دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

گزارش کتبی سمینار

درس پروتکل‌های امنیتی

عنوان

انتخابات‌های انتهابه‌انتها قابل راستی‌آزمایی

نگارش

سید محمدمهدی احمدپناه

۹۴۱۳۱۰۸۶

استاد راهنما

دکتر بابک صادقیان

مرداد ۱۳۹۵

چکیده

در گزارش پیش‌رو، به مطالعه اجمالی در خصوص خواسته‌های امنیتی در سیستم‌های رأی‌گیری الکترونیکی و انتخابات پرداخته می‌شود. سپس با بیان دقیق خواسته امنیتی *قابلیت راستی‌آزمایی انتهابه‌انتها* به کمک ویژگی‌های امنیتی مشخص‌تر و تعریف صوری آن با رویکردی مبتنی بر بازی، یک سیستم پیشنهادی با حداقل فرضیات و در مدل استاندارد؛ یعنی بدون فرضیات در مرحله راه‌اندازی و عدم نیاز به دسترسی به اوراکل تصادفی، ارائه می‌شود و پروتکل‌ها و جزئیات این طرح مطرح می‌شود. دیگر خواسته‌های امنیتی مورد توجه در طرح پیشنهادی، حریم خصوصی و تازگی رسید رأی‌دهندگان است.

اثبات می‌شود که طرح پیشنهادی از حیث نظریه اطلاعات در مدل استاندارد قابلیت راستی‌آزمایی انتهابه‌انتها، و تحت فرضیات محاسباتی حریم خصوصی و تازگی رسید را فراهم می‌آورد. از نکات جالب توجه در این طرح، عدم نیاز رأی‌دهندگان به استفاده از عملیات رمزنگاری در حین انداختن برگه رأی و فرض بدخواه‌بودن مرجع انتخابات و تبانی با تعدادی از رأی‌دهندگان است. این طرح پیشنهادی برای انتخابات ۱-از-m با حزئیات بیان شده که البته برای حالت چند-از-m نیز قابل ارائه است.

واژه‌های کلیدی:

انتخابات امن؛ رأی‌گیری الکترونیکی؛ راستی‌آزمایی انتهابه‌انتها؛ حریم خصوصی رأی‌دهندگان؛ تازگی رسید؛ تعریف صوری

فهرست عناوین

صفحه

فهرست اشکال

صفحه

فهرست جداول

صفحه

فصل اول

مقدمه

مقدمه

سیستم‌های رأی‌گیری الکترونیکی در کشورهای گوناگونی برای فراهم‌کردن کارایی بیشتر در رویه‌های رأی‌گیری معرفی و مطرح شد. این در حالیست که امنیت انتخابات‌های الکترونیکی بسیار مورد بحث است. تفاوت اصلی بین انتخابات‌های سنتی کاغذی با این گونه انتخابات‌ها، عدم وجود شفافیت است [۵]. در انتخابات‌های کاغذی معمولا امکان مشاهده تمامی مراحل، از انداختن برگه رأی در صندوق تا شمارش آرا وجود دارد و تغییر در برگه رأی در درون صندوق، به دلیل محدویت‌های فیزیکی، امکان‌پذیر نیست. اما مشاهده عملیات‌های الکترونیکی روی داده‌ها ممکن نیست.

لفظ راستی‌آزمایی انتهابه‌انتها در سال‌های گذشته در کارهای گوناگونی مورد استفاده قرار گرفته است اما این لفظ - تا سال ۲۰۱۵- هرگز به صورت صوری تعریف نشده است [۲]. به این ترتیب، معنا و مفهوم آن از یک سیستم انتخاباتی به سیستم انتخاباتی دیگر متفاوت خواهد بود.

در پروتکل‌های مطرح‌شده با قابلیت راستی‌آزمایی انتهابه‌انتها، طراحی‌ها اجازه می‌دهد تا روی روند انتخابات این بررسی صورت بگیرد که آیا همه رأی‌های انداخته‌شده[1] به درستی محسوب شده‌اند یا نه. به این توجه می‌شود که مستقل از صحت تجهیزات برگزاری انتخابات، نتیجه به درستی بیانگر تمایل رأی‌دهندگان باشد. پس خود انتخابات مورد بررسی قرار می‌گیرد، نه صرفاً تجهیزات آن.

روند انتخابات برای هر رأی‌دهنده تصدیق اصالت‌شده این‌گونه در نظر گرفته می‌شود که یک برگه رأی و مجموعه‌ای از انتخاب‌ها برای هر رأی‌دهنده ارائه می‌شود. سپس آن شخص برگه رأی که بیانگر انتخاب‌هاست را در صندوق می‌اندازد. این انتخاب‌ها ثبت می‌شوند و مجموعه ثبت‌شده‌ها شمارش می‌شود و در پایان، نتیجه شمارش اعلام می‌شود. در یک انتخابات انتهابه‌انتها قابل راستی‌آزمایی، باید بتوان بررسی کرد که آیا برگه رأی ارائه‌شده خوش‌ساخت است، برگه رأی انداخته‌شده معتبر است، برگه رأی انداخته‌شده به درستی ثبت شده است، شمارش به درستی محاسبه شده است، آرای شمارش‌شده همان آرا ثبت‌شده است، و سیستم رأی‌گیری در قبال دستورات رأی‌دهنده مطابق با پروتکل رفتار می‌کند.

[1] Cast

محدوده راستی‌آزمایی انتهابه‌انتها از مردمی که آرا را می‌اندازند تا نتیجه نهایی گسترده است. یک انتخابات، قابل راستی‌آزمایی انتهابه‌انتهاست هرگاه هر تفاوت قابل توجهی بین نتیجه گزارش‌شده و نتیجه درست که حاصل از شمارش آرای واقعی انداخته‌شده توسط رأی‌دهندگان وجود داشت، حداقل یکی از بررسی‌های فوق شکست بخورد.

در این مفهوم تنها صحت انتخابات اهمیت دارد. حریم خصوصی رأی‌دهنده، مقاومت در برابر تهدید و خرید رأی، قابلیت اطمینان[۲]، قابلیت استفاده[۳]، در دسترس‌بودن[۴]، و مقاومت در برابر حملات ممانعت از سرویس[۵] که در انتخابات در دنیای واقعی بسیار حائز اهمیت است، خارج از محدوده این مفهوم است.

سختی طراحی سیستم قابل راستی‌آزمایی انتهابه‌انتها ناشی از دشواری فراهم‌کردن محرمانگی برگه رأی در سیستم است. به این معنا که در صورتی که در سیستمی چگونگی رأی‌دادن هر فرد به صورت عمومی مشخص باشد، داشتن یک سیستم با قابلیت راستی‌آزمایی انتهابه‌انتها راحت‌تر است.

[2] Reliability

[3] Useablilty

[4] Accessibility

[5] Denial-of-Service

فصل دوم

کارهای گذشته

کارهای گذشته

در بررسی کارهای گذشته انجام‌شده، برای اولین بار چاوم [۶] انتقال بی‌نام را معرفی کرد که منجر به سیستم‌های رأی‌گیری با قابلیت راستی‌آزمایی انفرادی شد. به این معنا که رأی‌دهندگان بتوانند درستی نحوه شمارش آرای خود را در نتیجه انتخابات بررسی کنند. در [۷]، مفهوم راستی‌آزمایی همگانی مطرح شده است؛ یعنی این توانایی برای هر کسی وجود داشته باشد که بتواند از آرای انداخته‌شده صحت نتیجه انتخابات را بررسی کند. در [۸]، راستی‌آزمایی همگانی در مدل محاسباتی با فرض وجود راه‌اندازی مورد اعتماد بیان شده است. تعاریف نمادین برای راستی‌آزمایی انفرادی و همگانی در حساب پای کاربردی در [۵] عنوان می‌شود. تعریفی صوری از راستی‌آزمایی همگانی نیز در کار [۹] مطرح می‌شود.

راستی‌آزمایی انتهابه‌انتها به معنای cast-as-intended، recorded-as-cast و tallied-as-recorded به عنوان نتیجه‌ای کارهای چاوم [۱۰] و نِف [۱۱] است. در [۲] نیز همان‌طور که قبل‌تر ذکر شد، تعریفی از قابلیت راستی‌آزمایی انتهابه‌انتها به کمک لیستی از ویژگی‌ها بیان شده است.

تعاریف صوری از حریم خصوصی و تازگی رسید در حساب پای کاربردی[۶] در [۱۲] و در مدل محاسبه‌پذیری همگانی در [۱۳] آمده است. در [۱۴]، مفهومی مبتنی بر بازی از حریم خصوصی برگه رأی ارائه و مطالعه‌ای روی حریم خصوصی در Helios انجام شده است. اما این تعریف تازگی رسید را مورد توجه ندارد.

در [۵] تعریفی نمادین[۷] از قابلیت راستی‌آزمایی انتخابات ارائه می‌شود که سه جنبه مطرح‌شده فوق را شامل می‌شود و پروتکل‌های رأی‌گیری FOO، که از امضای کور استفاده می‌کند؛ Helios 2.0[۴] که بر پایه رمزنگاری هم‌ریختی[۸] است؛ و JCJ-Civitas که از میکس‌نت‌ها و عبارات محرمانه بی‌نامی استفاده می‌کند، را در حساب پای کاربردی مدل‌سازی کرده است. در تعریف ارائه‌شده این امکان را به ما

[6] Applied Pi Calculus

[7] Symbolic Definition

[8] Homomorphic Encryption

می‌دهد که به طور دقیق مشخص شود که کدام بخش‌های یک سیستم رأی‌گیری برای قابلیت راستی‌آزمایی باید مورد اعتماد باشند.

در [۲] تعریفی برای راستی‌آزمایی انتهابه‌انتها برای انتخابات‌های عمومی مبتنی بر خواسته‌های عملکردی، که در تضاد با خواسته‌های طراحی است، ارائه می‌شود. در واقع، مجموعه‌ای از ویژگی‌ها مطرح می‌شود که تجمیع آن‌ها به تعریف این لفظ منتج می‌شود. در [۲]، علاوه بر ذکر جزئیات، نحوه بررسی‌ها، طرف بررسی‌کننده و زمان هر بررسی، این بررسی‌های شش‌گانه را برای پروتکل‌های مختلف موجود در کارهای گذشته مورد بحث قرار گرفته است. پروتکل‌هایی نظیر Pret a Voter، PrunchScan، Scratch&Vote، ThreeBallot، Scantegrity II و Helios از جمله آن‌هاست. به طور مثال، برای سیستم Helios که ایده اصلی آن این است که رأی‌دهنده برگه رأی رمزشده‌ای در اختیار دارد و می‌تواند بین ترجمه[۹] برگه رأی خود یا انداختن برگه رأی رمزشده انتخاب کند. هرگاه که رأی‌دهنده ترجمه برگه رأی خود را انتخاب کند، می‌تواند بررسی کند که انتخاب‌های رمزشده صحیح باشند. سپس اجازه دارد تا رویه را تکرار کند تا زمانی که بخواهد یک برگه رأی را، بدون ترجمه‌کردن، بیندازد. در این سیستم انتخابات، به صورت هم‌ریخت برگه‌های رأی رمزشده جمع‌آوری می‌شوند.

در سیستم Helios، نسخه ضعیف‌تری از بررسی *برگه‌های رأی ارائه‌شده خوش‌ساخت باشد* را داراست. بررسی‌های *برگه‌های رأی انداخته‌شده خوش‌ساخت باشند*، *شمرده‌شدن همانی که ثبت‌شده* و *پیروی‌کردن از پروتکل رأی‌گیری* نیز در این سیستم به درستی انجام شده است. در نتیجه، سیستم‌های انتخاباتی که از Helios استفاده می‌کنند، قابلیت راستی‌آزمایی انتهابه‌انتها را دارند اما نسخه ضعیف‌تری از خواسته دوم را برآورده می‌کنند.

در جدول زیر، به طور خلاصه، مقایسه سیستم‌های انتخاباتی مختلف نام‌برده‌شده را از نظر برآورده‌سازی خواسته‌ها آورده شده است که در فصل بعدی توضیحات بیشتر مطرح شده است.

جدول ۱ – تعدادی از سیستم‌های انتخابات و تطبیق آن‌ها با خواسته‌های عملکردی انتهابه‌انتها [۲]

	BaWF	CBaWF	RaC	TaR	C	ERBiSttRaCC	FtP
Prêt à Voter	✓	✓	✓	✓	✓	✓	✓
PunchScan	✓	✓	✓	✓	✓	✓	✓
Scratch&Vote	✓	✓	✓	✓	✓	✓	✓
ThreeBallot	✓	no	✓	✓	✓	✓	✓
Scantegrity II	✓	✓	weak for added votes	✓	✓	✓	✓
Helios	weak	✓	✓	✓	✓	✓	weak

باید اشاره کرد که کارهای گذشته انجام‌شده برای فراهم‌کردن قابلیت راستی‌آزمایی انتهابه‌انتها در مدل استاندارد ناموفق بوده‌اند. در Helios لازم است تا رأی‌دهنده از یک دستگاه پشتیبانی‌کننده رأی‌دهنده برای فراهم‌کردن متن رمزشده استفاده کند و بعد از تعداد نامشخصی آزمایش، اقدام به انداختن برگه رأی رمزشده خود کند. این متن رمزشده‌ها باید از نظر هم‌ریختی قابل شمارش باشند و باید اثباتی برای درستی نحوه انجام محاسبه وجود داشته باشد. گرچه این چنین اثبات‌ها می‌توانند مطرح شوند اما تنها به صورت تعاملی قابل ارائه هستند که برای مفروضات انجام‌شده در مدل استاندارد و مدل مهاجم کافی نیست. پس به‌دست‌آوردن قابلیت راستی‌آزمایی انتهابه‌انتها در مدل استاندارد در Helios یا طرح‌های موجود مشابه دیگر امکان‌پذیر نیست.

در پروتکل Remotegrity/Scantegrity، نیاز به n سکه برای حصول به randomness beacon است تا بتوان اثباتی برای صحت انتخابات داشت. به سادگی می‌توان نشان داد که در صورتی که randomness beacon مغرضانه باشد، امنیت سیستم انتخابات به مخاطره خواهد افتاد. این در حالیست که دو طرف فعال در سیستم انتخابات؛ یعنی مرجع انتخابات و رأی‌دهندگان، نمی‌توانند randomness beacon مورد نظر برای این پروتکل را در سیستم مفروض پیاده‌سازی کنند. حال آن که در طرح پیشنهادی در [۱]، میزان تصادفی‌بودن برای راستی‌آزمایی انتخابات به صورت توزیع‌شده از رأی‌دهندگان جمع‌آوری می‌شود.

فصل سوم

قابلیت راستی‌آزمایی انتهابه‌انتها

قابلیت راستی‌آزمایی انتهابه‌انتها

سیستم‌های کامپیوتری ممکن است رکوردهای رأی‌گیری را به نحوی تغییر دهند که رأی‌دهندگان یا ناظرهای انتخابات تشخیص ندهند. یک نرم‌افزار پایانه رأی‌گیری احتمال دارد که توسط بدافزاری آلوده شود که می‌تواند رأی واردشده را تغییر دهد یا حتی یک پروتکل کاملا متفاوت با آن‌که انتظار می‌رود را اجرا کند.

مفهوم انتخابات یا راستی‌آزمایی انتهابه‌انتها[10] به همین مسئله اشاره دارد. در انتخابات‌ها، رأی‌دهندگان و ناظران انتخاباتی باید مستقل از اجرای نرم‌افزاری و سخت‌افزاری انتخابات، مجاز به راستی‌آزمایی باشند که رأی‌ها به درستی ثبت[11]، شمارش[12] و اعلام شده‌اند یا خیر.

دو جنبه کلی در این گونه راستی‌آزمایی‌ها مطرح می‌شود [۵ و ۱]:

- راستی‌آزمایی انفرادی[13]: یک رأی‌دهنده بتواند بررسی کند که برگه رأی خودش در تابلوی اعلانات انتخابات[14] وجود دارد.

- راستی‌آزمایی همگانی[15]: هر کسی بتواند بررسی کند که نتیجه انتخابات متناظر است با برگه‌های منتشرشده در تابلوی اعلانات.

جنبه دیگری نیز که می‌توان بیان کرد [۵]، راستی‌آزمایی صلاحیت[16] است. به این معنا که هر کسی بتواند بررسی کند که هر رأی در نتیجه انتخابات توسط یک رأی‌دهنده ثبت‌نام‌شده انداخته شده و به ازای هر رأی‌دهنده، حداکثر یک رأی وجود دارد.

---

[10] End-to-End Verifiability

[11] Record

[12] Tally

[13] Individual Verfiability

[14] Election’s Bulletin Board

[15] Universally Verifiability

[16] Elgibility Verifiablity

هر گاه یک سیستم انتخابات همه شش بررسی مطرح‌شده در [۲] را با موفقیت پشت سر بگذارد، آن انتخابات انتهابه‌انتها قابل راستی‌آزمایی خواهد بود. به بیان کلی، به این معناست که برگه‌های رأی انداخته‌شده توسط رأی‌دهندگان به درستی ثبت و شمرده شوند و مقدار شمرده‌شده به عنوان نتیجه نهایی گزارش شود. اگر رأی‌ای بعد از انداخته‌شدن اضافه، حذف، تغییر یا نامعتبر شود، احتمال آن وجود دارد که توسط ناظری که می‌تواند راستی‌آزمایی کند، تشخیص داده شود.

در ادامه خواسته‌های امنیتی به طور مفصل توضیح داده خواهد شد اما پیش از آن، درباره خواسته‌های امنیتی و تعریف راستی‌آزمایی، باید توجه داشت که فرضیاتی در خصوص وجود تابلوی اعلانات، رسید و عملیات رمزنگاری در تعریف مطرح نمی‌شود. محدوده خواسته‌های امنیتی نیز فقط برای اطمینان از صحت نتایج انتخابات است.

حال به تعریف انتخابات انتهابه‌انتها قابل راستی‌آزمایی می‌پردازیم [۲]. به یک انتخابات، انتهابه‌انتها قابل راستی‌آزمایی گفته می‌شود اگر و فقط اگر:

۱) برگه‌های رأی ارائه‌شده خوش‌ساخت باشند؛ یعنی نحوه نمایش انتخاب‌های رأی‌دهنده روی برگه رأی با نحوه نمایشی که در بقیه مراحل خوانده می‌شود، هم‌خوانی داشته باشد.

۲) برگه‌های رأی انداخته‌شده خوش‌ساخت باشند؛ یعنی برگه‌های رأی انداخته‌شده حاوی آرای ویژه یا منفی نباشد.

۳) ثبت‌شدن همانی که انداخته‌شده؛ یعنی برگه رأی انداخته‌شده توسط رأی‌دهنده، همانی باشد که دریافت می‌شود و توسط سیستم رأی‌گیری ذخیره می‌شود.

۴) شمرده‌شدن همانی که ثبت‌شده؛ یعنی آرای مربوط به برگه‌های رأی انداخته‌شده، به درستی محاسبه شود و در نتیجه عمومی قرار بگیرد.

۵) سازگاری؛ یعنی مجموعه برگه‌های رأی مرتبط با بررسی *ثبت‌شدن همانی که انداخته‌شده* متناسب و سازگار با مجموعه برگه‌های رأی مربوط به بررسی *شمرده‌شدن همانی که ثبت‌شده* باشد.

۶) هر برگه رأی ثبت‌شده، مرتبط با بررسی *ثبت‌شدن همانی که انداخته‌شده* باشد؛ یعنی هیچ برگه رأی‌ای در نتیجه نهایی وجود نداشته باشد که حداقل توسط یکی از رأی‌دهندگان بررسی نشده باشد.

علاوه بر موارد و بررسی‌های فوق، خواسته مهم دیگری نیز مطرح است. هرگاه بخشی از پروتکل رأی‌گیری که باید برای اطمینان از صحت انتخابات مطابق پروتکل رفتار کند، بررسی‌ای وجود داشته باشد تا بتوان تشخیص داد که سیستم رأی‌گیری از پیروی از پروتکل منحرف نشده است.

مقاله اصلی این گزارش، کار [۱] است. در این مقاله، پیاده‌سازی رمزنگارانه‌ای از DEMOS، یک سیستم رأی‌گیری الکترونیکی با قابلیت راستی‌آزمایی انتهابه‌انتها در مدل استاندارد ارائه شده است. منظور از مدل استاندارد یعنی هیچ فرضیات اضافه‌ای در گام راه‌اندازی[۱۷] یا دسترسی به یک اوراکل تصادفی[۱۸] (RO) نیاز نیست. سیستم‌های قبلی رأی‌گیری الکترونیکی با قابلیت راستی‌آزمایی انتهابه‌انتها نیازمند چنین فرضیاتی بوده‌اند. در سیستم انتخابات مطرح‌شده، علاوه بر قابلیت راستی‌آزمایی انتهابه‌انتها، خواسته‌های امنیتی حریم خصوصی و تازگی رسید نیز مورد توجه بوده است که برای تعاریف آن‌ها از دو بازی حمله استفاده شده است.

طرح ارائه‌شده خواسته امنیتی راستی‌آزمایی انتهابه‌انتها را از نظر نظریه اطلاعات و در مدل استاندارد و خواسته امنیتی حریم خصوصی و تازگی رسید را تحت یک فرض محاسباتی (زیرنمایی‌بودن[۱۹] تصمیم‌گیری دیفی-هلمن[۲۰]) برآورده می‌کند. در این کار، برای اولین بار از طرح‌هایی مانند منابع بیت-ثابت، اثبات‌های صفردانشِ با نقصان تصادفی‌بودنِ[۲۱] تحقیق‌کننده[۲۲] و پیچیدگی اِعمال نفوذ[۲۳] استفاده شده است.

در سیستم انتخابات قابل راستی‌آزمایی انتهابه‌انتها، رأی‌دهندگان توانایی راستی‌آزمایی رأی خود را دارند که آیا به درستی در صندوق انداخته شده، ثبت شده و در نتیجه انتخابات شمرده شده یا خیر. ویژگی امنیتی‌ای که یک انتخابات انتهابه‌انتها قابل راستی‌آزمایی در نظر دارد تا برآورده کند آن است که

[17] Setup

[18] Random Oracle

[19] Subexponential

[20] Decisional Diffie Helman

[21] Randomness

[22] Verfier

[23] Complexity Leveraging

رأی‌دهندگان بتوانند یک مرجع انتخابات[۲۴] بدخواه[۲۵] را شناسایی کنند که سعی در اختلال و تقلب در نتیجه انتخابات دارد. قابلیت راستی‌آزمایی انتهابه‌انتها یک سطح قوی از امنیت برای سیستم‌های انتخابات است که به عنوان یک خواسته امنیتی پایه‌ای و اصلی پذیرفته شده است. قابلیت راستی‌آزمایی انتهابه‌انتها حکم می‌کند که رأی‌دهنده بتواند یک رسید در پایان رویه انداختن برگه رأی بگیرد که اجازه راستی‌آزمایی رأیش را به او بدهد. این راستی‌آزمایی از سه منظر (۱) همانی که مورد نظرش بوده است را در صندوق انداخته، (۲) همانی که در صندوق ریخته‌شده، ثبت شود، و (۳) همانی که ثبت‌شده، در شمارش تأثیرگذار باشد. علاوه بر این، هر فرد ثالث خارجی باید بتواند اجرای رویه انتخابات را راستی‌آزمایی کند. در واقع، لازم است رسیدهای یک سیستم انتخابات انتهابه‌انتها قابل تفویض باشد؛ یعنی رأی‌دهنده ممکن است وظیفه راستی‌آزمایی را به یک فرد ثالث بسپارد. به عنوان مثال، رأی‌دهندگان یک سازمان بین‌المللی را انتخاب می‌کنند تا وظیفه راستی‌آزمایی را تجمیع و انجام دهد. باید توجه داشت که خواسته امنیتی دیگر آن است که نتوان از رسید یک رأی‌دهنده برای اثبات نحوه رأی‌دادن آن شخص استفاده کرد تا بتوان از خرید و فروش رأی جلوگیری کرد. ساخت و طراحی سیستم‌های قابل راستی‌آزمایی انتهابه‌انتها از این حیث به مسئله‌ای چالش‌برانگیز بدل می‌شود.

همه سیستم‌های رأی‌گیری الکترونیکی شناخته‌شده که قابلیت راستی‌آزمایی انتهابه‌انتها را ارائه می‌کنند تحت فرضیاتی در مرحله راه‌اندازی هستند یا در مدل اوراکل تصادفی مطرح شده‌اند. به عنوان مثال، Helios در مدل اوراکل تصادفی است در حالی‌که Remotegrity در مدلی مطرح شده است که لازم است تا یک طرف مورد اعتماد جریانی از سکه‌های تصادفی غیرقابل‌پیش‌بینی و بی‌طرفانه فراهم کند. رویکردهای کلی‌تر برای تعریف محاسبات چندطرفه قابل‌حسابرسی نیز اخیراً ارائه شده که وابسته به فرضیات راه‌اندازی مانند یک رشته ارجاع مشترک[۲۶] (CRS) است.

نقص اصلی استفاده از فرضیات در مرحله راه‌اندازی برای فراهم‌کردن سیستم انتخابات با قابلیت راستی‌آزمایی انتهابه‌انتها آن است که رأی‌دهندگان باید بدون اثبات باور داشته باشند و بپذیرند که فرض

[24] Election Authority

[25] Malicious

[26] Common Reference String

مرحله راه‌اندازی به درستی انجام گرفته تا بتوانند به درستی نتیجه انتخابات باور داشته باشند. اما از آن‌جایی که مرجع انتخابات (EA) نمی‌تواند صراحتاً اثبات کند که نتیجه انتخابات درست بوده است، لذا نتیجه انتخابات همیشه محل مناقشه و بحث خواهد بود.

در [۱]، یک سیستم رأی‌گیری الکترونیکی جدیدی مطرح می‌شود که قابلیت راستی‌آزمایی انتهابه‌انتها را از حیث نظریه اطلاعات در مدل استاندارد فراهم می‌کند. تنها فرض در مرحله راه‌اندازی در این طرح، وجود تابلوی اعلانات (BB) است که دائماً گزارش عمومی انتخابات را نشان می‌دهد. نکته اینجاست که در این سیستم، حداقل فرضیات ممکن برای توانایی محاسباتی رأی‌دهندگان در نظر گرفته شده است؛ به این معنا که رأی‌دهندگان صرفا به عنوان مبدل[۲۷]های حالت متناهی مدل شده‌اند و بنابراین از انجام هرگونه عملیات رمزنگارانه در طول انداختن برگه رأی ناتوان هستند. گرچه در طول مرحله حسابرسی پس از پایان انتخابات نیاز به عملیات رمزنگاری باشد، اما در طول فرایند انتخابات نیازی به این عملیات نیست. ضمناً می‌توانند حسابرسی را به فرد ثالثی بسپارند تا عملیات رمزنگارانه را انجام دهد.

در مدل‌سازی این طرح، از سه نوع موجودیت استفاده می‌شود: (۱) رأی‌دهندگان V_1 تا V_n، (۲) مرجع انتخابات، و (۳) تابلوی اعلانات که تنها نقش آن برای ذخیره‌سازی گزارش‌های عمومی به منظور راستی‌آزمایی انتخابات است. رأی‌دهندگان با شرکت در پروتکل انداختن برگه رأی، آرای خود را به مرجع انتخابات ارسال می‌کنند و مجاز به تعامل با یکدیگر نیستند. در تعریف صورت‌گرفته در [۱]، مدل مهاجم بسیار قدرت‌مندی در نظر گرفته می‌شود که از نظر محاسباتی توان نامحدود دارد و می‌تواند مرجع انتخابات را کاملاً کنترل کند. از طرف دیگر، تابلوی اعلانات کاملاً منفعل است و گرچه توسط همه موجودیت‌ها قابل خواندن است، اما فقط مرجع انتخابات می‌تواند روی آن بنویسد. به این ترتیب، تعریف صورت گرفته برآورده خواهد شد اگر و فقط اگر در حالی‌که تعدادی از رأی‌دهندگان درستکارانه رویه راستی‌آزمایی را انجام می‌دهند، مهاجم نتواند نتیجه انتخابات را دست‌کاری کند و تشخیص داده نشود. و از سمت دیگر، خواسته امنیتی حریم خصوصی باعث می‌شود تا مهاجم به همه رسیدهای رأی‌دهندگان دسترسی کامل داشته باشد و حتی در نقش تعدادی از رأی‌دهندگان نادرست‌کار وارد پروتکل انداختن

[27] Transducer

برگه رأی شود. برای هر نتیجه انتخابات، مهاجم نباید بتواند نحوه رأی‌دادن رأی‌دهندگان درستکار را متوجه شود.

در این سیستم ارائه‌شده از یک اثبات صفردانش جدید برای صحت کدگذاری کاندیداها استفاده می شود و سکه‌های انداخته‌شده توسط رأی‌دهندگان جمع‌آوری و از آن‌ها برای *چالش* در پروتکل‌های صفردانش استفاده می‌شود. گرچه به دلیل ضعیف‌بودن میزان تصادفی‌بودن سکه‌ها نمی‌توان به طور مستقیم از آن‌ها استفاده کرد. پس در ادامه این طرح به چگونگی تولید یک دنباله چالش حداقل‌انتروپی از بیت‌های تصادفی گرفته‌شده از رأی‌دهندگان و چگونگی انجام پروتکل اثبات صفردانش با یک بررسی‌کننده با میزان تصادفی‌بودن ناقص اشاره می‌شود. تعمیمی از لِم Schwartz-Zipple برای میزان تصادفی‌بودن ناقص و یک راهبرد مناسب برای تقسیم سکه‌های رأی‌دهندگان بیان می‌شود که انتروپی به خاطر استراتژی مهاجم در مرجع انتخابات که تعدادی از رأی‌دهندگان را نیز کنترل می‌کند، از دست برود.

برای حریم خصوصی رأی‌دهنده‌ها از پیچیدگی اعمال نفوذ استفاده شده تا یک شبیه‌ساز ساخته شود که توانایی کاهش‌دادن حمله نقض حریم خصوصی رأی‌دهنده به یک تمایزدهنده تصمیم‌گیری دیفی-هلمن زیرنمایی را دارد. پس به این ترتیب، سیستم پیشنهادشده می‌تواند تحت فرضیات محاسباتی، حریم خصوصی و تازگی رسید را فراهم کند.

پس به طور خلاصه می‌توان گفت که سیستم مطرح‌شده قابلیت راستی‌آزمایی انتهابه‌انتها، حریم خصوصی و تازگی رسید در مدل استاندارد را داراست و تنها فرضیات در نظر گرفته شده، فرض تصمیم‌گیری دیفی-هلمن زیرنمایی و وجود یک تابلوی اعلانات همیشگی است. دلیل فرض وجود تابلوی اعلانات نیز مشخص است. زیرا بدون وجود این تابلوی اعلانات و با توجه به امکانات زیاد مهاجم، می‌تواند نتیجه را انتخابات را به سادگی تغییر داده و رأی‌دهندگان به هیچ وجه امکان راستی‌آزمایی آرای خود و نتیجه انتخابات را نخواهند داشت. حال ممکن است نحوه پیاده‌سازی چنین تابلوی اعلانات همیشه برقراری به چالش دیگری تبدیل شود که این در حوزه کار فعلی نیست؛ گرچه ایده‌های بسیاری برای این در کارهای گذشته وجود داشته است.

در طرح پیشنهادی مرجع انتخابات به عنوان یک موجودیت واحد در نقش بدخواه در بازی راستی‌آزمایی و درست‌کار در بازی حریم خصوصی ظاهر می‌شود. در عمل ممکن است بخواهیم مرجع

انتخابات را به چند اعتمادشونده تقسیم کرد که با هم وظایف مرجع انتخابات را انجام می‌دهند. با طراحی یک پروتکل آستانه‌ای کارا امکان ساخت چنین مرجع انتخاباتی نیز در این طرح وجود دارد.

باید دقت داشت که سیستم پیشنهادشده مجموعه همه خواسته‌های امنیتی مورد انتظار برای یک سیستم انتخابات را فراهم نمی‌کند. تعریف حریم خصوصی مطرح‌شده به تازگی رسید وابسته است؛ یعنی باید رأی‌دهنده، کلید محرمانه خود را از طریق یک کانال بکر[۲۸] دریافت کند. یک کانال بکر باعث می‌شود تا رأی‌دهنده بتواند اطلاعات منتقل‌شده از طریق آن را انکار کند. ضمناً این نکته مقاومت در برابر تهدید و اجبار برای فاش‌کردن کلید محرمانه و رأی شرکت‌کنندگان در انتخابات قبل از مرحله انداختن رأی را بررسی نمی‌کند؛ گرچه این مسئله ناقض حریم خصوصی نیست. تکینک‌هایی برای افزایش مقاومت در برابر تهدید و اجبار برای فاش‌سازی در انتخابات‌ها و رأی‌گیری‌های الکترونیکی وجود دارد که با سیستم مطرح‌شده نیز سازگار است. همچنین خواسته‌های دیگری مانند قابلیت استفاده در محدوده این کار نبوده است.

در سیستم پیشنهادی در [۱]، تعریف مبتنی بر بازی ارائه می‌شود که هم حریم خصوصی برگه رأی و هم تازگی رسید برای یک مرجع انتخابات واحد، که قابل گسترش به مرجع انتخابات توزیع‌شده نیز هست، را دربردارد.

در ادامه به شرح سیستم رأی‌گیری الکترونیکی مطرح‌شده در [۱] پرداخته خواهد شد.

۱.۳ مقدمات اولیه

از علائم زیر برای نمادگذاری در سیستم پیشنهادی استفاده می‌شود.

Π: سیستم انتخابات

λ: پارامتر امنیتی

n: تعداد رأی‌دهنده‌ها

[28] Untappable Channel

m: تعداد کاندیداها

$\mathcal{V} = \{V_1, \ldots, V_n\}$: مجموعه رأی‌دهنده‌ها

$\mathcal{P} = \{P_1, \ldots, P_m\}$: مجموعه کاندیدا

$\mathcal{U} \subseteq 2^{\mathcal{P}}$: مجموعه زیرمجموعه‌های کاندیداهای مجاز

$\mathcal{U}_\ell$: کاندیداهای انتخاب‌شده توسط رأی‌دهنده V_ℓ

اگر $\mathcal{P}^*$ را مجموعه بردارهای انتخاب‌ها از کاندیداها با طول دلخواه در نظر بگیریم، f را با عنوان تابع ارزیابی انتخابات می‌توان چنین تعریف کرد:

$$f: \mathcal{P}^* \to \mathbb{Z}_+^m \quad \text{s.t.} \quad f(\mathcal{U}_1, \ldots, \mathcal{U}_n) = \langle t_1, \ldots, t_m \rangle$$

که معادل است با یک بردار m-عضوی که در مکان i-ام آن، تعداد دفعاتی است که کاندیدای P_i انتخاب شده است.

به این ترتیب یک سیستم انتخابات الکترونیکی Π، شامل رأی‌دهندگان $V_1, \ldots, V_l$، مرجع انتخابات (EA) و تابلوی اعلانات (BB) خواهد بود.

۲.۳ نحو و صحت

یک سیستم انتخابات Π، یک پنج‌تایی از الگوریتم‌ها و پروتکل‌های زیر است:

- الگوریتم Setup $(1^\lambda, \mathcal{P}, \mathcal{V}, \mathcal{U})$ که توسط مرجع انتخابات اجرا می‌شود و یک کلید محرمانه msk، به همراه پارامترهای عمومی سیستم انتخابات Pub حاوی $\mathcal{P}, \mathcal{V}, \mathcal{U}$، و مقادیر محرمانه رأی‌دهندگان $s_1, \ldots, s_n$ را تولید می‌کند. EA یک حالت st دارد که در ابتدا msk است. EA در ابتدا گزارش عمومی $T = \text{Pub}$ را به BB ارسال می‌کند.
- پروتکل تعاملی Cast بین V_ℓ، BB و EA برقرار می‌شود. V_ℓ با ورودی $(\text{Pub}, s_\ell, \mathcal{U}_\ell)$، EA با ورودی msk و BB با ورودی T در پروتکل وارد می‌شوند. EA حالت خود و BB نیز T را به‌روز می‌کنند. در صورت موفقیت‌آمیزبودن، V_ℓ رسید α_ℓ را دریافت می‌کند. منظور از $view_\ell$ دید رأی‌دهنده V_ℓ در پروتکل Cast است.

- پروتکل تعاملی Tally بین BB و EA با ورودی مشترک Pub و EA با ورودی msk و BB با ورودی T صورت می‌گیرد. در صورت موفقیت‌آمیزبودن، BB گزارش عمومی T را به‌روز می‌کند.
- الگوریتم Result(T) نتیجه انتخابات یا R_T را برمی‌گرداند. در صورت تعریف‌نشده‌بودن نتیجه، خروجی $\perp$ برگردانده می‌شود. خروجی این الگوریتم، همان نتیجه شمارش آرا و نتیجه انتخابات است.
- الگوریتم Verify(T, α) که در آن α رسید رأی‌دهنده از خروجی پروتکل Cast است، خروجی‌ای از مقدار یک یا صفر برمی‌گرداند که بیانگر درست‌بودن راستی‌آزمایی یا عدم آن است.

در ادامه تعریف صحت انتخابات برای این سیستم مدل بیان می‌شود.

تعریف صحت انتخابات - سیستم انتخابات Π صحت دارد اگر برای هر اجرای درستکارانه از آن:

$$\mathrm{Result}(T) = \mathrm{f}(\mathcal{U}_1,\ldots,\mathcal{U}_\mathrm{n}) \text{ and } \wedge_{\ell=1}^{n} (\mathrm{Verify}(T,\alpha_\ell) = 1).$$

۳.۳ قابلیت راستی‌آزمایی

برای تعریف صوری قابلیت راستی‌آزمایی از تعریف مبتنی بر بازی استفاده شده است. یک بازی $G_{E2E-Ver}^{A,\varepsilon,d,\theta}(1^\lambda, \mathrm{m}, \mathrm{n})$ بین مهاجم A و چالش‌گر C که از استخراج‌کننده رأی ε استفاده می‌کند، برگزار می‌شود که در آن d مقدار اختلافی است که مهاجم می‌خواهد به آن دست یابد و θ حداقل تعداد رأی‌دهنده که مهاجم باید اجازه دهد تا درست‌کارانه رأی دهند و موفقیت‌آمیز خاتمه یابد. مهاجم کنترل کامل EA را در اختیار دارد و اجرای پروتکل Cast، نقش EA در دست مهاجم است. برای هر رأی‌دهنده مهاجم می‌تواند انتخاب کند که خرابکاری کند یا اجازه بدهد چالش‌گر از طرف او بازی کند.

در این بازی مهاجم زمانی می‌برد که یا همه θ رأی‌دهنده درست‌کار که پروتکل Cast را با موفقیت به اتمام رسانده‌اند، حساب‌رسی نتایج را نیز انجام داده باشند اما اختلاف با نتایج واقعی انتخابات حداقل d باشد یا در حالت دیگر، ε نتواند مجموعه کاندیداها برای کاربر غیردرست‌کار را فراهم کند. در شکل ۱، بازی حمله با جزئیات مطرح شده است.

E2E Verifiability Game $G^{\mathcal{A},\mathcal{E},d,\theta}_{\text{E2E}-\text{Ver}}(1^\lambda, m, n)$

1. $\mathcal{A}$ chooses a list of candidates $\mathcal{P} = \{P_1, ..., P_m\}$, a set of voters $\mathcal{V} = \{V_1, ..., V_n\}$ and the set of allowed candidate selections $\mathcal{U}$. It provides $\mathcal{C}$ with the sets $\mathcal{P}, \mathcal{V}, \mathcal{U}$ along with information Pub and voter credentials $\{s_\ell\}_{\ell\in[n]}$. Throughout the game, $\mathcal{C}$ plays the role of the BB.
2. The adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ engages in an interaction where $\mathcal{A}$ schedules the Cast protocols of all voters. For each voter V_ℓ, $\mathcal{A}$ can either completely control the voter or allow $\mathcal{C}$ to operate on their behalf, in which case $\mathcal{A}$ provides a candidate selection $\mathcal{U}_\ell$ to $\mathcal{C}$. Then, $\mathcal{C}$ engages with the adversary $\mathcal{A}$ in the Cast protocol so that $\mathcal{A}$ plays the role of EA. Provided the protocol terminates successfully, $\mathcal{C}$ obtains the receipt α_ℓ on behalf of V_ℓ.
   Let $\tilde{\mathcal{V}}$ be the set of honest voters (i.e., those controlled by $\mathcal{C}$) that terminated successfully.
3. Finally, $\mathcal{A}$ posts the election transcript τ to the BB.

The game returns a bit which is 1 if and only if the following conditions hold true:

(i). $|\tilde{\mathcal{V}}| \geq \theta$, (i.e., at least θ honest voters terminated).

(ii). $\forall \ell \in [n]$: if $V_\ell \in \tilde{\mathcal{V}}$, then $\mathbf{Verify}(\tau, \alpha_\ell) = 1$ (i.e., the voters in $\tilde{\mathcal{V}}$ verify their ballot successfully).

and either one of the following two conditions:

(iii-a). If $\perp \neq \langle \mathcal{U}_\ell \rangle_{V_\ell \in \mathcal{V}\setminus\tilde{\mathcal{V}}} \leftarrow \mathcal{E}(\tau, \{\alpha_\ell\}_{V_\ell\in\tilde{\mathcal{V}}})$,
then
$$\mathrm{d}_1(\mathbf{Result}(\tau), f(\langle \mathcal{U}_1, \ldots, \mathcal{U}_n \rangle)) \geq d.$$

(iii-b). $\perp \leftarrow \mathcal{E}(\tau, \{\alpha_\ell\}_{V_\ell\in\tilde{\mathcal{V}}})$.

شکل ۱ – بازی قابلیت راستی‌آزمایی انتهابه‌انتها بین چالش‌گر C و مهاجم A با استفاده از استخراج‌کننده رأی ε [۱]

تعریف قابلیت راستی‌آزمایی انتهابه‌انتها – اگر $0 < \epsilon < 1$ و $n, m, d, \theta \in N$ و $0 < \theta \leq n$ و $d > 0$ باشد، پروتکل انتخابات Π با توجه به تابع ارزیابی f قابلیت راستی‌آزمایی انتهابه‌انتها با دقت ϵ را دارد، اگر برای تعداد حداقل θ رأی‌دهنده درست‌کار موفق و اختلاف نتیجه شمارش d، یک استخراج‌کننده رأی ε وجود داشته باشد به طوری‌که برای هر مهاجم A:

$$\Pr\left[G^{A,\varepsilon,d,\theta}_{E2E-Ver}(1^\lambda, m, n) = 1 \right] \leq \epsilon$$

لازم به ذکر است که لزومی ندارد که استخراج‌کننده رأی در مرتبه زمانی چندجمله‌ای باشد.

۴.۳ حریم خصوصی رأی‌دهنده (شامل تازگی رسید)

در این جا مهاجم به دنبال آن است که با داشتن (۱) رسیدهایی که بعد از انداختن رأی داده می‌شود و (۲) مجموعه‌ای از دیدهای پروتکل سازگار با همه دیدهای رأی‌دهندگان درست‌کار در پروتکل Cast، بتواند تشخیص دهد که چگونه رأی‌دهنده درست‌کار رأی داده است. به این معنا که آیا می‌تواند با داشتن رسیدها و سایر پارامترهای عمومی انتخابات، اطلاعاتی درباره کاندیداهای انتخاب‌شده توسط یک

رأی‌دهنده را یاد بگیرد. در تعریف حریم خصوصی اجازه مشاهده دیدهای رأی‌دهندگان در پروتکل Cast به مهاجم داده می‌شود. از طرف دیگر هم رأی‌دهنده اجازه دارد درباره دیدش در این پروتکل دروغ بگوید. پس ورودی رأی‌دهنده به پروتکل Cast باید در کانال بکر باشد تا مهاجم کلید محرمانه را نفهمد.

در تعریف صوری برای این خواسته‌های امنیتی، مجدداً از از رویکرد مبتنی بر بازی استفاده شده است. یک بازی $G_{t-priv}^{A,S}(1^{\lambda}, \mathrm{m}, \mathrm{n})$ بین یک مهاجم A و یک چالش‌گر C برگزار می‌شود. در این بازی وجود یک شبیه‌ساز رأی‌دهنده کارا S برای تهیه یک دید شبیه‌سازی‌شده از رأی‌دهنده در پروتکل Cast مفروض است. به طور شهودی، شبیه‌ساز نحوه دروغ‌گویی رأی‌دهنده درباره کاندیداهای انتخاب‌شده در پروتکل Cast را نیز مدل می‌کند.

در این بازی چالش‌گر یک سکه b را پرتاب می‌کند و پروتکل راه‌اندازی را انجام می‌دهد. سپس مهاجم همه پروتکل‌های Cast را مطابق با این‌که می‌خواهد دست‌کاری کند یا اجازه بدهد رأی‌دهنه درست‌کارانه رأی‌دهد، برنامه‌ریزی می‌کند. مهاجم مجاز به دست‌کاری حداکثر t رأی‌دهنده است. رأی‌دهندگانی که دست‌نخورده باقی مانده‌اند توسط چالش‌گر عمل خواهند کرد و از میان دو مجموعه کاندیداهای انتخاب‌شده حق انتخاب دارند. چالش‌گر بین دو مجموعه کاندیداهای انتخاب‌شده با توجه به مقدار بیت b انتخاب خواهد کرد. اگر b=0 باشد، مهاجم رسید گرفته‌شده توسط هر رأی‌دهنده را دریافت می‌کند که دید واقعی هر رأی‌دهنده در پروتکل Cast است، و اگر b=1، یک دید شبیه‌سازی‌شده. پس از اتمام انداختن برگه‌های رأی، چالش‌گر پروتکل Tally را اجرا می‌کند و نتیجه انتخابات را منتشر می‌کند. سپس مهاجم درباره مقدار b حدس می‌زند. این حمله زمانی موفقیت‌آمیز خواهد بود که مهاجم t رأی‌دهنده را دست‌کاری کرده باشد، نتیجه انتخابات مشابه با دو حالت فراهم‌شده برای هر رأی‌دهنده درست‌کار باشد و مهاجم حدس بیت b چالش‌گر را مدیریت کند. جزئیات بیشتر این بازی در شکل ۲ آمده است.

Voter Privacy/Receipt-freeness Game $G^{\mathcal{A},\mathcal{S}}_{t\text{-priv}}(1^\lambda, n, m)$

1. $\mathcal{A}$ on input $1^\lambda, n, m$, chooses a list of candidates $\mathcal{P} = \{P_1, ..., P_m\}$, a set of voters $\mathcal{V} = \{V_1, ..., V_n\}$, and the set of allowed candidate selections $\mathcal{U}$. It provides $\mathcal{C}$ the sets $\mathcal{P}$, $\mathcal{V}$, and $\mathcal{U}$.
2. $\mathcal{C}$ flips a coin $b \in \{0,1\}$ and performs the **Setup** protocol on input $(1^\lambda, \mathcal{P}, \mathcal{V}, \mathcal{U})$ to obtain $msk, s_1, \ldots, s_n$, Pub; it provides $\mathcal{A}$ with Pub.
3. The adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ engage in an interaction where $\mathcal{A}$ schedules the **Cast** protocols of all voters which may run concurrently. For each voter $V_\ell \in \mathcal{V}$, the adversary chooses whether V_ℓ is corrupted:
   - If V_ℓ is corrupted, then $\mathcal{C}$ provides s_ℓ to $\mathcal{A}$, and then they engage in a **Cast** protocol where $\mathcal{A}$ plays the role of V_ℓ and $\mathcal{C}$ plays the role of EA and BB.
   - If V_ℓ is not corrupted, $\mathcal{A}$ provides two candidate selections $\langle \mathcal{U}^0_\ell, \mathcal{U}^1_\ell \rangle$ to the challenger $\mathcal{C}$. $\mathcal{C}$ operates on V_ℓ's behalf, using $\mathcal{U}^b_\ell$ as the V_ℓ's input. The adversary $\mathcal{A}$ is allowed to observe the network trace of the **Cast** protocol where $\mathcal{C}$ plays the roles of V_ℓ, EA, and BB. When the **Cast** protocol terminates, the challenger $\mathcal{C}$ provides to $\mathcal{A}$: (i) the receipt α_ℓ that V_ℓ obtains from the protocol, and (ii) if $b = 0$, the current view of the internal state of the voter V_ℓ, $view_\ell$, that the challenger obtains from the **Cast** execution, or if $b = 1$, a simulated view of the internal state of V_ℓ produced by $\mathcal{S}(view_\ell)$.
4. $\mathcal{C}$ performs the **Tally** protocol playing the role of EA and BB. $\mathcal{A}$ is allowed to observe the network trace of that protocol.
5. Finally, $\mathcal{A}$ using all information collected above (including the contents of the BB) outputs a bit b^*.

Denote the set of corrupted voters as $\mathcal{V}_{\text{corr}}$ and the set of honest voters as $\bar{\mathcal{V}} = \mathcal{V} \setminus \mathcal{V}_{\text{corr}}$. The game returns a bit which is 1 if and only if the following hold true:

(i). $b = b^*$ (i.e., the adversary guesses b correctly).

(ii). $|\mathcal{V}_{\text{corr}}| \leq t$ (i.e., the number of corrupted voters is bounded by t).

(iii). $f(\langle \mathcal{U}^0_\ell \rangle_{V_\ell \in \bar{\mathcal{V}}}) = f(\langle \mathcal{U}^1_\ell \rangle_{V_\ell \in \bar{\mathcal{V}}})$ (i.e., the election result w.r.t. the set of voters $\bar{\mathcal{V}}$ does not leak b).

شکل ۲ – بازی حریم خصوصی رأی‌دهنده / تازگی رسید [۱]

تعریف حریم خصوصی رأی/تازگی رسید – اگر $n, m \in N$ باشد، پروتکل انتخابات Π با توجه به تابع ارزیابی f خواسته حریم خصوصی رأی‌دهنده / تازگی رسید برای حداکثر t رأی‌دهنده دست‌کاری‌شده را دارد، اگر یک شبیه‌ساز رأی PPT[۲۹] به نام S وجود داشته باشد که برای هر مهاجم $\mathcal{A}$:

$$\left| \Pr\left[G^{A,S}_{t-priv}(1^\lambda, m, n) = 1 \right] - \frac{1}{2} \right| = negl\,(\lambda)$$

[29] Probability Polynominal Time

فصل چهارم

بیان سیستم پیشنهادی

بیان سیستم پیشنهادی

سیستم پیشنهادی شامل سه مرحله راه‌اندازی، برگه رأی‌انداختن و شمارش است که به موازات یک پروتکل سیگما انجام می‌شود. در طول مرحله راه‌اندازی، EA تعدادی تعهد و داده پیش‌حساب‌رسی متناظر با گام اول یک پروتکل سیگما تولید می‌کند که برای اعتبارسنجی تعهدها به کار خواهد آمد. در طول مرحله برگه رأی‌انداختن، رأی‌دهندگان با EA وارد پروتکل می‌شوند که نتیجه آن ثبت آرای آن‌ها و ارسال یک سکه‌اندازی تصادفی که برای تولید چالش در پروتکل سیگما کاربرد دارد، خواهد بود. سپس رأی‌دهندگان یک رسید به عنوان خروجی مرحله انداختن برگه رأی دریافت می‌کنند که برای حساب‌رسی نتیجه انتخابات استفاده خواهد شد. در گام سوم و پایانی، EA نتیجه شمارش انتخابات را تولید می‌کند و پروتکل سیگما را با منتشرکردن بازکننده[۳۰]های تعهدهای صورت‌گرفته و اطلاعات دیگر برای راستی‌آزمایی تکمیل می‌کند. مرحله راستی‌آزمایی در هر زمانی پس از اتمام فرایند فوق با استفاده از مجموعه‌ای از حداقل یک رسید تولیدشده در مرحله انداختن برگه رأی قابل انجام است.

در این سیستم از یک رویکرد کد-رأی[۳۱] استفاده می‌شود. به این ترتیب که کد-رأی‌های متناظر با تعهدها را به BB ارسال می‌کند و رأی‌دهندگان آرای خود را با ارسال کد-رأی دلخواه خود به EA می‌اندازند. تعهدها دارای خاصیت هم‌ریختی جمع‌شونده هستند. بنابراین این امکان وجود دارد که با جمع‌زدن تعهدها و بازکردن نتیجه شمارش تعهدها، به نتیجه شمارش آرا دست یافت. اثبات برای اطمینان‌یافتن از قابلیت راستی‌آزمایی حاصل ترکیب یک اثبات برش‌وانتخاب[۳۲] به همراه اثبات سیگما است که مقدار متعهدشده متعلق به یک مجموعه است. چالش مورد نیاز برای اثبات سیگما توسط به‌کاربستن یک مکانیزم استخراج مناسب از سکه‌اندازی‌های کاربران است که توسط EA جمع‌آوری می‌شود.

در ادامه درباره جزئیات مورد نیاز برای شرح سیستم پیشنهادی بحث خواهد شد.

---

[30] Openning

[31] Vote-Code

[32] Cut-and-Choose

۱.۴ تعهد کاملا بسته‌شده

برای دست‌یابی به صحت در مقابل مهاجم‌های با توان محاسباتی نامحدود، باید از یک طرح تعهد کاملا بسته‌شده[۳۳] استفاده کرد. علاوه بر آن، در این طرح نیاز به ویژگی هم‌ریختی جمع‌شونده برای سهولت در فرایند شمارش و حساب‌رسی وجود دارد. از طرح تعهد مبتنی بر الجمال روی منحنی‌های بیضوی[۳۴] بهره گرفته می‌شود. پارامترهای دامنه منحنی‌های بیضوی Param := (p, a, b, g, q) که توسط مولد منحنی $\mathcal{G}(1^{\lambda})$ تولید می‌شود، شامل یک عدد اول p، دو عضو $a,b \in F_p$ که مشخص‌کننده معادله منحنی $E: y^2 = x^2 + ax + b \pmod p$ هستند، یک نقطه پایه $g = (x_g, y_g)$ روی منحنی و یک عدد اول q از مرتبه g است. فرض بر این است که تصمیم‌گیری دیفی-هلمن روی گروه G برقرار است. به این معنا که اگر a و b به طور تصادفی انتخاب شوند، آنگاه $g^{a.b}$ نیز تصادفی به نظر برسد.

جزئیات بیشتر این طرح تعهد به شرح زیر است.

Gen(Param; 1^{λ}):

picks $x \leftarrow Zq$, sets $h := g^x$, and outputs ck := (Param; h)

$Com_{ck}(m; r)$:

outputs $c := (g^r; g^m h^r)$

$Ver_{ck}(c; m; r)$:

outputs accept if $c = (g^r; g^m h^r)$; otherwise, outputs reject

واضح است که طرح تعهد فوق کاملا بسته‌شده و از نظر محاسباتی تحت فرض تصمیم‌گیری دیفی-هلمن پنهان‌کننده است؛ یعنی برای هر مهاجم A داریم:

$$\mathsf{Adv}_{\mathrm{hide}}(\mathcal{A}) := \left| \Pr \left[\begin{array}{l} \mathsf{Param} \leftarrow \mathcal{G}(1^\lambda); \mathsf{ck} \leftarrow \mathsf{Gen}(\mathsf{Param}, 1^\lambda); \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{Param}, \mathsf{ck}); b \leftarrow \{0,1\}; \\ r \leftarrow \mathbb{Z}_q : \mathcal{A}(\mathsf{Com}_{\mathsf{ck}}(m_b; r)) = b \end{array} \right] - 1/2 \right|$$

در برابر λ ناچیز است. از طرف دیگر، طرح تعهد ذکرشده هم‌ریختی جمع‌شونده است.

[33] Perfectly Binding Commitment Scheme

[34] Elliptic Curves

$$Com_{ck}(m_1; r_1) \,.\, Com_{ck}(m_2; r_2) = Com_{ck}(m_1+m_2; r_1+r_2)$$

۲.۴ یک پروتکل سیگما برای صحت کدگذاری کاندیداها

گیریم $N = n+1$، که در آن n تعداد رأی‌دهندگان است. به هر رأی‌دهنده یک برگه رأی داده می‌شود که شامل دو قسمت مشابه حاوی لیستی از m کد-رأی مربوط به لیست کاندیداهاست. رأی‌دهنده سکه‌ای می‌اندازد برای این‌که از یکی از قسمت‌های برگه رأی انتخاب کند. در مرحله راه‌اندازی، هر برگه رأی در قالب تعهدشده به BB ارسال می‌شود. در واقع، شامل دو مجموعه تعهدهای $E_{l,j}^{(a)}$ است که $a\in\{0,1\}$, $\ell = 1,...,n$, $j = 1,...,m$ و هر مجموعه به جایگشتی از کاندیداهای کدگذاری‌شده متعهد می‌شود. کاندیدای P_j با مقدار N^{j-1} کدگذاری می‌شود.

تأکید می‌شود که لزومی ندارد که حتما اثبات شود که در یک انتخابات ۱-از-m، هر مجموعه از تعهدها به جایگشتی از کاندیداهای کدگذاری‌شده متعهد می‌شود. این مسئله دو دلیل دارد: (۱) EA متناسب با سکه‌اندازی رأی‌دهنده یکی از دو مجموعه تعهدها را باز می‌کند. پس یک مرجع انتخابات بدخواه اگر مجموعه تعهدها جایگشتی از کاندیداهای کدگذاری نباشد یا جایگشتی ناسازگار از آن‌ها باشد، با احتمال ½ برای هر رأی‌دهنده درست‌کار لو می‌رود. در یک انتخابات ۱-از-m تنها یکی از تعهدها برای شمارش استفاده خواهد شد و بنابراین، اثبات این که مجموعه تعهدها به یک جایگشت نامعلوم از کدگذاری کاندیداها متعهد می‌شود تنها این تضمین را ایجاد می‌کند که تعهد شمارش به یک کاندیدای کدگذاری‌شده متعهد می‌شود. گرچه این تضمین بسیار مهم است. در غیر این صورت، با توجه به ویژگی هم‌ریختی‌بودن شمارش، ممکن بود EA متقلب اختلاف بزرگی را با استفاده از تنها یک برگه رأی تقلبی در نتایج واقعی انتخابات ایجاد کند. به عنوان مثال، EA ممکن است به $1000.N^{j-1}$ برای یکی از jها متعهد شود. بنابراین از EA می‌خواهیم تا نشان دهد که تنها به یکی از N^{j-1}ها متعهد شده است. تعهدهای E را در نظر بگیرید. اثبات‌کننده می‌خواهد بررسی‌کننده را متقاعد کند که r را می‌داند به طوری که $E = Com_{ck}(N^i; r)$ برای iهای بین صفر تا m-1. اگر i و r را ورودی خصوصی اثبات‌کننده در نظر بگیریم، می‌توان پروتکل سیگمای مطرح‌شده را داشت.

در قضیه عنوان‌شده در مقاله [۱] می‌توان بیان کرد که پروتکل مطرح‌شده، خواسته‌های امنیتی برای طرح تعهد مورد نظر را داراست. این پروتکل کاملا جامع[۳۵] و به طور آماری مانع[۳۶] است.

$P(i, r)$:

Define b_j such that $i = \sum_{j=0}^{\log m-1} b_j 2^j$. Pick

- $t_j, z_j, y_j, r_j, w_j, f_j \leftarrow \mathbb{Z}_q$ for $j \in [0, \log m - 1]$.

Compute the following commitments:

- For $j \in [0, \log m - 1]$,
  - $B_j = \mathsf{Com}_{\mathsf{ck}}(b_j; r_j)$; $T_j = \mathsf{Com}_{\mathsf{ck}}(t_j; z_j)$;
  - $Y_j = \mathsf{Com}_{\mathsf{ck}}((1 - b_j)t_j; y_j)$;
  - $W_j = \mathsf{Com}_{\mathsf{ck}}(w_j; f_j)$.

Define A_j, a_j, r'_j such that $A_j = B_j^{N^{2^j}-1} \cdot \mathsf{Com}_{\mathsf{ck}}(1; 0) = \mathsf{Com}_{\mathsf{ck}}(a_j; r'_j)$, for $j \in [0, \log m - 1]$. Define $\{\beta_j, \gamma_j\}_{j=0}^{\log m}$ such that $\prod_{j=0}^{\log m-1}(a_j X + w_j) = \sum_{j=0}^{\log m} \beta_j X^j$ and $\prod_{j=0}^{\log m-1}(r'_j X + f_j) = \sum_{j=0}^{\log m} \gamma_j X^j$. (Note that for efficiency reasons, the prover needs to choose the $\{r_j\}_{j=0}^{\log m-1}$ such that $\gamma_{\log m} = r$ in previous step.)

- For $j \in [0, \log m - 1]$, $D_j = \mathsf{Com}_{\mathsf{ck}}(\beta_j; \gamma_j)$.

Return $\phi_1 = \{B_j, T_j, Y_j, W_j, D_j\}_{j=0}^{\log m-1}$ and

$\mathrm{state}_\phi = \{t_j, z_j, y_j, r_j, b_j, w_j, f_j\}_{j=0}^{\log m-1}$.

$P \to V$: Send ϕ_1.

$V \to P$: Send $\rho \leftarrow \mathbb{Z}_q$.

$P(\mathrm{state}_\phi)$: Compute the following answers:

- For $j \in [0, \log m - 1]$,
  - $t'_j = b_j \rho + t_j, z'_j = r_j \rho + z_j, y'_j = -y_j - r_j t'_j$;
  - $w'_j = a_j \rho + w_j, f'_j = r'_j \rho + f_j$;

Set $\phi_2 = \{t'_j, z'_j, y'_j, w'_j, f'_j\}_{j=0}^{\log m-1}$.

$P \to V$: send ϕ_2

$V(E, \phi_1, \rho, \phi_2)$: Accept the proof (i.e. output accept) if and only if

- For $j \in [0, \log m - 1]$,
  - $B_j^\rho \cdot T_j = \mathsf{Com}_{\mathsf{ck}}(t'_j, z'_j)$,
  - $(\mathsf{Com}_{\mathsf{ck}}(1; 0)/B_j)^{t'_j}/Y_j = \mathsf{Com}_{\mathsf{ck}}(0; y'_j)$;
  - $A_j^\rho \cdot W_j = \mathsf{Com}_{\mathsf{ck}}(w'_j, f'_j)$;
- $E^{\rho^{\log m}} \prod_{j=0}^{\log m-1} D_j^{\rho^j} = \mathsf{Com}_{\mathsf{ck}}(\prod_{j=0}^{\log m-1} w'_j; \prod_{j=0}^{\log m-1} f'_j)$;

شکل ۳ –پروتکل سیگما برای صحت برگه رأی [۱]

[35] Complete

[36] Sound

۳.۴ تولید چالش‌های بررسی‌کننده

یکی از دشواری‌ها این است که به دنبال استخراج چالش‌های پروتکل سیگما از سکه‌های رأی‌دهندگان $a = <a_1, \ldots, a_n>$ با استفاده از الگوریتمی قطعی هستند. باید توجه داشت که ممکن است بعضی از رأی‌دهندگان بدخواه باشند و با EA تبانی کرده باشند. لذا انتروپی سکه‌های رأی‌دهندگان تنها ناشی از رأی‌دهندگان درست‌کار خواهد بود. ضمنا باید در نظر داشت که سکه‌های رأی‌دهندگان از نظر شماره سریال‌ها باید مرتب شود و نه ترتیب ارسال. زیرا در حالت دوم مهاجم می‌تواند پروتکل Cast را برنامه‌ریزی کند و باعث کاهش حداقل‌انتروپی به $\log\theta$ می‌شود که در آن θ تعداد رأی‌دهندگان درست‌کار است. این مقدار انتروپی برای فراهم‌کردن خطای اعتبارسنجی کوچک کافی نیست. برای همه برگه‌های رأی انداخته‌نشده، سکه‌های مرتبط با آن‌ها را به صورت پیش‌فرض صفر در نظر می‌گیرند. پس a یک منبع همواره n-بیتی است که یک منبع ضعیف‌تری نسبت به منبع بیت‌ثابت غیربی‌توجه[۳۷] است. برای افزایش میزان تصادفی‌بودن با توجه به وابستگی به مقدار سکه‌اندازی رأی‌دهندگان طرح زیر پیشنهاد شده است.

گیریم $\{0,1\}^{\ell_\Sigma}$ فضای چالش‌ها باشد که $\ell_\Sigma = \lfloor q \rfloor$ و q مرتبه گروه باشد. سکه‌های رأی‌دهندگان a به طور یکسان به k بلوک افراز می‌شوند؛ یعنی $a_1,\ldots,a_k$. برای هر a_i، صحت برگه رأی EA با استفاده از یک پروتکل سیگما جداگانه که در آن a_i چالش باشد، باید اثبات شود. صحت اثبات EA توسط بررسی‌کننده در صورتی‌که همه پروتکل‌های سیگما معتبر باشند، پذیرفته خواهد شد. قضیه بعدی مشخص می‌کند که خطای درستی با k-بار اجرای پروتکل سیگما به شرح بالا، به صورت نمایی افت می‌کند.

قضیه – اگر $a = (a_1,\ldots,a_k)$ و $H_\infty(a) = \theta$، برای همه اثبات‌کننده‌های مهاجم A داریم:

$$\epsilon(m,n,k,\theta) = \Pr\left[\begin{array}{l} \mathsf{ck} \leftarrow \mathsf{Gen}(\mathsf{Param}, 1^\lambda); (E, x, r, \{\phi_{1,i}\}_{i=1}^k) \leftarrow \mathcal{A}(\mathsf{Param}, \mathsf{ck}); \\ \{\phi_{2,i}\}_{i=1}^k \leftarrow \mathcal{A}(\mathrm{a}_1, \ldots, \mathrm{a}_k) : \mathsf{Ver}_{\mathsf{ck}}(E; x; r) = \mathsf{accept} \quad \wedge \\ x \notin \{N^0, \ldots, N^{m-1}\} \ \wedge \ \forall i \in [k], V(E, \phi_{1,i}, \mathrm{a}_i, \phi_{2,i}) = \mathsf{accept} \end{array}\right] \leq 2^{k \log\log m - \theta + k}.$$

[37] Non-Oblivious Bit-Fixing Source

۴.۴ شرح جزئیات سیستم پیشنهادی

برای سادگی، شرح سیستم برای انتخابات ۱-از-m بیان می‌شود که مشابه انتخابات ریاست جمهوری ایران است؛ یعنی $\mathcal{U} = \{\{P_1\}, ..., \{P_m\}\}$. طرح تعهد و پروتکل سیگمای مورد استفاده در سیستم، همان طرح‌های مطرح‌شده در قبل است. صحت سیستم پیشنهادی از طریق استقرا قابل اثبات است و سیستم پیشنهادشده، پیاده‌سازی نیز شده است [۱]. گام‌های سیستم به شرح زیر خواهند بود:

- $\text{Setup}(1^\lambda, \mathcal{P}, \mathcal{V}, \mathcal{U})$
  - اجرای $\text{Gen}(\text{Param}, 1^\lambda)$ توسط EA برای محاسبه کلید تعهد ck
  - برای هر $\ell \in [n]$، EA مراحل زیر را انجام می‌دهد:
    - انتخاب شماره منحصربه‌فرد برای برگه رأیِ دوتایی ℓام (tag_ℓ)
    - انتخاب جایگشت‌های تصادفی $\pi_\ell^{(0)}$ و $\pi_\ell^{(1)}$ روی [m] برای بهم‌ریختن ترتیب زوج‌های (کد-رأی، کاندیدا) در بخش $s_\ell^{(i)}$ از برگه رأی دوتایی s_ℓ
    - برای حفظ حریم خصوصی، جایگشت‌های برگه‌های رأی را به صورت متعهدشده به BB ارسال می‌کند.
    - برای $j \in [m]$، کد-رأی‌های منحصربه‌فرد $C_{\ell,j}^{(0)}, C_{\ell,j}^{(1)} \leftarrow Zq$
      - $C_{\ell,j}^{(i)}$ قسمتی از بخش $s_\ell^{(i)}$ از s_ℓ است که کاندیدای Pj را مشخص می‌کند.
    - برای $a \in \{0,1\}$، بخش $s_\ell^{(a)} = \{(P_j, C_{\ell,j}^{(a)})\}_{j \in [m]}$ و در نهایت، برگه رأی $s_\ell = (tag_l, s_\ell^{(0)}, s_\ell^{(1)})$ را تولید می‌کند.
    - برای $j \in [m]$، محاسبه $j' = \pi_\ell^{(0)}(j)$ و
      - برای $a \in \{0,1\}$، انتخاب مقدار تصادفی $t_{\ell,j'}^{(a)} \leftarrow Z_q$ و محاسبه تعهد کد-رأی برای $C_{\ell,j'}^{(a)}$:

$$U_{\ell,j'}^{(a)} = Com_{ck}(C_{\ell,j'}^{(a)}; t_{\ell,j'}^{(a)})$$

- برای a∈{0,1}، انتخاب مقدار تصادفی $r_{\ell,j'}^{(a)} \leftarrow Z_q$ و محاسبه تعهد کدشده کاندیدا برای $P_{j'}$:

$$E_{\ell,j'}^{(a)} = Com_{ck}((n+1)^{j'-1}; r_{\ell,j'}^{(a)})$$

که در آن $(n+1)^{j'-1}$ کدشده کاندیدای $P_{j'}$ است.

- برای a∈{0,1}، داده پیش‌حسابرسی $\phi_{1,\ell,j'}^{(a)}$ برای راستی‌آزمایی $E_{\ell,j'}^{(a)}$ تولید می‌شود. حالت اثبات‌کننده $state_{1,\ell,j'}^{(a)}$ را نیز نگه‌داری می‌کند. (نحوه تولید این دو در گام اول پروتکل سیگما)
- اطلاعات عمومی مربوط به s_ℓ، یعنی Pub_ℓ به شکل زیر است:

$$Pub_\ell = (tag_l, \{(U_{\ell,j'}^{(a)}, E_{\ell,j'}^{(a)}, \phi_{1,\ell,j'}^{(a)})\}_{j\in[m]}^{a\in\{0,1\}}$$

که بر اساس tag مرتب شده‌اند.

  - اطلاعات عمومی که توسط EA تولید می‌شود:

$$Pub = (ck, \mathcal{P}, \mathcal{U}, \{Pub_\ell\}_{l\in[n]}$$

و کلید محرمانه EA:

$$msk = \{Pub_\ell, s_l, msk_l, state_{\phi,l}\}_{l\in[n]}$$

$$msk_\ell = \{(C_{\ell,j}^{(a)}, t_{\ell,j}^{(a)}, \pi_\ell^{(a)}(j) = j', r_{\ell,j}^{(a)})\}_{j\in[m]}^{a\in\{0,1\}} \text{ and } \text{state}_{\phi,\ell} = \{\text{state}_{\phi,\ell,j'}^{(a)}\}_{j\in[m]}^{a\in\{0,1\}}$$

- Cast
  - ورودی $(Pub_\ell, s_l, \mathcal{U}_l)$
  - V_l با سکه‌اندازی $a_l \leftarrow \{0,1\}$ و انتخاب بخش برای $s_\ell^{(a)}$ رأی‌دادن
  - کاندیدای مورد نظر $\mathcal{U}_l = \{P_{j_l}\}$

- V_l باید $C_{\ell,j_l}^{(a_l)}$ که کد-رأی متناظر با P_{j_l} در بخش $s_\ell^{(a)}$ است، ارائه کند.
- در نهایت، V_l رأی $\psi_\ell = (tag_l, a_l, C_{\ell,j_l}^{(a_l)})$ را بیندازد.
- EA رأی را می‌گیرد و حالت st خود را با اضافه‌کردن ψ_ℓ به‌روز می‌کند. رسید α_ℓ حاوی رأی ψ_ℓ و بخش $s_\ell^{(1-a_l)}$ برای حسابرسی به V_l داده می‌شود.

- Tally
  - $\tilde{V}$: مجموعه رأی‌دهندگانی که با موفقیت رأی دادند.
  - برای هر $V_l \in \tilde{V}$، EA از (tag_l, a_l) از ψ_ℓ ، برای بازیابی اطلاعات حسابرسی $s_\ell^{(1-a_l)}$ از s_ℓ استفاده می‌کند.
  - ارسال لیست $\{(\psi_\ell, s_\ell^{(1-a_l)})\}_{V_l \in \tilde{V}}$ به BB
  - بازکردن همه تعهدهای کد-رأی‌ها $(\{U_{\ell,\mathrm{j}}^{(a)}\}_{l\in[n],\, j\in[m]}^{a\in\{0,1\}})$ با ارسال لیست زوج‌های $\{C_{\ell,\mathrm{j}}^{(a)}, t_{\ell,\mathrm{j}}^{(a)}\}_{l\in[n],\, j\in[m]}^{a\in\{0,1\}}$ به BB
  - EA برای هر ψ_ℓ متناظر با $V_l \in \tilde{V}$ مراحل زیر را انجام می‌دهد:
    - محل کد-رأی بازشده C_ℓ که با کد-رأی انداخته‌شده $C_{\ell,j_l}^{(a_l)}$ مطابقت می‌کند، را پیدا می‌کند.
    - کد-رأی C_ℓ را با نشان 'voted' مشخص می‌کند.
    - تعهد $E_{\ell,j'_l}^{(a_l)}$ مربوطه را به مجموعه $\mathrm{E_{tally}}$ اضافه می‌کند.
      - یادآوری: $j_{\ell'} = \pi_\ell^{(a_l)}(j_l)$
    - همه تعهدهای $\{E_{\ell,\mathrm{j}}^{(1-a_l)}\}_{j\in[m]}$ مرتبط با کد-رأی‌های موجود در $s_\ell^{(1-a_l)}$ را به مجموعه $\mathrm{E_{open}}$ اضافه می‌کند.
  - در نهایت، $\mathrm{E_{tally}}$ حاوی مجموعه آرا برای شمارش و $\mathrm{E_{open}}$ حاوی اطلاعات برای راستی‌آزمایی صحت برگه رأی است.

- ارسال لیست کد-رأی‌های نشان‌دار به همراه E_{tally} و E_{open} به BB
- تولید همه چالش‌های $\{\rho_E\}_{E\in E_{tally}}$ پروتکل‌های سیگما برای اعتبارسنجی تعهدهای موجود در E_{tally} و ارسال آن‌ها به BB (گام دوم پروتکل سیگما)
  - استخراج چالش‌ها از تصادفی‌بودن مربوط به سکه‌اندازی رأی‌دهندگان
- تهیه همه داده‌های پس‌حسابرسی $\{\phi_{2,E}\}_{E\in E_{tally}}$ پروتکل‌های سیگما برای اعتبارسنجی تعهدهای موجود در E_{tally}. (گام سوم پروتکل سیگما)
  - سه‌تایی داده پیش‌حسابرسی، چالش و پس‌حسابرسی برای تشکیل یک اثبات سیگمای کامل برای یک تعهد معتبر، به ازای هر تعهد در E_{tally}
- محاسبه شمارش آرا با استفاده از homomorphism
  - $E_{sum} = \prod_{E\in E_{tally}} E$
  - محاسبه (T, R)
  - T نتیجه انتخابات کدشده در مبنای N؛ تعهدشده با مقدارتصادفی R
  - R مجموعه همه مقادیر تصادفی استفاده‌شده در تعهدهای E_{tally} است.
- بازکردن همه تعهدهای E_{open}
  - Open: مجموعه همه openningها
- ارسال Open، E_{sum} و (T, R) به BB

- در پایان، BB حاوی اطلاعات کد-رأی‌های نشان‌دار و اطلاعات زیر خواهد بود:

$$\text{Pub}, \left\{(C_{\ell,j}^{(a)}, t_{\ell,j}^{(a)})\right\}_{\ell\in[n],j\in[m]}^{a\in\{0,1\}}, (\mathbf{E}_{\text{tally}}, E_{\text{sum}}, (T,R)),$$

$$(\text{Open}, \mathbf{E}_{\text{open}}), \{\rho_E\}_{E\in\mathbf{E}_{\text{tally}}}, \{\phi_{2,E}\}_{E\in\mathbf{E}_{\text{tally}}}.$$

- Result
  - با استفاده از الگوریتم زیر، نتیجه کدشده انتخابات در T را می‌توان مشخص کرد.

Set $X \leftarrow T$;
For $j = 1, \ldots, m$:
• $x_j \leftarrow X \bmod (n+1)$;
• $X \leftarrow (X - x_j)/(n+1)$;
Return $\langle x_1, \ldots, x_m \rangle$;

- Verify
  - رسید α به شکل $(\text{tag}, a, \text{C}, \text{s}^{(1\text{-}a)})$ تجزیه می‌شود.
  - نتیجه این الگوریتم برابر با یک خواهد بود اگر همه بررسی‌های زیر معتبر باشند:

۱) همه اطلاعات متعهدشده در گزارش عمومی T مربوط به n برگه رأی هستند، طبق tagهای جداگانه مرتب شده باشند و هیچ دو کد-رأی‌ای با tag مشابه، نشان 'voted' نداشته باشند.

۲) اگر $\hat{C}$ یک کد-رأی موجود در بخش $\hat{s}^{(\hat{a})}$ از یک برگه رأی باشد و نشان 'voted' داشته باشد، فقط اطلاعات متعهدشده در بخش دیگر $\hat{s}^{(1-\hat{a})}$ از آن برگه رأی باز شده باشد.

۳) همه اثبات‌های سیگما مرتبط با تعهدهای موجود در E_{tally} معتبر باشند.

۴) $E_{sum} = \prod_{E \in E_{tally}} E$

۵) همه openningهای تعهدها معتبر باشند.

۶) tag مربوط به رسید، برابر یکی از tag_lها $(l \in [n])$ باشد و $a = a_l$

۷) کد-رأی نشان‌دار و مربوط به tag_l (که در مرحله قبل مشخص شد)، همان C موجود در رسید باشد.

۸) تناظر بین کدشده کاندیدا و کد-رأی افشاشده در بازکردن تعهدهای $\{U_{l,j}^{(1-a_l)}, E_{l,j}^{(1-a_l)}\}_{j \in [m]}$ (که l همان مقدار مشخص‌شده در مرحله ۶ است) برابر با همان قسمت در بخش $s^{(1-a)}$ باشد.

فصل پنجم

جمع‌بندی، مسائل باز و پروژه کارشناسی ارشد

جمع‌بندی، مسائل باز و پروژه کارشناسی‌ارشد

۱.۵ جمع‌بندی

در این گزارش به بیان خواسته‌های امنیتی مرتبط با انتخابات امن و به ویژه، خواسته امنیتی راستی‌آزمایی انتهابه‌انتها پرداخته شد. علاوه بر مقایسه تعاریف و بیان نقاط قوت و ضعف کارهای گذشته در این حوزه، تعریف دقیقی از راستی‌آزمایی انتهابه‌انتها مطرح و با ویژگی‌های کوچک‌تری بیان شد. در ادامه، یک سیستم پیشنهادی برای انتخابات قابل راستی‌آزمایی انتهابه‌انتها که در مدل استاندارد و با مفروضات حداقلی، که حریم خصوصی رأی‌دهندگان و تازگی رسید را نیز مدنظر داشت، مطرح شد و پروتکل‌های گوناگون آن شرح داده شد.

۲.۵ مسائل باز

از مسائل بازی که برای این زمینه می‌توان پیشنهاد داد، ارائه سیستمی برای برآورده‌کردن سایر خواسته‌های امنیتی به همراه قابلیت راستی‌آزمایی انتهابه‌انتهاست. برای این کار باید تغییراتی در طرح پیشنهادشده در این گزارش ایجاد شود تا در صورت امکان، ویژگی‌ها و خواسته‌های امنیتی یا عملیاتی دیگری به این طرح اضافه کرد.

از جمله فرض‌های این سیستم پیشنهادی، وجود تابلوی اعلانات پایدار و همیشگی بوده است. به این ترتیب، مسئله امنیت این تابلوی اعلانات، شامل در دسترس‌پذیری و عدم دست‌کاری آن توسط مهاجمان می‌تواند چالش بعدی باشد. گرچه کارهای مرتبطی در این زمینه نیز انجام شده است، اما به دلیل نقش پررنگ این موجودیت در طرح پیشنهادی، نیازمند فکر اساسی‌تری است. این‌که آیا می‌توان با حذف‌کردن تابلوی اعلانات نیز خواسته امنیتی مورد را نظر را برآورده کرد، می‌تواند سوال دیگری در این حوزه باشد.

از دیگر مسائل باز می‌توان به بیان صوری قابلیت راستی‌آزمایی انتهابه‌انتها با رویکرد جدید، افزایش کارایی و کاهش پیچیدگی سیستم، توجه به قابلیت استفاده و کاربرپسندبودن و توجه به دیگر خواسته‌های عملیاتی اشاره کرد.

۳.۵ پروژه کارشناسی‌ارشد

یکی از پروژه‌های کارشناسی‌ارشد حاصل از این گزارش می‌تواند افزودن خواسته امنیتی جدید به سیستم موجود پیشنهادی باشد. از آن‌جا که در این سیستم پیشنهادی اکثر خواسته‌های امنیتی مرسوم در انتخابات امن برآورده می‌شود، اما هنوز تمامی آن‌ها پوشش داده نشده، پس می‌توان با توجه ویژه به سایر خواسته‌ها و ویژگی‌های امنیتی، یک سیستم انتخابات کاملاً امن در تمامی محورها ارائه کرد. برای این کار، مراحل کار زیر پیشنهاد می‌شود:

- مطالعه خواسته‌های امنیتی و تعیین محدودیت‌های اعمال هر یک
- مطالعه کارهای موجود در برآورده‌سازی خواسته‌های امنیتی
- امکان‌سنجی خواسته‌های امنیتی ممکن برای افزودن و انتخاب خواسته مورد نظر، طبق فرضیات و مشخصات سیستم پیشنهادی
- طرح سیستم جدید برای خواسته‌های امنیتی جدید
- اثبات درستی سیستم ارائه‌شده

با توجه به عدم وجود یک سیستم انتخابات امن که همه خواسته‌های امنیتی مدنظر را دارا باشد، انگیزه و توجیه انجام این پروژه بیش از پیش مشخص می‌شود. گرچه باید برای این پروژه، نوع انتخابات، خواسته‌های امنیتی و تعریف دقیق آن‌ها نیز تبیین شده باشد.

منابع و مراجع

[۱] Kiayias, Aggelos, Thomas Zacharias, and Bingsheng Zhang. "End-to-end verifiable elections in the standard model." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 468-498. Springer Berlin Heidelberg, 2015.

[۲] Popoveniuc, Stefan, John Kelsey, Andrew Regenscheid, and Poorvi Vora. "Performance requirements for end-to-end verifiable elections." In Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, pp. 1-16. USENIX Association, 2010.

[۳] Adida, Ben. "Helios: Web-based Open-Audit Voting." In USENIX Security Symposium, vol. 17, pp. 335-348. 2008.

[۴] Zagórski, Filip, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, and Poorvi L. Vora. "Remotegrity: Design and use of an end-to-end verifiable remote voting system." In International Conference on Applied Cryptography and Network Security, pp. 441-457. Springer Berlin Heidelberg, 2013.

[۵] Kremer, Steve, Mark Ryan, and Ben Smyth. "Election verifiability in electronic voting protocols." In European Symposium on Research in Computer Security, pp. 389-404. Springer Berlin Heidelberg, 2010.

[۶] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." Communications of the ACM 24, no. 2 (1981): 84-90.

[۷] Sako, Kazue, and Joe Kilian. "Receipt-free mix-type voting scheme." In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 393-403. Springer Berlin Heidelberg, 1995.

[۸] Juels, Ari, Dario Catalano, and Markus Jakobsson. "Coercion-resistant electronic elections." In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 61-70. ACM, 2005.

[۹] Chevallier-Mames, Benoit, Pierre-Alain Fouque, David Pointcheval, and Jacques Traoré. "On some incompatible properties of voting schemes." In In IAVoSS Workshop On Trustworthy Elections, WOTE'06. 2006.

[۱۰] Chaum, David. "Secret-ballot receipts: True voter-verifiable elections." CryptoBytes 7, no. 2 (2004): 13-26.

[۱۱] Neff, C. Andrew. "Practical high certainty intent verification for encrypted votes." (2004).

[۱۲] Delaune, Stéphanie, Steve Kremer, and Mark Ryan. "Verifying privacy-type properties of electronic voting protocols." Journal of Computer Security 17, no. 4 (2009): 435-487.

[۱۳] Groth, Jens. "Evaluating security of voting schemes in the universal composability framework." In International Conference on Applied Cryptography and Network Security, pp. 46-60. Springer Berlin Heidelberg, 2004.

[۱۴] Bernhard, David, Olivier Pereira, and Bogdan Warinschi. "How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios." In International Conference on the Theory and Application of Cryptology and Information Security, pp. 626-643. Springer Berlin Heidelberg, 2012.