فصل اول

مقدمه

۱-۱. مقدمه

در بسیاری از موارد ارزش داده‌های یک منبع زمانی بیشتر می‌شود که بتوان از آن داده‌ها در محاسباتی به همراه داده‌هایی از سایر منابع استفاده کرد. به طور مثال، اگر بتوان فهرست مشتریان یک فروشگاه را به منظور یافتن مشتریان مشترک و علایق آن‌ها، با فهرست مشتریان فروشگاه دیگری در یک محاسبه وارد نمود، ارزش این اطلاعات بیشتر خواهد شد. به نظر می‌رسد که در مثال فوق، یک فروشگاه نیازمند فاش کردن داده‌های محرمانه‌ی خود برای فروشگاه دیگر می‌باشد. این موضوع افراد را ناگزیر بر سر یک دوراهی قرار می‌دهد: حفظ محرمانگی و از دست دادن ارزش واقعی داده‌ها و یا عدم در نظر گرفتن محرمانگی و فاش نمودن اطلاعات محرمانه برای سایرین. محاسبات چندسویه‌ی امن[1] (SMC)، جایگزین مناسبی برای فاش کردن اطلاعات محرمانه می‌باشد. SMC، صاحبان داده‌ها را قادر می‌سازد که با حفظ محرمانگی و عدم فاش کردن اطلاعات محرمانه، از داده‌های خود در انجام محاسبات استفاده نمایند. پرکاربردترین دسته از محاسبات چندسویه‌ی امن، محاسبات دوسویه‌ی امن[2] می‌باشد که در آن تنها دو موجودیت به عنوان طرفین پروتکل، در پروتکل شرکت می‌کنند. محاسبات دوسویه‌ی امن، دو موجودیت A و B را با ورودی‌های به ترتیب a و b، قادر می‌سازد که بدون فاش نمودن ورودی‌های محرمانه‌ی خود، مقدار تابع دومتغیره‌ی $f(a,b)$ را محاسبه کنند. ایده‌ی محاسبات

---

1 Secure Multiparty Computation
2 Secure two-party computation

دوسویه‌ی امن (ارزیابی امن توابع[1]) در سال ۱۹۸۶ توسط یائو[2] به منظور حل مسئله‌ی میلیونرها مطرح شد [۱]. در مسئله‌ی میلیونرها، دو میلیونر قصد دارند که بدون فاش کردن مقدار ثروت خود برای میلیونر دیگر، و بدون مراجعه به طرف سوم قابل اعتماد متوجه شوند که کدام یک ثروت بیشتری دارد. با این حال، ارزش محاسبات چند/دوسویه‌ی امن در سال‌های اخیر بیشتر مورد توجه قرار گرفته است و از آن در حل بسیاری از مسائل واقعی استفاده شده است [۲-۳]. برای نمونه می‌توان به رای‌گیری‌های الکترونیکی[3] در انتخابات بدون فاش شدن رای هر فرد، اشاره نمود. از طرفی اگر بتوان محاسبات امن را با هزینه‌ی محاسباتی کم پیاده‌سازی کرد، می‌توان از آن در ادوات موبایل به منظور انجام رای‌گیری‌های مبتنی بر مجاورت[4]، یافتن علایق مشترک[5]، یافتن مخاطبین مشترک[6] و بازاریابی بلادرنگ[7] استفاده نمود [۴].

۱-۲. دسته‌بندی محاسبات چندسویه‌ی امن

محاسبات چندسویه‌ی امن به طور کلی به دو دسته تقسیم می‌شوند. در دسته‌ی اول، رویکرد محاسبات، بر مبنای تسهیم راز[8] است و به منظور محاسبه‌ی توابعی استفاده می‌شود که به شکل مدارهای حسابی نمایش داده می‌شوند. از این دسته می‌توان به پروتکل‌های BGW[9] [۵] و CCD[10] [۶] اشاره کرد. رویکرد فوق معمولا زمانی مورد استفاده قرار می‌گیرد که اکثریت شرکت‌کنندگان حاضر در پروتکل، درستکار[11] باشند [۲]. در دسته‌ی دوم، توابع به شکل مدارهای دودویی نمایش داده می‌شوند. این رویکرد در ساختار مدارهای آشفته‌ی یائو[12]، برای محاسبات دوسویه‌ی امن [۱] و در ساختار پروتکل GMW[13] [۷] که برای محاسبات چندسویه‌ی امن طراحی شده است، مورد استفاده قرار می‌گیرد.

در این پایان‌نامه، توجه اصلی بر روی رویکرد عمومی مدارهای آشفته‌ی یائو برای محاسبات دوسویه‌ی امن می‌باشد. در پروتکل مدارهای آشفته، دو موجودیت نیمه-درستکار A و B که با نام‌های "تولیدکننده‌ی مدار"[14] و "ارزیاب مدار"[15] شناخته می‌شوند، تابع $f(a,b)$ که به ترتیب a و b

---

[1] **Secure Function Evaluation**
[2] **Yao**
[3] **E-Voting**
[4] **Proximity-Based Voting**
[5] **Common Interests**
[6] **Contacts Matching**
[7] **Real-time Marketing**
[8] **Secret Sharing**
[9] **Ben-Or, Goldwasser and Widgerson**
[10] **Chaum, Crepeau and Damgård**
[11] **Honest**
[12] **Yao's Garbled Circuits**
[13] **Goldreich, Micali and Wigderson**
[14] **Circuit Generator**
[15] **Circuit Evaluator**

ورودی‌های محرمانه‌ی تولیدکننده‌ی مدار A و ارزیاب مدار B می‌باشند، به گونه‌ای محاسبه می‌شود که هر یک از موجودیت‌های A و B به غیر از خروجی تابع و هر آن چه از آن استنباط می‌شود، به اطلاعات دیگری دست نیابند.

تحقیقات انجام شده بر روی مدارهای آشفته به ۳ دسته‌ی کلی تقسیم می‌شود. هدف دسته‌ی اول که طرفداران زیادی نیز دارد، استفاده از مدارهای آشفته در حل مسایل موجود همانند طراحی مناقصه‌ها، اشتراک مجموعه‌ها و ... می‌باشد [۳-۷-۸]. دسته‌ی دوم سعی در بهبودهای فنّی در مدارهای آشفته دارند. از آن جمله می توان به بسط انتقال های فراموشکارانه [۱۰] و یا بهبود زیرپروتکل "بِبُر و انتخاب کن"[1] در شرایط بدخواهانه [۱۱] اشاره کرد. تاکید دسته‌ی آخر مقالات همچون طرح [۱۲]، بر بهبود نحوه‌ی آشفته‌سازی مدارها به خودی خود است. لازم به ذکر است که در اینجا، بهبود هم به معنای بهبود در زمان پردازش و هم بهبود ارتباطی می باشد؛ از آن جایی که معمولا پهنای باند شبکه اهمیت بیشتری دارد، بهبود ارتباطی نیز بیشتر مورد توجه قرار گرفته است.

رویکرد استفاده شده در این پایان‌نامه مربوط به دسته‌ی دوم می‌باشد. بر این اساس، این پایان‌نامه قصد دارد زیرپروتکل انتقال مبهم بکار رفته در مدارهای آشفته را بررسی کرده و بهبودهایی برای آن‌ها ارائه کند.

در روش مدارهای آشفته‌ی یائو، ابتدا تابع مورد نظر $f(a,b)$ به صورت یک مدار بولی دودویی با گیت‌های دو ورودی پیاده‌سازی می‌شود و به ازای هریک از دروازه‌های منطقی چهار متن رمزشده از تولیدکننده‌ی مدار به ارزیاب مدار منتقل می‌شود. ساختن این متن‌های رمزشده به نحوی است که ارزیاب فقط یکی از آن‌ها را می‌تواند رمزگشایی کند.

از مهم‌ترین کارهای پیشین که در این زمینه انجام شده‌اند، ابتدا ایده‌ی Point_and_permute بوده است که انتخاب متن رمز شده‌ی هدف را برای ارزیاب ساده می‌سازد و باعث صرفه‌جویی در زمان پردازش می‌شود [۱۳]. کار دیگر که به روش GRR3 معروف است به جای استفاده از ۴ متن رمز شده برای جدول آشفته‌ی هر گیت منطقی، تنها ۳ متن رمز شده را منتقل می کند [۱۴]. سپس GRR2 معرفی شد که به کمک درون یابی چندجمله ای[2] انتقال جدول آشفته را با ۲ متن رمز شده برای هر گیت منطقی انجام می‌دهد [۲]. در سال ۲۰۰۸، FreeXOR معرفی شد که توانست گیت‌های منطقی XOR را بدون متن رمز شده منتقل کند [۱۲]. سپس FleXOR معرفی شد که FreeXOR را بسط داده و از فرضیات امنیتی کمتری نیز استفاده کرد [۱۵]. آخرین کار انجام شده در این زمینه که با نام "نیم گیت"[3] شناخته می‌شود توانسته است گیت‌های AND را تنها با ۲ متن رمز شده منتقل کند و از طرفی با FreeXOR نیز سازگار باشد [۱۶].

[1] **Cut-and-Choose**
[2] **Polynomial Interpolation**
[3] **Half-Gate**

۱-۳. انتقال مبهم

یکی از قسمت‌های اساسی موجود در محاسبات دوسویه‌ی امن، پروتکل انتقال فراموشکارانه یا انتقال مبهم[1] (OT) می‌باشد. شناخته‌شده‌ترین نوع انتقال مبهم، "انتقال مبهم ۱ از ۲"[2] می‌باشد که در آن دو موجودیت "فرستنده"[3] و "گیرنده"[4]، شرکت‌کنندگان حاضر در پروتکل می‌باشند. در انتقال مبهم ۱ از ۲، فرستنده دارای دو راز S_0 و S_1 می‌باشد و گیرنده صاحب بیت انتخاب $i \in \{0,1\}$ می‌باشد. در انتهای پروتکل، گیرنده به مقدار S_i دست پیدا خواهد کرد؛ بدون اینکه فرستده مقدار i را متوجه شود و گیرنده به راز S_{1-i} دست یابد. در حقیقت، هر پروتکل انتقال مبهم باید دارای دو ویژگی حریم خصوصی[5] و ابهام[6] باشد. یک پروتکل انتقال مبهم دارای ویژگی حریم خصوصی است اگر و فقط اگر، گیرنده بتواند حداکثر به یکی از دو راز S_0 و S_1 دست یابد. همچنین یک پروتکل انتقال مبهم دارای ویژگی ابهام است اگر و فقط اگر، فرستنده نتواند مقدار بیت انتخاب i (که گیرنده انتخاب کرده است) را با احتمال بیش از $1/2$ حدس بزند.

از آن جایی که بر اساس نتیجه‌ی حاصل از تحقیقات امپاگلیازو[7] و رودیخ[8] [۱۷]، بسیار بعید است که بتوان پروتکل OT را بدون استفاده از رمزنگاری کلیدعمومی انجام داد، هزینه‌ی اجرای پروتکل‌های OT بسیارسنگین است. لذا مقالات متعددی سعی در بهبود پروتکل‌های OT داشته‌اند [۱۸-۱۹-۲۰-۲۱].

در طراحی پروتکل‌های OT، فرض بر این است که طرفین حاضر در پروتکل بر روی یک کانال احراز اصالت شده[9]، پروتکل را اجرا می‌کنند. به عبارت دیگر، در این‌گونه پروتکل‌ها احراز اصالت توسط یک مکانیزم خارج از پروتکل، قبل از شروع دورهای اصلی پروتکل تامین می‌شود. این فرض، موجب می‌شود که محدودیت‌هایی در طراحی و تحلیل محاسبات چندسویه‌ی امن پدید آید [۲۲]. به همین منظور در [۲۲] روشی به منظور تجمیع احراز اصالت و پروتکل محاسبات امن، ارائه شده است.

در این پایان‌نامه، هفت پروتکل ساده، امن و کارآمد برای انتقال مبهم احراز اصالت شده ارائه می‌شود. علی رغم پروتکل‌های OT پیشین، پروتکل‌های پیشنهادی در این پایان‌نامه، احراز اصالت شده هستند و احراز اصالت در بطن پروتکل OT می‌باشد. در نتیجه نیازی به وجود یک کانال احراز اصالت شده نیست. در این پایان‌نامه، با تغییر پروتکل‌های توافق کلید احراز اصالت شده‌ی مبتنی بر دیفی-

---

[1] **Oblivious Transfer**
[2] **1-out-of-2 OT**
[3] **Sender**
[4] **Receiver**
[5] **Privacy**
[6] **Obliviousness**
[7] **Impagliazzo**
[8] **Rudich**
[9] **Authenticated**

هلمن[1]، پروتکل‌های OT احراز اصالت شده‌ی مبتنی بر دیفی-هلمن معرفی می‌شوند. به طور خاص پروتکل‌های استفاده شده به ترتیب STS [۲۳]، MTI/A0 [۲۴]، Girault [۲۵]، EKE [۲۶]، KEA [۲۷]، Unified model [۲۸] و MQV [۲۹] هستند.

از سال ۱۹۸۱ که رابین[2] برای اولین بار مبحث OT را مطرح کرد [۳۰]، مقالات متعددی به منظور معرفی پروتکل‌های OT جدید و یا بهبود پروتکل‌های OT گذشته معرفی شده‌اند [۱۸-۱۹-۲۰-۱۰]. (در سال ۱۹۷۰ مبحث مشابهی با نام "کدگذاری مزدوج"[3] معرفی شده بود [۳۱].) دو پروتکل OT معروف که با پروتکل‌های پیشنهادی در این پایان‌نامه شباهت دارند، [۱۸] و [۲۱] هستند که به کارآمدی پروتکل‌های پیشنهادی در این پایان‌نامه نیستند. [۱۸] و [۲۱] نیز همانند پروتکل‌های پیشنهادی، مبتنی بر توافق کلید می‌باشند. اخیرا [۱۹]، با استفاده از توافق کلید دیفی-هلمن به یک OT بسیار کارآمد دست یافته است. مجددا اشاره می شود که پروتکل‌های مذکور، احراز اصالت شده نیستند در حالی که پروتکل‌های پیشنهادی در این پایان‌نامه احراز اصالت شده می‌باشند.

۱-۴. مدل‌های تهدید

یکی از مهم‌ترین پارامترهای هر پروتکل محاسبات امن، مدل تهدید[4] می‌باشد. مدل‌های تهدید به منظور نشان دادن نحوه‌ی رفتار دشمن در برابر پروتکل استفاده می‌شوند. بسته به محدودیت هایی که برای دشمن تصور می‌شود، مدل‌های موجود در بازه‌ای بین نیمه-درستکار[5] (با بیشترین محدودیت) و مدل کاملا بدخواهانه[6] (با کمترین محدودیت) قرار می‌گیرند.

مدل نیمه-درستکار: در مدل نیمه-درستکار (درستکار ولی کنجکاو[7])، فرض بر این است که تمامی موجودیت‌های حاضر در پروتکل همان‌گونه که مورد انتظار است از دستورات و قوانین پروتکل پیروی می‌کنند اما ممکن است برای به دست آوردن اطلاعات اضافی در مورد سایر موجودیت‌های حاضر در پروتکل، تلاش نمایند. اگرچه این مدل، عدم تخطی موجودیت‌ها از قوانین پروتکل و همچنین رعایت عدالت[8] (به این معنا که همه‌ی موجودیت‌ها هم‌زمان به خروجی دست یابند)، را تضمین نمی‌کند، مدل نیمه-درستکار مدل امنیتی استاندارد برای محاسبات امن می‌باشد [۳۲].

بررسی پروتکل‌ها در مدل نیمه-درستکار به دو دلیل بسیار مهم است:

---

[1] **Diffie-Hellman Based Authenticated Key Agreement Protocols**
[2] **Rabin**
[3] **Conjugate Coding**
[4] **Threat Model**
[5] **Semi-Honest**
[6] **Fully Malicious**
[7] **Honest-but-Curious**
[8] **Fairness**

- مواردی وجود دارند که در آن‌ها فرضیات مدل نیمه-درستکار کافیست. به طور مثال زمانی که موجودیت‌ها کاملا قابل اعتماد می‌باشند ولی به دلایل قانونی نباید اطلاعاتی را فاش کنند.

- ایجاد پروتکل‌هایی برای شرایط نیمه-درستکار، قدم اول برای ساخت پروتکل‌هایی است که در شرایط بدخواهانه نیز بتوانند عمل کنند. روش‌هایی وجود دارند که بتوان با استفاده از آن‌ها رویکرد مدارهای آشفته (که ذاتا در مدل نیمه-درستکار صحیح است) را برای محیط‌های پنهان[1] [۳۳] و یا محیط‌های بدخواهانه [۳۴-۳۵] تعمیم داد.

در این پایان‌نامه مدل امنیتی ما، مدل نیمه-درستکار می‌باشد.

مدل تهدید بدخواهانه: فرض وجود دشمنان غیرفعال[2] که از تمامی قوانین پروتکل پیروی می‌کنند، در دنیای واقعی ساده‌انگارانه است. یک دشمن فعال[3] می‌تواند با عدم پیروی از قوانین پروتکل به شکل‌های مختلفی موجب از دست رفتن امنیت پروتکل شود. یک پروتکل محاسبه دوسویه‌ی امن در مدل تهدید بدخواهانه امن است به شرطی که ویژگی‌های محرمانگی و صحت حتی در حضور چنین دشمن فعالی نیز تضمین شوند.

در پروتکل مدارهای آشفته در محیط نیمه-درستکار، یک دشمن فعال می‌تواند حملات متعددی به روش‌های گوناگون انجام دهد. یک تولیدکننده‌ی مدار بدخواه می‌تواند یک مدار آشفته طراحی نماید که ورودی محرمانه‌ی ارزیاب مدار را به دست آورد. از آن‌جایی که یک دشمن فعال با تعداد نامحدودی از روش‌ها می‌تواند از قوانین پروتکل تخطی نماید، برای اثبات امنیت پروتکل در برابر حملات فعال، نمی‌توان به امنیت پروتکل در برابر تعداد محدودی از حملات اکتفا کرد. در نتیجه برای اثبات فرمال امنیت پروتکل‌ها در محیط بدخواهانه، اجرای پروتکل‌ها را در دو دنیای "ایده‌آل" و "حقیقی" مقایسه می‌کنند [۳۲]. در دنیای ایده‌آل تصور می‌شود که یک موجودیت سوم قابل اعتماد[4] ورودی‌های طرفین را از طریق کانال امن دریافت می‌کند، محاسبات لازم را انجام می‌دهد و نتیجه را مجددا از طریق کانال امن به طرفین اعلام می‌کند. در مقابل، در دنیای واقعی، طرفین پروتکل بدون حضور طرف سوم قابل اعتماد، پروتکل را اجرا می‌کنند. یک پروتکل محاسبات دوسویه دارای امنیت است اگر یک دشمن $\mathcal{A}$ که به جای یکی از طرفین پروتکل نشسته است، توزیع داده‌هایی شامل دید خودش و خروجی طرف درستکار به دست بیاورد، که این توزیع داده‌ها از توزیعی که از خروجی دنیای ایده‌آل با در نظر گرفتن یک طرف درستکار و یک شبیه‌ساز زمان-چندجمله‌ای احتمالاتی[5] به عنوان دشمن به دست می‌آید، غیر قابل تمایز باشد [۳۲]. روش‌های استاندارد برای ساخت پروتکل‌های مقاوم

[1] **Covert**
[2] **Passive Adversaries**
[3] **Active Adversary**
[4] **Trusted Third Party**
[5] **Probabilistic Polynomial time Simulator**

در برابر دشمن بدخواه به سه دسته تقسیم می‌شوند: "ببر و انتخاب کن"، "تعهد کن و اثبات کن"[1] و "ابتدا MAC سپس محاسبه"[2] که توضیح این روش‌ها خارج از محدوده‌ی این پایان‌نامه است [۴].

مدل تهدید پنهان: پروتکل‌های مقاوم در برابر دشمن بدخواه در مقایسه با پروتکل‌های مدل نیمه-درستکار از لحاظ محاسبات بسیار ناکارآمد هستند. از سوی دیگر، امنیت تضمین شده توسط مدل نیمه-درستکار در بسیاری از سناریوها ضعیف است. این مشکلات باعث شد که به مدلی میان دو مدل فوق احساس نیاز شود. در نتیجه اومان[3] و لیندل[4] در [۳۳] مدل تهدید پنهان را معرفی نمودند. در مدل تهدید پنهان، موجودیت متخلف با احتمال ثابت ρ شناسایی می‌شود و با احتمال $1-\rho$ می‌تواند ورودی موجودیت درستکار را به دست آورد و یا به طور تصادفی خروجی موجودیت نیمه-درستکار را تحت تاثیر قرار دهد. اگر دشمن نتواند مخاطره‌ی شناخته شدن را بپذیرد، پروتکل‌های موجود در مدل پنهان در مجموع میزان تقلب و تخلف را کاهش می‌دهند. لازم به ذکر است که در بسیاری از موارد واقعی در صورتی که شخص بدخواه شناسایی شود، وی از انجام هرگونه عملیات محاسباتی در آینده منع می‌شود. اومان و لیندل نمونه‌ای از یک پروتکل محاسبات دوسویه‌ی امن را در مدل تهدید پنهان معرفی کردند [۳۳]. اگرچه پروتکل اومان و لیندل نسبت به پروتکل مدارهای آشفته‌ی یائو (که در مدل نیمه-درستکار مطرح شده است) نیازمند محاسبات بیشتری می‌باشد، اما میزان این محاسبات اضافه بسیار ناچیز است.

۱-۵. مدل پیشگوی تصادفی

در این بخش یک مدل ایده‌آل برای توابع درهم‌ساز[5] معرفی می‌شود. اگر یک تابع درهم‌ساز h به خوبی طراحی شده باشد، باید به گونه‌ای باشد که تنها یک راه برای محاسبه‌ی $h(x)$ (که x یک مقدار دلخواه است) وجود داشته باشد و آن راه، محاسبه‌ی تابع $h(\cdot)$ به ازای ورودی x است. این ویژگی، باید در همه‌ی حالات برقرار باشد حتی زمانی که تابع h به ازای بسیاری از مقادیر $x_1, x_2, x_3, \ldots$ محاسبه شده است.

مدل پیشگوی تصادفی[6]، یک مدل ریاضیاتی برای یک تابع درهم‌ساز ایده‌آل معرفی می‌کند [۳۶]. در این مدل، تابع درهم‌ساز $h: \mathcal{X} \to \mathcal{Y}$ به صورت تصادفی از مجموعه‌ی $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$ انتخاب می‌شود و تنها راه برای محاسبه‌ی h، رجوع به پیشگوی تصادفی است. به عبارت دیگر، هیچ‌گونه قاعده و الگوریتمی برای محاسبه‌ی h در دسترس نیست. در نتیجه، تنها راه محاسبه‌ی مقدار $y = h(x)$ که $x \in \mathcal{X}$ و $y \in \mathcal{Y}$، این است که مقدار x به پیشگو داده شود و پیشگو مقدار $h(x)$ را اعلام کند.

---

[1] **Commit-and-Prove**
[2] **MAC-then-Compute**
[3] **Aumann**
[4] **Lindell**
[5] **Hash Function**
[6] **Random Oracle Model**

با اینکه در دنیای واقعی، نمی‌توان یک پیشگوی تصادفی حقیقی یافت، امید است که توابع درهم‌ساز به گونه‌ای طراحی شوند که شبیه به یک پیشگوی تصادفی رفتار کنند. ذکر این نکته لازم است که، ویژگی‌های مقاومت در برابر یافتن پیش‌تصویر[1]، پیش‌تصویر دوم[2] و تصادم[3] در مدل پیشگوی تصادفی برقرار هستند.

پروتکل‌های پیشنهادی در این پایان‌نامه در مدل پیشگوی تصادفی امن هستند. به منظور آشنایی بیشتر با مدل پیشگوی تصادفی به [۳۷] مراجعه کنید.

۱-۶. برخی کاربردهای محاسبات امن

کاربردهایی که برای محاسبات چند/دوسویه‌ی امن وجود دارند، دارای دو خصیصه‌ی اصلی می‌باشند. اول این که در این کاربردها چند/دو ورودی به ترتیب از چند/دو موجودیت متمایز وجود دارند. ثانیا هر موجودیت می‌خواهد که داده‌ی ورودی وی محرمانه بماند. لازم به ذکر است که در محاسبات امن، همیشه ممکن است یک موجودیت بتواند از خروجی حاصل از تابع و ورودی خودش به بخشی و یا تمام ورودی موجودیت‌های دیگر دست یابد. این موضوع در محاسبات امن اجتناب‌ناپذیر است. کاربردهای بسیاری در دنیای واقعی دارای دو خصیصه‌ی فوق می‌باشند. برای نمونه دو مورد از این کاربردها را به اختصار بیان می‌کنیم.

AES محرمانه: AES یک رمز قالبی با طول قالب ۱۲۸ بیت است که در سال ۲۰۰۱ توسط NIST[4] به صورت یک استاندارد رمزگذاری پذیرفته شده است [۳۸]. در "رمز AES با حفظ محرمانگی"، باب که صاحب کلید محرمانه می‌باشد، پیام محرمانه‌ی آلیس را بدون این که محتویات پیام را ببیند، رمز می‌کند. از سوی دیگر، آلیس نیز نمی‌تواند به کلید محرمانه‌ی باب دست یابد. AES محرمانه کاربردهای متعددی دارد. به طور مثال، آلیس که صاحب پیام است می‌تواند از باب بخواهد که بدون خواندن پیام، پیام را (به صورت کورکورانه) رمز نماید. این کار می‌تواند برای مجوز دسترسی به داده‌های رمز شده در فضای ابری مورد استفاده قرار گیرد. "AES با حفظ محرمانگی" به یک معیار[5] برای ارزیابی پروتکل‌های محاسبات دوسویه‌ی امن تبدیل شده است.

اشتراک مجموعه‌های محرمانه: پروتکل‌های رمزنگاری که برای اشتراک مجموعه‌های محرمانه[6] (PSI) ایجاد شده‌اند، پایه و اساس بسیاری از کاربردهای حفظ محرمانگی می‌باشند. در اشتراک مجموعه‌های محرمانه دو موجودیت هر یک به ترتیب صاحب مجموعه‌ی S و S' هستند و هر موجودیت می‌خواهد بدون فاش کردن هرگونه اطلاعاتی (به جز اندازه‌ی مجموعه) در مورد مجموعه‌ی

---

[1] **Preimage**
[2] **Secend Preimage**
[3] **Collision**
[4] **National Institute of Standards and Technology**
[5] **Benchmark**
[6] **Private Set Intersection**

محرمانه‌ی خود به موجودیت دیگر، حاصل $I = S \cap S'$ را دریابد. PSI می‌تواند به طور مستقیم در یافتن مشتریان مشترک دو شرکت متفاوت و یا یافتن افراد تحت تعقیب در فهرست مسافرین پرواز در فرودگاه‌ها مورد استفاده قرار گیرد. همچنین می‌توان از PSI به عنوان یک زیرروال در سایر محاسبات امن استفاده نمود. به طور مثال، شرکت‌ها می‌توانند بر روی مشتریان مشترک خود، داده‌کاوی انجام دهند (PSI قبل از انجام پروسه‌ی اصلی). مثال‌های دیگری از کاربردهای PSI در [۳۹] موجود است.

رای‌گیری الکترونیکی: در انجام رای‌گیری الکترونیکی، هر موجودیت رای خود را با استفاده از یک پروتکل رای‌گیری الکترونیکی به کارگزار[1] ارسال می‌کند. سپس سرور با توجه به رای‌های دریافتی، رای اکثریت را اعلام می‌کند. در رای‌گیری الکترونیکی کارگزار و هیچ یک از رای‌دهندگان نباید از رای سایر رای‌دهندگان مطلع شوند. محاسبات چندسویه‌ی امن عنصر جدایی‌ناپذیر در پروتکل‌های رای‌گیری الکترونیکی است.

مناقصه و مزایده‌ی الکترونیکی: امروزه بسیاری از کالاها و خدمات با روش مناقصه یا مزایده‌ی الکترونیکی به فروش می‌رسند. در پروتکل‌های مناقصه‌ی الکترونیکی هر یک از موجودیت‌ها پیشنهاد[2] خود را به عنوان یک ورودی به تابع می‌دهند و در انتها خروجی تابع، شناسه‌ی موجودیتی است که کمترین پیشنهاد را ارائه کرده است. در نتیجه، مقدار پیشنهاد هر موجودیت محرمانه باقی می‌ماند.

پرسمان[3] از یک پایگاه داده: فرض کنید که یک کاربر می‌خواهد از یک پایگاه داده پرسشی بپرسد. در بسیاری از شرایط، هم باید داده‌های موجود در پایگاه داده محرمانه بماند و هم باید پرسش کاربر محرمانه بماند. به طور مثال اگر استفاده از پایگاه داده مستلزم پرداخت هزینه برای کاربران باشد، پاسخی که پایگاه داده به کاربر می‌دهد نباید اطلاعاتی به جز پاسخ پرسش را برای کاربر فاش کند. از سوی دیگر، فرض کنید یک شرکت تحقیقاتی قبل از ثبت یک اختراع جدید و بدون فاش کردن اختراع خود، بخواهد از وجود یا عدم وجود اختراع خود در پایگاه داده‌ی ثبت اختراعات مطلع شود. در این شرایط باید پرسش کاربر از دید پایگاه داده محرمانه باشد. لازم به ذکر است که در شرایط ایده‌آل نه تنها پرسش کاربر محرمانه است، بلکه پاسخ پایگاه داده نیز از دید پایگاه داده محرمانه است.

۱-۷. بیان مسئله

با توجه به استفاده‌ی گسترده‌ی پروتکل‌های محاسبات امن و کاربردهای این‌گونه محاسبات در زندگی روزمره، پروتکل‌های زیادی به منظور کاهش سربار محاسباتی و ارتباطی معرفی شده‌اند [۱۲-۱۵-۱۶]. از آن‌جایی که پروتکل انتقال مبهم یک زیرپروتکل اساسی در محاسبات امن است، بهبود سربار محاسباتی و ارتباطی در این پروتکل نیز باعث می‌شود که کارایی در طیف گسترده‌ای در پروتکل‌های محاسبات امن بهبود یابد.

---

[1] **Server**
[2] **Bid**
[3] **Query**

در طراحی پروتکل‌های محاسبات امن، فرض می‌شود که احراز اصالت پیش از انجام پروتکل اصلی و توسط یک پروتکل توافق کلید احراز اصالت شده انجام می‌شود و پیام‌های پروتکل محاسبات امن مذکور بر روی یک کانال احراز اصالت شده منتقل می‌شوند [۲۲]. این فرضیه باعث می‌شود که سربار محاسباتی و ارتباطی افزایش یابد. در نتیجه، معرفی پروتکل‌های انتقال مبهم احراز اصالت شده که احراز اصالت در بطن پروتکل انتقال مبهم است، می‌تواند سربار محاسباتی و ارتباطی را کاهش دهد.

۱-۸. دستاوردهای این پایان‌نامه

هدف این پایان‌نامه بهبود محاسبات دوسویه‌ی امن با رویکرد مدارهای آشفته می‌باشد. لذا در این راستا تحقیقات در راستای معرفی پروتکل‌هایی برای انتقال مبهم احراز اصالت شده انجام شده‌اند:

- معرفی پروتکل‌هایی برای انتقال مبهم احراز اصالت شده: در این پایان‌نامه، به وسیله‌ی تغییر در پروتکل‌های توافق کلید احراز اصالت شده‌ی مبتنی بر دیفی-هلمن، چندین پروتکل OT احراز اصالت شده معرفی شده است. لازم به ذکر است که در روش‌های موجود تاکنون، فرض بر این بوده است که کلیه‌ی عملیات OT بر روی یک کانال احراز اصالت شده انجام می‌شود. در پروتکل‌های پیشنهادی در این پایان‌نامه، نیازی به کانال احراز اصالت شده نیست. در عوض، احراز اصالت در بطن پروتکل OT انجام می‌شود.

۱-۹. ساختار این پایان‌نامه

با توجه به مطالب ذکر شده، ساختار این پایان‌نامه به صورت زیر است. در فصل دوم، پیشینه‌ی موضوع و روش‌های قبلی مرتبط با مدارهای آشفته و پروتکل‌های انتقال مبهم بیان می‌شوند. سپس در فصل‌های سوم و چهارم چندین پروتکل OT احراز اصالت شده معرفی و ارزیابی می‌شوند. در پایان در فصل پنجم با نتیجه‌گیری این پایان‌نامه را به پایان می‌بریم.