مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۷۴-۶۷

پروتکل جدید رای‌گیری الکترونیکی مبتنی بر خم بیضوی

عبدالرسول میرقدری [۱*]، سعید رحیمی [۲]، علیرضا رحیمی [۳]

۱- دانشیار، ۲- دانشجوی دکترای، ۳- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۵/۰۲/۲۵، پذیرش: ۹۵/۰۹/۲۳)

چکیده

با توجه به گسترش انتخابات متعدد و ضرورت سلامت و اطمینان فرآیند رای‌گیری، توجه زیادی به رای‌گیری الکترونیکی شده است. تحقیقات متعدد درخصوص رای‌گیری الکترونیکی نشان می‌دهد که با این پروتکل‌ها می‌توان الزامات یک فرایند رای‌گیری مطمئن را به اثبات رساند. یکی از روش‌های مناسب برای اجرای رای‌گیری الکترونیکی استفاده از رمزنگاری هم‌ریخت است. روش رمزنگاری هم‌ریخت یک طرح رمزنگاری است که نسبت به عملیات جمع هم‌ریخت می‌باشد. در این مقاله با استفاده از رمزنگاری الجمال روی خم‌های بیضوی یک پروتکل رای‌گیری الکترونیکی جدید ارائه شده که توسط همه قابل نظارت است. این پروتکل بر پایه سخت‌بودن حل مسئله لگاریتم گسسته روی خم بیضوی، امنیت رای‌دهندگان و امنیت کلید را تامین می‌کند. پروتکل پیشنهادی برای برگزاری رفراندومی به تعداد ۱۰۰ میلیون رای‌دهنده آزمون شده که زمان شمارش تعداد کل آرا حدود ۳۲ ثانیه طول کشید.

واژه‌های کلیدی: پروتکل رای‌گیری الکترونیکی، خم بیضوی، رمزنگاری هم‌ریخت

۱- مقدمه

یکی از اصول اولیه ایجاد دموکراسی در کشورها، اجرای صحیح و بدون نقص رای‌گیری است. در بسیاری از موارد پس از برگزاری انتخابات، مجری متهم به تقلب و تخلف در برگزاری انتخابات می‌گردد. رای‌گیری یکی از مهم‌ترین اصول دموکراسی است. با توجه به گسترش انتخابات متعدد و ضرورت سلامت در هر پروتکل رای‌گیری، به رای‌گیری الکترونیکی توجه زیادی شده است. با استفاده از رای‌گیری الکترونیکی می‌توان روش مناسبی را ایجاد کرد تا هر کس بتواند بر صحت انتخابات نظارت کند.

یکی از راه‌کارهای موثر برای مشارکت آحاد مردم در مسائل اجتماعی برگزاری انتخابات به روش رای‌گیری الکترونیکی است. رای‌گیری الکترونیکی، به‌طورکلی عبارت است از اجرای فرآیند انتخابات به کمک ابزارهای الکترونیکی به‌گونه‌ای‌که الزامات یک پروتکل رای‌گیری حفظ شود. ابزارهای الکترونیک برای اجرای الگوریتم‌های ریاضی استفاده می‌شوند. با روش‌های ریاضی اثبات می‌شود که الگوریتم‌ها شرایط و الزامات مدنظر را تامین می‌کنند. الزامات مورد نیاز یک پروتکل رای‌گیری عبارتند از:

حفظ حریم خصوصی: یکی از الزامات بسیار مهم یک پروتکل رای‌گیری الکترونیکی حفظ محرمانگی رای هر فرد است. مطابق این اصل رای هیچ فردی نباید در هیچ یک از مراحل رای‌گیری قابل مشاهده باشد.

قابلیت تایید عمومی: هنگام استفاده از رای‌گیری الکترونیکی هر کسی باید بتواند با نظارت بر فرآیند برگزاری انتخابات، صحت انجام مراحل انتخابات را تایید کند. این قابلیت در سامانه‌های سنتی امکان‌پذیر نیست و یکی از مهم‌ترین اهداف استفاده از رای‌گیری الکترونیکی است.

مقاوم‌بودن: لازم است پروتکل رای‌گیری نسبت به بروز خطای احتمالی مقاوم باشد. به‌طورکلی، یک پروتکل رای‌گیری الکترونیکی درصورتی مقاوم است که در صورت وقوع خطا یا تقلب توسط یکی از بخش‌های شرکت‌کننده انتخابات، مشکل قابل جبران بوده و بقیه اجزای پروتکل بتوانند باقی اطلاعات را بازسازی و فرآیند انتخابات را تمام کنند.

هزینه محاسباتی محدود: استفاده از الگوریتم‌های محاسباتی موجود در رای‌گیری الکترونیکی نباید مانعی برای اجرای انتخابات باشد. این هزینه محاسباتی باید به‌گونه‌ای باشد که عملیات اخذ رای و شمارش آرا در مدت زمان منطقی و معقول قابل انجام باشد.

رای‌گیری از افراد واجدالشرایط: در فرآیند رای‌گیری الکترونیکی تنها افرادی که واجد شرایط لازم هستند باید بتوانند در رای‌گیری شرکت کنند. هم‌چنین هیچ فرد واجد شرایطی نباید بتواند بیش از

* رایانامه نویسنده مسئول: amrghdri@ihu.ac.ir

یک رای ارسال کند. یعنی افراد واجد شرایط فقط یک بار حق رای‌دادن دارند.

غیرقابل اجبار و غیرقابل اثبات‌بودن رای‌ها: پروتکل رای‌گیری باید تضمین کند که هیچ‌کدام از رای‌دهندگان مجبور به رای‌دادن به یک فرد خاص نشده‌اند. از طرف دیگر سامانه مطلوب باید امکان اثبات رای را از رای‌دهندگان سلب کند.

کامل‌بودن سامانه: در سامانه رای گیری نباید امکان تغییر یا ابطال هیچ رایی جود داشته باشد. هم‌چنین نباید امکان اضافه‌شدن رای جعلی در سامانه وجود داشته باشد.

امنیت: سامانه رای‌گیری باید امن بوده و کسی نتواند قبل از اجرای قواعد پروتکل، هیچ اطلاعاتی را کشف کند [۲-۱].

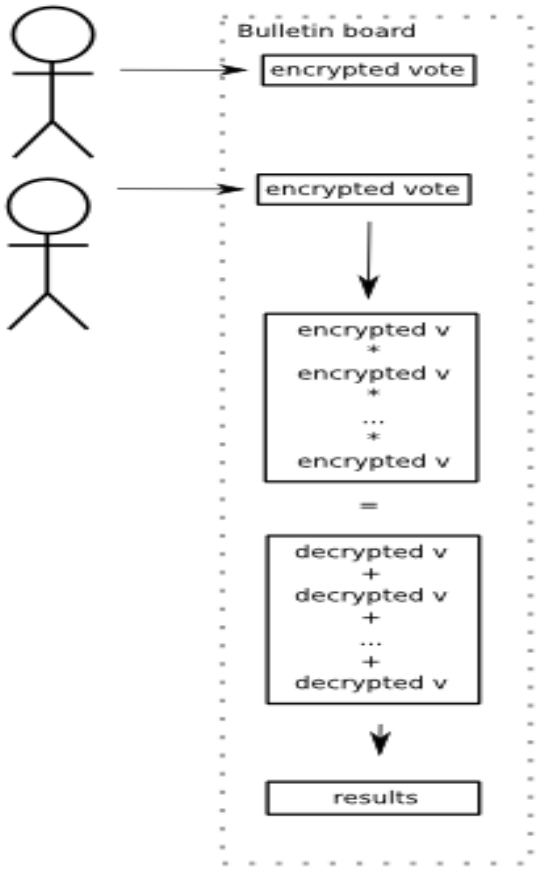
مابقی ساختار مقاله بدین شرح است که در بخش دوم شیوه-های برگزاری انتخابات الکترونیکی بیان شده و در بخش سوم مفاهیم اساسی شرح داده شده است. هم‌چنین در بخش چهارم پروتکل پیشنهادی و مراحل آن‌را که شامل اخذ آرا، شمارش آرا و مرحله اثبات صحت عملکرد است شرح داده می‌شود. در نهایت در بخش پنجم پروتکل پیشنهادی تحلیل و پیاده‌سازی شده و در بخش ششم نتیجه‌گیری و پیشنهاد آورده شده است.

۲- شیوه‌های برگزاری انتخابات الکترونیک

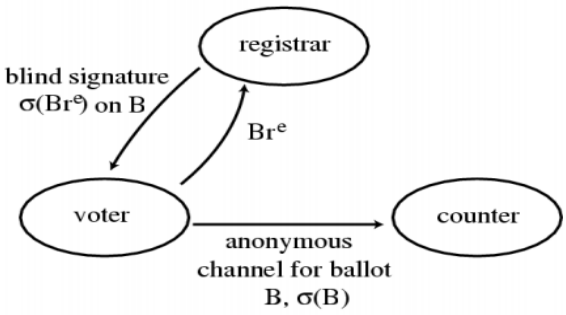
به‌طورکلی سه روش برای برگزاری انتخابات الکترونیک به‌شرح ذیل وجود دارد:

الف) رمزنگاری هم‌ریخت[1]: در این پروتکل‌ها همه واجدین شرایط رای خود را رمز کرده و ارسال می‌کنند [۴-۳]. اصل هم‌ریختی روی جمع بیان می‌دارد که مجموع رمزشده اطلاعات با رمزشده مجموع اطلاعات برابر است. لذا با استفاده از این خاصیت نهاد شمارش‌گر با رمزگشایی جمع آرا نتیجه انتخابات را معلوم می‌نماید. مراحل این روش در شکل (۱) دیده می‌شود.

ب) امضای کور[2]: در این روش متصدی ابتدا یک کلید عمومی را ارسال می‌کند. سپس رای‌دهنده با استفاده از ID خود، اطلاعات هر گزینه رای را می‌سازد و به‌صورت رمزشده برای متصدی می‌فرستد تا آن‌ها را امضا کند. رای‌دهنده با آشکارکردن پیام‌های امضاشده، گزینه مطلوب خود را انتخاب نموده و پیام منتخب خود را برای نهاد شمارش‌گر ارسال می‌کند. چنین پروتکل رای‌گیری قابل اعتبارسنجی می‌باشد [۵]. مراحل این روش در شکل (۲) دیده می‌شود.



شکل (۱): رای‌گیری با استفاده از رمزنگاری هم‌ریخت [۶]

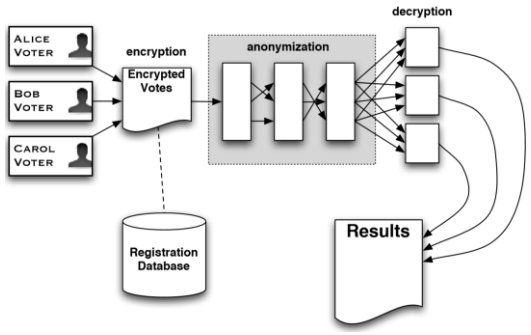


شکل (۲): عملیات انجام‌شده برای رای‌گیری با امضای کور [۷]

ج) شبکه مخلوط[3]: در این شیوه با استفاده از یک شبکه مخلوط، هر رای‌دهنده رای خود را مطابق قواعد شبکه رمز کرده و به گمنام‌کننده‌ها تحویل می‌دهد. هر گمنام‌کننده رای‌های دریافتی را با رمز خود باز کرده و آن‌ها را مخلوط می‌کند. در نهایت مقدار هر

1- Homomorphic Encryption
2- Blind Signature
3- Mixnet

رای مشخص شده و مجموع آرا جمع می‌شود [۹- ۸]. مراحل رای گیری با شبکه مخلوط در شکل (۳) در زیر نشان داده شده است.



شکل (۳): رای‌گیری با شبکه مخلوط [۱۰]

روش این مقاله بر اساس رمزنگاری هم‌ریخت روی خم بیضوی است. در سال ۱۹۹۷ کرامر و همکاران، پروتکل مبتنی بر رمزنگاری هم‌ریخت را ارایه کردند که بیش‌تر فعالیت‌های آتی در این حوزه را تحت تاثیر خود قرار داد. در سال ۲۰۱۰ پروکدی و همکارانش، روشی را بر مبنای خم بیضوی ارائه دادند که در آن با استفاده از یک نهاد ناظر یک پروتکل رای‌گیری الکترونیکی بنا شده بود [۱۱]. پس از آن در سال ۲۰۱۱ همان تیم با اصلاحاتی تلاش کردند تا یک نهاد ناظر را حذف کنند [۱۲]. اما روش اشاره‌شده نیازمند یک نهاد مرکزی بود که خود به خود امنیت سیستم را وابسته به همان نهاد می‌کرد. پروتکل پیشنهادی بر اساس رمزنگاری الجمال روی خم بیضوی طراحی شده است که دارای امنیت بهتر و هزینه ارسالی کم‌تری نسبت به سایر روش‌ها است. هم‌چنین عمل رمزنگاری به‌طور مستقیم نسبت به عملیات جمع هم‌ریخت است. در نهایت با پیاده‌سازی عملی این طرح نتایج امنیت و کارآیی این روش بسیاری از الزامات پروتکل رای‌گیری را تامین کرده و دارای امنیت بهتری است. در نهایت با پیاده‌سازی عملی طرح، نتایج امنیت و کارایی آن برای ۱۰۰ میلیون رای‌دهنده ارائه شده است.

۳- مفاهیم اساسی

برخی مفاهیم ریاضی مورد استفاده در تحقیق را شرح می‌دهیم:

الف) تعریف خم بیضوی

فرض کنید F یک میدان ریاضی باشد. خم بیضوی مجموعه‌ای از نقاط E است که دارای شرایط زیر می‌باشد:

$$E = \{(x,y) | \forall x,y \in F; y^2 = x^3 + ax + b\} \cup \{O_E\} \qquad (۱)$$

که به ازای a, b مشخص، $4a^3 + 27b^2 \neq 0$ است. در مجموعه E، نقطه O_E نقطه بی‌نهایت، نامیده می‌شود.

ب) عملیات جمع روی خم بیضوی

عملیات جمع روی خم بیضوی برای نقاط $P_1, P_2 \in E$ به صورت زیر تعریف می‌شود:

$$P_1 + P_2 = \begin{cases} O_E & \text{اگر } x_1 = x_2, y_1 = -y_2 \\ P_1 & \text{اگر } P_2 = O_E \\ P_3 = (x_3, y_3) & o.w. \end{cases}$$

$$P_3 = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

(۲)

$$\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} & \text{اگر } x_1 = x_2 \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{سایر} \end{cases}$$

با توجه به تعریف فوق خم بیضوی نسبت به عمل جمع بسته است. هم‌چنین با وجود عضو صفر (O_E)، خاصیت جابجایی و شرکت‌پذیری عملیات جمع در مجموعه E، نتیجه می‌دهد که $(E, +)$ یک گروه است [۱۳]. مراحل رمزنگاری الجمال روی خم بیضوی در شکل (۴) نشان داده شده است.

۱- مرحله راه‌اندازی: طرفین منحنی بیضوی E و مولد Q را از مرتبه q با یک دیگر توافق می‌کنند.

۲- مرحله تولید کلید: طرف اول عدد تصادفی x را انتخاب کرده و $H = xQ$ را تشکیل می‌دهد. در این رابطه H به‌عنوان کلید عمومی در اختیار همه قرار می‌گیرد. مقدار x کلید خصوصی بوده که طرف اول آن را برای بازگشایی رمز نزد خود نگه می‌دارد.

۳- مرحله رمزگذاری: برای رمزگذاری پیام $m \in E_Q$، عدد r به‌صورت تصادفی انتخاب شده و توسط رابطه زیر عملیات رمزگذاری انجام می‌شود.

$$C = Enc(m) = (c_1, c_2) = (rQ, m + rH)$$

طرف دوم برای ارسال پیام m مقدار C را به طرف اول ارسال می‌کند.

۴- مرحله رمزگشایی: طرف اول با دریافت C و با استفاده از کلید خصوصی x، از طریق رابطه زیر مقدار پیام m را به‌دست می‌آورد:

$$Dec(C) = c_2 - x.c_1 = m + rH - xrQ = m + rxQ - xrQ = m$$

شکل (۴): الگوریتم رمزنگاری الجمال روی خم بیضوی

ج) لگاریتم گسسته روی خم بیضوی

اگر میدان تعریف خم بیضوی E را F_p در نظر بگیریم، مجموعه نقاط خم بیضوی E به‌صورت $(x\ \%\ p, y\ \%\ p)$[۱] تعریف شده که با عمل جمع تشکیل گروه می‌دهد. زیرمجموعه $E_Q \subset E$ را مجموعه تمام مضارب عنصر $Q \in E$ تعریف نموده که این زیرمجموعه هم با عمل جمع یک گروه دوری تشکیل می‌دهد. در این مجموعه، Q مولد گروه و مقدار q که $qQ = O_E$، مرتبه Q نامیده می‌شود.

حال در این مجموعه معادله $R = lQ$ به مسئله لگاریتم گسسته روی خم بیضوی مشهور است که با داشتن مقدار R یافتن مقدار l یک مسئله سخت ریاضی می‌باشد. امنیت الگوریتم‌های رمزنگاری مبتنی بر خم بیضوی وابسته به پیچیدگی حل این مسئله سخت است.

د) رمزنگاری روی خم بیضوی

برپایه مسئله لگاریتم گسسته روی خم بیضوی می‌توان الگوریتم رمزنگاری الجمال را به‌صورت زیر بازتعریف کرد.

ه) هم‌ریختی عملیات جمع روی رمزنگاری الجمال

رمزنگاری الجمال روی خم بیضوی و نسبت به عملیات جمع هم‌ریخت است. زیرا اگر دو متن رمزی C' و C را به‌ترتیب برای پیام‌های آشکار m' و m فرض کنیم لذا خواهیم داشت:

$$C + C' = (c_1, c_2) + (c_1', c_2') = (c_1 + c_1', c_2 + c_2') = \left((r + r')Q, (m + m') + (r + r')H\right) \Rightarrow Dec(C + C') = m + m' \quad (۳)$$

یعنی حاصل جمع دو عبارت رمزشده برابر است با رمزشده حاصل جمع دو پیام.

۴- پروتکل پیشنهادی

با توجه به مفهوم رمزنگاری هم‌ریخت روی خم بیضوی و سختی حل مسئله لگاریتم گسسته ما یک پروتکل جدید براساس طرح رمزنگاری الجمال روی خم بیضوی برای رای‌گیری الکترونیکی پیشنهاد می‌دهیم که شامل سه مرحله به شرح ذیل است:

۴-۱- مرحله اخذ آرا

برای رای‌گیری بین مجموعه افراد $V_1, \dots, V_m$ به‌کمک نمایندگی‌های $A_1, \dots, A_n$، ابتدا سامانه راه‌اندازی می‌شود. در این پروتکل رای‌گیری فرض می‌شود که هر رای از مجموعه {بله، خیر} انتخاب شده است.

الف) برد عمومی

ابتدا یک برد عمومی برای اعلام مقادیر و نتایج عمومی فرض می‌شود. در این برد اطلاعات هر فرد برای عموم قابل مشاهده است و هم‌چنین انتشار هر مطلب بر روی آن قابل تغییر نیست. به‌علاوه فرض می‌شود که اطلاعات برد عمومی توسط یک مکانیزم مانند امضای الکترونیک ضمانت می‌شود که توسط فرستنده اصلی ارسال شده باشد. برد عمومی و ارتباطات با آن توسط هر کس قابل نظارت است [۱۱].

ب)راه اندازی

برای تامین توامان امنیت و مقاومت پروتکل، لازم است تا کلید خصوصی شمارش آرا برای هیچ نهادی قابل شناسایی نباشد. از سوی دیگر، نباید نیاز به همکاری همه n نمایندگی برای ساخت کلید خصوصی وجود داشته باشد. چرا که در صورت بروز خطا در یک یا چند نمایندگی، پروتکل غیرقابل استفاده می‌شود. برای این هدف با استفاده از روش تسهیم راز پدرسن[۲] کلید خصوصی را ساخته و بین نمایندگی‌ها توزیع می‌کنیم [۱۴]. با استفاده از این روش یک کلید خصوصی بین همه نمایندگی‌ها پخش می‌شود که برای استفاده از آن، همکاری t نمایندگی از n نمایندگی لازم است. برای هدف کشف راز با همکاری t نمایندگی از n نمایندگی، ابتدا نمایندگی‌ها بر سر یک Q, E_Q, t توافق می‌کنند و این اطلاعات روی برد عمومی اعلام می‌گردد. هم‌چنین برای اجرای این پروتکل لازم است که یک بستر ارتباط امن بین نمایندگی‌ها وجود داشته باشد.

پس از توافق اولیه هر کدام از A_iها یک x_i رندم انتخاب می‌کند و مقدار $H_i = x_i Q$ را محاسبه و در برد عمومی منتشر می‌کند. پس از آن، مقدار H توسط رابطه $H = \Sigma_1^n H_i$ به‌دست خواهد آمد. این مقدار کلید عمومی برای انجام محاسبات و انجام عملیات اخذ آراست. کلید خصوصی برابر با مقدار $x = \Sigma_1^n x_i$ خواهد بود.

برای اشتراک‌گذاری راز لازم است هر نمایندگی A_i یک چندجمله‌ای از درجه حداکثر t را با ضرایب تصادفی $f_{i,j}$ انتخاب کند که ضریب ثابت این چندجمله‌ای همان مقدار x_i باشد.

حال هر نمایندگی A_i مقدار تمام جملات $F_{i,j} = f_{i,j} Q$ را محاسبه کرده و این مقادیر را در برد عمومی منتشر می کند.

۱- عمل‌وند % در این رابطه به معنای باقی‌مانده است.

2- Pedersen

از طرف دیگر، هر نمایندگی مقدار $f_i(j)$ را طبق رابطه (۴) محاسبه و از طریق کانال ارتباطی امن بین A_i و $\mathrm{A_j}$ به‌صورت محرمانه برای نماینده A_j می‌فرستد.

$$f_i(z) = x_i + f_{i,1}z + f_{i,2}z^2 + \cdots + f_{i,k-1}z^{k-1} \quad (۴)$$

با توجه به اطلاعات برد عمومی A_i می‌تواند بررسی کرد که آیا A_j مقدار درست $f_i(j)$ را برای او فرستاده است یا خیر؟ برای این‌کار A_i حاصل رابطه زیر را محاسبه کرده و درصورتی‌که تساوی زیر برقرار نباشد اعلام عدم تطابق کرده و $f_j(i)$ را در برد عمومی اعلام می‌کند. در این مرحله $\mathrm{A_i}$ از ادامه فرآیند دست می‌کشد. با این‌کار همکاری با $\mathrm{A_j}$ توسط باقی نمایندگی‌ها زیر سوال می‌رود [۱۴].

$$f_j(i)Q = \prod_{l=0}^{k-1} i.l.F_{j,l} \quad (۵)$$

پس از تایید عملیات هر نمایندگی $\mathrm{A_i}$ مقدار $\mathrm{s_i = \sum_{j=1}^{n} f_j(i)}$ را محاسبه کرده و نگه‌داری می‌کند.

با توجه به روابط فوق وجود یک چندجمله‌ای درجه t از همکاری نمایندگی‌ها ساخته می‌شود که معادل جمع چندجمله‌ای تمام نمایندگی‌ها است و جمله ثابت آن کلید خصوصی است.

$$f(z) = \Sigma_1^n f_i(z) = x + f_1 z + \cdots + f_{k-1}z^{k-1} \quad (۶)$$

با توجه به پروتکل هر نمایندگی $\mathrm{A_i}$ اطلاعات $\mathrm{s_i = f(i)}$ را از چندجمله‌ای فوق در اختیار دارد. بنابراین مطابق با روش تقسیم راز شمیر[1] اثبات می‌شود که با همکاری t نمایندگی از n نمایندگی قابل ساخت مقدار x قابل ساخت است.

ج) رای گیری

هر فرد رای خود را مطابق با روش رمزنگاری الجمال رمز کرده و بر روی برد عمومی می‌فرستد. هر رای به‌صورت v_i از مجموعه $\{-1, 1\}$ انتخاب می‌شود که به‌ترتیب متناظر با رای‌های بله و خیر است. لذا رای ارسالی به‌صورت $(c_{i,1}, c_{i,2}) = (r_iQ, r_iH + v_iP)$ بر روی برد عمومی قرار می‌گیرد.

۴-۲- مرحله شمارش آرا

ابتدا همه آرا ارسالی روی برد عمومی جمع می‌شود. با این‌کار نتیجه جمع آرا مطابق رابطه زیر به‌صورت یک عبارت رمزی الجمال فرستاده می‌شود. با توجه به خاصیت هم‌ریختی در رمزنگاری الجمال با رمزگشایی از این عبارت نتیجه آرا قابل کشف خواهد بود.

$$(c_1, c_2) = \left(\Sigma_1^m c_{i,1}, \Sigma_1^m c_{i,2}\right)$$
$$= (\Sigma_1^m r_i Q, (\Sigma_1^m r_i)H + dQ) \quad (۷)$$

مقدار d در رابطه فوق برابر تفاضل تعداد آرا منفی از مثبت است. چرا که هر رای مثبت مقدار ۱ و هر رای منفی مقدار ۱- را ارسال کرده است. برای بازگشایی عبارت فوق لازم است تا xc_1 محاسبه شود. برای این منظور، به‌جای مقدار x مقدار xc_1 به‌صورت مستقیم از روش تقسیم راز شمیر محاسبه می‌شود و با استفاده از آن مقدار d کشف می‌گردد. با توجه به روش اشتراک راز شمیر می‌توان راز را با همکاری t نمایندگی از روش زیر استخراج کرد. برای این کار فرض می شود که اعضا مجموعه J اطلاعات s_jc_1 را محاسبه و به اشتراک گذاشته باشند و $||J|| \geq t$. بدین منظور، هرکدام از A_j ها مقدار $w_j = s_jc_1$ را بر روی برد عمومی اعلام می‌کند. با استفاده از این اطلاعات مقدار $\mathrm{xc_1}$ توسط رابطه زیر به‌دست می‌آید:

$$xc_1 = \Sigma_{j\in J}\left(\prod_{i\in J, i\neq j}\left(\frac{i}{i-j}\right)w_j\right) =$$
$$\Sigma_{j\in J}\left(\prod_{i\in J, i\neq j}\left(\frac{i}{i-j}\right)s_jc_1\right) \quad (۸)$$

حال با استفاده از این اطلاعات می‌توان نتیجه محاسبات را رمزگشایی کرد که از طریق زیر خواهیم داشت:

$$Y = c_2 - xc_1 = (\Sigma_1^m r_i)H + dQ - (x\Sigma_1^m r_i Q) =$$
$$(\Sigma_1^m r_i)H + dQ - \Sigma_1^m r_i H = dQ \quad (۹)$$

برای کشف مقدار d، لازم است تا نتیجه به‌دست‌آمده Y را با مقادیر $-\mathrm{mQ}, -(\mathrm{m}-1)\mathrm{Q}, \ldots, -\mathrm{Q}, 0, \mathrm{Q}, \ldots, \mathrm{mQ}$ مقایسه می‌کنیم. این‌کار به‌خاطر سختی مسئله لگاریتم گسسته عملیاتی پیچیده است. برای این‌کار از روش گام بزرگ و کوچک[2] استفاده می‌شود.

برای تعیین مقدار $-\mathrm{m} \leq \mathrm{d} \leq \mathrm{m}$ از رابطه (۹)، دستورالعمل زیر را اجرا می‌کنیم. با درنظرگرفتن مقدار d به‌صورت $\mathrm{d = ik + j}$، می‌توان مقدار i,j را با فرض k مشخص پیدا کرد. این فرض معادل است با $\mathrm{Y - i(kQ) = jQ}$. برای تعیین مقادیر i,j از روش آمده در شکل (۵) در زیر استفاده می‌شود.

۱- مقدار $k = \lceil\sqrt{2m}\rceil$ را تعیین می‌شود.
۲- به ازای تمام مقادیر $0 \leq \mathrm{j} < \mathrm{k}$، مقدار $(\mathrm{j, jQ})$ محاسبه و در یک جدول درهم‌ساز[3] ذخیره می‌شود.
۳- مقدار $\alpha = \mathrm{Y}$ و $-kQ$ محاسبه می‌شود.
۴- با شمارش i از 0 تا $\mathrm{k-1}$:
آیا α در جدول ذخیره شده موجود است؟
a. بله: نتیجه $\mathrm{ik + j}$ پیدا شده است.
b. خیر: $\alpha = \alpha + (-\mathrm{kQ})$

شکل(۵): الگوریتم روش گام بزرگ گام کوچک برای حل لگاریتم گسسته

1- Shamir

2- Baby Step Giant Step

در این روش، جستجو در جدول درهم‌ساز از مرتبه زمانی $O(1)$ می‌باشد. لذا در این بهینه‌سازی، کشف مقدار d از مرتبه زمانی $O(\sqrt{n})$ انجام می‌گیرد که نسبت به روش خطی با مرتبه زمانی $O(n)$ بهبود قابل توجهی است. پس از این محاسبه، اگر تعداد آرای مثبت، a و تعداد آرای منفی، b باشد مقدار d، اختلاف آن‌ها و مقدار m، تعداد رای‌دهنده‌ها، برابر مجموع این دو مقدار خواهد بود. لذا مقدار هر یک با حل دو معادله زیر به‌دست می‌آید:

$$\begin{cases} a-b=d \\ a+b=m \end{cases} \rightarrow a=\frac{d+m}{2}, b=\frac{m-d}{2} \qquad (۱۰)$$

۴-۳- مرحله اثبات صحت عملکرد

در این بخش، بحث درخصوص اثبات صحت عملکرد نمایندگی‌ها، صحت عملکرد رای‌دهنده‌ها و اثبات با روش هیچ آگاهی می‌باشد.

الف) اثبات صحت عملکرد نمایندگی‌ها

هر نمایندگی باید ثابت کند که مقدار $w_i = s_i c_1$ را بر روی برد عمومی اعلام کرده است. مقدار $h_i = s_i Q$ بر روی برد عمومی اعلام شده است. بنابراین مقادیر h_i و w_i به ترتیب نسبت به Q و c_1 لگاریتم گسسته برابر دارند و نمایندگی A_i مقدار این لگاریتم را می‌داند. در ادامه شیوه اثبات این دانش آمده است.

ب) اثبات صحت عملکرد رای دهنده‌ها

هم‌چنین رای دهنده V_i باید ثابت کند که رای صحیحی داده است. یعنی در مقدار ارسالی $c_i = (c_{i,1}, c_{i,2}) = (r_i Q, r_i H + v_i Q)$ مقدار $v_i \in \{-1,1\}$ است. برای این کار کافی است که V_i ثابت کند مقدار r_i را می‌داند به طوری که $c_{i,1} = r_i Q$ و یکی از دو حالت $c_{i,2} - Q = r_i H$ یا $c_{i,2} + Q = r_i H$ برقرار است. همانند شرایط اثبات برای نمایندگی‌ها، این متغیرها لگاریتم گسسته یکسانی نسبت به پایه‌های H و Q دارند.

ج) شیوه اثبات با هیچ آگاهی

برای این روش اثبات از دو مقدار $y_1 = kQ_1$ و $y_2 = kQ_2$ استفاده می‌شود. مقادیر (Q_1, y_1, Q_2, y_2) معلوم هستند که y_2 و y_1 لگاریتم گسسته یکسان با (مقدار k) به‌ترتیب نسبت به Q_1 , Q_2 دارند. اثبات‌کننده باید بدون دادن اطلاعات اضافی به تاییدکننده ثابت کند که این مقدار را می‌داند. برای این اثبات دو روش وجود دارد. روش اول روش تعاملی و روش دوم به‌صورت غیرتعاملی است. الگوریتم اثبات تعاملی در شکل (۶) در زیر آمده است.

روش اثبات تعاملی

۱- اثبات‌کننده ابتدا یک مقدار تصادفی r را انتخاب نموده و $(a_1, a_2) = (rQ_1, rQ_2)$ را برای تاییدکننده می‌فرستد. (a_1, a_2 لگاریتم گسسته یکسانی دارند)

۲- تاییدکننده یک عدد تصادفی c انتخاب کرده و برای اثبات‌کننده می‌فرستد.

۳- اثبات‌کننده مقدار $b = r - ck$ را محاسبه کرده و برای تاییدکننده می‌فرستد.

۴- تایید کننده درصورت برقراری توامان دو شرط

$a_1 = bQ_1 + cy_1$

$a_2 = bQ_2 + cy_2$

مقادیر $y_1 = kQ_1, y_2 = kQ_2$ را تایید می‌کند.

شکل (۶): الگوریتم اثبات با روش هیچ آگاهی تعاملی

روش اثبات تعاملی با تغییر کوچکی به اثبات غیرتعاملی تبدیل می‌شود. برای انجام این‌کار، اثبات‌کننده چالش c را از رابطه زیر تعیین می‌کند.

$$c = hash(y_1, Q_1, y_2, Q_2, rQ_1, rQ_2) \qquad (۱۱)$$

با این‌کار هر تاییدکننده‌ای می‌تواند مقدار c و شرایط را بررسی کند. در این رابطه برای عملیات hash می‌توان از یک تابع چکیده‌ساز مطمئن مانند SHA-1 استفاده نمود [۱۵].

۵- تحلیل و پیاده‌سازی

در این بخش ابتدا ویژگی‌های رای‌گیری الکترونیکی را تحلیل نموده و سپس آن را برای تعداد مشخصی رای‌دهنده پیاده‌سازی عملی کرده‌ایم.

الف) تحلیل ویژگی‌های رای‌گیری الکترونیکی

روش ارائه‌شده دارای ویژگی‌های زیر از الزامات رای‌گیری الکترونیکی می‌باشد:

حریم خصوصی: از آن‌جایی که رای هر فرد رمز شده است و هیچ نهادی کلید خصوصی برای بازگشایی رمز را ندارد، درنتیجه حریم خصوصی تامین شده است.

قابلیت تایید عمومی: تمام افراد می‌توانند توسط روش‌های ارائه‌شده عملکرد درست سامانه را به‌طور کلی تایید کنند.

مقاوم بودن: با توجه به استفاده از روش تسهیم راز، برای مقاوم‌بودن پروتکل در برابر خطا یا خرابی بعضی از نمایندگی‌ها،

پیشنهاد می‌شود مقدار t به‌گونه‌ای انتخاب شود که در رابطه $n \geq 2t-1$ صدق کند. با توجه به این رابطه پروتکل در برابر خطای t نمایندگی مقاوم است.

رای‌گیری از افراد واجد: چون مشخصات همه رای‌دهندگان ابتدا در سامانه ثبت شده و فقط آرا این رای‌دهندگان قابل قبول است لذا اگر کسی دو بار رای دهد رای وی در برد عمومی مشخص شده و هر دو رای وی حذف خواهد شد.

غیرقابل اجباربودن رای‌ها: با توجه به این‌که در این پروتکل هر فرد می‌تواند با ارائه مقدار r رای خود را اثبات کند، درنتیجه این سامانه بدون رسید نیست و در آن هم اجبار و هم اثبات ممکن است رخ دهد. این نقطه ضعفی است که باید در کارهای آینده رفع شود.

کامل‌بودن سامانه: براساس تعریف، کامل‌بودن یک سامانه به این معنی است که هیچ رأیی قابل حذف یا تغییر نباشد. با توجه به تایید عمومی همه آرا در این پروتکل، ملاحظه می‌شود که هیچ رایی قابل حذف یا تغییر نیست.

امنیت: طبق تعریف امنیت، نباید هیچ اطلاعاتی قبل از موعد مقرر از دستگاه فاش شود. با توجه به ساختار رمزنگاری الجمال روی خم بیضوی واضح است که بدون دانستن کلید امکان کشف آرا وجود ندارد. هم‌چنین کشف کلید در رمزنگاری خم بیضوی نیازمند حل مسئله سخت لگاریتم گسسته روی خم بیضوی است که در عمل غیرقابل حل است. با توجه به شیوه کشف راز قبل از اجرای دستورالعمل سامانه، هیچ نهادی توانایی کشف اطلاعات را ندارد لذا امنیت کامل برقرار است.

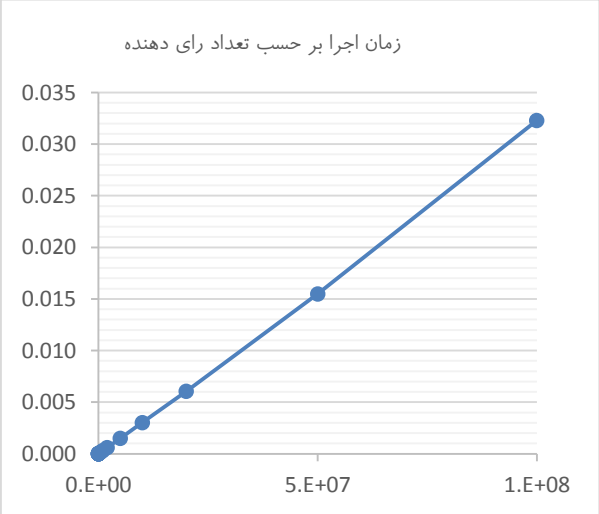
ب) پیاده‌سازی عملی

با توجه به نیاز پروتکل به حل مسئله لگاریتم گسسته، برای تعیین و تایید نتایج شمارش آرا به زمان زیادی نیاز است. با توجه به وجود روش‌های گام میانی[1] همانند گام بزرگ گام کوچک، بازکردن مسئله لگاریتم گسسته به $O(\sqrt{n})$ محاسبه نیاز دارد. بنابراین، برای رسیدن به حداقل امنیت ۸۰ بیت لازم برای رمزنگاری، باید اعداد مورد استفاده ۱۶۰ بیتی انتخاب شوند [۱۶]. برای مشاهده زمان عملی این محاسبات و برای تامین امنیت مناسب با اعداد ۱۶۰ بیتی زیر الگوریتم پیشنهادی پیاده‌سازی و آزمون شده است.

p = 1268133167195989090596625406312984755854486256116
a = 38673694026982765521411885280659652760289257373 4
b = 1461501637330902918203684832716283019655932542983

1- Meet in the Middle

در این پیاده‌سازی که بر روی یک دستگاه رایانه با پردازنده core i7 و میزان حافظه ۸ گیگابایت انجام شده از روش حل خطی استفاده شده است. با توجه به این که هر محاسبه در بردارنده یک عمل جمع است، لذا مطابق با عملیات جمع روی خم بیضوی هر عملیات شامل یک عمل تقسیم، دو عمل ضرب و شش عمل تفریق در میدان F_p است. با توجه به نتایج پیاده‌سازی، زمان لازم برای محاسبه نتیجه آرا برای ۱۰۰ میلیون رای‌دهنده حدود ۳۲ ثانیه است که در شکل (۷) در زیر دیده می‌شود.



شکل (۷): نمودار زمان اجرا بر اساس تعداد رای دهندگان

۶- نتیجه‌گیری

در این مقاله، یک پروتکل کارا بر اساس رمزنگاری هم‌ریخت روی خم‌های بیضوی برای شمارش آرا به‌صورت الکترونیکی ارائه شد. این پروتکل براساس رمزنگاری الجمال روی خم بیضوی پیاده‌سازی شده که در آن هیچ نهادی به کلید خصوصی دسترسی نداشته و امنیت آن کامل بوده و نیز ویژگی‌های مطلوب رای‌گیری الکترونیکی در آن تامین می‌شود. هم‌چنین بنا بر محاسبات انجام‌شده این پروتکل نیاز به رای‌گیری از ۱۰۰ میلیون رای‌دهنده را در حدود ۳۰ ثانیه پاسخ می‌گوید. برخی نقاط ضعف این پروتکل برای اجرا، نیاز به رای‌دادن در مجموعه محدود بله یا خیر، برگزاری انتخابات با تعداد محدود رای‌دهنده و نداشتن قابلیت غیرقابل اجباربودن رای‌ها است. لذا باید راه‌کار مناسبی برای توسعه پروتکل و رفع نقاط ضعف رای‌دادن با گزینه محدود دوتایی و قابل اجباربودن رای پیشنهاد شود.

۷- مراجع

[1] L. Fouard, M. Duclos, and P. Lafourcade, "Survey on Electronic Voting Schemes", supported by the ANR project AVOTÉ, 2007.

[2] H. Lipmaa, "Secure Electronic Voting Protocols," Cybernetica AS and University of Tartu(Estonia), 2005.

[3] R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimally Efficient Multi- authority Election Scheme," European transactions on Telecommunications, Vol. 8, No. 5, pp. 481-490, 1997.

[4] G. Kalman, and A. Huszti, "A Homomorphic Encryption-based Secure Electronic Voting Scheme," University of Debrecen. Hungary, 2011, avilable at: www.semanticscholar.org/.

[5] P. P. Ferreira, "Traceable Electronic Voting," Lisboa, Instituto Superior Técnico–Universidade Técnica de Lisboa (Dissertação de Doutoramento), 2007.

[6] M. Mesbahuddin Sarker and Dr. Md. Sharif Uddin, "Electronic Voting Algorithm and Its Algebraic Formation", International Journal of Mathematics Trends and Technology, vol. 10, no. 1, 2014.

[7] L. R. Rivest, and S. Ledlie, "Voting Homorphic Encryption", Lecture Notes 15, 2002.

[8] A. Jivanyan and G. Khachatryan, "New Receipt-Free E-Voting Scheme and Self-Proving Mix Net as New Paradigm", IACR Cryptology ePrint Archive, p. 325, 2011.

[9] R. Joaquim, A. Zúquete, and P. Ferreira, "REVS a Robust Electronic Voting System", IADIS International Journal of WWW/Internet, vol. 1, no. 2, pp. 47-63, 2003.

[10] B. Adida, "Mixnet Voting", Cambrige University Press, 2005.

[11] C. Porkodi, R. Arumuganathan, and K. Vidya, "Single Authority Electronic Voting based on Elliptic Curves," Journal of Discrete Mathematical Sciences and Cryptography, vol. 13, no. 3, pp. 209-217, 2010.

[12] C. Porkodi, R. Arumuganathan, and K. Vidya, "Multi-authority Electronic Voting Scheme Based on Elliptic Curves," IJ Network Security, vol. 12, no. 2, pp. 84-91, 2011.

[13] L. C. Huang, and M. S. Hwang, "Two-party Authenticated Multiple-key Agreement based on Elliptic Curve Discrete Logarithm Problem," International Journal of Smart Home, vol. 7, no. 1, pp. 9-18, 2013.

[14] T. P. A. Pedersen, "Threshold Cryptosystem Without a Trusted Party," in Advances in Cryptology-Eurocrypt'91, Springer, 1991.

[15] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis and Y. C. Stamatiou, "Elliptic Curve based Zero Knowledge Proofs and their Applicability on Resource Constrained Devices," in Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on, 2011.

[16] M. Cerveró Abelló, V. Mateu, J. M. Miret, F. Sebe, and J. Valera, "An Elliptic Curve Based Homomorphic Remote Voting System," RECSI2014, -5 September 2014.