پروتکل کارا برای جمع چندسویهٔ 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 سویهٔ امن، گروهی از کاربران، نتیجهٔ یک تابع ریاضی را بر روی دادهٔ محرمانهٔ خود، با حفظ حریم خصوصی داده‌ها محاسبه می‌کنند. از موارد پرکاربرد محاسبات چندسویهٔ امن، جمع چندسویهٔ امن است که هدف آن انجام عملیات جمع بر روی دادهٔ محرمانهٔ کاربران است. در برخی کاربردها ممکن است، هر عضو چندین مقدارِ محرمانه داشته و هدف، محاسبهٔ مجموعِ داده‌های متناظر باشد؛ در این صورت لازم است، پروتکلِ جمعِ چندسویهٔ امن، چندین‌بار برای محاسبهٔ مجموع داده‌های گروه تکرار شود. در این پژوهش، مسئلهٔ جمع چندسویهٔ امن با قابلیت تکرار، بدون افزایش هزینهٔ محاسباتی و ارتباطی، مورد توجه قرار گرفته است؛ در این مسئله هر کاربر چندین مقدار محرمانه دارد و اعضا قصد دارند مجموع داده‌های محرمانهٔ خود را به‌صورت نظیربه‌نظیر محاسبه کنند؛ به‌طوری‌که محرمانگی داده‌های هر کاربر حفظ شود. در این مقاله یک پروتکل کارا جهت محاسبهٔ جمع چندسویهٔ امن با قابلیت تکرار در مدل شبه‌درست‌کار ارائه شده است. راه‌کار 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 هزینهٔ محاسبات و ارتباطات بسیار کاراست.

واژگان کلیدی: جمع چندسویهٔ امن، کانال ناامن، تبانی جزئی، مدل شبه‌درست‌کار.

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 $\{P_1, P_2, .., P_n\}$ 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 $V_i =< d_{i1} + r_i, d_{i2} + r_i, \dots, d_{im} +$**

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

[DOI: 10.29252/jsdp.15.4.31]

$r_i >$. After it, P_i computes the vector $V =< \sum_{i=1}^{n} d_{i1} + \sum_{i=1}^{n} r_i , \sum_{i=1}^{n} d_{i2} + \sum_{i=1}^{n} r_i , \dots , \sum_{i=1}^{n} d_{im} + \sum_{i=1}^{n} r_i >$, 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 $K = K_i = (g^{e_{i-1}})^{ne_i} . t_i^{n-1} . t_{i+1}^{n-2} \dots t_{i-2} (mod\ p^2)$; $g^{a_i b_i}$ 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_is results in canceling the AV-net mask and getting the value of $\prod_{i=1}^{n} w_i = (1 + p \sum_{i=1}^{n} r_i) K\ mod\ p^2$. 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:

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

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 چندسویهٔ امن، گروهی از کاربران قصد دارند نتیجهٔ محاسبهٔ تابع f را بر روی مقادیر محرمانهٔ خود به‌دست آورند؛ به‌طوری‌که درنهایت هر کاربر فقط از نتیجهٔ تابع و دادهٔ محرمانهٔ خود اطلاع داشته باشد. محاسبات چندسویهٔ امن نخستین‌بار توسط *یائو* تحت عنوان مسئله میلیونرها مطرح شد [1]: در این مسئله دو میلیونر بدون افشای میزان ثروت خود تعیین می‌کنند کدام‌یک ثروتمندتر است. تاکنون توابع مختلفی در قالب محاسبات چندسویهٔ امن ارائه شده است. در این مقاله جمع چندسویهٔ امن درنظرگرفته شده که در آن تابع f برابر مجموع مقادیر محرمانهٔ اعضای گروه است.

جمع چندسویهٔ امن در موارد متعددی مانند استخراج قوانین انجمنی در پایگاه داده [2]، الگوریتم‌های رأی‌گیری الکترونیکی[3]، الگوریتم‌های پالایش گروهی در سامانه‌های پیشنهاددهنده [4]، یافتن نزدیک‌ترین همسایه به گروهی از افراد در خدمات مبتنی بر مکان [5-8]، تجمیع داده در شبکهٔ هوشمند برق [9] و بسیاری مسائل دیگر [10-12] کاربرد دارد. یکی از نیازهایی که در استفاده از جمع چندسویهٔ امن به‌وجود می‌آید، نیاز به تکرارکردن پروتکل جهت محاسبهٔ حاصل جمع‌های مقادیر محرمانهٔ مختلف است. به‌عنوان مثال در کاربردهای مبتنی بر مکان، گروهی از افراد را در نظر بگیرید که قصد دارند، جلسه‌ای را در نزدیک‌ترین مکان به گروه از بین مکان‌های نامزد برگزار کنند، به‌طوری‌که حریم مکانی اعضای گروه محافظت شود. در این‌صورت لازم است، مجموع فاصلهٔ افراد از هر یک از مکان‌های نامزد به‌طور امن محاسبه شده و مکان متناظر با کم‌ترین مجموع فاصله به‌عنوان محل جلسه انتخاب شود. در این مسئله و مسائل مشابه لازم است پروتکل جمع چندسویهٔ امن به‌ازای تعداد مقادیر محرمانهٔ کاربران تکرار شود. با افزایش تعداد مقادیر محرمانهٔ کاربران، هزینهٔ محاسبات و ارتباطات پروتکل افزایش می‌یابد و منجر به ناکارآمدی پروتکل می‌شود. در این مقاله راه‌کاری کارا برای جمع چندسویهٔ امن با قابلیت تکرار ارائه شده است. این راه‌کار علاوه‌بر این‌که به‌ازای یک‌بار اجرا نسبت به راه‌کارهای پیشین کاراتر است، مسئلهٔ تکرار پروتکل را نیز درنظر می‌گیرد و راه‌کاری ارائه می‌دهد که هزینهٔ محاسبات هر کاربر مستقل از تعداد داده‌های محرمانه کاربران باقی بماند.

راه‌کارهای جمع چندسویهٔ امن براساس فرض کانال ارتباطی به دو دستهٔ: راه‌کارهای با فرض کانال امن و ناامن تقسیم می‌شوند. در راه‌کارهای با فرض کانال امن، کانال ارتباطی بین اعضای گروه غیر قابل شنود است و درصورت

[DOI: 10.29252/jsdp.15.4.31]

ارسال پیام در کانال، فقط گیرنده از محتوای آن مطلع می‌شود. در راه‌کارهای با فرض کانال ناامن، کانال ارتباطی بین اعضای گروه، قابل شنود توسط مهاجم و جهت محرمانه‌ماندن پیام‌های ارتباطی نیاز به روش‌های رمزنگاری است، از این‌رو راه‌کارهای با فرض کانال ناامن پرهزینه‌تر و امن‌تر از راه‌کارهای با فرض کانال امن هستند. در راه‌کار پیشنهادی کانال ارتباطی به‌صورت ناامن درنظرگرفته می‌شود.

در محاسبات چندسویهٔ امن دو مدل مهاجم وجود دارد: مدل شبه‌درست‌کار و مدل بدخواه. در مدل شبه‌درست‌کار، اعضای گروه از روال پروتکل تبعیت کرده اما جهت به‌دست‌آوردن اطلاعاتی راجع به دادهٔ محرمانهٔ سایر اعضای گروه کنجکاوی می‌کنند؛ اما در مدل بدخواه، اعضا از روال پروتکل تبعیت نمی‌کنند و به‌دلخواه رفتار می‌کنند. در این مقاله مدل مهاجم شبه‌درست‌کار درنظرگرفته شده است.

بنابراین در این مقاله راه‌کاری کارا جهت جمع چندسویهٔ امن با قابلیت تکرار و با فرض کانال ناامن در مدل شبه‌درست‌کار ارائه شده است. راه‌کار ارائه‌شده در برابر حملهٔ تبانی جزئی تا سطح $n-2$ نفر امن است. به‌علاوه در این راه‌کار به‌ازای هرچندبار تکرار، محرمانگی نتایج حاصل‌جمع‌های محاسبه‌شده حفظ می‌شود و فقط اعضای گروه قادر به محاسبهٔ حاصل‌جمع‌ها هستند.

ساختار مقاله به‌صورت زیر است: در بخش دوم مسألهٔ جمع چندسویهٔ امن به‌صورت فرمال بیان می‌شود. در بخش سوم، کارهای مرتبط با جمع چندسویهٔ امن با فرض کانال امن و کانال ناامن مرور می‌شوند. در بخش چهارم روش‌های استفاده‌شده در این مقاله به‌اختصار توضیح داده می‌شود؛ در بخش پنجم، راه‌کار پیشنهادی را شرح داده و امنیت و کارایی آن تحلیل می‌شود؛ به‌منظور مقایسه، در بخش ششم پروتکل پیشنهادی با راه‌کارهای پیشین مقایسه می‌شود. در بخش هفتم مقاله جمع‌بندی می‌شود.

۲- تعریف مسئله

فرض کنید n کاربر $\{P_1, P_2, \dots, P_n\}$ وجود دارند و هر کاربر P_i، مجموعه داده‌های محرمانهٔ $\{d_{i1}, d_{i2}, \dots, d_{im}\}$ را در اختیار دارد. اعضای گروه قصد دارند با m مرتبه تکرار جمع چندسویهٔ امن، حاصل‌جمع مقادیر محرمانه و متناظر خود را محاسبه کنند؛ به عبارت دیگر پروتکل پیشنهادی باید مقدار $(\sum_{i=1}^{n} d_{ij})$ را به‌ازای $j = 1,2,\dots,m$ به‌طور امن محاسبه کند؛ به‌طوری‌که هر کاربر P_i فقط از دادهٔ محرمانهٔ خود یعنی d_{ij} و $\sum_{i=1}^{n} d_{ij}$ اطلاع داشته باشد. در پروتکل پیشنهادی فرض می‌شود، اعضای گروه به یک کانال عمومی و احراز اصالت‌شده دسترسی دارند؛ این فرض یک نیاز اولیه و کلی در محاسبات چندسویهٔ امن است [1]. راه‌کار پیشنهادی نیازهای امنیتی زیر را برآورده می‌کند:

۱- تأمین محرمانگی داده‌های کاربران از دید دیگر کاربران گروه و نیز مهاجمان خارجی؛

۲- تأمین محرمانگی نتایج مجموع داده‌های کاربران از دید مهاجمان خارجی؛

۳- امنیت در برابر تبانی جزئی کاربران تا سطح $n-2$ نفر

۳- کارهای مرتبط

در این بخش راه‌کارهای جمع چندسویهٔ امن در دو دستهٔ با فرض وجود کانال امن و ناامن بررسی می‌شوند.

۳-۱- راه‌کارهای با فرض وجود کانال امن

کلیفتون و همکاران در راستای داده‌کاوی راه‌کاری برای جمع چندسویهٔ امن ارائه دادند که در آن اعضا در چیدمان حلقه قرار می‌گیرند [2]. عضو نخست چیدمان دادهٔ محرمانهٔ خود را با یک عددتصادفی جمع و برای عضو دوم حلقه می‌فرستد؛ او نیز مقدار محرمانهٔ خود را با مقدار دریافتی جمع کرده و برای عضو بعدی می‌فرستد؛ روال تا کامل‌شدن حلقه ادامه دارد؛ سپس عضو آغازگر با کم‌کردن مقدار تصادفی اولیه، مجموع مقادیر محرمانه را محاسبه و برای اعضا می‌فرستد این راه‌کار در برابر تبانی دو نفر امن نیست. راه‌کار بعدی توسط *شیخ* و همکاران ارائه شد [13] که در آن هر عضو دادهٔ محرمانهٔ خود را به n بلوک تقسیم و به‌ازای هر بلوک روال راه‌کار کلیفتون و همکاران طی می‌شود؛ اما این راه‌کار در برابر تبانی جزئی دو نفر امن نیست. بنابراین در راه‌کار بعدی [14] عضو دوم چیدمان اولیه در هر دور با عضو کناری جابه‌جا می‌شود، این راه‌کار نیز در برابر تبانی جزئی تا سطح $n-2$ نفر امن نیست. پس در ارتقای بعدی راه‌کار شیخ و همکاران [15] هر کاربر دادهٔ محرمانهٔ خود را به n بلوک تقسیم و بین اعضا توزیع می‌کند؛ به‌طوری‌که هرکاربر n بلوک داشته و یکی از آن‌ها متعلق به اوست. بدین طریق این راه‌کار در برابر تبانی جزئی تا سطح $n-2$ نفر امن است.

در ادامه راه‌کارهای [16] و [17] نیز ارائه شدند که هزینهٔ ارتباطی کم‌تری دارند؛ اما به طرفِ سومِ موردِ اعتماد نیاز دارند؛ سپس یوون و همکاران راه‌کاری را با دو مرحله ارائه دادند [18] که در مرحلهٔ نخست هر عضو اعداد تصادفی را انتخاب و در بین اعضا به‌طور محرمانه توزیع می‌کند. گیرنده عدد تصادفی را از دادهٔ محرمانهٔ خود کم یا به آن اضافه می‌کند و فقط به فرستده اطلاع می‌دهد تا عکس عمل انجام‌شده را

[DOI: 10.29252/jsdp.15.4.31]

روی دادهٔ محرمانهٔ خود انجام دهد. در مرحلهٔ دوم روال راه‌کار کلیفتون طی می‌شود. این راه‌کار با افزایش هزینهٔ ارتباطی در برابر تبانی جزئی تا سطح n-2 نفر امن است.

سپس *راوتاری* و همکاران راه‌کاری را در چیدمان باس ارائه دادند [19] که هر عضو، دادهٔ محرمانهٔ خود را به n بلوک تقسیم و به‌ازای هر دور روال راه‌کار کلیفتون طی می‌شود؛ اما این راه‌کار در برابر تبانی جزئی دونفر امن نیست. بنابراین در راه‌کار بعدی راوتاری و همکاران [20] کاربر نخست چیدمان اولیه در هردور با سایر اعضا جابه‌جا می‌شود؛ این راه‌کار در برابر تبانی جزئی امن نیست؛ در راه‌کار بعدی [21] هر کاربر پس از تقسیم دادهٔ محرمانه به n بلوک آن را در بین اعضا توزیع می‌کند و مابقی روال مانند [19] طی می‌شود. این راه‌کار در برابر تبانی جزئی تا سطح $n-2$ نفر امن است.

۲-۳- راه‌کارهای با فرض کانال ناامن

جانگ و همکاران راه‌کاری برای جمع چندسویهٔ امن بدون نیاز به کانال امن ارائه دادند [22]. در این راه‌کار عدد نخست بسیار بزرگ p انتخاب و p^2 به‌عنوان پیمانهٔ محاسباتی انتخاب می‌شود، اعضا در چیدمان حلقه قرار گرفته و هر عضو با انجام عمل نمارسانی، مقداری را برای گروه می‌فرستد و سپس با کمک مقادیر دریافتی از دو عضو کناری خود در حلقه مقدار محرمانهٔ R_i را محاسبه و با ضرب دادهٔ محرمانهٔ خود در R_i آن را مخفی و پخش همگانی می‌کند. با ضرب مقادیر ارسالی اعضای گروه، مقادیر R_i حذف و مجموع داده‌های محرمانه محاسبه می‌شود. این راه‌کار در برابر تبانی جزئی دو نفر امن نیست و به‌منظور افزایش امنیت در برابر تبانی جزئی تا سطح $n-2$ نفر هزینهٔ عملیات $O(n^2)$ نمارسانی و درصورت m بار تکرار پروتکل هزینه از مرتبهٔ $O(mn^2)$ نمارسانی می‌شود. به‌علاوه محرمانگی حاصل‌جمع نیز حفظ نمی‌شود.

راه‌کار بعدی توسط *عاشوری* و همکاران بر مبنای شبکهٔ وتوی گمنام و پروتکل توافق کلید Burmester-Desmedt (BD) ارائه شد که در آن سه پروتکل ارائه شده است [23]. در این راه‌کار عدد مرکب $N = p_1 p_2$ انتخاب می‌شود که تجزیهٔ N برای همه مجهول است. در پروتکل نخست، یعنی securesum-v1 اعضا شبکهٔ وتوی گمنام راه‌اندازی می‌کنند و هر عضو با ضرب دادهٔ محرمانه در مقادیر شبکهٔ وتوی گمنام، دادهٔ محرمانهٔ خود را مخفی و پخش همگانی می‌کند؛ با ضرب مقادیر گروه، ماسک شبکه از بین رفته و حاصل‌جمع آشکارا محاسبه می‌شود. در پروتکل دوم یعنی securesum-v2 اعضا علاوه‌بر راه‌اندازی شبکهٔ وتوی گمنام، براساس روش BD، کلید جلسه به اشتراک می‌گذارند و پس از ضرب دادهٔ محرمانه در مقادیر شبکه و سهم هر کاربر از کلید آن را پخش همگانی می‌کنند. با ضرب مقادیر گروه حاصل‌جمع رمزشده حاصل می‌شود. در پروتکل سوم تحت عنوان securesum-v3 با هزینهٔ محاسباتی پایین‌تر حاصل‌جمع به‌صورت رمزشده محاسبه می‌شود. 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 راه‌کار عدد مرکب N وجود دارد و درصورت m بار تکرار هزینه $O(nm)$ نمارسانی می‌شود.

مِهناز و همکاران با استفاده از زیرساخت کلید عمومی روشی جهت محاسبه مجموع داده‌های محرمانه به‌صورت 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 به‌صورت رمزشده با کلید عمومی یکی از اعضای گروه به‌صورت منفرد ارسال می‌کند، به‌طوری‌که هر عضو تنها یک بخش از دادهٔ تصادفی هر عضو دیگر گروه را در اختیار دارد؛ سپس هر عضو گروه مجموع داده‌های ارسالی خود را محاسبه و (P_{iS}). سپس داده‌های دریافتی از $n-1$ عضو دیگر گروه را رمزگشایی کرده و مجموع داده‌های دریافتی را نیز محاسبه می‌کند (P_{iR}). آن‌گاه هر عضو، مجموع دادهٔ محرمانه خود، P_{iS} و P_{iR} را محاسبه و برای مدیر گروه ارسال می‌کند. مدیر مجموع داده‌های دریافتی را که برابر با مجموع داده‌های محرمانه است، محاسبه کرده و به اعضا اطلاع می‌دهد. واضح است که این روش هزینهٔ محاسباتی زیادی را به اعضای گروه تحمیل می‌کند ($n-1$ عمل رمزگذاری و $n-1$ عمل رمزگشایی برای هر عضو). این پروتکل در مقابل تبانی $n-2$ نفر ایمن است.

۴- روش‌های مورد استفاده

در راه‌کار ارائه‌شده در این مقاله از پروتکل‌های شبکهٔ وتوی گمنام [25] و اشتراک کلید جلسه به روش Burmester–Desmedt (BD) [26] و از خاصیت پیمانه‌ای رابطهٔ (۱) [22] استفاده می‌شود که در آن p عدد اول است:

$$\prod_{i=1}^{n}(1+d_i p) = \left(1 + p\sum_{i=1}^{n} d_i\right) \bmod p^2 \qquad (۱)$$

در ادامه پروتکل شبکهٔ وتوی گمنام و پروتکل توافق کلید BD به‌اختصار شرح داده می‌شوند.

[DOI: 10.29252/jsdp.15.4.31]

۴-۱- پروتکل شبکهٔ وتوی گمنام

پروتکل شبکهٔ وتوی گمنام توسط *هائو* و همکاران برای حل مسئلهٔ وتوی گمنام ارائه شد [25]. در این پروتکل، دو عدد اول بسیار بزرگ p و q انتخاب می‌شوند؛ به‌طوری‌که $q|\ p-1$. گروه حلقوی G از مرتبه q و با مولد g درنظر گرفته می‌شود. n کاربر داریم و مقادیر (G,g,p,q) آشکار هستند. پروتکل شامل دو مرحله است: در مرحلهٔ 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 باتوجه 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 مرحلهٔ دوم، هر عضو مقدار $g^{c_i b_i}$ را پخش همگانی می‌کند؛ به‌طوری‌که مقدار c_i برابر a_i است، اگر کاربر وتو نکند و درغیراین‌صورت c_i یک عدد تصادفی از گروه G است؛ سپس هر کاربر مقادیر $g^{c_i b_i}$ کل کاربران درهم ضرب می‌کند؛ در صورتی‌که کل کاربران در وتو شرکت نکنند، حاصل‌ضرب برابر یک خواهد شد $(\prod_i g^{c_i b_i} = g^{\sum_{i=1}^{n} a_i b_i} = 1)$ و درصورتی‌که دست‌کم یک کاربر در وتو شرکت کند، حاصل‌ضرب مخالف یک خواهد شد $(\prod_i g^{c_i b_i} \neq 1)$.

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

هدفِ پروتکل توافق کلید (BD)، برقراری یک کلید تازه و برروی یک کانال امن در بین گروهی از افراد است؛ به‌طوری‌که تنها، اعضایِ گروه، کلید تشکیل‌شده را می‌دانند و هیچ کس دیگری امکان ساخت یا کشف کلید را ندارد. در راه‌کار *برمستر* و همکاران دو عدد نخست بسیار بزرگ p,q و $g \in z_p$ انتخاب می‌شوند به‌طوری‌که 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 رابطهٔ $K_i = (g^{e_{i-1}})^{ne_i}.\, t_i^{n-1}.\, t_{i+1}^{n-2}.\ldots.\, t_{i-2}$ محاسبه می‌کند. کلید مشترک محاسبه‌شده برای کل کاربران برابر $K = g^{e_1e_2+e_2e_3+\cdots+e_ne_1}$ خواهد بود.

۵- راه‌کار پیشنهادی

دو عدد نخست بسیار بزرگ p و q به‌عنوان پیمانه اعداد انتخاب می‌شوند؛ به‌طوری 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 مولد $g = g_0^p \bmod p^2$ درنظرگرفته می‌شوند. بنابراین اعضای گروه بر روی گروه حلقوی G از مرتبهٔ q توافق کرده‌اند. پروتکل پیشنهادی با نام Frequent-sum دارای سه مرحلهٔ زیر است که در شکل (۱) نشان داده شده است:

- مرحلهٔ نخست: ارسال مقادیر توسط اعضای گروه و محاسبهٔ مجموع مقادیر ارسالی
- مرحلهٔ دوم: راه‌اندازی شبکهٔ وتوی گمنام و اشتراک کلید جلسه
- مرحلهٔ سوم: محاسبهٔ نتایج حاصل‌جمع‌ها

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

$$\boldsymbol{V_i} =< \boldsymbol{d_{i1}} + \boldsymbol{r_i}, \boldsymbol{d_{i2}} + \boldsymbol{r_i}, \ldots, \boldsymbol{d_{im}} + \boldsymbol{r_i} > \qquad (۲)$$

حال، هر عضو گروه مقادیر ارسالی کل اعضا را با یکدیگر جمع و بردار حاصل‌جمع 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.

$$V =< \sum_{i=1}^{n} d_{i1} + \sum_{i=1}^{n} r_i, \sum_{i=1}^{n} d_{i2} + \sum_{i=1}^{n} r_i, \ldots, \sum_{i=1}^{n} d_{im} + \sum_{i=1}^{n} r_i > \qquad (۳)$$

در مرحلهٔ دوم، هر عضو P_i دو مقدار تصادفی $a_i, e_i \in_R Z_q$ انتخاب می‌کند و g^{a_i} را به‌منظور برقراری شبکه وتوی گمنام و مقدار g^{e_i} را در راستای تشکیل کلید مشترک پخش‌همگانی 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 محاسبهٔ مقدار $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^{n} g^{a_j})$ و کلید مشترک K به‌صورت زیر است:

$$K = K_i = (g^{e_{i-1}})^{(ne_i)}.\, t_i^{(n-1)}.\, t_{i+1}^{(n-2)} \ldots t_{i-2} (mod\ p^2)$$

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

$$\boldsymbol{w_i} = (\boldsymbol{1} + \boldsymbol{r_i p}) \boldsymbol{g^{a_i b_i} g^{e_{i-1} e_i}} \qquad (۴)$$

[DOI: 10.29252/jsdp.15.4.31]

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

Phase 1. Sending users' values

i. $\boldsymbol{P_i \rightarrow *:\ V_i =< d_{i1} + r_i, d_{i2} + r_i, \dots, d_{im} + r_i >}$ where $\boldsymbol{r_i \in_R Z_q}$

ii. $\boldsymbol{P_i}$ computes $\boldsymbol{V =< D_1, D_2, \dots, D_m >=}$
$\boldsymbol{< \sum_{i=1}^{n} d_{i1} + \sum_{i=1}^{n} r_i, \sum_{i=1}^{n} d_{i2} + \sum_{i=1}^{n} r_i, \dots, \sum_{i=1}^{n} d_{im} + \sum_{i=1}^{n} r_i >}$

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

i. $\boldsymbol{P_i \rightarrow *:\ (g^{a_i}, g^{e_i})}$ where $\boldsymbol{a_i, e_i \in_R Z_q}$

ii. $\boldsymbol{P_i \rightarrow *:\ t_i = (g^{e_{i+1}} / g^{e_{i-1}})^{e_i}}$

iii. $\boldsymbol{P_i}$ computes $\boldsymbol{g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^{n} g^{a_j})}$ and $\boldsymbol{K_i \equiv (g^{e_{i-1}})^{ne_i} \cdot t_i^{n-1} \cdot t_{i+1}^{n-2} \cdot \dots \cdot t_{i-2}}$

Phase 3. Finding the results

i. $\boldsymbol{P_i \rightarrow *:\ w_i = (1 + r_i p) g^{e_{i-1}e_i} g^{a_i b_i}}$

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

iii. $\boldsymbol{P_i}$ computes $\boldsymbol{\sum_{i=1}^{n} r_i}$ as follows:
$\boldsymbol{\sum_{i=1}^{n} r_i = \frac{(\prod_{i=1}^{n} w_i) K^{-1} - 1}{p}}$

iv. $\boldsymbol{P_i}$ computes $\boldsymbol{V_{sum} = V - \sum_{i=1}^{n} r_i =< D_1 - \sum_{i=1}^{n} r_i, \dots, D_m - \sum_{i=1}^{n} r_i >=< \sum_{i=1}^{n} d_{i1}, \sum_{i=1}^{n} d_{i2}, \dots, \sum_{i=1}^{n} d_{im} >$

(شکل-۱): مراحل پروتکل پیشنهادی

(Figure-1): sequences of proposed protocol

ساختار w_i شامل مقدار $(1 + r_i p)$، مقدار شبکهٔ وتوی 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:

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

اعضای گروه قادرند نتیجهٔ رابطهٔ (۵) را در K^{-1} ضرب کرده و مقدار $c = (1 + p \sum_{i=1}^{n} r_i)$ و درنتیجه $\sum_{i=1}^{n} r_i = \frac{c-1}{p}$ 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 حاصل‌جمع در بردار V_{sum} محاسبه می‌شود:

$$\boldsymbol{V_{sum} =< \sum_{i=1}^{n} d_{i1}, \sum_{i=1}^{n} d_{i2}, \dots, \sum_{i=1}^{n} d_{im} >} \qquad (۶)$$

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 $g^{a_i b_i}$ محرمانه‌ماندن r_i و درنهایت محرمانه‌بودن d_i است و هدف از $g^{e_{i-1}e_i}$ محرمانه‌بودن مقدار $\sum_{i=1}^{n} r_i$ و درنهایت محرمانه‌بودن حاصل‌جمع $(\sum_{i=1}^{n} d_i)$ است؛ بنابراین فقط اعضای گروه قادر به محاسبهٔ حاصل‌جمع‌ها هستند و مهاجم بیرونی از نتایج حاصل‌جمع مطلع نمی‌شود؛ به‌علاوه دادهٔ محرمانهٔ 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 محاسبهٔ نتایج حاصل‌جمع داده‌های محرمانهٔ کاربران به‌صورت نظیر به نظیر است. در این پروتکل هر عضو P_i عدد تصادفی $\boldsymbol{r_i}$ را انتخاب و با هر کدام از مقادیر محرمانهٔ خود جمع کرده و بردار $\boldsymbol{V_i}$ را تشکیل داده و در گروه ارسال می‌کند؛ بنابراین جهت محاسبهٔ بردار V_{sum}، کافی است مقدار $\boldsymbol{\sum_{i=1}^{n} r_i}$ به‌صورت امن محاسبه شده و از مؤلفه‌های بردار V کم شود؛ بنابراین جهت اثبات درستی پروتکل Frequent-sum کافی است ثابت کنیم در مرحلهٔ سوم، مقدار $\sum_{i=1}^{n} r_i$ به‌درستی محاسبه می‌شود. لم زیر این مسئله را ثابت می‌کند:

لم۱. مرحلهٔ سوم پروتکل Frequent-sum مقدار $\sum_{i=1}^{n} r_i$ را به‌درستی محاسبه می‌کند.

[DOI: 10.29252/jsdp.15.4.31]

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

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

۵-۱- تحلیل امنیت

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

۱) محرمانگی دادهٔ کاربران از دید سایر کاربران و مهاجمان خارجی،

۲) محرمانگی حاصل‌جمع‌ها از دید مهاجمان خارجی

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

در ادامه این سه ویژگی امنیتی پروتکلFrequent-sum بررسی می‌شود.

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

عضو P_i هر دادهٔ محرمانهٔ خود (d_{ij}) را با عدد تصادفی r_i جمع کرده و در بردار V_i، لازم است، مهاجمان جهت افشای مقادیر محرمانهٔ کاربر مقدار r_i و درنتیجه مقدار شبکهٔ 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 کند. مقدار $g^{e_{i-1}e_i}$ را کاربر P_i و P_{i-1} می‌تواند محاسبه کند، اما محاسبهٔ مقدار $g^{a_i b_i}$ نیاز به آگاهی از مقدار a_i دارد که محاسبهٔ آن برای سایر اعضا و مهاجم بیرونی براساس مسئلهٔ سخت DDH غیر ممکن است.

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

در حملهٔ تبانی، مهاجمان جهت کشف داده‌های محرمانهٔ 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 محرمانهٔ 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 محاسبهٔ $g^{e_{i-1}e_i}$ از طریق کاربر P_{i-1} خواهند بود؛ بنابراین جهت افشای مقدار محرمانهٔ کاربر P_i کافی است، مقدار b_i محاسبه شود؛ اما ساختار شبکهٔ وتوی گمنام [25] تضمین می‌کند که امکان محاسبهٔ مقدار b_i در تبانی جزئی وجود ندارد؛ بنابراین مهاجمان قادر به محاسبهٔ b_i و درنتیجه کشف مقدار محرمانهٔ 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 حاصلِ جمع‌ها را حفظ می‌کند.

جهت محاسبهٔ نتایج حاصل‌جمع‌ها، 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 مقالهٔ [26] و سختی مسئلهٔ دیفی هلمن، مهاجمان خارجی قادر به یافتن کلید K نخواهند بود و درنتیجه محرمانگی حاصل‌جمع‌ها تأمین می‌شود. بنابراین فقط اعضای گروه قادر به رمزگشایی $(1+p\sum_{i=1}^{n} r_i)$ و محاسبهٔ $\sum_{i=1}^{n} r_i$ هستند. درنتیجه فقط اعضای گروه حاصل‌جمع‌ها را محاسبه می‌کنند.

۵-۲- تحلیل کارایی

هزینهٔ ارتباطی: در مرحلهٔ نخست، هر عضو گروه برداری با m مؤلفه را محاسبه و پخش همگانی می‌کند؛ هزینهٔ ارتباطی به‌ازای یک کاربر $m\lceil \log p^2 \rceil$ بیت و به‌ازای $\boldsymbol{n}$ کاربر $mn\lceil \log p^2 \rceil$ بیت است. در مرحلهٔ دوم اعضا باید شبکهٔ وتوی گمنام را راه‌اندازی کنند و کلید جلسه را به اشتراک بگذارند؛ بدین منظور هر کاربر P_i باید مقادیر g^{e_i} و g^{a_i} و t_i را برای گروه ارسال کند؛ بنابراین هزینهٔ ارتباطی هر کاربر $3\lceil \log p^2 \rceil$ بیت و برای n کاربر $3n\lceil \log p^2 \rceil$ بیت است. در مرحلهٔ سوم، هر کاربر مقادیر محرمانه خود را به‌کمک مقادیر شبکهٔ 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 هزینهٔ ارتباطی برای یک کاربر $\lceil \log p^2 \rceil$ بیت و برای کل گروه $n\lceil \log p^2 \rceil$ بیت است. درنتیجه، به‌طورکلی هزینهٔ ارتباطی پروتکل Frequent-sum برای یک کاربر $(4+m)\lceil \log p^2 \rceil$ بیت و برای n کاربر $(4n+nm)\lceil \log p^2 \rceil$ بیت است.

هزینهٔ محاسباتی: در مرحلهٔ نخست اعضای گروه m جمع ساده انجام می‌دهند. در مرحلهٔ دوم، شبکهٔ وتوی گمنام راه اندازی می‌کنند و کلید جلسه به اشتراک می‌گذارند؛ بدین منظور هر کاربر جهت محاسبهٔ g^{e_i} و g^{a_i} و t_i و $g^{a_i b_i}$ و K نیاز به 5 عمل نمارسانی 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 مرحلهٔ سوم هر کاربر m عمل ضرب انجام می‌دهد. از آن‌جا که هزینهٔ عمل جمع و ضرب در مقایسه با نمارسانی ناچیز است، فقط هزینهٔ عملیات نمارسانی را درنظر می‌گیریم؛ بنابراین هزینهٔ محاسباتی

[DOI: 10.29252/jsdp.15.4.31]

(جدول-۱): مقایسهٔ 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)

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

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

۶- مقایسه

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

راه‌کارهای 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 تبانی 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 هزینهٔ ارتباطی $O(mn^2)$ و هزینهٔ محاسباتی $O(mn^2)$ عمل جمع می‌شود. با توجه به این‌که پروتکل Frequent-sum از کانال ناامن استفاده می‌کند، این پروتکل را با راه‌کارهای [22]، [23] و [24] مقایسه خواهیم کرد. نتایج مقایسه در جدول (۱) آمده است.

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

در راه‌کار secure-sumv-2 [23] پیمانهٔ محاسباتی N^2 است که N عدد مرکب است و به‌ازای m بار تکرار پروتکل هزینهٔ محاسباتی $O(nm)$ نمارسانی است.

در راه‌کار [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 سامانهٔ رمز الجمال، هزینه محاسباتی این روش برابر با $6n(n-1)$ نمارسانی و از مرتبه $O(n^2)$ خواهد بود؛ هزینه ارتباطی این روش برابر با $2n(n-1)\lceil \log p\rceil$ بیت و از مرتبه $O(n^2)$ است.

[DOI: 10.29252/jsdp.15.4.31]

به‌ازای m بار تکرار پروتکل، هزینهٔ محاسباتی $O(mn^2)$ نمارسانی و هزینه ارتباطی $O(mn^2)\lceil \log p \rceil$ بیت است.

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

۷- نتیجه‌گیری

در این مقاله یک پروتکل کارا جهت محاسبهٔ جمع چندسویهٔ امن در مدل شبه‌درست‌کار و با فرض کانال ناامن ارائه شده است. پروتکل ارائه‌شده قابلیت m بار تکرار را بدون افزایش هزینهٔ ارتباطی و محاسباتی و بدون کاهش امنیت کاربران دارد. به‌علاوه محرمانگی نتایج حاصل‌جمع 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 ایدهٔ کلی جهت حفظ کارایی پروتکل است و ممکن است در کاربردهای مختلف جهت حفظ امنیت کاربران، نیاز به بهبودهایی داشته باشد.

۸- مراجع 8- References

[1] A. C. Yao, “Protocols for Secure Computations”, *Proceedings of the 23 rd 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.

[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”.

[DOI: 10.29252/jsdp.15.4.31]

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.

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 علاقهٔ ایشان: استخراج قوانین انجمنی از پایگاه داده‌ها، حفظ حریم مکانی در خدمات مبتنی بر مکان، کنترل دسترسی و پروتکل‌های امنیتی.

نشانی رایانامهٔ ایشان عبارت است از:

sh.azizi93@eng.ui.ac.ir

مائده عاشوری تلوکی مدرک کارشناسی مهندسی کامپیوتر را در سال ۱۳۸۲ و مدرک کارشناسی ارشد را درسال 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 علاقهٔ ایشان، امنیت شبکه‌های موبایل، گمنامی و حریم خصوصی کاربران و پروتکل‌های امنیتی است.

نشانی رایانامهٔ 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 درسال 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 علاقهٔ ایشان، طراحی و تحلیل رمزهای قالبی، امضای دیجیتال و پروتکل‌های امنیتی است.

نشانی رایانامهٔ ایشان عبارت است از:

h.mala@eng.ui.ac.ir

[DOI: 10.29252/jsdp.15.4.31]