

پروتکل جدید رای گیری الکترونیکی مبتنی بر خم بیضوی

عبدالرسول میرقدری^{۱*}، سعید رحیمی^۲، علیرضا رحیمی^۳

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

(دریافت: ۹۵/۰۲/۲۵، پذیرش: ۹۵/۱۰/۱۴)

چکیده

با توجه به گسترش انتخابات متعدد و ضرورت سلامت و اطمینان فرآیند رای گیری، توجه زیادی به رای گیری الکترونیکی شده است. تحقیقات متعدد در خصوص رای گیری الکترونیکی نشان می دهد که با این پروتکل ها می توان الزامات یک فرآیند رای گیری مطمئن را به اثبات رساند. یکی از روش های مناسب برای اجرای رای گیری الکترونیکی استفاده از رمزنگاری هم ریخت است. روش رمزنگاری هم ریخت یک طرح رمزنگاری است که نسبت به عملیات جمع هم ریخت می باشد. در این مقاله با استفاده از رمزنگاری الجمال روی خم های بیضوی یک پروتکل رای گیری الکترونیکی جدید ارائه شده که توسط همه قابل نظارت است. این پروتکل بر پایه سخت بودن حل مسئله لگاریتم گسسته روی خم بیضوی، امنیت رای دهندگان و امنیت کلید را تامین می کند. پروتکل پیشنهادی برای برگزاری رفراندومی به تعداد ۱۰۰ میلیون رای دهنده آزمون شده که زمان شمارش تعداد کل آرا حدود ۳۲ ثانیه طول کشید.

واژه های کلیدی: پروتکل رای گیری الکترونیکی، خم بیضوی، رمزنگاری هم ریخت

۱- مقدمه

اصل رای هیچ فردی نباید در هیچ یک از مراحل رای گیری قابل مشاهده باشد.

قابلیت تایید عمومی: هنگام استفاده از رای گیری الکترونیکی هر کسی باید بتواند با نظارت بر فرآیند برگزاری انتخابات، صحت انجام مراحل انتخابات را تایید کند. این قابلیت در سامانه های سنتی امکان پذیر نیست و یکی از مهم ترین اهداف استفاده از رای گیری الکترونیکی است.

مقاوم بودن: لازم است پروتکل رای گیری نسبت به بروز خطای احتمالی مقاوم باشد. به طور کلی، یک پروتکل رای گیری الکترونیکی در صورتی مقاوم است که در صورت وقوع خطا یا تقلب توسط یکی از بخش های شرکت کننده 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 الگوریتم های محاسباتی موجود در رای گیری الکترونیکی نباید مانعی برای اجرای انتخابات باشد. این هزینه محاسباتی باید به گونه ای باشد که عملیات اخذ رای و شمارش آرا در مدت زمان منطقی و معقول قابل انجام باشد.

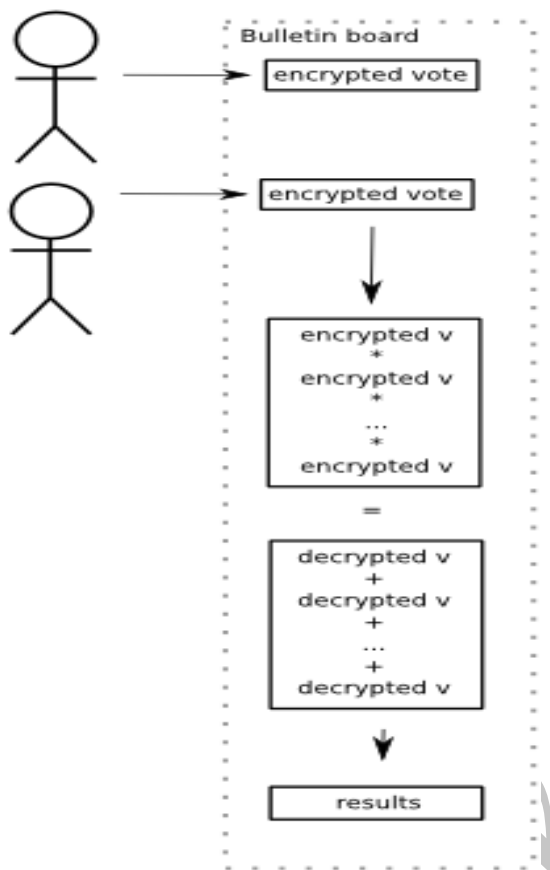
رای گیری از افراد واجد شرایط: در فرآیند رای گیری الکترونیکی تنها افرادی که واجد شرایط لازم هستند باید بتوانند در رای گیری شرکت کنند. هم چنین هیچ فرد واجد شرایطی نباید بتواند بیش از

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

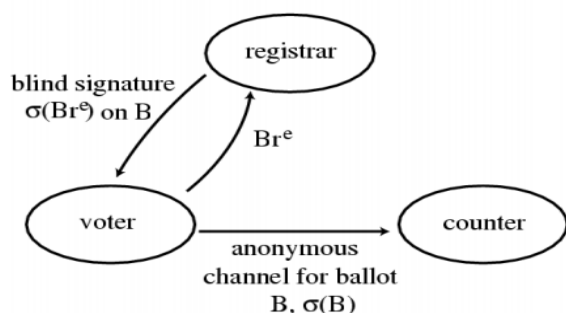
یکی از راه کارهای موثر برای مشارکت آحاد مردم در مسائل اجتماعی برگزاری انتخابات به روش رای گیری الکترونیکی است. رای گیری الکترونیکی، به طور کلی عبارت است از اجرای فرآیند انتخابات به کمک ابزارهای الکترونیکی به گونه ای که الزامات یک پروتکل رای گیری حفظ شود. ابزارهای الکترونیک برای اجرای الگوریتم های ریاضی استفاده می شوند. با روش های ریاضی اثبات می شود که الگوریتم ها شرایط و الزامات مدنظر را تامین می کنند. الزامات مورد نیاز یک پروتکل رای گیری عبارتند از:

حفظ حریم خصوصی: یکی از الزامات بسیار مهم یک پروتکل رای گیری الکترونیکی حفظ محرمانگی رای هر فرد است. مطابق این

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^۳: 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

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

غیرقابل اجبار و غیرقابل اثبات بودن 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.

کامل بودن سامانه: در سامانه رای‌گیری نباید امکان تغییر یا ابطال هیچ رای‌ی وجود 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 [۱-۲].

مابقی ساختار مقاله بدین شرح است که در بخش دوم شیوه‌های 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 آراء، شمارش آراء 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 به شرح ذیل وجود دارد:

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

ب) امضای کور^۲: 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 رمز شده 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

1- Homomorphic Encryption
2- Blind Signature

ب) عملیات جمع روی خم بیضوی

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

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

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

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

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

۱- مرحله راه اندازی: طرفین منحنی بیضوی E و مولد Q را از مرتبه q با یک دیگر توافق می کنند.

۲- مرحله تولید کلید: طرف اول عدد تصادفی x را انتخاب کرده و $H = xQ$ را تشکیل می دهد. در این رابطه H به عنوان کلید عمومی در اختیار همه قرار می گیرد. مقدار x کلید خصوصی بوده که طرف اول آن را برای بازگشایی رمز نزد خود نگه می دارد.

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

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

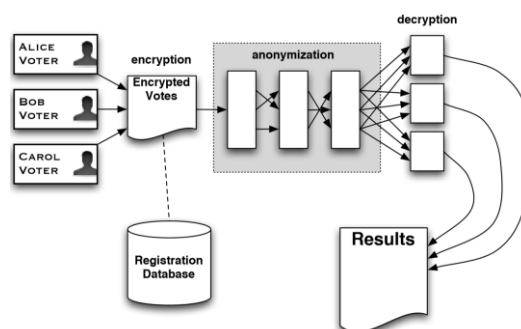
طرف دوم برای ارسال پیام m مقدار C را به طرف اول ارسال می کند.

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

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

شکل (۴): الگوریتم رمزنگاری الجمال روی خم بیضوی

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



شکل (۳): رای گیری با شبکه مخلوط [۱۰]

روش این مقاله بر اساس رمزنگاری هم ریخت روی خم بیضوی است. در سال ۱۹۹۷ کرامر و همکاران، پروتکل مبتنی بر رمزنگاری هم ریخت را ارائه کردند که بیش تر فعالیت های 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 رای گیری 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 اشاره شده نیازمند یک نهاد مرکزی بود که خود به خود امنیت سیستم را وابسته به همان نهاد می کرد. پروتکل پیشنهادی بر اساس رمزنگاری الجمال روی خم بیضوی طراحی شده است که دارای امنیت بهتر و هزینه ارسالی کمتری نسبت به سایر روش ها است. همچنین عمل رمزنگاری به طور مستقیم نسبت به عملیات جمع هم ریخت است. در نهایت با پیاده سازی عملی این طرح نتایج امنیت و کارایی این روش بسیاری از الزامات پروتکل رای گیری را تامین کرده و دارای امنیت بهتری است. در نهایت با پیاده سازی عملی طرح، نتایج امنیت و کارایی آن برای ۱۰۰ میلیون رای دهنده ارائه شده است.

۳- مفاهیم اساسی

برخی مفاهیم ریاضی مورد استفاده در تحقیق را شرح می دهیم:

الف) تعریف خم بیضوی

فرض کنید F یک میدان ریاضی باشد. خم بیضوی مجموعه ای از نقاط F است که دارای شرایط زیر می باشد:

$$E = \{(x, y) \mid \forall x, y \in F; y^2 = x^3 + ax + b\} \cup \{O_E\} \quad (1)$$

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

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. به علاوه 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_i ها 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 $H = \sum_{i=1}^n H_i$ به دست خواهد آمد. این مقدار کلید عمومی برای انجام محاسبات و انجام عملیات اخذ آراست. کلید خصوصی برابر با مقدار $x = \sum_{i=1}^n x_i$ 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 می‌کند.

ج) لگاریتم گسسته روی خم بیضوی

اگر میدان تعریف خم بیضوی E را F_p در نظر بگیریم، مجموعه نقاط خم بیضوی E به صورت $(x \% p, y \% p)$ 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 $R = IQ$ به مسئله لگاریتم گسسته روی خم بیضوی مشهور است که با داشتن مقدار R یافتن مقدار I 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 به صورت 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 به ترتیب برای پیام‌های آشکار m و m' فرص کنیم لذا خواهیم داشت:

$$\begin{aligned} C + C' &= (c_1, c_2) + (c'_1, c'_2) = (c_1 + c'_1, c_2 + c'_2) \\ &= ((r + r')Q, (m + m') + (r + r')H) \Rightarrow \text{Dec}(C + C') = m + m' \end{aligned} \quad (3)$$

یعنی حاصل جمع دو عبارت رمز شده برابر است با رمز شده 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 به کمک نمایندگی‌های A_1, \dots, A_n ، ابتدا سامانه راه‌اندازی می‌شود. در این پروتکل رای‌گیری

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

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 -1 را ارسال کرده است. برای بازگشایی عبارت فوق لازم است تا xc_1 محاسبه شود. برای این منظور، به جای مقدار x مقدار xc_1 به صورت مستقیم از روش تقسیم راز شمیر محاسبه می شود و با استفاده از آن مقدار d کشف می گردد. با توجه به روش اشتراک راز شمیر می توان راز را با همکاری t نمایندگی از روش زیر استخراج کرد. برای این کار فرض می شود که اعضا مجموعه J اطلاعات $s_j c_1$ را محاسبه و به اشتراک گذاشته باشند و $t \geq |J|$. بدین منظور، هر کدام از A_j ها مقدار $w_j = s_j c_1$ را بر روی برد عمومی اعلام می کند. با استفاده از این اطلاعات مقدار xc_1 توسط رابطه زیر به دست می آید:

$$xc_1 = \sum_{j \in J} \left(\prod_{i \in J, i \neq j} \left(\frac{i}{i-j} \right) w_j \right) = \sum_{j \in J} \left(\prod_{i \in J, i \neq j} \left(\frac{i}{i-j} \right) s_j c_1 \right) \quad (8)$$

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

$$Y = c_2 - xc_1 = (\sum_1^m r_i)H + dQ - (x \sum_1^m r_i Q) = (\sum_1^m r_i)H + dQ - \sum_1^m r_i H = dQ \quad (9)$$

برای کشف مقدار d ، لازم است تا نتیجه به دست آمده Y را با مقادیر $-mQ, -(m-1)Q, \dots, -Q, 0, Q, \dots, mQ$ مقایسه می کنیم. این کار به خاطر سختی مسئله لگاریتم گسسته عملیاتی پیچیده است. برای این کار از روش گام بزرگ و کوچک^۲ استفاده می شود. برای تعیین مقدار $-m \leq d \leq m$ از رابطه (۹)، دستورالعمل زیر را اجرا می کنیم. با در نظر گرفتن مقدار d به صورت $d = ik + z$ می توان مقدار z ، i را با فرض k مشخص پیدا کرد. این فرض معادل است با $Y - i(kQ) = zQ$. برای تعیین مقادیر z ، i از روش آمده در شکل (۵) در زیر استفاده می شود.

- ۱- مقدار $k = \lfloor \sqrt{2m} \rfloor$ را تعیین می شود.
 ۲- به ازای تمام مقادیر $0 \leq z < k$ مقدار (j, zQ) محاسبه و در یک جدول درهم ساز^۳ ذخیره می شود.
 ۳- مقدار $\alpha = Y - kQ$ محاسبه می شود.
 ۴- با شمارش i از ۰ تا $k-1$:
 آیا α در جدول ذخیره شده موجود است؟
 a. بله: نتیجه $z + ik$ پیدا شده است.
 b. خیر: $\alpha = \alpha + (-kQ)$

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

از طرف دیگر، هر نمایندگی مقدار $f_i(j)$ را طبق رابطه (۴) محاسبه و از طریق کانال ارتباطی امن بین A_i و A_j به صورت محرمانه برای نماینده A_j می فرستد.

$$f_i(z) = x_i + f_{i,1}z + f_{i,2}z^2 + \dots + f_{i,k-1}z^{k-1} \quad (4)$$

با توجه به اطلاعات برد عمومی A_i می تواند بررسی کرد که آیا A_j مقدار درست $f_i(j)$ را برای او فرستاده است یا خیر؟ برای این کار A_i حاصل رابطه زیر را محاسبه کرده و در صورتی که تساوی زیر برقرار نباشد اعلام عدم تطابق کرده و $f_j(i)$ را در برد عمومی اعلام می کند. در این مرحله A_i از ادامه فرآیند دست می کشد. با این کار همکاری با A_j توسط باقی نمایندگی ها زیر سوال می رود [۱۴].

$$f_j(i)Q = \prod_{l=0}^{k-1} i.l.F_{j,l} \quad (5)$$

پس از تایید عملیات هر نمایندگی A_i مقدار $s_i = \sum_{l=1}^n f_l(i)$ را محاسبه کرده و نگهداری می کند.

با توجه به روابط فوق وجود یک چندجمله ای درجه t از همکاری نمایندگی ها ساخته می شود که معادل جمع چندجمله ای تمام نمایندگی ها است و جمله ثابت آن کلید خصوصی است.

$$f(z) = \sum_1^n f_i(z) = x + f_1z + \dots + f_{k-1}z^{k-1} \quad (6)$$

با توجه به پروتکل هر نمایندگی A_i اطلاعات $s_i = f(i)$ را از چندجمله ای فوق در اختیار دارد. بنابراین مطابق با روش تقسیم راز شمیر^۱ اثبات می شود 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 می فرستد. هر رای به صورت v_i از مجموعه $\{-1, 1\}$ انتخاب می شود که به ترتیب متناظر با رای های بله و خیر است. لذا رای ارسالی به صورت $(c_{i,1}, c_{i,2}) = (r_i Q, r_i H + v_i P)$ بر روی برد عمومی قرار می گیرد.

۴-۲- مرحله شمارش آرا

ابتدا همه آرا ارسالی روی برد عمومی جمع می شود. با این کار نتیجه جمع آرا مطابق رابطه زیر به صورت یک عبارت رمزی الجمال فرستاده می شود. با توجه به خاصیت هم ریختی در رمزنگاری الجمال با رمزگشایی از این عبارت نتیجه آرا قابل کشف خواهد بود.

$$(c_1, c_2) = (\sum_1^m c_{i,1}, \sum_1^m c_{i,2}) = (\sum_1^m r_i Q, (\sum_1^m r_i)H + dQ) \quad (7)$$

روش اثبات تعاملی

- ۱- اثبات کننده ابتدا یک مقدار تصادفی r را انتخاب نموده و $(a_1, a_2) = (rQ_1, rQ_2)$ را برای تایید کننده می فرستد. (a_1, a_2) لگاریتم گسسته یکسانی دارند
- ۲- تایید کننده یک عدد تصادفی c انتخاب کرده و برای اثبات کننده می فرستد.
- ۳- اثبات کننده مقدار $b = r - ck$ را محاسبه کرده و برای تایید کننده می فرستد.
- ۴- تایید کننده در صورت برقراری توامان دو شرط $a_1 = bQ_1 + cy_1$ و $a_2 = bQ_2 + cy_2$ مقادیر $y_1 = kQ_1, y_2 = kQ_2$ را تایید می کند.

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

روش اثبات تعاملی با تغییر کوچکی به اثبات غیرتعاملی تبدیل می شود. برای انجام این کار، اثبات کننده چالش c را از رابطه زیر تعیین می کند.

$$c = \text{hash}(y_1, Q_1, y_2, Q_2, rQ_1, rQ_2) \quad (11)$$

با این کار هر تایید کننده ای می تواند مقدار c و شرایط را بررسی کند. در این رابطه برای عملیات hash می توان از یک تابع چکیده ساز مطمئن مانند SHA-1 استفاده نمود [۱۵].

۵- تحلیل و پیاده سازی

در این بخش ابتدا ویژگی های رای گیری الکترونیکی را تحلیل نموده و سپس آن را برای تعداد مشخصی رای دهنده پیاده سازی عملی کرده ایم.

الف) تحلیل ویژگی های رای گیری الکترونیکی

روش ارائه شده دارای ویژگی های زیر از الزامات رای گیری الکترونیکی می باشد:

حریم خصوصی: از آن جایی که رای هر فرد رمز شده است و هیچ نهادی کلید خصوصی برای بازگشایی رمز را ندارد، در نتیجه حریم خصوصی تامین شده است.

قابلیت تایید عمومی: تمام افراد می توانند توسط روش های ارائه شده عملکرد درست سامانه را به طور کلی تایید کنند.

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

در این روش، جستجو در جدول درهم ساز از مرتبه زمانی $O(1)$ می باشد. لذا در این بهینه سازی، کشف مقدار d از مرتبه زمانی $O(\sqrt{n})$ انجام می گیرد 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 آن ها و مقدار m ، تعداد رای دهنده ها، برابر مجموع این دو مقدار خواهد بود. لذا مقدار هر یک با حل دو معادله زیر به دست می آید:

$$\begin{cases} a - b = d \\ a + b = m \end{cases} \rightarrow a = \frac{a+m}{2}, b = \frac{m-d}{2} \quad (10)$$

۳-۴- مرحله اثبات صحت عملکرد

در این بخش، بحث در خصوص اثبات صحت عملکرد نمایندگی ها، صحت عملکرد رای دهنده ها و اثبات با روش هیچ آگاهی می باشد.

الف) اثبات صحت عملکرد نمایندگی ها

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 می داند. در ادامه شیوه اثبات این دانش آمده است.

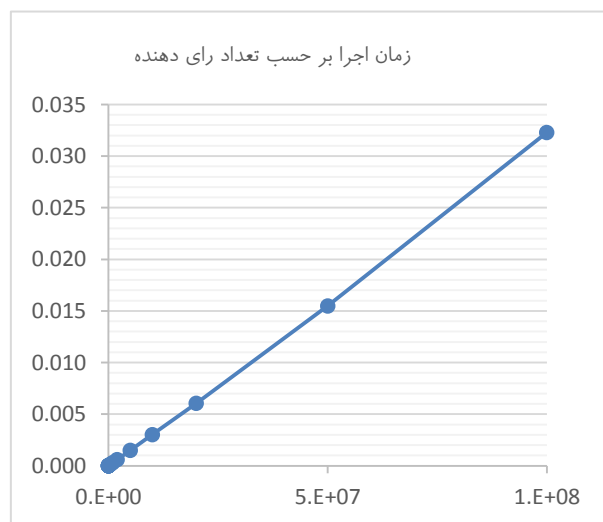
ب) اثبات صحت عملکرد رای دهنده ها

هم چنین 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 $v_i \in \{-1, 1\}$ برای این کار کافی است که V_i ثابت کند مقدار r_i را می داند 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 نمایندگی ها، این متغیرها لگاریتم گسسته یکسانی نسبت به پایه های 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 می شود. مقادیر (Q_1, y_1, Q_2, y_2) معلوم هستند که y_1 و y_2 لگاریتم گسسته یکسان با (مقدار k) به ترتیب نسبت به Q_1, Q_2 دارند. اثبات کننده باید بدون دادن اطلاعات اضافی به تایید کننده ثابت کند که این مقدار را می داند. برای این اثبات دو روش وجود دارد. روش اول روش تعاملی و روش دوم به صورت غیرتعاملی است. الگوریتم اثبات تعاملی در شکل (۶) در زیر آمده است.

در این پیاده سازی 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 تقریق در میدان F_p است. با توجه به نتایج پیاده سازی، زمان لازم برای محاسبه نتیجه آرا برای ۱۰۰ میلیون رای دهنده حدود ۳۲ ثانیه است که در شکل (۷) در زیر دیده می شود.



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

۶- نتیجه گیری

در این مقاله، یک پروتکل کارا بر اساس رمزنگاری هم ریخت روی خم های بیضوی برای شمارش آرا به صورت الکترونیکی ارائه شد. این پروتکل بر اساس رمزنگاری الجمال روی خم بیضوی پیاده سازی شده که در آن هیچ نهادی به کلید خصوصی دسترسی نداشته و امنیت آن کامل بوده و نیز ویژگی های مطلوب رای گیری الکترونیکی در آن تامین می شود. هم چنین بنا بر محاسبات انجام شده این پروتکل نیاز به رای گیری از ۱۰۰ میلیون رای دهنده را در حدود ۳۰ ثانیه پاسخ می گوید. برخی نقاط ضعف این پروتکل برای اجرا، نیاز به رای دادن در مجموعه محدود بله یا خیر، برگزاری انتخابات با تعداد محدود رای دهنده و نداشتن قابلیت غیرقابل اجبار بودن رای ها است. لذا باید راه کار مناسبی برای توسعه پروتکل و رفع نقاط ضعف رای دادن با گزینه محدود دوتایی و قابل اجبار بودن رای پیشنهاد شود.

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

رای گیری از افراد واجد: چون مشخصات همه رای دهندگان ابتدا در سامانه ثبت شده و فقط آرا این رای دهندگان 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.

غیر قابل اجبار بودن رای ها: با توجه به این که در این پروتکل هر فرد می تواند با ارائه مقدار r رای خود را اثبات کند، در نتیجه 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.

کامل بودن سامانه: بر اساس تعریف، کامل بودن 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 می شود که هیچ رأیی 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. هم چنین کشف کلید در رمزنگاری خم بیضوی نیازمند حل مسئله سخت لگاریتم گسسته روی خم بیضوی است که در عمل غیر قابل 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) پیاده سازی 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 روش های گام میانی^۱ همانند گام بزرگ گام کوچک، باز کردن 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 پیاده سازی و آزمون شده است.

$p = 1268133167195989090596625406312984755854486256116$
 $a = 386736940269827655214118852806596527602892573734$
 $b = 1461501637330902918203684832716283019655932542983$

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, available 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.

A New Elliptic Curve Based Electronic Voting Protocol

A. Mirghadri*, S. Rahimi, A. Rahimi

*Imam Hossein University

(Received: 14/05/2016, Accepted: 03/01/2017)

ABSTRACT

According to the spread of various elections and the need for safety and confidence of the voting process, electronic voting has been of considerable attention. Numerous studies show that the electronic voting system can be proved to the requirements of a voting process. One suitable method for the implementation of electronic voting can be homomorphic encryption. Homomorphic encryption method is an encryption system that is isomorphic to the operation. In this paper, using elliptic curve encryption, a new electronic voting protocol is provided, which can be monitored by all. The system is based on the difficulty of solving discrete logarithm problem on elliptic curve and provides voters and key safety. The proposed protocol was tested for 100 milion voters in a referendum in which the total number of votes was counted in the 30 seconds.

Keywords: Electronic Voting, Elliptic Curve, Homomorphic Encryption

* Corresponding Author Email: amrghdri@ihu.ac.ir