بررسی انتخابات الکترونیکی مبتنی بر رمزنگاری هم‌ریخت

سجاد رضایی آدریانی*[1]، سید مهدی سجادیه[2] و علی زاغیان[3]

[1و3]دانشگاه صنعتی مالک اشتر، مجتمع علوم کاربردی، دانشکده ریاضی و رمز
sajjad21367@yahoo.com
ali_zaghian1338@yahoo.com

[2]دانشگاه آزاد اسلامی اصفهان واحد خوراسگان، دانشکده برق
mahdisajadieh@yahoo.com

چکیده

انتخابات یکی از مباحث مهم در ایفای مردم‌سالاری است. همچنین مبحث انتخابات در مجامع تجاری از جمله بورس و یا تعیین هیئت‌مدیرهٔ یک شرکت جایگاه به‌سزایی دارد. با توجه به پیشرفت مباحث رمزنگاری و ارائهٔ سامانهٔ رمزنگاری نامتقارن، تلاش‌های زیادی در طراحی پروتکل های انتخابات الکترونیکی صورت گرفته است؛ اما تمامی پروتکل‌های طراحی‌شده، پیچیدگی بالا یا در جنبهٔ ویژگی‌های، دارای نقطه‌ضعف‌هایی دارند. همچنین بیش‌تر طرح‌های انتخابات الکترونیکی وابسته به تعدادی مسئول درست‌کار هستند که این موضوع درعمل سخت است. علاوه‌براین در بیش‌تر آن‌ها برای تولید برگهٔ رأی، رأی‌دهنده نقش کلیدی را ایفا می‌کند که باعث می‌شود در صورت تحمیل اجبار، محرمانگی رأی از بین برود و یا این که رأی‌دهنده قادر به تهیهٔ رسیدی برای نشان‌دادن محتوای رأی خویش باشد و در این صورت زمینهٔ خرید و فروش رأی و مسایل غیراخلاقی را در انتخابات ایجاد می‌کند. در این مقاله بعد از بررسی ویژگی‌های امنیتی یک طرح انتخابات الکترونیکی، پروتکل‌های انتخابات الکترونیکی بر اساس رمزنگاری هم‌ریخت را بیان کرده و تفاوت رسیداربودن و بدون رسیدبودن یک پروتکل انتخاباتی بررسی می‌شود.

واژگان کلیدی: رمزنگاری هم‌ریخت، بازرمزگذاری، اثبات صفر دانش، سامانهٔ رمزنگاری الجمال، انتخابات الکترونیکی، بدون رسیدبودن

۱-مقدمه

لازمهٔ یک حکومت مردم‌سالار، اظهار نظر عمومی مردم در مورد تصمیمات مهم و تأثیرگذار حکومتی مانند تعیین رئیس‌جمهور و غیره است. برای دست‌یافتن به این مهم، سامانه‌های رأی‌گیری زیادی طراحی شده‌اند. این سامانه‌ها باید برای عموم مردم در هنگام رأی‌گیری رایگان باشند. مرسوم‌ترین روش رأی‌گیری در جهان سامانهٔ اخذ رأی مبتنی بر کاغذ است. در این سامانه، در روزِ انتخابات، رأی‌دهندگان با مراجعه به مراکز اخذ رأی، بعد از احراز هویت، یک برگهٔ رأی دریافت کرده و در اتاقی نظر خود را روی برگهٔ رأی نوشته و آن را در مقابل مسئول اخذ رأی در صندوق می‌اندازند. بعد از مرحلهٔ رأی‌گیری، صندوق‌های رأی‌گیری توسط مسئولان باز شده و نتیجهٔ انتخابات محاسبه و منتشر می‌شود. مردم معتقدند که این سامانه، گم‌نامی و اینکه آن‌ها رأی داده‌اند، تضمین می‌کند؛ اما در سامانهٔ یادشده احتمال تقلب وجود دارد و نیز برای به‌کار گیری آن هزینهٔ زیادی باید صرف شود. درضمن این فرآیند احتیاج به زمان زیادی برای شمارش آرا به‌عنوان مثال چندین روز را دارد. به همین دلایل پس از ارائهٔ سامانه‌های رمز کلید عمومی، پروتکل‌های انتخابات الکترونیکی مطرح شد و به‌دلیل نیازهای متنوع از جنبهٔ نظری اهمیت پیدا کردند. در حال حاضر انتخابات الکترونیکی به‌عنوان راه‌کاری مطرح شده‌اند که مشکلات مطرح‌شده در انتخابات سنتی مبتنی بر کاغذ، از جمله کاهش هزینه‌ها برای برگزاری، افزایش امنیت، به‌کارگیری آسان و در همه جا برای عموم مردم (حتی در منازل در روز رأی‌گیری) و غیره را می تواند برطرف سازد و همچنین آن را دارای قابلیت وارسی برای عموم سازد تا نشان دهد که انتخابات به‌درستی انجام شده است [۱-۱۰].

*نویسندهٔ مسؤول

۱-۱- تاریخچه

در سال ۱۸۸۴ میلادی توماس ادیسون[1] گواهی ثبت اختراع را برای دستگاه رأی‌گیری الکتریکی دریافت و تلاش کرد تا اختراعش را به مجموعهٔ قانون‌گذاری بفروشد که این تلاش ناکام ماند. بعد از او هم دستگاه‌هایی با همین نام ساخته شدند. این دستگاه‌ها برگزاری رأی‌گیری‌های کوچک را در جایی مانند مجلس نمایندگان تسریع می‌کردند؛ ولی سازندگانشان هیچ توجهی به مسائل امنیتی نداشتند [۱]. بعد از ارائهٔ سامانه‌های کلید عمومی[2] در سال ۱۹۷۰ میلادی نگاه به سامانه‌های رمزنگاری و به‌خصوص پروتکل‌های امن متحول شد. سامانه‌های انتخابات، به‌دلیل نیازهای متنوع و دشوار امنیتی از لحاظ نظری اهمیت پیدا کردند و در دهه‌های ۱۹۸۰ میلادی پروتکل‌هایی برای غلبه به مسائل مطرح‌شده، پیشنهاد شد که البته چون در آن زمان هدف عملی دنبال نمی‌شد، این پروتکل‌ها به‌صورت کاملاً غیر کاربردی طراحی شدند و به این ترتیب، لفظ انتخابات الکترونیکی[3] در رمزنگاری نه به‌معنای برگزاری انتخابات یا شمارش به شیوهٔ الکترونیکی، بلکه به معنای انتخابات بر بستر یک شبکهٔ رایانه‌ای با حفظ مشخصات امنیتی مطلوب به کار می‌رفت[۱-۳]. در دههٔ ۱۹۹۰ میلادی پس از گسترش و فراگیری اینترنت از یک سو و دسترسی عمومی به رایانه‌های شخصی از سوی دیگر مسأله بعد عملی هم پیدا کرد و از این منظر نیز مورد توجه قرار گرفت. این توجه منجر به انجام چندین پژوهش علمی و چند پیاده‌سازی عملی برای رأی‌گیری دانشجویی شد[۱-۳]. به‌طور کلی دشوارترین ویژگی یک انتخابات را ویژگی محرمانگی محتوای آرا در کنار وارسی عمومی و فردی می‌توان دانست؛ زیرا می خواهیم نه‌تنها آرا شمارش شوند و نتیجهٔ نهایی انتخابات به‌دست آید، بلکه این نتایج قابل وارسی نیز باشند. به این ترتیب روشن است که نیل به این دو ویژگی به‌ظاهر متضاد، به‌سادگی ممکن نیست. نخستین طرح مدرن رأی‌گیری توسط چوآم[4] در سال ۱۹۸۱ مطرح شد، که بر اساس سامانهٔ کلید عمومی رمزنگاری و با به‌کارگیری امضای کور[5]، هویت رأی‌دهنده را مخفی می‌کرد. در این‌گونه طرح‌ها از کانال مخصوصی به نام کانال گمنام[6] برای مخفی‌کردن هویت رأی‌دهنده استفاده می‌شود. این کانال به‌گونه‌ای است که دریافت‌کنندهٔ پیام از مبدأ آن با خبر نمی‌شود. به این ترتیب رأی‌دهنده با استفاده از یک نام مستعار که با امضای کور به‌دست آورده است، از طریق یک کانال گمنام رأی خود را برای مسئول مربوطه می‌تواند ارسال کند. مشکل اساسی این روش‌ها این بود که رأی‌دهنده باید در چند مرحله از قبیل مراحلی چون ثبت‌نام، تولید نام مستعار، رأی‌دادن و اعلام نتایج و شمارش انتخابات شرکت داشته باشند [۱-۵]. در سال ۱۹۷۸ میلادی روش دیگری برای حفظ محرمانگی آرا پیشنهاد شد که باعث پدیدارشدن خانوادهٔ جدیدی از پروتکل های انتخابات بر اساس رمزنگاری هم‌ریخت[7] شد. به‌سادگی می‌توان گفت، رأی‌دهنده رأی رمز شدهٔ خود را به‌صورت عمومی اعلام می‌کند؛ سپس مسئولان حاصل‌ضرب تمام رأی‌های رمزشده را محاسبه کرده و یکجا رمزگشایی می‌کنند. حاصل‌ضرب رمزگشایی شدهٔ به‌دست آمده برابر با حاصل‌جمع تمام آرا است. این پروتکل‌ها برتری چشم‌گیری بر پروتکل‌های قبلی از قبیل امکان وارسی بهتر، سادگی از دید رأی‌دهندگان و توزیع ساده‌تر و بهتر بین مسئولان انتخابات را داشت؛ ولی هزینهٔ بالای پردازشی یکی از نقاط ضعف این‌گونه پروتکل‌ها قلمداد می‌شد [۱-۸]. در سال ۱۹۸۵ کوهن[8] و فیشر[9] یک طرح انتخابات را بر اساس رمزنگاری هم‌ریخت طراحی کردند. سپس بنالوه[10]، یانگ[11]، ساکو[12] و کیلیان[13] طرح‌های مختلف رأی‌گیری را بر اساس رمزنگاری هم‌ریخت ارائه دادند. در طرح های موجود رأی‌گیری برخی از آن‌ها پیچیدگی دو چندان دارند و برای انتخابات وسیع نامناسب‌اند. برخی از آنها نیز امنیت شکننده دارند. نخستین طرحی که برای یک انتخابات در حد وسیع مطرح شد، توسط فو[14] و با همکاری فوجیوکا[15] و اکاماتو[16] در سال ۱۹۹۲ طراحی شد. بعد از آن سامانه‌های رأی‌گیری در موارد غیر دولتی به کار گرفته شدند. بسیاری از پژوهش‌ها، نیز در مؤسسات دانشگاهی برای پیشرفت در نرم افزارهای رأی‌گیری صورت پذیرفت که EVOX و MIT در دانشگاه واشنگتن از معروف‌ترین آن‌ها هستند. در پژوهش‌های روی سامانه‌های رأی‌گیری بعضی از پژوهش‌گران راه‌حل‌های مختلفی را برای مشکلات امنیتی پروتکل فو مطرح و سامانه‌های رأی‌گیری مناسب را برای کاربردهای مختلف

[1] Tomas Edison
[2] Public key system
[3] Electronic voting
[4] Chaum
[5] Blind signature
[6] Anonymous channel
[7] Homomorphic encryption
[8] Cohen
[9] Fisher
[10] Benaloh
[11] Yung
[12] Sako
[13] Kilian
[14] FOO
[15] Fujioka
[16] Okamoto

طراحی کردند. در ادامه، کرامر[1] یک طرح رأی‌گیری را بر اساس رمزنگاری هم‌ریخت آستانه‌ای و اثبات صفر دانش طراحی کرد. این طرح قابلیت وارسی عمومی و گمنامی را برآورده می‌ساخت [۱-۱۰]. در سال ۱۹۹۴ میلادی برای برطرف‌کردن مسائل غیرقانونی در زمینهٔ رأی‌گیری مانند خرید و فروش رأی یا اجباری رأی‌دادن، بنالوه یک مفهوم جدید و البته دشوار را برای طرح‌های انتخاباتی مطرح کرد که خاصیت بدون رسیدبودن[2] نام گرفت که در آن رأی‌دهنده حتی در صورت تمایل، قادر به اثبات رأی خود(که به یک نامزد خاص رأی داده است) برای شخص ثالثی، نبود [۱۱-۱۸]. به این ترتیب با وجود چنین خاصیتی در یک پروتکل رأی‌گیری، امکان خرید و فروش رأی یا اجباری رأی‌دادن از بین می‌رود. پس از این، تلاش‌های زیادی در جهت ارائهٔ نسخه های بدون رسید از پروتکل‌های پیشین که بر اساس رمزنگاری هم‌ریخت طراحی شده بود، انجام گرفت. مارتین[3] نشان داد که طرح بنالوه در مدل وارسی عمومی بدون رسید نیست [۵]. لی[4] طرح کرامر را اصلاح و بهبود داد. طرح لی نیز برای بدون رسیدبودن احتیاج به یک سازمان درست‌کار برای رأی‌گیری داشت، که این شرط مشکلی برای برآورده‌شدن داشت [۱-۱۰].

در دههٔ گذشته، چند انتخابات به‌صورت الکترونیکی برگزار شده است؛ اما هیچ‌کدام در مقیاس بزرگ نبوده و علاوه‌براین به‌طورعمومی انتخابات مهمی هم نبوده‌اند و بیشتر حالت نظرسنجی در احزاب آمریکا برای انتخاب نامزدهایشان را داشته است. در چند سال اخیر با توجه به مبحث دولت الکترونیکی در کشورهای مختلف، از جمله ایران، بر اهمیت عملی انتخابات الکترونیکی افزوده شده و به نظر می‌رسد که در آینده‌ای نزدیک بیش‌تر انتخابات به شیوهٔ الکترونیکی انجام شود و به همین دلیل شرکت‌های تجاری در زمینهٔ خدمات انتخابات الکترونیکی برای انجام انتخابات صنفی و غیره رشد چشم‌گیری کنند [۵و۶].

در این مقاله تلاش می‌شود مدل مناسبی برای پی‌ریزی یک پروتکل انتخابات الکترونیکی تبیین شود؛ لذا ابتدا به بیان ملزومات یک انتخابات الکترونیک پرداخته و سپس در ادامه پروتکل‌های مهم رأی‌گیری بر اساس روش‌های موجود بیان‌شده در قسمت ملزومات انتخابات مطرح می‌شوند.

[1] Cramer
[2] Receipt-Free
[3] Martin
[4] Lee

۲- ملزومات انتخابات الکترونیکی

در این قسمت انواع موجودیت‌ها (شرکت‌کنندگان) را در یک انتخابات الکترونیکی معرفی کرده و در ادامه انواع رأی‌گیری، ویژگی‌های مطلوب یک طرح رأی‌گیری، انواع کانال‌های ارتباطی استفاده‌شده در یک پروتکل انتخاباتی، حملات و غیره را بیان می‌کنیم و در پایان به تبیین انواع روش‌های انتخابات به‌منظور نیل به این ویژگی‌ها پرداخته می‌شود.

۲-۱- موجودیت‌ها

در بیش‌تر پروتکل‌های انتخابات الکترونیکی دو گروه کلی از شرکت‌کنندگان در انتخابات وجود دارند. نخستین گروه رأی‌دهندگان[5] هستند و دومین گروه که در انتخابات شرکت دارند، مسئولان انتخابات هستند. در بعضی از آن‌ها گروه خاصی موسوم به خراب‌کار[6] یا دشمن حضور دارند؛ اما در تمامی پروتکل‌های انتخابات الکترونیکی، هدف آماده‌کردن بستری است که رأی‌دهندگان حتی در صورت وجود خراب‌کار بتوانند رأی خود را به‌درستی واریز کنند. لازم بذکر است که شرکت‌کنندگان می‌توانند از طریق کانال‌های عمومی[7] ارتباط داشته باشند. تعداد رأی‌دهندگان را با M و تعداد مراجع قانونی با N نمایش داده می‌شود [۱-۱۸].

رأی‌دهندگان: رأی‌دهندگان به‌احتمال طیف گسترده‌ای را تشکیل می‌دهند که ممکن است از امکانات پردازشی بالایی برخوردار نباشند. علاوه‌براین، انتخابات باید از دید رأی‌دهندگان از نهایت سهولت برخوردار باشد؛ به‌گونه‌ای که به‌صورت ایده‌آل یک رأی‌دهنده تنها با انجام یک عمل بتواند رأی بدهد. رأی‌دادن برای رأی‌دهندگان در بیش‌تر مواقع اختیاری است و رأی‌دهنده حتی در حین عملیات هم باید قدرت انصراف داشته باشد. به‌طورمعمول فرض می‌شود که رأی‌دهنده امکان ذخیره و مخفی‌کردن کمینه‌ای از اطلاعات را دارد؛ به‌عنوان مثال یک کلید خصوصی یا یک کلمهٔ عبور[۱-۱۸].

مسئولان انتخابات[8]: مسئولان انتخابات یا مراجع قانونی، درحقیقت مدیران انتخابات هستند که از قدرت پردازشی بالایی برخوردارند و فرض می‌شود اطلاعات لازم را می‌توانند ذخیره کنند. نکتهٔ قابل توجه دیگر این است که این مراجع به‌طورمعمول به‌سبب دسترسی به حجم بالای اطلاعات و

[5] Voters
[6] Adversary
[7] Public channel
[8] Voting authorities

قدرت پردازشی بیشتر، آسیب‌پذیرترند و درنتیجه باید حدود امنیتی بالایی برای آن‌ها در نظر گرفته شود. به‌طورکلی مسئولان باید سه وظیفهٔ زیر را انجام دهند:

۱) کنترل و نظارت بر صحت برگزاری انتخابات؛

۲) همکاری با افرادی که شرایط رأی‌دادن دارند، برای تولید برگهٔ رأی و گرفتن رأی از آنان؛

۳) محاسبه و اعلام نتایج نهایی انتخابات.

اگر یک مسئول قابل اطمینان داشته باشیم که بدانیم هرگز از وظایفی که برایش تعریف شده است، تخطی نکرده و با خراب کاران و یا افراد دیگر تبانی نمی‌کند، احتیاج به چند مرجع دیگر مرتفع می‌شود؛ ولی چنین اتفاقی درعمل غیرممکن است و به همین منظور تلاش می‌شود که از چندین مسئول که دارای قدرت پردازشی برابر و با وظایف تعیین‌شده باشند، استفاده شود؛ به‌طوری‌که از درست‌کاربودن تعدادی از آن‌ها اطمینان داشته باشیم تا از سوءِ رفتار احتمالی برخی از مسئولان جلوگیری به‌عمل آید. رأی‌دهندگان و مسئولان باید بپذیرند که دست‌کم $N-t+1$ عدد از مسئولان درست‌کارند. رأی‌دهندگان می‌توانند به امانت‌داری هر یک از مسئولان ظنین باشند؛ ولی درکل بر این باورند که تعداد مراجع ناصالح کمتر از t است. از سوی دیگر لازم نیست که مسئولان به رأی‌دهندگان اعتماد داشته باشند [۱-۱۸].

نامزدهای انتخابات[1]: این افراد سعی در جذب‌کردن آرای رأی‌دهندگان دارند [۱-۱۸].

دشمن: هر گروه یا شخصی که سعی در برهم‌زدن روند انتخابات را داشته و یا درصدد تبانی‌کردن با یکی از موجودیت‌های دیگر از طریق غیرقانونی باشد، دشمن یا خراب‌کار به‌شمار می‌آید[۱-۱۸].

۲-۲- انواع رأی‌گیری

انواع رأی‌گیری ارتباط نزدیکی به ساختار آرا و ساختار آرا نیز بستگی به نوع رأی‌گیری و نحوهٔ برگزاری انتخابات دارد. بنابراین می‌توان گفت که ساختار آرا به موارد زیر بستگی دارد:

نخست، پرسشی که هدف از انتخابات یافتن پاسخ برای آن است؛ و دیگری پاسخ‌های محتمل این پرسش است. برای داشتن دید بهتر در تحلیل روش‌ها لازم است به انواع رأی‌گیری از لحاظ ساختار آرا اشاره شود. انواع رأی‌گیری‌ها عبارتند از:

۱) **بلی/خیر:** پاسخ یکی از این دو کلمه و درنتیجه یک‌بیتی است. این نوع رأی‌گیری بیشتر در نظرسنجی‌ها کاربرد دارد.

۲) **1 از L**: هدف، انتخاب یک نفر از میان L نفر است که مثال بارز آن انتخابات ریاست جمهوری است.

۳) **k از L**: هدف انتخاب k مورد از بین L گزینه یا انتخاب از یک تا k مورد از بین L گزینه است. که مثال بارز آن انتخابات مجلس است.

۴) **رأی نوشتنی:** رأی‌دهنده، رأی مورد نظر خود را با استفاده از مجموعهٔ علائم معتبر می‌نویسد. این رأی باید از بیشینه طول مجاز کوتاه‌تر باشد. به این ترتیب امکان برگزاری انتخابات بدون داشتن گزینه‌های مشخص فراهم می‌شود.

از منظر دیگر انتخابات را به‌طور کلی به دو دسته می‌توان تقسیم کرد:

انتخابات ناهم ارز: رأی‌ها در ضرایب مشخص ضرب و سپس نتیجه محاسبه می‌شود. به‌عنوان مثال، کسی که مدرک تحصیلی بالاتری دارد، دارای رأی بااهمیت‌تری است.

انتخابات هم ارز: هر رأی‌دهنده صلاحیت دارد یک‌بار رأی بدهد و رأی‌ها بدون هیچ وزنی شمرده می‌شوند.

در مورد نخست، توزیع قدرت یکسان نیست؛ ولی در مورد دوم توزیع قدرت یکسان است. این توزیع غیر یکسان که در برخی موارد، مثل مجامع عمومی شرکت‌های سهامی لازم است، باعث افزایش پیچیدگی پروتکل می‌شود؛ ولی در پروتکل های مبتنی بر رمزنگاری هم‌ریخت که در ادامه به آنها می پردازیم، به‌دلیل اینکه هر کس با هویت مشخص خود در انتخابات شرکت می‌کند، رأی او را در ضریب مشخص می‌توان ضرب کرد. هر یک از پروتکل‌های مربوط به انتخابات ناهم‌ارز در روش رمزنگاری هم‌ریخت به‌سادگی قابل پیاده بوده و درضمن تمامی پروتکل‌های هم‌ارز مبتنی بر رمزنگاری هم‌ریخت را به پروتکل‌های ناهم‌ارز می‌توان تبدیل کرد [۱-۱۸].

۲-۳- حملات

به یک طرح انتخابات الکترونیک، حملات زیر را می‌توان انجام داد[۱-۱۸]:

۱) **حملهٔ رأی‌دادن تصادفی**[2]: شخص حمله‌کننده، رأی‌دهنده را مجبور کند که به‌صورت تصادفی از میان

[1] Candidates

[2] Randomization attack

گزینه‌های موجود، یکی را انتخاب کند(چون در این حمله یک فهرست رمزشده به‌هم‌ریخته تشکیل می‌شود). در این حمله نمی‌توان فهمید که رأی‌دهنده به کدام گزینه رأی می‌دهد.

۲) **حملهٔ انصراف اجباری**[1]: شخص حمله‌کننده، از رأی‌دهنده می‌خواهد که در انتخابات شرکت نکند، به این ترتیب به‌عنوان مثال افرادی را که حدس می‌زند، نظرشان با نظر خودش موافق نباشند، از حقشان در رأی‌گیری می‌تواند محروم کند.

۳) **حملهٔ شبیه‌سازی‌شده**[2]: در این حمله شخص حمله‌کننده از مشخصات الکترونیکی افراد استفاده کرده و به جای آن‌ها رأی می‌دهد.

۴-۲- کانال‌های ارتباطی

در این قسمت کانال‌های ارتباطی مختلفی را که در پروتکل های انتخابات الکترونیک استفاده می‌شوند، معرفی می‌کنیم و مشخصات هر یک را توضیح خواهیم داد [۱۸-۱].

۱) **کانال عمومی:** کانالی است که شرکت‌کنندگان اعم از مسئولان و رأی‌دهندگان و حتی خراب‌کاران اطلاعات خود را از طریق آن می‌توانند ارسال کنند. حمله‌کنندگان به این کانال ضربه می‌توانند وارد و یا هویت فرستنده را ردیابی کنند.

۲) **تابلو اعلانات**[3]: محلی عمومی است که در آن شرکت‌کنندگان انتخابات اطلاعات عمومی خود را در آن می‌توانند درج کنند. به عبارت دیگر تابلوی اعلانات یک محل عمومی برای خواندن اطلاعات تمامی موجودیت‌های یک انتخابات الکترونیک است. رأی‌دهنگان و مسئولان در قسمت مربوط به خود می‌توانند بنویسند و هیچ‌کس دیگری قادر به اصلاح یا تغییر محتوای آن‌ها نیست؛ لذا تابلوی اعلانات را یک کانال عمومی دارای حافظه می‌توان دانست.

۳) **کانال گمنام**[4]: این کانال غیرقابل ردگیری بوده و گمنامی فرستندهٔ پیام را تضمین می‌کند.کانال گمنام غیرقابل رد گیری، کانالی است که در آن پیام از فرستنده به گیرنده می‌رسد، ولی خاصیتش این است که نه‌تنها گیرنده از هویت فرستنده باخبر نمی‌شود؛ بلکه هیچ‌کس دیگری هم قادر نخواهد بود که ردیابی پیام را تا مشخص‌کردن فرستنده دنبال کند. درصورتی‌که این کانال دو طرفه باشد، امکان گفتگو میان فرستنده و گیرندهٔ پیام را مهیا می‌سازد.

۴) **کانال غیرقابل شنود**[5]: کانال غیرقابل شنود، کانالی است که در آن غیر از دو موجودیت در انتهای کانال، کسی قادر به مشاهدهٔ محتوای پیام نباشد و خود آن افراد هم بعداً ابزاری برای اثبات آنچه بینشان مبادله‌شده نداشته باشند. این کانال بین مسئولان و رأی‌دهندگان پیاده‌سازی می‌شود.

۵) **کانال گمنام غیرقابل شنود:** ترکیب دو کانال قبلی است؛ یعنی نخست پیام به‌صورت محرمانه از فرستنده به گیرنده می‌رود و دوم‌این‌که فرستنده از خود هیچ رد پایی برجا نمی‌گذارد. بنابراین هم مبادله به‌صورت غیرقابل شنود برگزار می‌شود و هم هویت فرستنده آشکار نمی‌شود و به این ترتیب باز هم دو طرف ارتباط، بعداً ادعایی در مورد پیام نمی‌توانند داشته باشند.

۵-۲- مراحل انتخابات

انتخابات الکترونیکی به‌طورکلی از سه مرحلهٔ عمده که عبارتند از مرحلهٔ آغازین، مرحلهٔ رأی‌دادن و مرحلهٔ شمارش و اعلام نتایج آن تشکیل می‌شود. البته روشن است که مراحل جزیی تری را می‌توان در نظر گرفت.

مرحلهٔ آغازین: در این مرحله مسئولان، مراحل مقدماتی انتخابات را انجام می‌دهند. هدف انتخابات، گزینه‌های موجود و نحوهٔ پاسخ به آن‌را اعلام و همچنین ملزومات نرم‌افزاری انتخابات را فراهم می‌کنند که شامل تهیه و توزیع مناسب کلیدهای خصوصی و عمومی و یا کلمات عبور برای ارتباطات مورد نیاز است.

مرحلهٔ رأی‌گیری: در این مرحله رأی‌دهندگان پس از- یا ضمن- اثبات هویت خود (در برخی از پروتکل‌های انتخابات الکترونیکی احراز هویت رأی‌دهندگان مرحلهٔ جداگانه‌ای محسوب می‌شود) رأی‌شان را طبق ضوابط پروتکل آماده و برای مسئول یا مسئولان مربوطه ارسال می‌کنند.

مرحلهٔ شمارش و اعلام نتایج: در این مرحله، مسئولان، آرای جمع‌شده را شمارش و نتایج را اعلام می‌کنند. علاوه‌براین،

[1] Forced-abstention attack
[2] Simulation attack
[3] Bulletin board
[4] Anonymous channel
[5] Untappable channel

به‌طورمعمول اطلاعات اضافه‌ای هم برای آشکارسازی خطا، اطمینان از صحت انتخابات، اطلاع از شرکت‌کنندگان و غیره از طریق تابلوی اعلانات انتخابات در معرض دید عموم قرار می گیرد[۱-۱۸].

۶-۲- ویژگی‌های مطلوب انتخابات

یک انتخابات الکترونیکی، علاوه‌بر این‌که باید تمام خواص یک انتخابات مبتنی بر کاغذ را داشته باشد، باید دارای امنیت بیشتری نسبت به انتخابات سنتی باشد؛ لذا ویژگی‌های مطلوب یک انتخابات را در یک نگاه کلی به‌صورت زیر می‌توان بیان کرد [۱-۱۸]:

۱) استحقاق[1]: فقط افرادی که دارای حق رأی هستند بتوانند رأی بدهند؛

۲) محرمانگی[2]: به‌منظور حفظ حریم خصوصی افراد لازم است، رأی‌ها محرمانه باشند و هیچ ائتلافی از افرادی که فرد رأی‌دهنده در آن‌ها نیست قادر به نسبت‌دادن یک رأی به رأی‌دهنده نباشند و یا از محتوای آن با خبر نشوند؛

۳) عدالت[3] (در نتایج انتخابات): هیچ گروهی نتوانند از نتایج میانی انتخابات با خبر شوند. به‌عنوان مثال اگر قرار است که انتخابات ده ساعت به‌طول بینجامد، کسی در ساعت ششم اطلاعی از نتایج انتخابات تا آن لحظه نداشته باشد؛

۴) وارسی عمومی و فردی[4]: هر کس بتواند صحت روند برگزاری انتخابات را وارسی کند. همچنین هر کس بتواند از شمرده‌شدن رأیش مطمئن شود؛

۵) بدون رسیدبودن[5] و عدم امکان اجبار[6]: در یک انتخابات ممکن است، شخص ثالثی با پرداخت رشوه به رأی‌دهنده سعی در جذب رأی وی برای نامزد خاصی باشد. این سناریو را خرید رأی می‌نامند و هنگامی رخ می‌دهد که رأی‌دهنده دارای ابزاری باشد تا بتواند به شخص ثالث، اثباتی برای محتوای رأیش ارائه دهد و با بدون رسیدبودن طرح انتخاباتی از بین می‌رود. عدم امکان اجبار نیز یعنی اینکه اجبارکننده رأی‌دهنده را نتواند تهدید کند؛

۶) صحت[7]: منظور از صحت در انتخابات این است که رأی‌دهنده قادر به تولید رأی معیوب با توجه به ساختار آرا نباشد؛

۷) کامل بودن[8]: تمام رأی‌ها شمرده شوند؛

۸) سلامت[9]: تبهکاران و هیچ ائتلافی با تعداد کمتر از t مسئول امکان تخریب نداشته باشند؛

۹) عدم امکان رأی دادن مجدد؛

۱۰) پایداری: امکان تغییردادن نتیجه برای کسی نباشد؛

۱۱) تکثیرناپذیری: کسی رأی کس دیگری را به‌عنوان رأی خود نتواند اعلام کند.

برخی از ویژگی‌های بالا ممکن است گاهی اصلاً مطلوب نباشد؛ به‌عنوان مثال ممکن است، ویژگی قابلیت وارسی عمومی و فردی در برخی کاربردها نامطلوب باشد. برخی از موارد هم ممکن است، چندان اهمیت خاصی نداشته باشند. به‌عنوان مثال تکثیرناپذیری در مقیاس‌های بزرگ اهمیتی ندارد؛ اما در یک رأی‌گیری سه‌نفره بسیار حیاتی است.

محرمانگی و بدون رسیدبودن را از مهم‌ترین عواملی می‌توان دانست که هدف اصلی در پروتکل‌های انتخابات الکترونیکی غلبه به همین دو مورد است. اهمیت بدون رسیدبودن ممکن است در نگاه نخست آشکار نباشد؛ ولی با اشاره به این نکته که درصورت نبودن چنین خاصیتی خطر فروش رأی وجود خواهد داشت یا خطر اجبار رأی‌دهنده‌ها به دادن رأیی خاص، علت توجه به این موضوع روشن می‌شود. همچنین به این موضوع می‌توان اشاره کرد که اگر کسی بخواهد دیگری را به رأی مشخص وادار کند، محرمانگی مانع از آشکارشدن رأی می‌شود. حال اگر خود رأی‌دهنده را مجبور کنند که رأیش را نشان دهد، می‌خواهیم رأی‌دهنده چنین امکانی نداشته باشد.

۲-۷- رویکردهای مختلف در نیل به ویژگی‌ها

برای روشن‌شدن ایده‌ها و نیازهای اساسی، پیش از ورود به بیان پروتکل‌ها، روش‌های مختلف انتخابات الکترونیکی مرور می‌شود. در این قسمت، هدف صرفاً بیان روش‌هایی است که باعث تولید خانواده‌های متفاوتی از پروتکل‌های انتخابات شده است. بنابراین، روش‌ها و طرح‌های بیان‌شده تمام جوانب امر را پوشش نمی‌دهد. حساس‌ترین خاصیتی که برای رسیدن به آن روش مناسبی برگزید، محرمانگی است. اگر الزام به محرمانگی برداشته شود، رسیدن به سایر ویژگی‌ها چندان دشوار نیست. به‌عنوان مثال تصور کنید که رأی‌دهنده، رأی خود را در تابلوی اعلانات در قسمت مربوط به خود که سایرین

[1] Eligibility
[2] Privacy
[3] Fairness
[4] Individual and Universal verifiability
[5] Receipt-freeness
[6] Uncoercibility
[7] orrectness
[8] Ompletentss
[9] Soundness

نمی‌توانند تغییرش دهند، بنویسند و هر کس قادر باشد، نتیجهٔ انتخابات را با آنچه روی تابلو می‌بیند مقایسه کند، یا از شمردن رأیش اطمینان حاصل کند [۱-۱۸]. تاکنون چند ایدهٔ اصلی برای رسیدن به محرمانگی بیان شده است. محرمانگی یعنی اتصال شخص رأی‌دهنده و رأی مورد نظر شخص برای همه‌ی مسئولین کور شده باشد و یا غیرقابل دسترسی شود. انجام این مهم از سه طریق زیر ممکن است:

۱) مشاهدهٔ رأی ممکن باشد، ولی نسبت‌دادن آن به رأی‌دهنده غیرممکن باشد.

۲) دیدن محتوای رأی غیرممکن باشد، ولی هویت رأی‌دهنده معلوم باشد.

۳) هم مشاهدهٔ رأی غیرممکن باشد و هم معلوم‌کردن هویت رأی‌دهنده.

به‌کارگیری هر یک از سه رویکرد بالا، باعث می‌شود که محتوای رأی رأی‌دهنده از دید سایرین مخفی بماند.

طرح‌های مبتنی بر رویکرد نخست نیاز به استفاده از کانال‌های گمنام است. در مورد نخست، آرا به‌صورت عمومی عرضه می‌شوند و هر کسی خود نیز اقدام به شمارش آن‌ها می تواند کند؛ ولی کسی نمی‌داند که کدام رأی را چه کسی داده است. به هر حال در این حالت باید توجه ویژه‌ای نیز به استحقاق شرکت‌کنندگان در انتخابات شود تا اطمینان حاصل شود که فقط شرکت‌کنندگان واجد شرایط رأی می‌دهند و آن هم حداکثر یک رأی. این روش‌ها در عنوان روش‌های مبتنی بر کانال گمنام(امضای کور) بررسی می‌شوند.

در طرح‌های مبتنی بر رویکرد دوم، استحقاق شرکت‌کنندگان مسألهٔ حادی ایجاد نمی‌کند. چون در مواجهه با هر کس هویت واقعی او آشکار است؛ ولی مشکل در نحوهٔ شمارش آرا است. علاوه‌براین، بدون هیچ تلاشی هر کس می تواند مطلع شود که چه کسانی در انتخابات شرکت کرده‌اند. گروهی از این طرح‌ها در خانوادهٔ روش‌های مبتنی بر رمزنگاری هم‌ریخت است [۱-۱۸].

۳- پروتکل‌های انتخابات الکترونیک بر اساس رمزنگاری هم‌ریخت

در این بخش ابتدا پروتکلی بر اساس رمزنگاری هم‌ریخت که بدون رسید است، بیان و در ادامه پروتکلی بر اساس رمزنگاری دارای خاصیت بدون رسید بیان می‌شود.

۳-۱- ملزومات مورد نیاز پروتکل‌های رسیددار و بدون رسید رأی‌گیری الکترونیکی مبتنی بر رمزنگاری هم‌ریخت

مهم‌ترین طرح انتخاباتی که در ادامه به تشریح آن می‌پردازیم، پروتکل انتخابات الکترونیکی از نوع انتخابات k از L است. این طرح توسط مارتین هیرت بیان شده است [۴و ۱۸]. قبل از بیان این طرح، ابتدا یک پروتکل رأی‌گیری از نوع انتخابات k از L را که فاقد خاصیت بدون رسید است، تشریح و در ادامه طرح هیرت را بیان می‌کنیم.

ملزوماتی که در این قسمت مورد نیاز است:

۱) فرض کنیم که یک تابع رمزنگار کلید عمومی با امنیت اثبات‌پذیر به‌صورت $E_h: V \times R \to \mathbb{E}$ موجود باشد که h کلید عمومی، V مجموعهٔ رأی‌های ممکن و R مجموعهٔ رشته‌های تصادفی و $\mathbb{E}$ مجموعهٔ رأی‌های رمزشدهٔ ممکن باشد. در ادامه به جای E_h ، E به‌کار برده می‌شود. تابع رمزگشایی به‌صورت $D_z: \mathbb{E} \to V$ است که z کلید خصوصی است. توجه کنید که پیچیدگی تابع رمزگشایی D_z باید در هنگام رمزگشایی به متن ساده v به‌صورت چندجمله‌ای باشد. برای یک متن ساده‌ای مانند v که رمزگذاری شده است، رمزگشایی نباید با شکست روبه‌رو شود. علاوه‌براین تابع رمزنگار بایستی q_معکوس‌پذیر باشد $q \in Z$. این بدین معنی است که اگر متن ساده‌ای مانند v را qبار با به‌کارگیری E و اعداد تصادفی مختلف رمز کنیم، رمزگشایی آن به‌صورت ساده میسر باشد و کار سختی نباشد. با تعریف q ، فرض کنید $u < q$ وجود داشته باشد، به‌طوری‌که u عددی نخست باشد.

۲) فرض کنید V گروهی با عمل $+$ و R گروهی با عمل $\boxplus$ و $\mathbb{E}$ گروهی با عمل $\times$ و تابع رمزنگار E دارای خاصیت هم‌ریختی به‌صورت زیر باشد:

$$E(v_1, \alpha_1) \times E(v_2, \alpha_2) = E(v_1 + v_2, \alpha_1 \boxplus \alpha_2) \quad (۱)$$

۳) یک باز رمزگذاری تصادفی $\acute{e}$ از متن رمزشدهٔ $e = E(v, \alpha)$ به‌صورت رمزکردن e با استفاده از عدد تصادفی Ψ است. یک باز رمزگذاری می‌تواند به‌صورت افزودن رمزشدهٔ صفر با e صورت گیرد. که حاصل برابر $\acute{e}$ است. فرض کنید $\Psi \in R$ یک شاهد برای باز رمزگذاری باشد، در این صورت داریم:

$$\acute{e} = R(e, \Psi) = e \times E(0, \Psi) \quad (۲)$$

۴) به سبب خاصیت هم‌ریختی E ، $\acute{e}$ تصادفی به‌صورت یکنواخت در R توزیع می‌شود. درصورتی که $\ominus$معکوس عملیات × باشد، برای نشان‌دادن این‌که $\acute{e}$ باز رمز شدهٔ e است (از طریق اثبات صفر دانش)، با استفاده از رابطه (۲) می‌توان با نشان‌دادن $\acute{e} \ominus e$ برابر رمز شدهٔ صفر است، صورت گیرد، یعنی:

$$\acute{e} \ominus e = E(0, \Psi) \quad (۳)$$

اثبات صفر دانش در جدول (۱) اثباتی برای نشان دان $\acute{e}$ باز رمزشدهٔ e است، خواهد بود:

(جدول-۱): نحوهٔ انجام اثبات صفر دانش‌ِ باز رمزشدهٔ e است[۱۸].

اثبات‌کننده		وارسی کننده
$know\ e, \Psi\ \ s.t\acute{e}$ $\ominus e = E(0, \Psi)$ $choose: \acute{\alpha} \in_R R$ $comput: \acute{e}$ $= E(0, \acute{\alpha})$	$\xrightarrow{\acute{e}}$	
	$\xleftarrow{c}$	$choose: c \in_R Z_q$
$Comput: \beta$ $= c\Psi \boxplus \acute{\alpha}$	$\xrightarrow{\beta}$	$verify:\ E(0, \beta)$ $= c(\acute{e} \ominus e) \times \acute{e}$

۲-۳- پروتکل رسیددار رأی‌گیری الکترونیکی مبتنی بر رمزنگاری همریخت

در پروتکل(پروتکل هیرت رسیددار [۱۸]) فرض کنید که N مسئول به‌صورت $A_N, \dots, A_1$ وجود داشته باشند و M تعداد رأی‌دهندگان است. رأی‌دهندگان و مسئولان اطلاعات عمومی خود را در تابلوی اعلانات درج می‌کنند. درضمن عدد آستانه ای t، که نشان‌دهندهٔ کمینهٔ تعداد مسئولان برای رمزگشایی نتیجهٔ نهایی انتخابات است، تعیین می‌شود. همچنین یک برگهٔ رأی شامل برداری از $\vec{v} = (v_1, \dots, v_L)$ آراست که در آن v_i رأی به نامزد i_ام است. بر اساس [۱۸] در یک *انتخابات k از L ، یک برگهٔ رأی معتبر است اگر و تنها اگر رأی v_i یکی از مقادیر صفر یا یک باشد و مجموع مؤلفه‌های یک بردار رأی برابر k باشد*. برای نمادگذاری آسان، $E(\vec{v}, \vec{\alpha})$ برای نمایش‌دادن رمزشدهٔ بردار $\vec{v} = (v_1, \dots, v_L)$ با بردار تصادفی $\vec{\alpha} = (\alpha_1, \dots, \alpha_L)$استفاده می‌شود تا $E(\vec{v}, \vec{\alpha}) = (E(v_1, \alpha_1), \dots, E(v_L, \alpha_L)$ به‌دست آید.

۱-۲-۳- مرحلهٔ آغازین

در این مرحله، مسئولان مشغول تولید کلید خصوصی و کلید عمومی مطابق با آن می‌شوند؛ به‌طوری‌که کلید خصوصی میان آن‌ها تسهیم شده و کلید عمومی هم به‌صورت عمومی منتشر می‌شود.

۲-۲-۳- مرحلهٔ رأی‌گیری

در مرحلهٔ رأی‌گیری ابتدا یک برگه‌ی رأی به‌صورت زیر آماده می‌شود:

رأی‌دهنده، رمزشدهٔ تصادفی $\vec{e} = E(\vec{v}, \vec{\alpha})$ را که در آن، $\vec{v}$ بردار رأی و $\vec{\alpha}$ بردار تصادفی است، می‌سازد و آن‌را به تابلوی اعلانات ارسال می‌کند. به‌علاوه اثبات‌هایی را برای اعتبار این برگهٔ رأی رمزشده، در تابلوی اعلانات درج می‌کند. همان‌طورکه درقبل گفتیم، یک برگهٔ رأی $\vec{v}$ معتبر است، اگر و تنها اگر $\sum_{i=1}^{L} v_i = k$ که در آن $v_i \in \{0,1\}$.

حال رأی‌دهنده به‌صورت زیر یک اثبات صفردانش برای نشان‌دادن اعتبار برگهٔ رأی رمزشدهٔ$\vec{e} = (e_1, \dots, e_L)$ آماده می‌کند. در این اثبات از نماد گذاری‌های زیر استفاده می‌شود: $e_{i,0} = e_i$ و $e_{i,1} = e_i \ominus E(1,0)$ به‌طوری‌که e_{i,v_i} رمزشدهٔ صفر با استفاده از عدد تصادفی α_i است؛ این بدان معناست درصورتی‌که رأی‌دهنده صفر را به‌عنوان رأیش انتخاب کرده باشد، در اثبات از $e_{i,0}$ استفاده و در غیر این صورت از $e_{i,1}$ استفاده می‌کند. همچنین از نمادهای $e_{\sum} = (e_1 \times \dots \times e_L)$ و $\alpha_{\sum} = \alpha_1 \boxplus \dots \boxplus \alpha_L$ و $e_{\sum,L} = e_{\sum} \ominus E(k,0)$ استفاده می‌شود. یک برگهٔ رأی معتبر است، اگر برای هر i، هر یک از $e_{i,0}$ یا $e_{i,1}$ رمزشدهٔ صفر باشند و $e_{\sum,L}$ رمزشدهٔ صفر باشد. اثبات به شکل زیر در جدول (۲) انجام می‌شود:

(جدول-۲): نحوهٔ اثبات صفر دانش برای اثبات اعتبار برگهٔ رأی[۱۸].

رأی‌دهنده		وارسی کننده
$knows: v_i$ $\in \{0,1\}, \alpha_i$ $\acute{\alpha}_{i,v_i} \in_R R$ $\acute{e}_{i,v_i} = E(0, \acute{\alpha}_{i,v_i})$ $c_{i,1-v_i} \in_R Z_u$ $\beta_{i,1-v_i} \in_R R$ $e_{i,1-v_i}$ $= E(0, \beta_{i,1-v_i})$ $\ominus c_{i,1-v_i} e_{i,1-v_i}$	$\xrightarrow{e_{i,0}\ ,\ e_{i,1}}$	
	$\xleftarrow{c}$	$c \in_R Z_u$

$c_{i,v_i} = c - c_{i,1-v_i}$ β_{i,v_i} $= c_{i,v_i}\alpha_i \boxplus \acute{\alpha}_{i,v_i}$	$\xrightarrow{c_{i,0},c_{i,1},\beta_{i,0},\beta_{i,1}}$	c $\stackrel{?}{=} c_{i,0} + c_{i,1}$ $E(0,\beta_{i,0})$ $\stackrel{?}{=} e_{i,0}c_{i,0}$ $\times \acute{e}_{i,0}$ $E(1,\beta_{i,1})$ $\stackrel{?}{=} e_{i,1}c_{i,1}$ $\times \acute{e}_{i,1}$

سرانجام در پروتکل بالا برای $i = 1, \dots, L$ مجموع $e_{\sum,k}$ باید رمزشدهٔ صفر باشد. در این اثبات صفر دانش در صورتی که بردار $[c, c_{1,0}, \dots, c_{L,0}, \beta_{1,0}, \dots, \beta_{L,0}, \beta_{1,1}, \dots, \beta_{L,1}, \beta_{\sum}]$ تساوی زیر را برآورده سازد، یک اثبات صفر دانش غیر تعاملی انجام می‌شود.

$$\begin{aligned} & c \\ & \stackrel{?}{=} H(E(0,\beta_{1,0}) \\ & \ominus c_{1,0}e_{1,0} \| \dots \| E(0,\beta_{L,0}) \\ & \ominus c_{L,0}e_{L,0} \| E(0,\beta_{1,1}) \\ & \ominus (c - c_{1,0})e_{1,1} \| \dots \| E(0,\beta_{L,1}) \\ & \ominus (c - c_{L,0})e_{L,1} \| E(0,\beta_{\sum}) \\ & \ominus ce_{\sum,L}) \end{aligned} \quad (۴)$$

۳-۲-۳- مرحلهٔ شمارش

شمارش‌کردن آرا برای هر نامزد به‌صورت زیر انجام می‌شود:

برای نامزد iـام، iـامین مؤلفهٔ هر برگهٔ رأی معتبر با به‌کارگیری خاصیت هم‌ریختی تابع رمزنگار جمع می‌شود و سپس بعد از رمزگشایی توسط مسئولان نتیجه به‌دست می‌آید. دقت کنید که دامنهٔ مقادیر رمزگشایی‌شده باید در بازهٔ $(0, M)$ قرار گیرد.

۴-۲-۳- خواص به‌دست‌آمده

محرمانگی این پروتکل، با این فرض تضمین می‌شود که بیشینه $t-1$ مسئول با همکاری هم قادر به کشف اطلاعات نیستند؛ و علاوه‌براین استفاده از اثبات صفر دانش محرمانگی را کامل می‌کند؛ اما این طرح به‌وضوح بدون رسید نیست؛ زیرا رأی‌دهنده خود اقدام به رمزنگاری برگهٔ رأی می‌کند.

در ادامه با استفاده از پروتکل بیان‌شده در بخش ۳-۲ پروتکل بدون رسید هیرت بیان می‌شود. بنابراین روشن است که مرحلهٔ رأی‌گیری بایستی اصلاح شود. پروتکل زیر به یک مسئول مخصوص که تصادفی‌کننده[1] نامیده می‌شود، اتکا دارد. این مسئول برگهٔ رأی رمزشده را باز رمزگذاری می‌کند. به طور دقیق‌تر هر رأی‌دهنده یک برگهٔ رأی رمزشده شامل رأیش را می‌سازد و آن‌را به‌طور مخفیانه به تصادفی کننده ارسال می کند. تصادفی‌کننده برگهٔ رأی را باز رمزگذاری کرده و آن‌را به تابلو اعلانات می‌فرستد. علاوه‌بر این تصادفی‌کننده به رأی دهنده نشان می‌دهد که برگهٔ رأی باز رمزگذاری‌شده، شامل رأی وی بوده است. بنابراین رأی‌دهنده و تصادفی‌کننده مشغول تولید اثباتی برای اعتبار این برگهٔ رأی جدید می‌شوند. در ادامه به‌اختصار مرحلهٔ رأی‌گیری را بیان و سپس جزئیات آن‌را شرح می‌دهیم.

۳-۳- روش رأی‌گیری الکترونیکی بدون رسید مبتنی بر رمزنگاری هم‌ریخت

بنابر [۱۸] پروتکل بدون رسید هیرت پیش رو از یک مسئول مخصوص به‌نام تصادفی‌کننده استفاده می‌کند. واضح است که تبانی این مسئول با موجودیت‌های خرابکار در مرحلهٔ رأی‌گیری مورد تحمل نمی‌تواند قرار گیرد. تصادفی‌کننده چیزی در مورد محتوای رأی نمی‌داند و همچنین در صحت شمارش حتی در صورت تبانی، نمی‌تواند خللی وارد کند؛ ولی او برگهٔ باز رمزشده را می‌تواند رد کند و بدین‌وسیله رأی مورد نظر در مرحلهٔ شمارش قرار نمی‌گیرد و یک حملهٔ انصراف اجباری به وقوع می‌پیوندد. فرض می‌کنیم که کانال ارتباطی میان رأی‌دهنده و تصادفی‌کننده برای مهاجم غیر قابل شنود باشد؛ لذا در ارتباط میان رأی‌دهنده و تصادفی‌کننده از کانال غیر قابل شنود استفاده می‌شود. همچنین، هر رأی‌دهنده یک کلید خصوصی و یک کلید عمومی مطابق آن دارد که کلید عمومی در تابلوی اعلانات درج شده است.

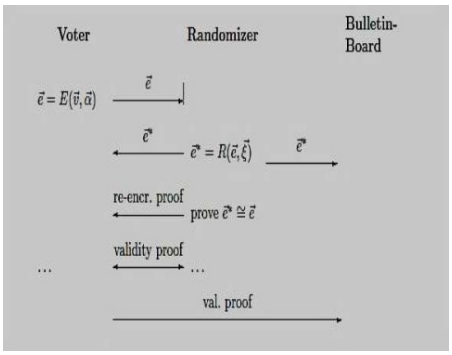
۱-۳-۳- طرح رأی‌گیری

این طرح دارای سه مرحلهٔ آغازین، رأی‌گیری و شمارش است. مراحل آغازین و شمارش مانند پروتکل قبلی است؛ از این‌رو از بیان این مراحل صرف نظر کرده و فقط مرحله رأی‌گیری را توضیح می‌دهیم.

[1] randomizer

۲-۳-۳- مرحلهٔ رأی‌گیری

یک برگهٔ رأی به این صورت آماده می‌شود که ابتدا یک رأی‌دهنده، بردار رأی را به‌صورت $\vec{e} = E(\vec{v}, \vec{\alpha})$ رمز می‌کند که در آن $\vec{v}$ بردار رأی و $\vec{\alpha} \in_R R^L$ بردار تصادفی($\vec{\alpha}$ برداری L عنصری است که هر عنصر آن عضوی از مجموعه R است) است؛ سپس آن‌را$(\vec{e})$ از میان یک کانال غیر قابل شنود برای تصادفی‌کننده می‌فرستد. تصادفی‌کننده بردار رأی رمزشدهٔ $\vec{e}$ را به‌صورت $\overrightarrow{e^*} = R(\vec{e}, \vec{\xi})$ باز رمزگذاری می‌کند؛ سپس رأی‌دهنده و تصادفی‌کننده مشغول تولید اثبات درستی $\vec{e}$ می شوند، بدون اینکه تصادفی‌کننده چیزی در مورد بردار رأی $\vec{v}$ بفهمد و رأی‌دهنده نیز چیزی در مورد شاهد $\vec{\xi}$ به‌دست آورد. سرانجام تصادفی‌کننده اثبات درستی برگهٔ رأی را به تابلو اعلانات می‌فرستد و رأی‌دهنده نیز برگهٔ رأی باز رمزشده را واریز می‌کند. روند این مرحله به‌صورت زیر در شکل (۱) آمده است:



(شکل-۱): نحوهٔ پروتکل بدون رسید هیرت [۱۸]

(جدول-۳): نحوهٔ انجام اثبات صفر دانش باز رمزگذاری [۱۸].

رأی‌دهنده		تصادفی‌کننده
$c \in_R Z_u$	$\xrightarrow{\vec{e},\ t_2}$ $\xleftarrow{c}$	$know\ \vec{\xi}, \vec{e}$ $\vec{\alpha} \in_R R^L$ $= E(\vec{0}, \vec{\alpha})$ $c_2 \in_R Z_u\ , s_2 \in_R Z_q$ $t_2 = g^{s_2} h_V^{-c_2}$
$c \stackrel{?}{=} c_1 + c_2$ $E(\vec{0}, \vec{\beta})$ $\stackrel{?}{=} c_1 \vec{e} \times \vec{e}$ g^{s_2} $\stackrel{?}{=} h_V^{c_2} t_2$	$\xrightarrow{c_1, c_2, \vec{\beta}, s_2}$	$c_1 = c - c_2\ mod\ u$ $\vec{\beta} = c_1 \vec{\xi} \boxplus \vec{\alpha}$

اما همان‌طور که واضح است، اساس این پروتکل بر انجام اثبات‌های صفر دانش است. بنابراین در مرحلهٔ رأی‌گیری تصادفی‌کننده باید نشان دهد که از شاهد $\vec{\xi}$ مطلع است؛ طوری‌که $\overrightarrow{e^*} = R(\vec{e}, \vec{\xi})$. اثبات صفر دانش پیش‌رو در جدول (۳) نشان می‌دهد که تصادفی‌کننده از شاهد $\vec{\xi}$ مطلع است؛ به‌طوری‌که $\vec{\vec{e}} = \mathrm{E}(\vec{0}, \vec{\xi})$ زیرا همان‌طور که درقبل گفته شد، بازرمزگذاری از رابطهٔ $\overrightarrow{e^*} = R(\vec{e}, \vec{\xi}) = \mathrm{E}(\vec{v}, \vec{\alpha}) \times \mathrm{E}(\vec{0}, \vec{\xi})$ میسر است؛ لذا داریم:

$$\begin{aligned}\vec{\vec{e}} = \overrightarrow{e^*} \ominus \vec{e} &= R(\vec{e}, \vec{\xi}) \ominus \mathrm{E}(\vec{v}, \vec{\alpha}) \\ &= \mathrm{E}(\vec{v}, \vec{\alpha}) \times \mathrm{E}(\vec{0}, \vec{\xi}) \\ &\ominus \mathrm{E}(\vec{v}, \vec{\alpha}) = \mathrm{E}(\vec{0}, \vec{\xi})\end{aligned}$$

بنابراین در روند اثبات زیر تصادفی‌کننده بعد از آماده و ارسال یک سری از اعداد تصادفی تولید و یا انتخاب‌شده یک عدد تصادفی از سوی رأی‌دهنده به‌عنوان چالش دریافت می کند که با آن فقط قادر است که به رأی‌دهنده نشان دهد که از یک شاهد، برای بازرمزگذاری برگهٔ رأی رمزشده استفاده کرده است. درصورتی‌که تساوی‌های بررسی‌شده توسط رأی‌دهنده برقرار نباشد، تصادفی‌کننده برگهٔ رأی رأی‌دهنده را بازرمزگذاری نکرده است.

اثبات بالا می‌تواند به‌صورت غیر تعاملی به نحوهٔ زیر انجام شود. بردار $[c_1, c_2, \vec{\beta}, s_2]$ تساوی زیر را باید برآورده سازد.

$$\begin{aligned}&c_1 + c_2 \qquad (۵)\\ &\stackrel{?}{=} H(\overline{E}(0, \beta_1)\\ &\ominus c_1 \overline{\beta_1} \| \dots \| E(0, \beta_L)\\ &\ominus c_1 \overline{e}_L \| g^{s_2} h_V^{-c_2})\end{aligned}$$

اما یک برگهٔ رأی معتبر است، اگر و تنها اگر هر e_i رمزشدهٔ صفر یا یک باشد و به‌طوردقیق k تا یک در این بردار وجود داشته باشد. همچنین رأی‌دهنده (که شاهد بازرمزگذاری $\vec{\xi}$ را نمی‌داند) و یا تصادفی‌کننده (که محتوای رأی $\vec{v}$ را نمی‌داند) قادر به انجام اثبات، به‌طور شخصی نیستند؛ ازاین‌رو آن‌ها به یک اثبات تعاملی نیاز دارند؛ که در آن رأی‌دهنده به تصادفی‌کننده نشان می‌دهد برگهٔ رأی رمزشدهٔ ارسالی حاوی مقادیر صفر یا یک است و دقیقاً شامل k تا یک است و تصادفی‌کننده نیز به رأی‌دهنده نشان می‌دهد که باز رمزگذاری به‌صورت $\overrightarrow{e^*} = \vec{e} \times E(0, \vec{\xi})$ انجام

گرفته است. در همین راستا، اثبات صفر دانشی که در جدول (۲) بیان شده است را در نظر بگیرید. این اثبات نشان می‌دهد که رأی‌دهنده رأی معتبر را تولید نموده است. همچنین برای این‌که تصادفی‌کننده نشان دهد که باز رمزگذاری را به‌صورت $\overrightarrow{e^*} = \vec{e} \times E(0, \vec{\xi})$ انجام داده است اقدامات زیر را انجام می‌دهد:

۱) تصادفی‌کننده $c'_{i,0} \in_R Z_u$ را به‌صورت تصادفی انتخاب کرده و قرار می‌دهد $c'_{i,1} = -c'_{i,0}$. با این کار داریم $c'_{i,0} + c'_{i,1} = 0$. همچنین مقادیر $\beta'_{i,0}, \beta'_{i,1} \in_R Z_u$ را انتخاب می‌کند که در تمامی مقادیر بالا $i = 1, \dots, L$ است.

۲) بعد از دریافت $(e'_{i,0}, e'_{i,1})$، تصادفی‌کننده، موارد زیر را محاسبه می‌کند:

$$e''_{i,0} = e'_{i,0} \times E(0, \beta'_{i,0}) \ominus c'_{i,0} e_{i,0} \quad (۶)$$

$$e''_{i,1} = e'_{i,1} \times E(0, \beta'_{i,0}) \ominus c'_{i,1} e_{i,1} \quad (۷)$$

و چالش c را به‌صورت $c = H(e''_{i,0}, e''_{i,1})$ آماده می‌کند.

۳) بعد از دریافت $(c_{i,0}, c_{i,1}, \beta_{i,0}, \beta_{i,1})$، تصادفی‌کننده موارد زیر را محاسبه می‌کند:

$$c''_{i,0} = c_{i,0} \boxplus c'_{i,0} \quad (۸)$$

$$c''_{i,1} = c_{i,1} \boxplus c'_{i,1} \quad (۹)$$

$$\beta''_{i,0} = \beta_{i,0} \boxplus \beta'_{i,0} \quad (۱۰)$$

$$\beta''_{i,1} = \beta_{i,1} \boxplus \beta'_{i,1} \quad (۱۱)$$

$$(c, c''_{1,0}, \dots, c''_{L,0}, \beta''_{\Sigma} \boxplus (\xi_1 \boxplus \dots \boxplus \xi_L), \beta''_{1,0} \boxplus c''_{1,0}\xi_1, \dots, \beta''_{L,1} \boxplus c''_{L,0}\xi_L, \beta''_{1,1} \boxplus c''_{1,1}\xi_1, \dots, \beta''_{L,1} \boxplus c''_{L,1}\xi_L) \quad (۱۲)$$

تا این‌جای کار، رأی‌دهنده نشان داده است که یک برگهٔ رأی معتبر را تولید کرده است و تصادفی‌کننده نیز بردار $(c, c''_{1,0}, \dots, c''_{L,0}, \beta''_{1,0}, \dots, \beta''_{L,0}, \beta''_{1,1}, \dots, \beta''_{L,1}, \beta''_{\Sigma})$ را برای این‌که باز رمزگذاری به‌صورت $\overrightarrow{e^*} = \vec{e} \oplus E(0, \vec{\xi})$ انجام شده، مهیا کرده است. در ادامه هر کسی از جملهٔ رأی‌دهنده بردار زیر را به‌عنوان اثبات درستی باز رمزگذاری از سوی تصادفی‌کننده می‌تواند وارسی کند که تساوی آخرین تساوی در جدول (۴) را ارضا می‌کند.

اثبات‌های بالا نشان می‌دهند که رأی‌دهنده برگهٔ رأی معتبر را تولید کرده و نیز تصادفی‌کننده به‌صورت $\overrightarrow{e^*} = \vec{e} \oplus E(0, \vec{\xi})$ باز رمزگذاری کرده است. روند اثبات بیان‌شده در جدول (۴) به‌تفصیل آمده است.

۳-۳-۳- بررسی امنیت

برای این‌که محرمانگی محفوظ بماند، در پروتکل واریز رأی، تصادفی‌کننده نباید در مورد محتوای برگهٔ رأی چیزی بفهمد که این مهم با رمزکردن برگهٔ رأی توسط رأی‌دهنده امکان‌پذیر است. درضمن تمامی اثبات‌های انجام‌شده از نوع صفر دانش هستند و با توجه به چگونگی آن‌ها کسی قادر به کشف اطلاعات مهم از جمله محتوای برگهٔ رأی و یا اعداد تصادفی استفاده‌شده در آن‌ها نیست.

در مورد خاصیت بدون رسیدبودن باید گفت که اگرچه رأی‌دهنده به‌شخصه برگهٔ رأی را رمز می‌کند؛ اما درصورتی می‌تواند برگهٔ رأی را واریز کند که تصادفی‌کننده آن‌را باز رمزگذاری کند. نکته‌ای که در آن باید بدان توجه داشت این است که رأی‌دهنده قادر به ایجاد ارتباط میان برگهٔ رأی باز رمزگذاری و برگهٔ اصلی نیست؛ زیرا او از شاهد استفاده‌شده برای بازرمزگذاری خبر ندارد و تصادفی‌کننده در اثبات‌های صفر دانش فقط از وجود چنین شاهدی خبر می‌دهد. بنابراین پروتکل بدون رسید است.

در پروتکل بالا یک مسئول، به‌عنوان تصادفی‌کننده وجود دارد که وظیفهٔ باز رمزگذاری آرای رمزشده را برعهده دارد. در صورتی این مسئول درست‌کار نباشد و یا این‌که با دشمن تبانی کند، امنیت این پروتکل به خطر می‌افتد. همچنین در واقعیت وجود یک مسئول درست‌کار، کاری سخت است.

(جدول-۴): نحوه اثبات صفر دانش برای اثبات اعتبار برگهٔ رأی و درستی بازرمزگذاری [۱۸]

رأی‌دهنده		وارسی‌کننده
$knows: v_i \in \{0,1\}, \alpha_i$ $\acute{\alpha}_{i,v_i} \in_R R$ $\acute{e}_{i,v_i} = E(0, \alpha'_{i,v_i})$ $c_{i,1-v_i} \in_R Z_u$ $\beta_{i,1-v_i} \in_R R$		$c'_{i,0} \in_R Z_u$ $c'_{i,1} = -c'_{i,0}$ $\beta'_{i,0}, \beta'_{i,1} \in_R Z_u$

$e_{i,1-v_i}^{'} = E(0,\beta_{i,1-v_i}) \ominus c_{i,1-v_i} e_{i,1-\ i}$	$\xrightarrow{e_{i,0}^{'},\ e_{i,1}^{'}}$	
	$\xleftarrow{c}$	$e_{i,0}^{''} = e_{i,0}^{'} \times E(0,\beta_{i,0}^{'}) \ominus c_{i,0}^{'} e_{i,0}$ $e_{i,1}^{''} = e_{i,1}^{'} \times E(0,\beta_{i,0}^{'}) \ominus c_{i,1}^{'} e_{i,1}$ $c = H(e_{i,0}^{''}, e_{i,1}^{''})$
$c_{i,v_i} = c - c_{i,1-v_i}$ $\beta_{i,v_i} = c_{i,v_i} \boxplus \acute{\alpha}_{i,v_i}$ بردار زیر باید تساوی زیر را ارضا کند $verify: (c, c_{1,0}^{''}, \dots, c_{L,0}^{''}, \beta$ $\boxplus (\xi_1 \boxplus \dots \boxplus \xi_L), \beta_{1,0}^{''}$ $\boxplus c_{1,0}^{''}\xi_1, \dots, \beta_{L,0}$ $\boxplus c_{L,0}^{''}\xi_L, \beta_{1,1}^{''}$ $\boxplus c_{1,1}^{''}\xi_1, \dots, \beta_{L,1}^{''}$ $\boxplus c_{L,1}^{''}\xi_L)$ $c \stackrel{?}{=} H(E(0,\beta_{1,0}^{''}$ $\boxplus c_{1,0}^{''}\xi_1)$ $\ominus c_{1,0}^{''} e_{1,0} \Big\| \dots \Big\| E(0,\beta_{L,0}^{''}$ $\boxplus c_{L,0}^{''}\xi_L)$ $\ominus c_{L,0}^{''} e_{L,0} \Big\| E(0,\beta_{1,1}^{''}$ $\boxplus c_{1,1}^{''}\xi_1)$ $\ominus (c - c_{1,0}^{''}) e_{1,1} \Big\| \dots \Big\| E(0,\beta_{L,1}^{''}$ $\boxplus c_{L,1}^{''}\xi_L)$ $\ominus (c - c_{L,0}^{''}) e_{L,1} \Big\| E(0,\beta_{\Sigma}^{''}$ $\boxplus (\xi_1 \boxplus \dots \boxplus \xi_L))$ $\ominus c e_{\Sigma,L}^{''})$	$\xrightarrow{c_{i,0}, c_{i,1}, \beta_{i,0}, \beta_{i,1}}$	$c \stackrel{?}{=} c_{i,0} + c_{i,1}$ $E(0,\beta_{i,0}^{''}) \stackrel{?}{=} e_{i,0} c_{i,0} \times \acute{e}_{i,0}$ $E(1,\beta_{i,1}^{''}) \stackrel{?}{=} e_{i,1} c_{i,1} \times \acute{e}_{i,1}$ $c_{i,0}^{''} = c_{i,0} \boxplus c_{i,0}^{'}$ $c_{i,1}^{''} = c_{i,1} \boxplus c_{i,1}^{'}$ $\beta_{i,0}^{''} = \beta_{i,0} \boxplus \beta_{i,0}^{'}$ $\beta_{i,1}^{''} = \beta_{i,1} \boxplus \beta_{i,1}^{'}$

۴- نتیجه‌گیری

در این مقاله بعد از بیان ملزومات و ویژگی‌های مطلوب یک انتخابات الکترونیکی، یکی از روش‌های رسیدن به یک انتخابات امن الکترونیکی را که همان روش مبتنی بر رمزنگاری هم‌ریخت بود، بیان و تفاوت بین یک پروتکل رسیددار و بدون رسید را تبیین کردیم. برای نیل به یک پروتکل بدون رسید، لازم است تا رأی‌دهنده نقشی در فرایند رمزنگاری و یا بازرمزگذاری نداشته باشد؛ بدیهی است برای محقق‌کردن این موضوع، فرایند رمزگذاری بایستی به طریقی توسط مسئول انتخابات انجام گیرد و اثباتی در این مورد نیز برای رأی‌دهنده ارائه شد. از چالش‌های پیش‌رو در سامانه‌های انتخابات الکترونیک امن به چگونگی استفاده از چندین مسئول رأی‌گیری، امن‌سازی هرچه بیش‌تر پروتکل‌ها بر اساس سایر روش‌های رمزنگاری کلید عمومی، طراحی اثبات‌های صفر دانش کارا، استفاده از ویژگی‌های بیومتریک در پروتکل انتخابات الکترونیک، اثبات امنیت در روش‌های انتخابات الکترونیک از راه دور، فازی‌سازی این پروتکل‌ها بر اساس روش کدگذاری و چگونگی رمزگذاری آن‌ها و چگونگی پیاده‌سازی این سامانه‌ها می‌توان اشاره کرد.

۵- مراجع

[1] Rallings C, Thrasher M. *Local elections in Britain*. Routledge; 2013 Feb 1.

[2] Chaum D, Jakobsson M, Rivest RL, Ryan PY, Benaloh J, Kutylowski M, Adida B, editors. *Towards trustworthy elections: new directions in electronic voting*. Springer; 2010 May 31.

[3] Gentry C. *Fully homomorphic encryption using ideal lattices*. Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09. Vol. 9.

[4] Peng K, Aditya R, Boyd C, Dawson E, Lee B. *Multiplicative homomorphic e-voting*. In International Conference on Cryptology in India 2004 Dec 20 (pp. 61-72). Springer, Berlin, Heidelberg.

[5] Hirt M, Sako K. *Efficient receipt-free voting based on homomorphic encryption*. InInternational Conference on the Theory and Applications of Cryptographic Techniques 2000 May 14 (pp. 539-556). Springer, Berlin, Heidelberg.

[6] Kim BL. *Receipt-free electronic voting through collaboration of voter and honest verifier*. *ICU*(2000)305-348.

[7] T.Rössler , *e-voting A survey and intro-duction*. Austria Secure Information Tech-nology Center – Austria (2005)1-14.

[8] Lee B, Kim K. *Receipt-free electronic voting scheme with a tamper-resistant randomizer*. In International Conference on Information Security and Cryptology 2002 Nov 28 (pp. 389-406). Springer, Berlin, Heidelberg.

[9] Abe M, Ohkubo M. *A framework for univer-sally composable non-committing blind signatures*. International Journal of Applied Cryptography. 2012 Jan 1;2(3):229-49.

[10] Cramer R, Franklin M, Schoenmakers B, Yung M. *Multi-authority secret-ballot elections with linear work*. In International Conference on the

Theory and Applications of Cryptographic Techniques 1996 May 12 (pp. 72-83). Springer, Berlin, Heidelberg.

[11] Iversen KR. *A cryptographic scheme for computerized general elections*. In Annual International Cryptology Conference 1991 Aug 11 (pp. 405-419). Springer, Berlin, Heidelberg.

[12] Park C, Itoh K, Kurosawa K. *Efficient anonymous channel and all/nothing elec-tion scheme*. InWorkshop on the Theory and Application of of Cryptographic Techniques 1993 May 23 (pp. 248-259). Springer, Berlin, Heidelberg.

[13] J.Benaloh,D. Tuinstra, *Receipt-free secret-ballot elections*. Proceedings of the26th ACM Symposiumon the Theory of Computing. ACM (1994)544-553.

[14] Sako K, Kilian J. *Receipt-free mix-type voting scheme*. In the proceeding of EUROCRYPT'95. Springer-Verlag, LNCS. 1995;921:393-403.

[15] Ohkubo M, Miura F, Abe M, Fujioka A, Okamoto T. *An improvement on a practical secret voting scheme*. In International Workshop on Information Security 1999 Nov 6 (pp. 225-234). Springer, Berlin, Heidelberg.

[16] Weber S. *A coercion-resistant crypto-graphic voting protocol-evaluation and prototype implementation*. Darmstadt Uni-versity of Technology, http://www. cdc. in-formatik. tudarmstadt. de/reports/reports/Stefan Weber. diplom. pdf. 2006 Jul.

[17] Huszti A. *A homomorphic encryption-based secure electronic voting scheme*. Publ. Math. Debrecen. 2011 Jan 1;79(3-4):479-96.

[18] Hirt M. *Receipt-free K-out-of-L voting based on ElGamal encryption*. In Towards Trustworthy Elections 2010 (pp. 64-82). Springer, Berlin, Heidelberg.

سید مهدی سجادیه مدرک کارشناسی، کارشناسی ارشد و دکترای خود را از دانشگاه صنعتی اصفهان در سال‌های ۸۲، ۸۴ و۹۱ در رشته مهندسی مخابرات کسب کرده است. ایشان از سال ۱۳۹۰ تا کنون عضو هیئت علمی دانشگاه آزاد اسلامی اصفهان (خوراسگان) است. زمینه پژوهشی وی الگوریتم‌ها و پروتکل‌های رمز به‌ویژه الگوریتم‌های رمز دنباله‌ای و قالبی است.

علی زاغیان مدرک کارشناسی خود را درسال ۶۳ در رشته ریاضی از دانشگاه اصفهان، مدرک کارشناسی ارشد و دکترای خود را از دانشگاه تربیت معلم در سال‌های ۶۵، ۸۹ در رشته ریاضی گرایش رمز و کد کسب کرده است. وی هم‌اکنون دانشیار دانشگاه صنعتی مالک اشتر است. زمینه پژوهشی ایشان الگوریتم‌های رمز و کد است.

سجاد رضایی ادریانی مدرک کارشناسی را درسال ۱۳۹۰ در رشته ریاضی کاربردی دانشگاه اصفهان اخذ و مدرک کارشناسی ارشد را در رشته رمز از دانشگاه صنعتی مالک اشتر در سال ۱۳۹۲ کسب کرد. زمینهٔ پژوهشی مورد علاقه وی سیستم‌های رمز کلید خصوصی و عمومی است.