent-Sum: Securely find m summation values of m dimensional private inputs correspondingly, in the semi-honest model

Phase 1. Sending users' values

- i. $P_i \rightarrow *: V_i = \langle d_{i1} + r_i, d_{i2} + r_i, \dots, d_{im} + r_i \rangle$ where $r_i \in_R \mathbb{Z}_q$
- ii. P_i computes $V = \langle D_1, D_2, \dots, D_m \rangle = \langle \sum_{i=1}^n d_{i1} + \sum_{i=1}^n r_i, \sum_{i=1}^n d_{i2} + \sum_{i=1}^n r_i, \dots, \sum_{i=1}^n d_{im} + \sum_{i=1}^n r_i \rangle$

Phase 2. Computing the AV-net value and the Burmester-Desmedt Key

- i. $P_i \rightarrow *: (g^{a_i}, g^{e_i})$ where $a_i, e_i \in_R \mathbb{Z}_q$
- ii. $P_i \rightarrow *: t_i = (g^{e_{i+1}} / g^{e_{i-1}})^{e_i}$
- iii. P_i computes $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^n g^{a_j})$ and $K_i \equiv (g^{e_{i-1}})^{n e_i} \cdot t_i^{n-1} \cdot t_{i+1}^{n-2} \cdot \dots \cdot t_{i-2}$

Phase 3. Finding the results

- i. $P_i \rightarrow *: w_i = (1 + r_i p) g^{e_{i-1} e_i} g^{a_i b_i}$
- ii. P_i computes $\prod_{i=1}^n w_i = \prod_{i=1}^n (1 + r_i p) g^{e_{i-1} e_i} g^{a_i b_i} = (1 + p \sum_{i=1}^n r_i) \times K \bmod p^2$
- iii. P_i computes $\sum_{i=1}^n r_i$ as follows:

$$\sum_{i=1}^n r_i = \frac{(\prod_{i=1}^n w_i) K^{-1} - 1}{p}$$
- iv. P_i computes $V_{sum} = V - \sum_{i=1}^n r_i = \langle D_1 - \sum_{i=1}^n r_i, \dots, D_m - \sum_{i=1}^n r_i \rangle = \langle \sum_{i=1}^n d_{i1}, \sum_{i=1}^n d_{i2}, \dots, \sum_{i=1}^n d_{im} \rangle$

(شکل-۱): مراحل پروتکل پیشنهادی
(Figure-1): sequences of proposed protocol

$$V_{sum} = \langle \sum_{i=1}^n d_{i1}, \sum_{i=1}^n d_{i2}, \dots, \sum_{i=1}^n d_{im} \rangle \quad (۶)$$

هر عضو P_i در فاز سوم مقدار $w_i = (1 + r_i p) g^{a_i b_i} g^{e_{i-1} e_i}$ را ارسال می‌کند. هدف از $g^{a_i b_i}$ محرمانه ماندن r_i و در نهایت محرمانه بودن d_i است و هدف از $g^{e_{i-1} e_i}$ محرمانه بودن مقدار $\sum_{i=1}^n r_i$ و در نهایت محرمانه بودن حاصل جمع $(\sum_{i=1}^n d_i)$ است؛ بنابراین فقط اعضای گروه قادر به محاسبه حاصل جمع‌ها هستند و مهاجم بیرونی از نتایج حاصل جمع مطلع نمی‌شود؛ به علاوه داده محرمانه هر کاربر از دید سایر کاربران و نیز مهاجمان خارجی مخفی باقی می‌ماند؛ در بخش تحلیل امنیت، بیشتر در این موارد بحث می‌شود:

اثبات درستی پروتکل Frequent-sum. هدف پروتکل Frequent-sum محاسبه نتایج حاصل جمع داده‌های محرمانه کاربران به صورت نظیر به نظیر است. در این پروتکل هر عضو P_i عدد تصادفی r_i را انتخاب و با هر کدام از مقادیر محرمانه خود جمع کرده و بردار V_i را تشکیل داده و در گروه ارسال می‌کند؛ بنابراین جهت محاسبه بردار V_{sum} ، کافی است مقدار $\sum_{i=1}^n r_i$ به صورت امن محاسبه شده و از مؤلفه‌های بردار V کم شود؛ بنابراین جهت اثبات درستی پروتکل Frequent-sum کافی است ثابت کنیم در مرحله سوم، مقدار $\sum_{i=1}^n r_i$ به درستی محاسبه می‌شود. لم زیر این مسئله را ثابت می‌کند:

لم ۱. مرحله سوم پروتکل Frequent-sum مقدار $\sum_{i=1}^n r_i$ را به درستی محاسبه می‌کند.

ساختار w_i شامل مقدار $(1 + r_i p)$ ، مقدار شبکه و توی گمنام $(g^{a_i b_i})$ و سهم کاربر P_i از کلید مشترک K (یعنی $g^{e_{i-1} e_i}$) است. با ضرب مقادیر ارسالی کل اعضای گروه، ماسک شبکه از بین می‌رود و مقدار $\prod_{i=1}^n w_i = (1 + p \sum_{i=1}^n r_i) K \bmod p^2$ محاسبه می‌شود:

$$\begin{aligned} w &= \prod_{i=1}^n w_i \quad (۵) \\ &= \prod_{i=1}^n (1 + r_i p) g^{a_i b_i} g^{e_{i-1} e_i} \\ &= \prod_{i=1}^n (1 + r_i p) \prod_{i=1}^n g^{a_i b_i} \prod_{i=1}^n g^{e_{i-1} e_i} \\ &= \left(1 + p \sum_{i=1}^n r_i\right) \times g^{\sum_{i=1}^n a_i b_i} \\ &\quad \times g^{e_1 e_2 + e_2 e_3 + \dots + e_n e_1} \\ &= \left(1 + p \sum_{i=1}^n r_i\right) \times K \bmod p^2 \end{aligned}$$

اعضای گروه قادرند نتیجه رابطه (۵) را در K^{-1} ضرب کرده و مقدار $c = (1 + p \sum_{i=1}^n r_i)$ و در نتیجه $\sum_{i=1}^n r_i = \frac{c-1}{p}$ را محاسبه کنند؛ چون فقط اعضای گروه کلید K را در اختیار دارند، فقط اعضای گروه قادر به محاسبه $\sum_{i=1}^n r_i$ خواهند بود.

حال چون $\sum_{i=1}^n r_i$ در تمام مؤلفه‌های بردار V یکسان است، اگر از تمام مؤلفه‌های بردار V کم شود و نتایج حاصل جمع در بردار V_{sum} محاسبه می‌شود:

مهاجمان قادر به محاسبه b_i و در نتیجه کشف مقدار محرمانه P_i نخواهند بود. بنابراین پروتکل Frequent-sum در برابر تبانی جزئی تا سطح $n - 2$ نفر امن است.

ویژگی سوم: پروتکل Frequent-sum محرمانگی حاصل جمع‌ها را حفظ می‌کند.

جهت محاسبه نتایج حاصل جمع‌ها، لازم است، مهاجمان مقدار $\sum_{i=1}^n r_i$ و در نتیجه مقدار کلید مشترک جلسه (K) را محاسبه کنند؛ اما براساس تئوری یک از مقاله [26] و سختی مسئله دیفی هلمن، مهاجمان خارجی قادر به یافتن کلید K نخواهند بود و در نتیجه محرمانگی حاصل جمع‌ها تأمین می‌شود. بنابراین فقط اعضای گروه قادر به رمزگشایی $(1 + p \sum_{i=1}^n r_i)$ و محاسبه $\sum_{i=1}^n r_i$ هستند. در نتیجه فقط اعضای گروه حاصل جمع‌ها را محاسبه می‌کنند.

۵-۲- تحلیل کارایی

هزینه ارتباطی: در مرحله نخست، هر عضو گروه برداری با m مؤلفه را محاسبه و پخش همگانی می‌کند؛ هزینه ارتباطی به‌ازای یک کاربر $m[\log p^2]$ بیت و به‌ازای n کاربر $mn[\log p^2]$ بیت است. در مرحله دوم اعضا باید شبکه وتوی گمنام را راه‌اندازی کنند و کلید جلسه را به اشتراک بگذارند؛ بدین منظور هر کاربر P_i باید مقادیر g^{a_i} و g^{t_i} را برای گروه ارسال کند؛ بنابراین هزینه ارتباطی هر کاربر $3[\log p^2]$ بیت و برای n کاربر $3n[\log p^2]$ بیت است. در مرحله سوم، هر کاربر مقادیر محرمانه خود را به کمک مقادیر شبکه وتوی گمنام و کلید مشترک مخفی و ارسال می‌کند: $g^{e_{i-1}e_i} g^{a_i b_i} (1 + r_i p)$ بنابراین هزینه ارتباطی برای یک کاربر $[\log p^2]$ بیت و برای کل گروه $n[\log p^2]$ بیت است. در نتیجه، به‌طور کلی هزینه ارتباطی پروتکل Frequent-sum برای یک کاربر $(4 + m)[\log p^2]$ بیت و برای n کاربر $(4n + nm)[\log p^2]$ بیت است.

هزینه محاسباتی: در مرحله نخست اعضای گروه m جمع ساده انجام می‌دهند. در مرحله دوم، شبکه وتوی گمنام راه‌اندازی می‌کنند و کلید جلسه به اشتراک می‌گذارند؛ بدین منظور هر کاربر جهت محاسبه g^{e_i} و g^{a_i} و t_i و $g^{a_i b_i}$ و K نیاز به 5 عمل نماسانی دارد. پس هر کاربر مقدار w_i را محاسبه و پخش همگانی می‌کند که تنها به دو عمل ضرب نیاز دارد. در ادامه با ضرب w_i ها در مرحله سوم هر کاربر m عمل ضرب انجام می‌دهد. از آن‌جا که هزینه عمل جمع و ضرب در مقایسه با نماسانی ناچیز است، فقط هزینه عملیات نماسانی را در نظر می‌گیریم؛ بنابراین هزینه محاسباتی

اثبات. همان‌طور که گفته شد هر کاربر مقدار w_i شامل $(1 + r_i p)$ مقدار شبکه وتوی گمنام و سهم کاربر P_i از کلید مشترک K را ارسال می‌کند.

پس از محاسبه حاصل ضرب مقادیر w_i و با توجه به ویژگی مقادیر شبکه وتوی گمنام [25] $(\sum a_i b_i = 0)$ ، ماسک شبکه وتوی گمنام خنثی شده و حاصل ضرب مقدار $(1 + p \sum_{i=1}^n r_i)$ در کلید K حاصل می‌شود. بنابراین اعضای گروه با دانستن K ، قادر به محاسبه $\sum_{i=1}^n r_i$ خواهند بود.

۵-۱- تحلیل امنیت

همان‌طور که در قبل بیان شد، پروتکل Frequent-sum لازم است، ویژگی‌های امنیتی زیر را برآورده کند:

(۱) محرمانگی داده کاربران از دید سایر کاربران و مهاجمان خارجی،

(۲) محرمانگی حاصل جمع‌ها از دید مهاجمان خارجی

(۳) امنیت در برابر تبانی جزئی تا سطح $n - 2$ نفر امن.

در ادامه این سه ویژگی امنیتی پروتکل Frequent-sum بررسی می‌شود.

ویژگی نخست: پروتکل Frequent-sum محرمانگی داده کاربر را تأمین می‌کند.

عضو P_i هر داده محرمانه خود (d_{ij}) را با عدد تصادفی r_i جمع کرده و در بردار V_i ، لازم است، مهاجمان جهت افشای مقادیر محرمانه کاربر مقدار r_i و در نتیجه مقدار شبکه وتوی گمنام $(g^{a_i b_i})$ و سهم کاربر P_i از کلید مشترک K (یعنی $g^{e_{i-1}e_i}$) را محاسبه کنند. مقدار $g^{e_{i-1}e_i}$ را کاربر P_{i-1} و P_i می‌تواند محاسبه کند، اما محاسبه مقدار $g^{a_i b_i}$ نیاز به آگاهی از مقدار a_i دارد که محاسبه آن برای سایر اعضا و مهاجم بیرونی براساس مسئله سخت DDH غیر ممکن است.

ویژگی دوم: پروتکل Frequent-sum در برابر تبانی جزئی تا سطح $n - 2$ نفر امن است.

در حمله تبانی، مهاجمان جهت کشف داده‌های محرمانه برخی کاربران، با یکدیگر تبانی می‌کنند. در تبانی جزئی، در بدترین حالت، تنها یک کاربر (P_k) در تبانی علیه کاربر (P_i) شرکت نمی‌کند. حال جهت کشف مقدار محرمانه کاربر P_i لازم است، مهاجمان مقدار $g^{a_i b_i}$ و مقدار $g^{e_{i-1}e_i}$ را به‌دست آورند. با فرض $P_k \neq P_{i-1}$ ، مهاجمان قادر به محاسبه $g^{e_{i-1}e_i}$ از طریق کاربر P_{i-1} خواهند بود؛ بنابراین جهت افشای مقدار محرمانه کاربر P_i کافی است، مقدار b_i محاسبه شود؛ اما ساختار شبکه وتوی گمنام [25] تضمین می‌کند که امکان محاسبه مقدار b_i در تبانی جزئی وجود ندارد؛ بنابراین

(جدول-۱): مقایسه پروتکل Frequent-sum با کارهای پیشین (m: تعداد داده‌های هر کاربر، n: تعداد کاربران)
(Table-1): Comparing Frequent-sum with previous works (m: number of inputs of each user, n: number of users)

محرمانگی حاصل جمع	هزینه ارتباطی به‌ازای m تکرار (بیت)	هزینه محاسباتی به‌ازای m تکرار (نمارسانی)	هزینه ارتباطات به‌ازای ۱ بار اجرای پروتکل (بیت)	هزینه محاسبات به‌ازای ۱ بار اجرای پروتکل (نمارسانی)	امنیت در برابر تباری	کانال امن	
×	$mn^2 [\log p^2]$	$O(mn^2)$	$n^2 [\log p^2]$	$O(n^2)$	$n - 2$	×	جانگ و همکاران، 2015 [22]
✓	$6mn [\log N^2]$	$O(mn)$	$6n [\log N^2]$	$O(n)$	$n - 2$	×	عاشوری و همکاران، 2016 [23]
×	$2mn(n - 1) [\log p]$	$O(mn^2)$	$2n(n - 1) [\log p]$	$O(n^2)$	$n - 2$	×	مهنار و همکاران، 2017 [24]
✓	$(4n + mn) [\log p^2]$	$O(n)$	$(4n + 1n) [\log p^2]$	$O(n)$	$n - 2$	×	پروتکل پیشنهادی (Frequent-sum)

کانال ناامن استفاده می‌کند، این پروتکل را با راه کارهای [22]، [23] و [24] مقایسه خواهیم کرد. نتایج مقایسه در جدول (۱) آمده است.

راه کار مقاله [22] به کانال امن نیاز ندارد؛ اما از محاسبات نماسانی استفاده می‌کند و به‌ازای هر کاربر سه نماسانی و برای n کاربر هزینه عملیات $3n$ نماسانی است؛ اما در برابر تباری جزئی دو کاربر امن نیست. اگر بخواهیم در برابر تباری جزئی تا سطح $n - 2$ نفر امن باشد، هزینه محاسباتی به‌ازای هر کاربر $(n - 2)$ نماسانی و به‌ازای n کاربر از مرتبه $O(n^2)$ نماسانی می‌شود و هزینه ارتباطی به‌ازای هر کاربر $(n - 2) [\log p^2]$ و به‌ازای n کاربر از مرتبه $O(n^2)$ می‌شود؛ به‌علاوه دصورت m بار تکرار پروتکل هزینه محاسباتی $O(mn^2)$ نماسانی و هزینه ارتباطی $O(mn^2) [\log p^2]$ بیت خواهد شد.

در راه کار [23] secure-sumv-2 پیمانه محاسباتی N^2 است که عدد مرکب است و به‌ازای m بار تکرار پروتکل هزینه محاسباتی $O(nm)$ نماسانی است.

در راه کار [24] به‌ازای یک‌بار اجرای پروتکل، هزینه محاسباتی برابر با $n(n - 1)$ عملیات رمزگذاری و $n(n - 1)$ عملیات رمزگشایی است. با فرض استفاده از سامانه رمز الجمال، هزینه محاسباتی این روش برابر با $6n(n - 1)$ نماسانی و از مرتبه $O(n^2)$ خواهد بود؛ هزینه ارتباطی این روش برابر با $2n(n - 1) [\log p]$ بیت و از مرتبه $O(n^2)$ است.

پروتکل Frequent-sum به‌ازای هر کاربر پنج نماسانی و به‌ازای n کاربر $5n$ نماسانی است. بنابراین تعداد داده‌های محرمانه کاربر بر روی هزینه محاسباتی پروتکل تأثیری ندارد و این هزینه مستقل از تعداد داده محرمانه هر کاربر یعنی m است. درواقع پروتکل یک‌بار اجرا می‌شود و مجموع m داده متناظر اعضای گروه را محاسبه می‌کند؛ به‌طوری هزینه محاسباتی نماسانی‌های انجام‌شده کاربر ثابت باقی می‌ماند.

۶- مقایسه

در این بخش به مقایسه پروتکل پیشنهادی و راه کارهای پیشین پرداخته می‌شود. برتری اصلی پروتکل Frequent-sum، انجام جمع چندسویه امن با قابلیت تکرار، بدون نیاز به کانال امن، به‌صورت کارا و بدون وابستگی هزینه محاسباتی به m (تعداد داده‌های محرمانه هر کاربر) است.

راه کارهای ارائه‌شده در مقالات [2، 13-21] به کانال امن نیاز دارند. در این مقالات به‌دلیل فرض وجود کانال امن از میزان محاسبات کاسته شده است و اعضا فقط عملیات جمع انجام می‌دهند. در این مقالات برای مقابله با تباری جزئی هزینه محاسباتی و ارتباطی افزایش می‌یابد و از مرتبه $O(n^2)$ می‌شود و درصورت m بار تکرار، عمل جمع امن توسط n کاربر هزینه ارتباطی $O(mn^2)$ و هزینه محاسباتی $O(mn^2)$ عمل جمع می‌شود. با توجه به این که پروتکل Frequent-sum از

- [4] H. Kaur, N. Kumar and S. Batra, "An efficient multi-party scheme for privacy preserving collaborative filtering for healthcare recommender system", *Future Generation Computer Systems*, 2018.
- [5] M. Ashouri-Talouki, A. Baraani-Dastjerdi and A. A. Selçuk, "GLP: A cryptographic approach for group location privacy", *Computer Communications*, vol. 35, pp. 1527-1533, 2012.
- [6] M. Ashouri-Talouki, A. Baraani-Dastjerdi and A. A. Selçuk, "The Cloaked-Centroid protocol: location privacy protection for a group of users of location-based services", *Knowledge and Information Systems*, vol. 45, pp. 589-615, 2015.
- [7] M. Ashouri-Talouki, A. Baraani-Dastjerdi and A. A. Selçuk, "Preserving location privacy for a group of users", *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 21, pp. 1857-1870, 2013.
- [8] Y. Wu, K. Wang, Z. Zhang, W. Lin, H. Chen and C. Li, "Privacy Preserving Group Nearest Neighbor Search", In *Proceedings of the 21st International Conference on Extending Database Technology (EDBT)*, 2018.
- [9] S. Li, K. Xue, Q. Yang and P. Hong, "PPMA: Privacy-preserving multisubset data aggregation in smart grid", *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 462-471, 2018.
- [10] M. Joye, "Cryptanalysis of a privacy-preserving aggregation protocol", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 693-694, 2017.
- [11] Y. Zhang, Q. Chen and S. Zhong, "Efficient and Privacy-Preserving Min and k -th Min Computations in Mobile Sensing Systems", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 9-21, 2017.
- [12] Y. Mo and R. M. Murray, "Privacy preserving average consensus", *IEEE Transactions on Automatic Control*, vol. 62, pp. 753-765, 2017.
- [13] R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k -Secure Sum Protocol", *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 6, pp. 184-188, 2009.
- [14] R. Sheikh, B. Kumar and D. K. Mishra, "A Distributed k -Secure Sum Protocol for Secure Multi-Party Computations", *Journal of Computing*, vol. 2, no. 3, 2010.
- [15] R. Sheikh, B. Kumar and D. K. Mishra, "Changing Neighbors k -Secure Sum Protocol for Secure Multi-Party Computation", *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 7, pp. 239-243, 2010.
- [16] M. Jangde, M. S. Chandel and M. K. Mishra, "Hybrid Technique For Secure Sum Protocol".

به‌ازای m بار تکرار پروتکل، هزینه محاسباتی $O(mn^2)$ نامرسانی و هزینه ارتباطی $O(mn^2)[\log p]$ بیت است.

در پروتکل Frequent-sum، به‌ازای یک‌بار انجام جمع چندسویه امن، بدون نیاز به کانال امن، هزینه محاسباتی برای n کاربر، $5n$ نامرسانی و $O(n)$ عمل جمع است و در برابر تبانی جزئی تا سطح $n - 2$ نفر امن است. پیمانۀ محاسباتی p^2 است به‌طوری‌که p یک عدد اول است. در صورت تکرار برای m بار جمع چندسویه امن، تعداد عملیات نامرسانی ثابت باقی مانده و برابر $5n$ نامرسانی است؛ اما واضح است که n کاربر باید به‌ازای هر بار انجام جمع چندسویه امن، عملیات جمع را انجام دهند، بنابراین برای m بار تکرار جمع چندسویه امن هزینه $O(n \times m)$ عمل جمع حاصل می‌شود. بنابراین هزینه محاسباتی پروتکل Frequent-sum به‌ازای m بار تکرار، $O(n)$ نامرسانی و $O(n \times m)$ جمع است. هزینه ارتباطی $O(nm)[\log p^2]$ بیت است.

۷- نتیجه‌گیری

در این مقاله یک پروتکل کارا جهت محاسبۀ جمع چندسویه امن در مدل شبه‌درست کار و با فرض کانال ناامن ارائه شده است. پروتکل ارائه‌شده قابلیت m بار تکرار را بدون افزایش هزینه ارتباطی و محاسباتی و بدون کاهش امنیت کاربران دارد. به‌علاوه محرمانگی نتایج حاصل جمع نیز حفظ می‌شود و در برابر تبانی جزئی تا سطح $n - 2$ نفر امن است. نتایج ارزیابی نشان می‌دهد، پروتکل پیشنهادی نسبت به پروتکل‌های موجود، امنیت و کارایی بالاتری دارد. لازم به ذکر است که راه‌کار این مقاله یک ایده کلی جهت حفظ کارایی پروتکل است و ممکن است در کاربردهای مختلف جهت حفظ امنیت کاربران، نیاز به بهبودهایی داشته باشد.

8- References

۸- مراجع

- [1] A. C. Yao, "Protocols for Secure Computations", *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*. Chicago: IEEE . 1982. pp. 160-164.
- [2] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin and M. Y. Zhu, "Tools for Privacy Preserving Distributed Data Mining", *ACM SIGKDD Explorations Newslette*, volume 4, pp. 28-34. 2002.
- [3] M. Ashouri-Talouki and A. Baraani-Dastjerdi, "Anonymous Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks", *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, pp. 361-368, 2014.



شادیه عزیزی مدرک کارشناسی مهندسی فناوری اطلاعات را در سال ۱۳۹۱ از دانشگاه کردستان اخذ کرد و از سال ۱۳۹۳ دانشجوی کارشناسی ارشد دانشگاه اصفهان در رشته مهندسی فناوری اطلاعات گرایش

امنیت اطلاعات است. زمینه‌های پژوهشی مورد علاقه ایشان: استخراج قوانین انجمنی از پایگاه داده‌ها، حفظ حریم مکانی در خدمات مبتنی بر مکان، کنترل دسترسی و پروتکل‌های امنیتی.

نشانی رایانامه ایشان عبارت است از:

sh.azizi93@eng.ui.ac.ir



مأده عاشوری تلوقی مدرک کارشناسی مهندسی کامپیوتر را در سال ۱۳۸۲ و مدرک کارشناسی ارشد را در سال ۱۳۸۵ و مدرک دکترا را نیز در سال ۱۳۹۱ از دانشگاه اصفهان اخذ کرده و در حال حاضر

عضو هیئت علمی و استادیار دانشکده کامپیوتر دانشگاه اصفهان است. زمینه‌های پژوهشی مورد علاقه ایشان، امنیت شبکه‌های موبایل، گمنامی و حریم خصوصی کاربران و پروتکل‌های امنیتی است.

نشانی رایانامه ایشان عبارت است از:

m.ashouri@eng.ui.ac.ir



حمید ملا مدرک کارشناسی مهندسی کامپیوتر را در سال ۱۳۸۲ و مدرک کارشناسی ارشد را در سال ۱۳۸۴ و مدرک دکترا را نیز در سال ۱۳۸۹ از دانشگاه صنعتی اصفهان اخذ کرده و در حال حاضر

عضو هیئت علمی و استادیار دانشکده کامپیوتر دانشگاه اصفهان است. زمینه‌های پژوهشی مورد علاقه ایشان، طراحی و تحلیل رمزهای قالبی، امضای دیجیتال و پروتکل‌های امنیتی است.

نشانی رایانامه ایشان عبارت است از:

h.mala@eng.ui.ac.ir

World of Computer Science and Information Technology Journal (WCSIT), vol. 1, pp. 198-201, 2011.

- [17] I. Jahan, N. N. Sharmy, S. Jahan, F. A. Ebha and N. J. Lisa, "Design of a Secure Sum Protocol using Trusted Third Party System for Secure Multi-Party Computations". *6th International Conference on Information and Communication Systems (ICICS)* IEEE, pp. 136-141, 2015.
- [18] Z. Youwen, H. Liusheng, Y. Wei and Y. Xing, "Efficient Collusion-Resisting Secure Sum Protocol". *Chinese Journal of Electronics*, pp. 407-413, 2011.
- [19] J. Rautaray and R. Kumar, "Distributed Database RK-Secure Sum Protocol". *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, vol. 2, pp. 559-562, March 2013.
- [20] J. Rautaray and R. Kumar, "Distributed RK-Secure Sum Protocol for Privacy Preserving". *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 9, pp. 49-52, Feb. 2013.
- [21] J. Rautaray, R. Kumar and G. Bajpai, "Modified Distributed Rk Secure Sum Protocol". *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, vol. 2, pp. 734-736, March 2013.
- [22] T. Jung and X. Yang Li, "Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel", *IEEE Transactions on Dependable and secure computing*, pp. 45-57, 2015.
- [23] M. Ashouri-Talouki and A. Baraani-Dastjerdi, "Cryptographic collusion-resistant protocols for secure sum", *International Journal of Electronic Security and Digital Forensics*, vol. 9, pp. 19-34, 2017.
- [24] S. Mehnaz, G. Bellala and E. Bertino, "A Secure Sum Protocol and Its Application to Privacy-preserving Multi-party Analytics". In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, pp. 219-230, 2017.
- [25] F. Hao and P. Zielinski, "A 2-Round Anonymous Veto Protocol". In *Security Protocols*, Springer Berlin Heidelberg, pp. 202-211, 2009.
- [26] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system". In *Advances in Cryptology*. Springer-Verla, pp. 275-286, 2006.