رأی‌گیری الکترونیک

مقدمه‌ای بر رمزنگاری

[بهار ۹۹]

گردآورنده: سعید هدایتیان

۱ مقدمه

برگزاری انتخابات آزاد لازمه‌ی ادامه حیات هر دموکراسی است. در چند سال اخیر شاهد کاهش مشارکت مردم در رأی‌گیری‌های مختلفی که برگزار شده‌اند، بوده‌ایم. از علل این امر، می‌توان به اتلاف وقت رأی‌دهندگان در صف‌های طولانی رأی‌گیری و عدم اعتماد مردم به نهادهای برگزاری انتخابات اشاره کرد. با فراگیرتر شدن اینترنت و پیشرفت علم رمزنگاری، به نظر می‌رسد رأی‌گیری‌های الکترونیک جایگزین مناسبی برای انتخابات سنتی باشد. علاوه بر سرعت و راحتی بیشتر سیستم‌های رأی‌گیری الکترونیک، در عمل این سیستم‌ها بسیار قابل اعتمادتر هستند؛ در صورت استفاده از آن‌ها، تقلب‌کردن(چه برای نهادهای برگزاری انتخابات و چه برای کاندیداها) بسیار سخت‌تر می‌شود، و در صورت بروز هرگونه تخلف، به سادگی می‌توان آن را شناسایی و اثبات کرد. این سیستم‌ها در جلوگیری از خرید و فروش رأی نیز می‌توانند بسیار بهتر از ساز و کارهای مورد استفاده در انتخابات‌های سنتی عمل کنند. استفاده از ابزارهای الکترونیک برای برگزاری بهتر رأی‌گیری‌ها در بسیاری از کشورها سابقه‌ی طولانی دارد. بررسی‌های زیادی در مورد دستگاه‌های رأی‌گیری و شمارش آرا انجام شده‌است(برای مثال می‌توان به پروژه مشترک MIT و Caltech در سال ۲۰۰۱ اشاره کرد [۱]). هر چند استفاده از باجه‌های رأی‌گیری که امروزه رواج بسیاری دارد نیز رأی‌گیری الکترونیک نامیده می‌شود، اما تلاش برای حذف کامل حوزه‌های رأی‌گیری همچنان ادامه دارد. امروزه از نظر تئوری توانایی برگزاری انتخابات امن در بستر اینترنت را داریم؛ اما مشکلاتی(مثل عدم دسترسی یکسان جمعیت به اینترنت و...) باعث شده‌اند که هنوز با برگزاری یک انتخابات سراسری بزرگ به صورت کاملاً آنلاین فاصله داشته باشیم. با این حال اتفاقاتی مثل شیوع کرونا شاید باعث شوند که بسیار زود شاهد برگزاری رأی‌گیری‌های الکترونیک به صورت گسترده‌تر باشیم.

در این مقاله ابتدا یک پروتکل رأی‌گیری الکترونیک را به صورت دقیق معرفی می‌کنیم. سپس ویژگی‌های مطلوب یک سیستم رأی‌گیری الکترونیک را تعریف می‌کنیم، و عملکرد پروتکل اخیر در دستیابی به این ویژگی‌ها را بررسی می‌کنیم. در آخر، چند ایده دیگر را که در طراحی انواع پروتکل‌های رأی‌گیری الکترونیک قابل استفاده هستند، به صورت بسیار مختصر معرفی می‌کنیم.

۲ طرحی برای رأی‌گیری الکترونیک

پروتکلی که در این قسمت قصد بررسی آن را داریم توسط لیاو [۲] در سال ۲۰۰۴ معرفی شده‌است.[۱] این پروتکل در عین سادگی بسیاری از ویژگی‌های مطلوب را دارد. به عنوان مثال در این پروتکل باجه‌های رأی‌گیری فیزیکی به طور کامل حذف شده‌اند. البته این پروتکل کاستی‌هایی را هم دارد که در ادامه مورد بررسی قرار خواهند گرفت. در این بخش ابتدا با چند تکنیک و اولیه‌های مورد استفاده در این پروتکل آشنا می‌شویم. سپس به صورت دقیق پروتکل را معرفی می‌کنیم.

[۱] از اینجا می‌توانید در مورد این پروژه بیشتر بخوانید.

[۲] Horng-Twu Liaw

۱.۲ مقدمات

۱.۱.۲ امضای کور[۳]

امضای کور که اولین بار توسط دیوید چاوم [۴] معرفی شد، نوعی امضای دیجیتال [۵] است.[۲] در پروتکل امضای کور، دو طرف امضاکننده و درخواست‌کننده وجود دارند. طرف امضاکننده قابلیت تولید امضا برای متن‌های دلخواه را دارد؛ هدف درخواست‌کننده به دست آوردن یک امضای معتبر برای یک متن مشخص است. ویژگی مهم پروتکل امضای کور این است که امضاکننده متوجه ارتباط میان متن مورد نظر درخواست‌کننده و امضایی که تولید می‌کند، نمی‌شود [۶] . به عنوان نمونه سیستم امضای کور RSA به صورت زیر عمل می‌کند.

فرض کنید m پیامی است که درخواست‌کننده قصد امضای آن را دارد. d کلید خصوصی امضاکننده و e و n کلیدهای عمومی امضاکننده هستند. R عددی تصادفی است که توسط درخواست‌کننده انتخاب می‌شود و ویژگی $\gcd(R,n)=۱$ را دارد. در نهایت s امضای پیام m است.

برای درخواست امضای پیام m ، ابتدا درخواست‌کننده $m' = mR^e \mod n$ را به امضاکننده ارسال می‌کند. امضاکننده با دریافت m' ، مقدار $s' = (m')^d \mod n$ را به درخواست‌کننده می‌دهد. در نهایت درخواست‌کننده امضای مورد نظرش را با استفاده از رابطه زیر محاسبه می‌کند.

$$s = s'R^{-۱} \mod n = ((mR^e \mod n)^d \mod n)R^{-۱} \mod n = m^d \mod n.$$

۲.۱.۲ تکنیکی برای کسب اجبارناپذیری جزئی

در بسیاری از پروتکل‌های رأی‌گیری الکترونیک، رأی‌دهنده‌ها پس از ثبت رأیشان نوعی *رسید* دریافت می‌کنند. از این رسید بعد از اعلام نتایج برای اعتبارسنجی یا موارد مشابه دیگر می‌توان استفاده کرد. مشکل این روش‌ها این است که وجود رسید رأی‌دهی، راه را برای خرید و فروش رأی باز می‌کند. در نتیجه بیشتر این پروتکل‌ها فاقد ویژگی اجبارناپذیری‌اند.

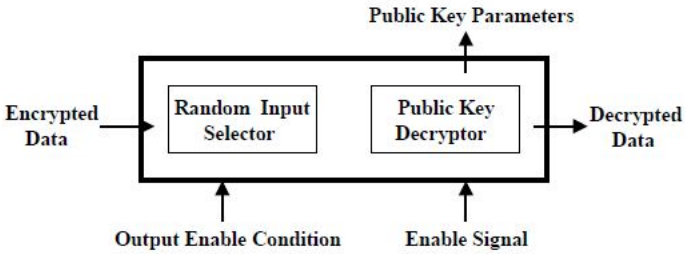
برای حل این مسئله راهکارهایی پیشنهاد شده است. در سیستم رأی‌گیری الکترونیکی‌ای که قصد بررسی آن را داریم، از ایده‌ای که توسط ریرا [۷] و دیگران در ۱۹۹۸ ارائه شده، استفاده می‌شود. در این روش رأی‌دهندگان از *کارت‌های هوشمندی* که در برابر دستکاری مقاوم هستند، استفاده می‌کنند. این کارت‌ها با ذخیره رسیدهای رأی‌دهی به صورت رمزشده، دسترسی رأی‌دهندگان به رسیدها را محدود می‌کنند. در واقع رأی‌دهندگان تنها پس از اعلام نتایج نهایی و دریافت یک کلید خصوصی امکان دسترسی به رسید ذخیره شده روی کارت هوشمند را خواهند داشت. به این ترتیب هر چند سیستم به طور کامل اجبارناپذیر نخواهد بود، اما می‌توان به اجبارناپذیری جزئی دست یافت.

۳.۱.۲ رمزگشایی غیرقابل ردیابی[۸]

سیستمی که قصد بررسی آن را داریم از اولیه‌ای به نام *رمزگشایی غیرقابل ردیابی* استفاده می‌کند. رمزگشای غیرقابل ردیابی در عمل قابل ساخت است. شمای کلی این وسیله در شکل ۱ آمده است و در اینجا به طور مختصر عملکرد آن را توضیح می‌دهیم. به طور کلی رمزگشا تعدادی متن رمزشده را به عنوان ورودی دریافت، و در حافظه موقتش ذخیره می‌کند. بعد از مدتی متون ذخیره شده را رمزگشایی می‌کند و با ترتیبی تصادفی به عنوان خروجی برمی‌گرداند. کلید خصوصی مورد استفاده در رمزگشایی متون رمز شده، در حافظه‌ای از نوع PROM

---

[۳] Blind Signature
[۴] David Chaum
[۵] Digital Signature
[۶] به این ویژگی unlink-ability گفته می‌شود.
[۷] Andreu Riera
[۸] Untraceable Decryption



شکل ۱: رمزگشای غیرقابل ردیابی

ذخیره می‌شود و پس از شروع به کار دستگاه و تولید کلیدهای عمومی و خصوصی، دیگر قابل تغییر نیست. حافظه اصلی این دستگاه(که ورودی‌ها را ذخیره می‌کند) مشابه RAM عمل می‌کند و پس از اتمام کار دستگاه و با خاموش کردن آن، اطلاعات ذخیره شده روی آن پاک می‌شوند. این دستگاه را می‌توان به گونه‌ای تنظیم کرد که پس از دریافت تعداد مشخصی ورودی یا پس از مدت زمان مشخصی شروع به تولید خروجی کند. بنابراین به طور خلاصه، وظیفه این دستگاه، رمزگشایی از تعدادی متن رمزشده و اعلام آن‌ها با ترتیبی تصادفی است.

۲.۲ پروتکل لیاو

حال که با اولیه‌ها و تکنیک‌های بالا آشنا شدیم، می‌توانیم به معرفی پروتکل بپردازیم. این پروتکل متشکل از سه طرف است. ۱. رای دهندگان ۲. امضاکننده ۳. منتشرکننده. همچنین از دو نوع وسیله استفاده می‌شود: کارت هوشمند که در اختیار رأی‌دهندگان است، و یک دستگاه رمزگشای غیرقابل ردیابی. فرضیات مورد استفاده در این پروتکل به شرح زیر هستند:

۱. هر رأی‌دهنده قادر به ارتباط با نهادهای برگزاری انتخابات(شامل امضاکننده و منتشرکننده) است.

۲. یک سیستم پیام‌رسانی الکترونیک امن و غیرقابل ردیابی موجود است.[۳]

۳. در صورت سخت‌بودن مسئله تجزیه، سیستم رمز RSA امن است.

۴. هر رأی‌دهنده یک کارت هوشمند و دستگاه مورد نیاز برای خواندن اطلاعات روی آن را دارد.

در ادامه لیستی از نمادهایی که در حین بیان و بررسی پروتکل از آن‌ها استفاده خواهیم کرد، آمده است.

d_i: کلید خصوصی iـامین رأی‌دهنده.

e_i, n_i: کلیدهای عمومی iـامین رأی‌دهنده.

d_s: کلید خصوصی امضاکننده.

e_s, n_s: کلیدهای عمومی امضاکننده.

d_p: کلید خصوصی منتشر کننده.

e_p, n_p: کلیدهای عمومی منتشرکننده

ID: شناسه(عدد) یکتا که درون کارت هوشمند ذخیره شده است.

f: یک جایگشت(تابع یک‌به‌یک و پوشا) یک‌طرفه که توسط مرکز رأی‌گیری تولید شده است.

RD: یک عدد تصادفی که توسط مرکز رأی‌گیری تولید شده است.

V_i: انتخاب(رأی) iـ‌امین رأی‌دهنده

R_i: یک رشته تصادفی که توسط iـ‌امین رأی‌دهنده تولید شده.

r_i: عددی تصادفی که توسط iـ‌امین رأی‌دهنده تولید شده، و در رابطه $\gcd(r_i, n) = ۱$ صدق می‌کند.

t_i: عددی تصادفی که توسط iـ‌امین رأی‌دهنده تولید شده، و در رابطه $\gcd(t_i, n) = ۱$ صدق می‌کند.

پروتکل شامل چهار مرحله به شرح زیر است:

مرحله اول: آماده‌سازی سیستم

در ابتدا هر یک از رأی‌دهنده‌ها، امضاکننده و منتشر کننده کلیدهای عمومی و خصوصی خود را تولید می‌کنند. هرگاه یکی از طرفین به کلید عمومی دیگری نیاز داشت، می‌تواند آن را از طریق یک کانال ارتباطی امن، از *مرجع صدور گواهی دیجیتال* [۹] دریافت کند. هر یک از رأی‌دهندگان یک کارت هوشمند حاوی یک شناسه‌ی یکتا که توسط این مرجع تأیید شده را در اختیار دارد. یک دستگاه رمزگشای غیرقابل ردیابی در مرکز رأی‌گیری قرار دارد. همچنین مرکز رأی‌گیری جایگشت یک‌طرفه f و عدد تصادفی RD را تولید، و به طور عمومی اعلام می‌کند(این دو نیز از طریق مرجع صدور گواهی دیجیتال برای همه قابل دسترسی هستند).

مرحله دوم: رأی دادن

۱. رأی‌دهنده iـ‌ام

ابتدا رأی‌دهنده رأی خود(V_i) را انتخاب می‌کند. سپس رشته تصادفی R_i و اعداد تصادفی t_i و r_i را تولید می‌کند. رأی‌دهنده iـ‌ام این مقادیر را در کارت هوشمندش ذخیره می‌کند. کارت هوشمند طبق روابط زیر، $\mathrm{VT_i}$ را تولید می‌کند.

$$H_i = f(\mathrm{ID}_i, R_i)$$

$$M_i = t_i^{e_p}(H_i||V_i) \mod n_p||\mathrm{RD}$$

$$Y_i = (r_i^{e_s})M_i \mod n_s$$

$$\mathrm{REG}_i = \mathrm{RD}^{d_i} \mod n_i$$

$$\mathrm{VT_i} = Y_i||\mathrm{REG}_i$$

در نهایت رأی‌دهنده iـ‌ام مقدار $\mathrm{VT_i}$ را به امضاکننده ارسال می‌کند.

۲. امضاکننده:

امضاکننده با دریافت VT_i ابتدا صحت REG_i را بررسی می‌کند.

$$\mathrm{REG}_i^{e_i} \mod n_i = (\mathrm{RD}^{d_i} \mod n_i)^{e_i} \mod n_i = \mathrm{RD}$$

چنانچه $\mathrm{REG}_i^{e_i}$ برابر RD نباشد، امضاکننده VT_i را رد می‌کند. البته حتی اگر شرط قبلی برقرار باشد، باز هم ممکن است VT_i رد شود. این در حالتی اتفاق می‌افتد که REG_i قبلاً توسط شخص دیگری استفاده شده باشد.

[۹] Certification Authority

پس از اطمینان از اینکه رأی‌دهنده iـام مجاز به رأی‌دهی است، امضاکننده مقدار Z_i را طبق رابطه زیر محاسبه می‌کند و برای رأی‌دهنده iـام ارسال می‌کند.

$$Z_i = Y_i^{d_s} \mod n_s$$

۳. رأی‌دهنده iـام

کارت هوشمند با دریافت Z_i از امضاکننده، ابتدا مقدار X_i را طبق رابطه زیر محاسبه می‌کند.

$$X_i = Z_i r_i^{-1} \mod n_s = ((r_i^{e_s} M_i \mod n_s)^{d_s} \mod n_s) r_i^{-1} \mod n_s = M_i^{d_s} \mod n_s.$$

(X_i در واقع همان امضای کور امضاکننده روی پیام M_i است) در نهایت کارت هوشمند سه‌تایی (X_i, M_i, t_i) را برای امضاکننده ارسال، و یک کپی از آن را به عنوان رسید در خود ذخیره می‌کند.

مرحله سوم: بررسی

در این مرحله امضاکننده رأی نهایی رأی‌دهنده iـام را به صورت سه‌تایی (X_i, M_i, t_i) دریافت می‌کند. ابتدا اعتبار امضای X_i طبق رابطه زیر بررسی می‌شود. اگر امضا معتبر باشد، باید داشته باشیم:

$$X_i^{e_s} \mod n_s = (M_i^{d_s} \mod n_s)^{e_s} \mod n_s = M_i.$$

اگر X_i و M_i در رابطه بالا صدق کنند و مربوط به REG_iای که قبلاً تأیید شده است باشند، امضاکننده سه‌تایی (X_i, M_i, t_i) را به رمزگشای غیرقابل ردیابی ارسال می‌کند.

مرحله چهارم: اعلام نتایج

پس از اتمام زمان رأی‌گیری، رمزگشای غیرقابل ردیابی شروع به تولید خروجی می‌کند. برای محاسبه V_i و H_i با داشتن M_i و t_i به صورت مقابل عمل می‌شود. ابتدا توجه کنید که:

$$M_i = t_i^{e_p}(H_i||V_i) \mod n_p||\mathrm{RD}.$$

رمزگشا ابتدا RD را از آخر M_i حذف می‌کند تا M_i' حاصل شود. حال با استفاده از کلید خصوصی d_p طبق روابط زیر M_i رمزگشایی می‌شود:

$$M_i'' = ((M_i')^{d_p} \mod n_p) t_i^{-1} \mod n_p = (H_i||V_i)^{d_p} \mod n_p.$$

$$(M_i'')^{e_p} \mod n_p = ((H_i||V_i)^{d_p} \mod n_p)^{e_p} \mod n_p.$$

زوج‌های $H_i||V_i$ به صورت عمومی اعلام می‌شوند. در آخر منتشر کننده REG_i همه رأی‌دهنده‌های مجاز و مقدار d_p را اعلام می‌کند.

پس از این مراحل، هر یک از رأی‌دهندگان با استفاده از رسید (X_i, M_i, t_i) که در کارت هوشمندشان ذخیره شده است، می‌تواند از شمرده‌شدن رأیش اطمینان حاصل کند. به این صورت که چنانچه رأی او (یعنی $(H_i||V_i)$) در بین آرای اعلام شده نبود، می‌تواند با ارسال رسید ذخیره شده روی کارت هوشمندش به مراجع برگزاری انتخابات، شمرده نشدن رأیش را اثبات کند.

۳ ویژگی‌های یک پروتکل رأی‌گیری

هدف نهایی یک سیستم رأی‌گیری الکترونیکی، برگزاری کامل یک انتخابات در بستر اینترنت است. این شامل فرایند احراز هویت، رأی دادن، شمارش آرا و صحت‌سنجی انتخابات است. در زیر تعدادی از ویژگی‌های مطلوب برای چنین سیستمی آورده شده است. همچنین در مورد میزان موفقیت پروتکل لیاو در دستیابی به هر یک، صحبت شده است.

۱.۳ کامل بودن[۱۰]

منظور از کامل بودن این است که همواره هر رأی‌دهنده‌ی مجاز، توسط مجری انتخابات قبول شود و بتواند رأی دهد. در انتخابات سنتی، احراز هویت و رأی‌دادن به صورت حضوری انجام می‌گیرد؛ اما در رأی‌گیری الکترونیک باید از ساز و کارهای دیگری برای احراز هویت استفاده شود. در نتیجه ممکن است هویت یک رأی‌دهنده‌ی مجاز توسط سیستم تأیید نشود و نتواند رأی دهد. در پروتکل بالا ID یک شناسه یکتا است که در کارت هوشمند هر رأی‌دهنده ذخیره شده‌است و R نیز یک عدد تصادفی است. با توجه به اینکه f یک جایگشت است، $f(\mathrm{ID}, R)$ مقداری یکتا است. در نتیجه مقدار H_i برای هر رأی‌دهنده متفاوت از دیگران است. بنابراین درخواست هیچ رأی‌دهنده‌ی مجازی توسط امضاکننده رد نمی‌شود. پس پروتکل لیاو کامل است.

۲.۳ اجبارناپذیری[۱۱]

اجبارناپذیری یا اختیار کامل رأی‌دهنده در انتخاب، یکی از ویژگی‌هایی است که در انتخابات سنتی امیدی به برقراری کامل و مطلق آن نداریم؛ اما در سیستم‌های انتخابات الکترونیکی می‌توان به آن دست یافت. به طور کلی یک سیستم انتخابات الکترونیکی اجبارناپذیر است اگر اولاً یک رأی‌دهنده نتواند به شخص دیگری اثبات کند که به چه گزینه‌ای رأی داده است، و ثانیاً فقط شخص رأی‌دهنده بتواند رأی خود را انتخاب کند. به این ترتیب یک سیستم اجبارناپذیر، در برابر مشکلاتی مانند خرید و فروش رأی مقاوم است. در بسیاری از پروتکل‌ها، برای دستیابی به اجبارناپذیری از باجه‌های رأی‌گیری استفاده می‌شود. در پروتکل لیاو، رسید رأی‌دهی تا قبل از انتشار d_p توسط منتشرکننده قابل استفاده نیست. بنابراین تا قبل از پایان رأی‌گیری، هر چند رسید در کارت هوشمند ذخیره شده، اما با استفاده از آن نمی‌توان به رأی داده شده پی برد. به این ترتیب هرچند به اجبارناپذیری کامل نرسیده‌ایم، اما بدون استفاده از باجه‌های رأی‌گیری که باعث ایجاد محدودیت فیزیکی برای رأی دادن می‌شوند، به اجبارناپذیری جزئی دست یافته‌ایم. به نظر می‌رسد که دستیابی به اجبارناپذیری کامل نیازمند این باشد که انتخابات *بدون رسید* باشد. یکی از تکنیک‌هایی که ممکن است در تلاش برای حذف رسید مفید واقع شود استفاده از اعتبارسنجی جامع و عمومی است که در ادامه در مورد آن بیشتر توضیح می‌دهیم.

۳.۳ غیرقابل تقلب[۱۲]

در رأی‌گیری‌های سنتی جهت اطمینان از شمارش صحیح آرا از روش‌های خلاقانه‌ای همچون حضور نماینده‌ای از طرف‌های ذی‌نفع در هنگام شمارش آرا و شمارش چندباره‌ی آرا استفاده می‌شود. با این وجود کماکان احتمال تبانی و تقلب در شمارش آرا وجود دارد، و معمولاً اثبات صحت انتخابات به راحتی امکان‌پذیر نیست. سیستم‌های رأی‌گیری الکترونیک می‌توانند در حل این مشکل کمک‌کننده باشند. یک سیستم رأی‌گیری الکترونیک را غیرقابل تقلب گوییم اگر اولاً رأی‌دهنده‌ها بتوانند بدون فاش‌کردن رأیشان، مقامات برگزارکننده انتخابات را به تقلب متهم کنند، و ثانیاً در صورت تهمت نادرست، مقامات بتوانند صحت انتخابات را اثبات کنند. در پروتکل لیاو رأی‌دهندگان برای اعتراض به شمرده نشدن رأیشان، رسید رأی‌دهیشان را از طریق ایمیل و به صورت محرمانه ارسال می‌کنند. پس برای اعتراض، نیازی به افشای رأی نیست. همچنین در صورتی که کسی بخواهد صحت انتخابات را زیر سؤال ببرد، بایستی یک رسید رأی‌دهی معتبر تولید کند که رأی متناظر با آن اعلام نشده باشد. یکی از شروط لازم برای تولید یک رسید رأی‌دهی جعلی، تولید یک امضای معتبر برای یک پیام است. پس در صورتی که سیستم امضای کور استفاده شده امن باشد (در بالا از سیستم امضای کور RSA استفاده شده که تحت فرض RSA امن است)، پروتکل غیر قابل تقلب است.

---

[۱۰] Completeness
[۱۱] Uncoercibility
[۱۲] Non-Cheating

۴.۳ استحکام[۱۳]

به صورت کلی، استحکام یک سیستم به معنای مقاومت در برابر حملاتی که به آن انجام می‌شود است. به طور دقیق‌تر سیستم رأی‌گیری الکترونیکی‌ای مستحکم است که

- یک رأی‌دهنده مخرب یا هر شخص دیگری توانایی برهم‌زدن یا ایجاد اخلال در روند برگزاری انتخابات را نداشته باشد.
- فرایند دریافت رأی از رأی‌دهنده‌ها، مستقل از یکدیگر باشد تا رأی‌دهنده‌های مخرب نتوانند با توقف انتخابات در آن اخلال ایجاد کنند.
- هیچ‌کس(حتی مسئولین برگزاری انتخابات) نتواند به وسیله‌ی اطلاعات شخصی لورفته‌ی یک رأی‌دهنده، رأی آن شخص را تغییر دهد.

در پروتکل لیاو برای جلوگیری از ایجاد وقفه یا اختلال در روند اجرای انتخابات توسط مهاجم، می‌توان همه محاسبات را در یک محیط توزیع‌شده و بدون استفاده از تنها یک سرور مرکزی(که ممکن است تحت حمله دچار اختلال شود) انجام داد. همچنین برخلاف بعضی پروتکل‌های دیگر، رفتار مخرب یک رأی‌دهنده کل فرایند انتخابات را دچار وقفه نخواهد کرد.

۵.۳ یکتایی[۱۴]

در یک انتخابات، هیچ رأی‌دهنده‌ای نباید بتواند بیش از یک بار رأی بدهد. به این ویژگی (که هم در انتخابات الکترونیکی و هم در انتخابات سنتی بسیار مهم است) یکتایی می‌گوییم. پروتکل لیاو برای دستیابی به این ویژگی، از REG_i استفاده می‌کند. فقط در صورتی که REG_i بدون مشکلی با استفاده از کلید عمومی رأی‌دهنده‌ی iـ‌ام رمزگشایی شد، و قبلاً هم برای رأی دادن استفاده نشده بود، فرایند رأی‌دادن بدون مشکل طی می‌شود. چون مقدار REG_i یک فرد قابل تغییر نیست، یک نفر نمی‌تواند بیش از یک بار رأی دهد.

۶.۳ اعتبارسنجی[۱۵]

اعتبارسنج‌بودن سیستم‌های رأی‌گیری الکترونیک(که معمولاً با غیرقابل تقلب بودن هم در ارتباط است) به این معناست که رأی‌دهنده‌ها بتوانند شمرده‌شدن رأی خود را بررسی کنند. در رأی‌گیری‌های الکترونیکی این ویژگی بسیار مهم است زیرا ارتباط میان رأی‌دهنده و مرکز رأی‌گیری از طریق اینترنت(یا بسترهای مشابه) صورت می‌گیرد، و در این فضا، داده‌هایی که به صورت امن رمزنگاری نشده باشند قابل تحریف و تغییر هستند. در پروتکل لیاو، پس از اعلام نتایج هر رأی‌دهنده با استفاده از رسید رأی‌دهی، می‌تواند از وجود رأیش در میان آرای نهایی اعلام شده، اطمینان حاصل کند. پس در این پروتکل، قابلیت اعتبارسنجی فردی وجود دارد. *اعتبارسنجی جامع و عمومی* به این معناست که پس از اعلام نتایج هر کس بتواند صحت اجرای انتخابات را به طور کامل بررسی و تأیید کند. در پروتکل فعلی، هرکس فقط توانایی بررسی رأی خودش را دارد، و برای اعتبارسنجی کامل، نیاز به داشتن دسترسی به همه‌ی رسیدهای رأی‌دهی داریم. در اعتبارسنجی جامع و عمومی تلاش بر این است که برای بررسی صحت اجرای انتخابات نیازی به مشارکت همه‌ی شرکت‌کنندگان در فرایند اعتبارسنجی نباشد. در صورت دستیابی به این هدف، احتمالاً می‌توان رسیدهای رأی‌دهی را نیز حذف کرد که برای دستیابی به اجبارناپذیری کامل نیز ضروری به نظر می‌رسد.

---

[۱۳] Robustness
[۱۴] Uniqueness
[۱۵] Verifiability

۷.۳ عادلانه بودن[۱۶]

عادلانه بودن انتخابات به این معناست که قبل از مرحله اعلام نتایج، هیچ‌کس نتواند در مورد آرای دریافت‌شده اطلاعاتی کسب کند. در بسیاری از پژوهش‌ها، مفهوم محرمانگی شامل عادلانه بودن هم می‌شود. در پروتکل لیاو همه ارتباطات به وسیله سیستم رمز RSA رمزنگاری می‌شوند. بنابراین با فرض امنیت RSA این پروتکل هیچ نشتی اطلاعاتی ندارد و کاملاً عادلانه است.

۸.۳ محرمانگی[۱۷]

محرمانگی یا ناشناس‌بودن، به این معناست که هیچ‌کس، حتی برگزارکنندگان انتخابات، نتواند بین یک رأی و رأی‌دهنده صاحب آن، ارتباطی برقرار کند. در پروتکل لیاو با استفاده از یک سیستم ایمیل غیرقابل ردیابی (در هنگام برقراری ارتباطات لازم برای رأی‌دادن و نیز برای اعتراض به شمرده نشدن رأی) و رمزگشای غیرقابل ردیابی، ارتباط میان پیام‌ها و رأی‌دهندگان شکسته می‌شود.

۹.۳ سهولت در استفاده[۱۸]

رأی‌دهنده‌ها باید بتوانند بدون معطلی، با سرعت، یکباره و بدون استفاده از تجهیزات خاصی رأی بدهند. در پروتکل لیاو محدودیت مکانی (مثل لزوم حضور در باجه‌های رأی‌گیری) وجود ندارد و تنها ابزارهای لازم، یک کارت هوشمند، و وسیله‌ای برای خواندن اطلاعات روی آن است. این مورد، به ویژه با توجه به استفاده فراگیر از وسایل الکترونیکی در جامعه‌ی امروزی، محدودیت بزرگی به شمار نمی‌رود. با این حال در پژوهش‌های آینده می‌توان برای حذف کارت هوشمند، تلاش کرد. در صورت حذف کارت‌های هوشمند، یکی از مشکلاتی که بایستی حل شود، تأیید هویت رأی‌دهندگان مجاز است. در این سیستم‌ها باید به گونه‌ای عمل شود که حتی در صورت لو رفتن اطلاعات هویتی فرد (که در دنیای امروزه بسیار محتمل است) کسی نتواند به جای دیگری رأی دهد.

۱۰.۳ کارایی[۱۹]

یک سیستم رأی‌گیری الکترونیک کارا، با کم کردن پیچیدگی و کاهش گام‌های لازم، سرعت برگزاری را افزایش می‌دهد. به طور دقیق‌تر، منظور از کارایی این است که کل فرایند انتخابات، در زمان معقولی صورت گیرد؛ به عنوان مثال رأی‌دهنده‌ها برای ثبت رأی خودشان نیازی به صبرکردن برای دیگران نداشته باشند. در پروتکل لیاو رأی‌دهندگان نیازی به یادگیری تکنیک‌های خاص ندارند. همچنین می‌توان به گونه‌ای پروتکل را پیاده‌سازی کرد که همه ارتباطات لازم در زمان معقول (و حتی سریع‌تر از انتخابات سنتی) انجام شود.

۱۱.۳ پویایی[۲۰]

پویایی یک سیستم رأی‌گیری الکترونیک به این معنا است که رأی‌دهنده‌ها برای شرکت در انتخابات محدود به محل سکونتشان نباشند. به عنوان مثال برای ثبت رأی، نیازی به حضور فیزیکی در حوزه‌های رأی‌گیری معینی نباشد. همانطور که گفته شد، در بسیاری از پژوهش‌ها برای اجبارناپذیر شدن انتخابات، استفاده از باجه‌های رأی‌گیری پیشنهاد شده است، که با پویایی انتخابات در تضاد است. رأی‌گیری با استفاده از پروتکل لیاو در بستر اینترنت قابل انجام است. در واقع برای رأی‌دادن تنها نیاز به ارتباط با اینترنت و یک کارت هوشمند است. بنابراین، این پروتکل از نظر پویایی وضعیتی مطلوب (اما نه ایده‌آل) دارد.

---

[۱۶] Fairness
[۱۷] Anonymity
[۱۸] Convenience
[۱۹] Efficiency
[۲۰] Mobility

۱۲.۳ جامعیت[۲۱]

در یک انتخابات جامع، رأی‌دهنده‌ها قادر به انتخاب از بین چندین گزینه هستند و انتخاب‌ها محدود به دو گزینه‌ی «آری» یا «خیر» نیست. به راحتی می‌توان دید که پروتکل لیاو در برگزاری رأی‌گیری‌های چند گزینه‌ای هیچ محدودیتی ندارد.

۴ دیگر روش‌ها

در سال ۲۰۰۹، لی و دیگران با استفاده از روش‌هایی مشابه پروتکل لیاو، یک پروتکل رأی‌گیری الکترونیک ارائه کردند.[۴] این پروتکل بخش اعظم مشکلاتی که در پروتکل لیاو وجود داشت را برطرف کرد. به طور خاص، در پروتکل پیشنهادی نیاز به استفاده از کارت‌های هوشمند حذف شده، و انتخابات به طور کامل در بستر اینترنت انجام می‌پذیرد. همچنین این پروتکل موفق به دستیابی به اجبارناپذیری کامل شده است (هر چند رسید رأی‌دهی حذف نشده است). در نتیجه به نظر می‌رسد با استفاده از تکنیک‌های مبتنی بر امضای کور و رمزنگاری عمومی(مانند RSA) بتوان پروتکل‌هایی با کارایی بالا و ویژگی‌های مناسب طراحی کرد.

با این حال تکنیک‌ها و اولیه‌های دیگری نیز وجود دارند که در طراحی پروتکل‌های رأی‌گیری الکترونیک استفاده شده‌اند. در ادامه به طور خلاصه چند مورد را معرفی می‌کنیم.

۱.۴ رمزنگاری هوموورفیک[۲۲]

تعریف ۱. *سیستم رمزنگاری (Gen, Enc, Dec) را هوموورفیک نامیم هرگاه عملگر $\odot$ وجود داشته باشد به طوری که با داشتن $Enc_k(m_1)$ و $Enc_k(m_2)$ ، بدون رمزگشایی و به دست آوردن m_1 و m_2 ، بتوان $Enc_k(m_1 \odot m_2)$ را محاسبه کرد. در این صورت می‌گوییم سیستم رمزنگاری فوق نسبت به عملگر $\odot$ خاصیت هوموورفیک را دارد.*

مثال: سیستم رمز RSA نسبت به عملگر ضرب دارای خاصیت هوموورفیک است. همچنین سیستم‌های رمز الگمال [۲۳] و پایلییر [۲۴] نسبت به عملگر جمع دارای خاصیت هوموورفیک هستند. ⊠

رمزنگاری هوموورفیک در طراحی انواع پروتکل‌های رمزنگاری کاربرد بسیاری دارد. به عنوان مثال از آن در طراحی شمارنده‌های رمزنگارانه استفاده می‌شود.

۲.۴ شمارنده‌های رمزنگارانه

تعریف ۲. *یک B-شمارنده رمزنگارانه یا به طور خلاصه یک B-شمارنده، متشکل از سه الگوریتم به شکل زیر است:*

$Gen(1^n)$: سه‌تایی (pk, sk, S_0) را تولید می‌کند که pk کلید عمومی، sk کلید خصوصی و S_0 وضعیت اولیه شمارنده است.

$Dec(S, sk)$: خروجی آن عضوی از $\{0, \cdots, B\}$ است و $Dec(S_0, sk) = 0$.

$Inc(S, pk)$: تابعی است که در رابطه‌ی روبه‌رو صدق می‌کند: $Dec(Inc(S, pk), sk) = Dec(S, sk) + 1$

[۲۱] Generality
[۲۲] Homomorphic Encryption
[۲۳] اطلاعات بیشتر در این مورد را اینجا بخوانید.
[۲۴] اطلاعات بیشتر در این مورد را اینجا بخوانید.

تعریف ۳. *یک B-شمارنده را (t,ϵ)- امن نامیم هر گاه برای هر مهاجم $\mathcal{A}$ که در زمان حداکثر t اجرا می‌شود، داشته باشیم*

$$\Pr[\mathcal{A}(pk,S)=Dec(S,sk)|(pk,sk,S_\circ)\leftarrow Gen(1^n),i\leftarrow\{\circ,\cdots,B\},S\leftarrow Inc^i(S_\circ,pk)]\leqslant\epsilon.$$

مثال: با استفاده از خاصیت هوموورفیک سیستم رمز پایلییر می‌توان یک شمارنده ساخت که امنیت آن وابسته به فرض *تمایزناپذیری مانده‌ی Nام* باشد. [۲۵] ⊠

مثال: به عنوان نمونه‌ای دیگر می‌توان به طرح پیشنهادی کاتز و دیگران[۵] اشاره کرد که امنیت آن وابسته به فرض *تمایزناپذیری مانده‌های مربعی از مانده‌های نامربعی با نماد ژاکوبی ۱* است. این طرح چیزی بیش از یک شمارنده ساده است و در واقع عملکردی مشابه یک LFSR دارد. ⊠

یکی از روش‌های استفاده از شمارنده‌ها در رأی‌گیری الکترونیک در ادامه آمده است. ابتدا مسئول برگزاری انتخابات الگوریتم Gen را اجرا می‌کند. سپس $(S_\circ,pk)$ را برای اولین رأی‌دهنده ارسال می‌کند. رأی‌دهنده یا با استفاده از Inc مقدار $S_\circ$ را افزایش می‌دهد، یا مقدارش را به صورت تصادفی تغییر می‌دهد. سپس مقدار جدید شمارنده را به همراه یک اثبات دانش‌صفر به نفر بعدی می‌فرستد، و این کار تا اخذ رأی آخرین نفر ادامه پیدا می‌کند. البته این سیستم بسیار ساده است و بسیاری از ویژگی‌های مطلوب(مثلاً استحکام یا کارآمدی) را ندارد.(در این حالت شمارنده باید تابعی مثل $Randomize$ داشته باشد که $Randomize(S,pk)\neq S$ و $Dec(Randomize(S,pk),sk)=Dec(S,sk)$. همچنین شرط امنیت برای این تابع نیز مشابه با Inc برقرار باشد.)

۳.۴ کانال‌های محرمانه[۲۶]

در فرایند اخذ رأی یکی از راه‌های مخفی‌کردن هویت رأی‌دهنده و از بین بردن ارتباط میان رأی و رأی‌دهنده، استفاده از کانال‌های ارتباطی محرمانه است. در یک کانال ارتباطی محرمانه هویت فرستنده پیام از گیرنده پیام و هر شنودگری [۲۷] مخفی نگه داشته می‌شود. به این ترتیب می‌توان به هدف محرمانگی هویت رأی‌دهنده دست یافت. چاوم در ۱۹۸۱ برای ساخت یک کانال محرمانه، سیستم‌های *تور ترکیبی* [۲۸] را که بر پایه رمزنگاری و جایگشت دادن ورودی ساخته می‌شود، پیشنهاد کرد. این سیستم‌ها بر اساس نوع تبدیل رمزنگارانه‌ای که در آن‌ها استفاده می‌شود، به دو دسته‌ی *تور ترکیبی رمزگشایی* [۲۹] و *تور ترکیبی باز_ رمزنگاری* [۳۰] تقسیم می‌شوند. این ساختارها معمولاً استحکام زیادی ندارند. البته برای حل این مشکل تلاش‌هایی شده است.[۶]

یک راهکار دیگر استفاده از یک سیستم اعلان عمومی محرمانه [۳۱] است. این ساختارها که $DC\text{-}net$ نیز نامیده می‌شوند، اولین بار توسط چاوم در ۱۹۸۸ معرفی شدند. [۷] ایده کلی به این صورت است که می‌خواهیم در یک شبکه n نفره، پیدا کردن فرستنده یک پیام بدون تبانی $n-1$ نفر با همدیگر، غیرممکن باشد. مشکل اصلی این طرح، پیاده‌سازی آن در مقیاس بزرگ و استحکام آن است. البته در ۲۰۰۴ گال و جوئلز با پیدا کردن افراد مخرب به طور کارا، موفق به بهبود طرح اولیه شده‌اند. [۸]

---

[۲۵] جزئیات دقیق این طرح را اینجا بخوانید
[۲۶] Anonymous Channels
[۲۷] Eavesdropper
[۲۸] Mixnet
[۲۹] Decryption Mixnet
[۳۰] Re-encryption Mixnet
[۳۱] Anonymous Broadcast Channel

۴.۴ تابلوی اعلانات[۳۲]

تابلوی اعلانات اولین بار توسط کرامر و دیگران در ۱۹۹۷ معرفی شد. [۹] منظور از یک تابلو اعلانات یک کانال پخش عمومی دارای حافظه است. هر ارتباطی که از طریق این کانال صورت گیرد، ذخیره می‌شود و هر کسی قادر به خواندن اطلاعات ذخیره شده در تابلواعلانات است. هیچ‌کس قادر به حذف یا تغییر اطلاعات ذخیره شده در تابلو اعلانات نیست، اما هر کسی می‌تواند پیام‌هایی را به بخش اختصاص داده شده به او اضافه کند. برای دستیابی به این هدف، از پروتکل‌های امضای دیجیتال استفاده می‌شود. در [۹] با استفاده از تابلوی اعلانات و سیستم رمز الگمال یک پروتکل رأی‌گیری الکترونیک معرفی شده‌است.

مراجع

[1] Liaw, Horng-Twu. "A Secure Electronic Voting Protocol for General Elections." *Computers & Security* 23, no. 2 (2004): 107-19.

[2] Chaum, David. "Blind Signatures for Untraceable Payments." *Advances in Cryptology*, 1983, 199-203.

[3] Chaum, David. "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms." *Advances in Information Security Secure Electronic Voting*, 2003, 211-19.

[4] Li, Chun-Ta, Min-Shiang Hwang, and Yan-Chi Lai. "A Verifiable Electronic Voting Scheme over the Internet." *2009 Sixth International Conference on Information Technology: New Generations*, 2009.

[5] Katz, Jonathan, Steven Myers, and Rafail Ostrovsky. "Cryptographic Counters and Applications to Electronic Voting." *Lecture Notes in Computer Science Advances in Cryptology — EUROCRYPT 2001*, 2001, 78-92.

[6] Sako, Kazue, and Joe Kilian. "Receipt-Free Mix-Type Voting Scheme." *Advances in Cryptology — EUROCRYPT '95 Lecture Notes in Computer Science*, 1995, 393-403.

[7] Chaum, David. "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability." *Journal of Cryptology 1*, no. 1 (1988): 65-75.

[8] Golle, Philippe, and Ari Juels. "Dining Cryptographers Revisited." *Advances in Cryptology - EUROCRYPT 2004 Lecture Notes in Computer Science*, 2004, 456-73.

[9] Cramer, Ronald, Rosario Gennaro, and Berry Schoenmakers. "A Secure and Optimally Efficient Multi-Authority Election Scheme." *Advances in Cryptology — EUROCRYPT '97 Lecture Notes in Computer Science*, 1997, 103-18.

[10] Sampigethaya, Krishna, and Radha Poovendran. "A Framework and Taxonomy for Comparison of Electronic Voting Schemes." *Computers & Security* 25, no. 2 (2006): 137-53.

---

[۳۲] Bulletin Board