TEEGES

Technovations in Electrical Engineering & Green Energy System

Research Article (2022) 1(3):91-103

Electronic Voting Based on Homomorphic Encryption in Elliptic Curve

Sajjad Rezaee Adaryani[1], *M.Sc*, Sayyed Mahdi Sajadieh[2], *Assistant Professor*

[1] *Faculty of Applied Sciences, Malek-Ashtar University of Technology, Isfahan, Iran*
[2] *Department of Computer Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Khorasgan, Isfahan, Iran*

Abstract:

Today, elections play an important role in fulfilling democracy, which should be available in all situations. Electronic voting provides a platform to do this anywhere. In this case, there are many electronic selection plans that have good security but do not have the required efficiency. In this article, an election plan based on the cryptography of the elliptic curve collective group is expressed, which fulfills the characteristics such as entitlement, confidentiality, without receipt, the impossibility of coercion, and due to the use of the elliptic curve group, along with equivalent security, it has good performance. Compared to the designs based on number analysis problem and discrete logarithm problem (with 160-bit elliptic curve key, it has security equivalent to 1024-bit RSA key). Although the elections based on hommorphic cryptography and the discrete logarithm problem are included in Hozti's scheme, but the more robust method presented with the necessary changes and also by presenting a blind signature that fits the voting plan, it has been tried that this method is compared to the issues presented.

Keywords: Electronic Elections, Elliptic Curve, Homomorphic Encryption, Eljamal Encryption System, Blind Digital Signature Elliptic Curve

Received: 9 May 2022
Revised: 15 July 2022
Accepted: 31 August 2022
Corresponding Author: Sajjad Rezaee Adaryani, s. rezaee @mut-es.ac.ir
DOI: http://dx.doi.org/10.30486/TEEGES.2022.1964503.1028

فناوری‌های نوین در مهندسی برق و سیستم انرژی سبز

TEEGES

مقاله پژوهشی

رأی‌گیری الکترونیکی بر اساس رمزنگاری هم‌ریخت در گروه خم بیضوی

سجاد رضایی آدریانی[1]، *کارشناسی ارشد*، سید مهدی سجادیه[2]، *استادیار*

۱- *مجتمع علوم کاربردی، دانشگاه صنعتی مالک اشتر، اصفهان، ایران*

۲- *دانشکده مهندسی برق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، خوراسگان، اصفهان، ایران*

چکیده: امروزه انتخابات نقش مهمی در برآورده کردن مردم‌سالاری دارد به‌نحوی‌که در همه حالات در دسترس باشد. رأی‌گیری الکترونیکی بستری را فراهم می‌آورد تا در هر مکان بتوان این کار را انجام داد. در این مورد بسیاری از طرح‌های انتخاب الکترونیک وجود دارند که امنیت خوبی دارند ولی کارایی لازم را ندارند. در این مقاله، یک طرح انتخابات بر اساس رمزنگاری هم‌ریخت در گروه جمعی خم بیضوی بیان می‌شود که ویژگی‌هایی ازجمله استحقاق، محرمانگی، بدون رسید بودن، عدم امکان اجبار و غیره را برآورده می‌سازد و به دلیل استفاده از گروه خم بیضوی، در کنار امنیت معادل، کارایی خوبی در مقایسه با طرح‌هایی که بر اساس مسئله‌ی تجزیه اعداد و مسئله‌ی لگاریتم گسسته هستند را ارائه می‌دهد (با کلید ۱۶۰ بیتی خم بیضوی امنیت معادل کلید ۱۰۲۴ بیتی RSA دارد). هرچند انتخابات مبتنی بر رمزنگاری هم‌ریخت و مسئله‌ی لگاریتم گسسته در طرح هوزتی آمده است ولی روش مستحکم‌تر ارائه‌شده با تغییرات لازم و همچنین با ارائه‌ی یک امضای کور که متناسب با طرح رأی‌گیری، سعی شده است که این روش نسبت به مباحث ارائه‌شده تا به امروز امن‌تر باشد.

واژه‌های کلیدی: انتخابات الکترونیکی، گروه خم بیضوی، رمزنگاری هم‌ریخت، سیستم رمزنگاری الجمال، امضای دیجیتالی کور.

تاریخ ارسال مقاله: ۱۴۰۱/۰۲/۱۹

تاریخ بازنگری مقاله: ۱۴۰۱/۰۴/۲۴

تاریخ پذیرش مقاله: ۱۴۰۱/۰۶/۰۹

نویسنده‌ی مسئول: سجاد رضایی آدریانی ، s.rezaee @mut-es.ac.ir

DOI: http://dx.doi.org/10.30486/TEEGES.2022.1964503.1028

۱- مقدمه

یک انتخابات الکترونیکی علاوه بر اینکه باید تمام خواص یک انتخابات مبتنی بر کاغذ (گمنامی، محرمانگی، در دسترس بودن برای عموم افراد و ...) را داشته باشد، باید دارای امنیت بیشتری نسبت به این نوع انتخابات باشد. لذا ویژگی‌های مطلوب یک انتخابات را در یک نگاه کلی می‌توان به‌صورت زیر بیان کرد [۱-۱۵]:

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

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

۳) عدالت[۳](در نتایج انتخابات): هیچ گروهی نتوانند از نتایج میانی انتخابات با خبر شوند.

۴) وارسی عمومی و فردی[۴]: هر کس بتواند صحت روند برگزاری انتخابات را وارسی نماید. همچنین هر فردی بتواند از شمرده شدن رأی خود مطمئن گردد.

۵) بدون رسید بودن[۵] و عدم امکان اجبار[۶]: 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 رأی خود ارائه دهد و با بدون رسید بودن طرح انتخاباتی از بین می‌رود. عدم امکان اجبار نیز یعنی اینکه اجبار کننده نتواند رأی‌دهنده را تهدید نماید. در طرحی که توسط اندری هوزتی[۷] در [۲] مطرح گردیده است یک تعریف دقیق از خاصیت بدون رسید بودن یک طرح انتخابات الکترونیکی بیان‌شده است. فرض کنید X اطلاعات عمومی منتشرشده باشد (پارامترهای عمومی و اطلاعات منتشرشده در تابلو اعلانات). همچنین فرض کنید C رأی موردنظر شخص رأی‌دهنده و C^* رأی موردنظر دشمن باشد و دشمن C با رأی‌دهنده‌ی V ارتباط برقرار نماید و او را مجبور کند که به نامزد برگزیده‌ی C رأی C^* بدهد و C تصمیم بگیرد که view(X:V) (اطلاعاتی که در تابلو اعلانات ظاهر می‌گردد)را بپذیرد و یا خیر و مسئول انتخابات A تصمیم بگیرد که C^* را بپذیرد و یا خیر. اجبار کننده، هر پیامی را از روی تابلو اعلانات درج می‌شود می‌گیرد. یک طرح رأی‌گیری بدون رسید است اگر یک رأی‌دهنده V وجود داشته باشد به‌طوری‌که برای هر دشمن C، رأی‌دهنده V بتواند رأی $C(\neq C^*)$ را بدهد طوری که توسط مسئول رأی‌گیری A پذیرفته‌شده باشد وC قدار view(X:V) را قبول نماید.

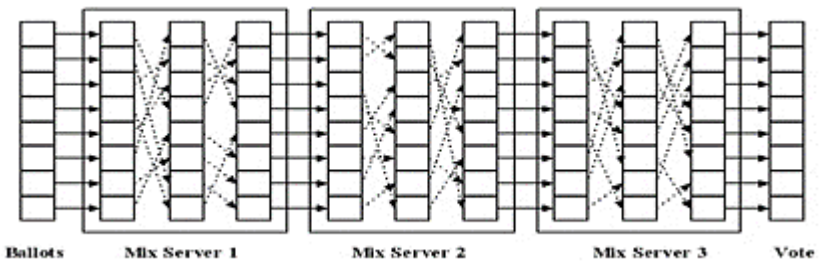
۶) صحت[۸]: منظور از صحت در انتخابات این است که رأی‌دهنده قادر به تولید رأی معیوب با توجه به ساختار آرا نباشد.

۷) کامل بودن[۹]: تمام رأی‌ها شمرده شوند.

۸) سلامت[۱۰]: تبهکاران و هیچ ائتلافی با تعداد کمتر از t مسئول امکان تخریب نداشته بباشند (تعداد مسئولانی است که می‌توانند کلید رمزگشایی تسهیم شده را بازیابی نمایند).

برای رسیدن به ویژگی‌های مطرح‌شده، می‌توان از روش کلی انتخابات که به‌صورت زیر هستند استفاده کرد:

- روش مخلوط کننده[۱۱]: مخلوط کننده یک سرویس اینترنتی است که در آن مجموعه‌ی متون رمز شده به‌عنوان ورودی دریافت می‌کند و خروجی آن، جایگشت داده‌شده و باز رمز شده‌ی ورودی‌ها میان رأی‌دهنده و دفتر شمارش آرا است (شکل ۱ را مشاهده کنید) [۱۵].



شکل ۱: مخلوط کننده [۱۵]

- روش امضای کور[۱۲]: این طرح اولین بار توسط چوآم ارائه شد. در آن روش یک مسئول رأی‌گیری، بدون دیدن محتوی پیام آن را امضا می‌کند و با این کار به پیام اعتبار می‌بخشد و اگر بعداً امضا برای عموم آشکار گردد امکان ارتباط بین امضا و رأی‌دهنده غیرممکن است. طرح‌هایی که بر اساس امضای کور هستند معمولاً از کانال‌های گمنام برای ارسال امضای کور و همچنین برگه رأی امضاشده برای مسئولین رأی‌گیری استفاده می‌کنند تا گمنامی فرستنده را تضمین نمایند [۱۴و۱۷].
- روش رمزنگاری هم‌ریخت[۱۳]: این طرح‌ها بر اساس رمزنگاری هم‌ریخت نوشته می‌شوند و دارای خاصیت وارسی عمومی با محفوظ ماندن محرمانگی رأی‌دهندگان هستند [۲و۸].

در ادامه‌ی این مقاله در بخش دوم ملزومات موردنیاز جهت بیان طرح پیشنهادی از جمله هستارها، کانال‌ها و الگوریتم‌های موردنیاز مانند امضای کور خم بیضوی بیان می‌گردد. در ادامه در بخش سوم طرح رأی الکترونیک مبتنی بر خم بیضوی بیان می‌شود و در نهایت در بخش‌های چهارم و پنجم به ترتیب ارزیابی امنیتی و ارزیابی محاسباتی بیان می‌شود.

۲- ملزومات طرح

۲-۱- هستارها

این طرح دارای شرکت‌کنندگان (هستارها)زیر است [۲]:

فرض کنید که در انتخابات n نامزد وجود داشته باشد و نامزد i-ام که توسط رأی‌دهنده v_k انتخاب‌شده است به‌صورت $c_i^{(k)}$ نمایش داده می‌شود. همچنین فرض نمایید $\{V_1,\cdots,V_M\}$ مجموعه‌ی رأی‌دهندگان بوده و $\{A_1,\cdots,A_N\}$ مسئولین انتخابات هستند. یکی از این مسئولین که مسئول وارسی (VA) نامیده می‌شود با استفاده از اثبات‌های صفر دانش برگه‌ی رأی‌ها را بازبینی می‌کند. دقت کنید که از VA انتظار درستکار بودن نمی‌رود. بعد از پایان دوره‌ی رأی‌گیری مسئولین، صحت رأی‌ها را وارسی می‌کنند. در ضمن فرض می‌شود حداقل یکی از مسئولین در خصوص تولید کلید و رمزگشایی پیام درستکار باشد. همچنین RA بیانگر بایگانی[۱۴] بوده و مسئول اداره کردن و مرحله‌ی احراز هویت است.

دشمن: هر گروه یا شخصی که سعی در بر هم زدن روند انتخابات دارد و یا درصدد تبانی کردن با یکی از هستارهای دیگر از طریق غیرقانونی باشد، دشمن تلقی می‌شود.

۲-۲- کانال‌ها

در این قسمت کانال‌های ارتباطی مختلفی که در این مقاله استفاده می‌شوند را معرفی می‌شود و مشخصات هر یک را توضیح داده می‌شود [۲].

۱. کانال عمومی: کانالی است که شرکت‌کنندگان اعم از مسئولین و رأی‌دهندگان و حتی خرابکاران می‌توانند اطلاعات خود را از طریق آن ارسال کنند.
۲. تابلو اعلانات[۱۵] (BB): محلی عمومی است که در آن شرکت‌کنندگان انتخابات می‌توانند اطلاعات عمومی خود را در آن درج نمایند.
۳. کانال گمنام[۱۶] : این کانال غیرقابل ردگیری بوده و گمنامی فرستنده‌ی پیام را تضمین می‌کند.

۲-۳- سیستم الجمال هم‌ریخت در گروه خم بیضوی

هرچند سیستم الجمال بر اساس لگاریتم گسسته است ولی می‌توان آن را به‌صورت زیر برحسب خم بیضوی بیان کرد. فرض کنید $E =< G >$ یک خم بیضوی روی میدان متناهی F_p باشد. در این صورت سیستم الجمال روی این گروه بدین‌صورت بیان می‌گردد:

$$E(mG,k)=(kG,mG+kH) \qquad (۱)$$

که در آن k یک عدد تصادفی است. با سیستم بیان‌شده اگر $c_1=\mathrm{E}(m_1G,\mathrm{k}_1)$ و $\mathrm{c}_2=\mathrm{E}(m_2G,\mathrm{k}_2)$ باشد. آنگاه سیستم یادشده به‌صورت زیر دارای خاصیت هم‌ریختی است. داریم:

$$\begin{aligned} c_1 + c_2 &= E(m_1 G, k_1) + E(m_2 G, k_2) \\ &= \left((k_1 + k_2)G, (m_1 + m_2) + (k_1 + k_2)H\right) \\ &= E((m_1 + m_2)G, k_1 + k_2) \end{aligned} \quad (۲)$$

۲-٤- مولد کلید الجمال

مسئول رأی‌گیری شماره i-ام با نماد A_i فرض می‌شود. در این صورت:

۱. در ابتدا A_i، $k_i \in Z_p^*$ انتخاب نموده و نقطه $Q_{A_i} = k_i G$ محاسبه می‌نماید. در ادامه A_i، Q_{A_i} را منتشر می‌کند و یک اثبات صفر دانش برای انتخاب k_i ارائه می‌دهد.

۲. حال RA منتظر می‌ماند تا Q_{A_i} در BB ظاهر گردد. در ادامه RA تمامی اثبات‌ها را وارسی می‌کند.

۳. کلید عمومی برابر است با $H = \sum_{i=1}^{N} Q_{A_i}$.

۲-۵- رمزگشایی الجمال

فرض کنید $(A, B) = (rG, mG + rH)$ یک پیام رمز شده به‌وسیله‌ی سیستم کلید عمومی الجمال در خم بیضوی باشد. برای رمزگشایی آن توسط N مسئول بدین‌صورت عمل می‌شود:

در ابتدا A_i تسهیم شده $\nabla_i = k_i.A$ را محاسبه می‌کند. در ادامه $U = \sum_{i=1}^{N} \nabla_i$ محاسبه‌شده و نتیجه $mG = B - U$ به دست می‌آید زیرا داریم:

$$\begin{aligned} B - U &= m.G + rH - U = mG + rH - \sum_{i=1}^{N} k_i.U \\ &= mG + rH - \sum_{i=1}^{N} r k_i G = mG + rH - rH = mG \end{aligned} \quad (۳)$$

در فاز ارزیابی رأی، رأی‌دهنده‌ی V_k، یک شماره‌ی شناسایی به‌طوری‌که توسط مسئول $P \in \{RA, VA\}$ امضای کور شده است تولید می‌کند. ازاین‌رو، مسئول رأی‌گیری قادر به شناسایی رأی‌دهنده از روی شماره شناسایی کور شده نیست. دشمن نیز نمی‌تواند هیچ‌گونه اطلاعاتی را در صورت تبانی با این مسئول به دست آورد.

طرح انتخابات الکترونیکی پیشنهادی از سیستم کلید عمومی الجمال در گروه جمعی خم بیضوی استفاده می‌کند. در ادامه‌ی این مقاله، فرض کنید p یک عدد اول بزرگ و E یک خم بیضوی روی میدان متناهی F_p باشد و نقطه G روی خم بیضوی از مرتبه اول q باشد به‌طوری‌که مسئله لگاریتم گسسته در $< G >$ یک مسئله سخت باشد. همچنین فرض کنید $H : \{0,1\}^* \to \{0,1\}^s$ یک تابع درهم‌ساز یک‌طرفه باشد که در برابر تصادم مقاوم است (s عددی ثابت و طبیعی است).

۲-٦- الگوریتم امضا دیجیتالی خم بیضوی

الگوریتم امضا دیجیتالی خم بیضوی $(ECDSA)$ همانند الگوریتم امضا دیجیتال کلید عمومی (DSA) بوده و امنیت آن بر اساس لگاریتم گسسته خم بیضوی[۱۷] است. برای هر تبادل، نحوه‌ی امضا کردن و روش تصدیق آن در [۳] آورده شده است در این مقاله امضای دیجیتال $ECDSA$ به‌صورت $SigGenEC(*)$ فراخوانی می‌شود و الگوریتم وارسی آن نیز به‌صورت $SigVerEc$ مورداستفاده قرار می‌گیرد.

۲-۷- امضای کور بر اساس خم بیضوی ($BlindEC(*)$)

همان‌طور که می‌دانیم امضاهای دیجیتال بر اساس خم بیضوی از امنیت و سرعت محاسبات و کاهش طول کلید نسبت به امضاهای مبتنی بر الجمال و RSA برخوردار است. لذا با به‌کارگیری این سیستم در امضای کور می‌توان امنیت و سرعت را در حد بالایی

تضمین نمود. در زیر به بیان یک روش امضای کور که بر اساس سختی مسئله‌ی لگاریتم گسسته خم بیضوی بناشده و برای این طرح انتخاباتی طراحی گردیده است می‌پردازیم:

الف) راه‌اندازی

فرض کنید p یک عدد اول بزرگ و E یک خم بیضوی روی میدان متناهی F_p باشد و نقطه‌ی G روی خم بیضوی از مرتبه اول q باشد به‌طوری‌که مسئله لگاریتم گسسته در $<G>$ غیرقابل‌حل باشد. انتخاب عدد تصادفی k_{VA} از بازه‌ی $[0, q-1]$ به‌عنوان کلید خصوصی و محاسبه $Q_{VA} = k_{VA}G$ و اختیار Q_{VA} به‌عنوان کلید عمومی در این مرحله انجام می‌شود.

ب) کور کردن

۱. مسئول رأی‌گیری یک عدد تصادفی $d \in Z_q$ انتخاب می‌کند و $\bar{R} = d.G = (x_{\bar{r}}, y_{\bar{r}})$ را محاسبه کرده و $\bar{R}$ را برای رأی‌دهنده ارسال می‌کند.

۲. رأی‌دهنده $a, b \in Z_q^*$ را به‌طور تصادفی انتخاب و مقادیر زیر را محاسبه کرده و $\bar{m}$ را که کور شده پیام $H(ID) = m$ است برای مسئول جهت اخذ امضا ارسال می‌کند.

$$\hat{R} = a.\bar{R} + b.G = (x_{\hat{r}}, y_{\hat{r}}) \quad (۴)$$

$$t = x_{\hat{r}} \bmod q \quad (۵)$$

$$\bar{m} = mt^{-1}\bar{t} \bmod q \quad (۶)$$

که در روابط بالا $\bar{t} = x_{\hat{r}} \bmod p$ است.

پ) امضا کردن

مسئول رأی‌گیری به‌صورت زیر پیام کور را امضا می‌کند و $\bar{s}$ را برای رأی‌دهنده ارسال می‌کند:

$$\bar{s} = d^{-1}(\bar{m} + \bar{t}.k_{VA}) \quad (۷)$$

ت) وارسی امضا

زوج مرتب $(\bar{s}, \bar{t})$ برای وارسی شدن برای مسئول وارسی ارسال می‌گردد. وارسی با استفاده از الگوریتم $sigVerEC$ بیان‌شده در قسمت ۲-۶ به‌صورت زیر انجام می‌پذیرد:

۱. $W = \bar{s}^{-1} \bmod q$ محاسبه می‌شود و $\bar{m}$ که کور شده‌ی پیام است در اختیار وارسی کننده قرار دارد.

۲. $U_1 = \bar{t}.w \bmod q$ و $U_2 = \bar{m}.w \bmod q$ محاسبه می‌شود.

۳. $V = x_1 mod p$ که در آن x_1 به‌صورت زیر محاسبه می‌گردد:

$$X = U_1.G + U_2.Q_{VA} = (x_1, y_1) \quad (۸)$$

۴. درصورتی‌که $\bar{t} = V$ باشد امضا موردقبول است زیرا:

$$\bar{s} = d^{-1}(\bar{m} + \bar{t}.k_{VA}) \Rightarrow d = \bar{s}^{-1}(\bar{m} + \bar{t}.k_{VA}) \Rightarrow G.d = G.\bar{s}^{-1}(\bar{m} + \bar{t}.k_{VA})$$
$$\Rightarrow \bar{R} = G.w.\bar{m} + G.w.\bar{t}.k_{VA} \Rightarrow \bar{R} = U_2.G + U_2.Q_{VA}$$

۳- طرح رأی‌گیری

این طرح دارای سه مرحله‌ی احراز هویت، مرحله‌ی رأی‌گیری و مرحله‌ی شمارش آرا بوده که جزئیات مراحل پروتکل پیشنهادی به شرح زیر است:

۳-۱- مرحله احراز هویت

۱. فرض کنید p یک عدد اول بزرگ و E یک خم بیضوی روی میدان متناهی F_p باشد و نقطه‌ی G روی خم بیضوی از مرتبه اول q باشد به‌طوری‌که مسئله لگاریتم گسسته در $<G>$ یک مسئله‌ی سخت باشد. همچنین $k \in Z_p^*$ و $H = kG \ mod q$ است.

۲. مسئول بایگانی به‌طور تصادفی $v_i \in Z_q$ را که $i = 1,\ldots,n$ انتخاب می‌کند. در ادامه $C_i = v_i.G$ که C_i بیانگر نامزد i-ام است و $H()$ تابع درهم‌ساز است. همچنین v_i و C_i و $H()$ به‌طور عمومی تولید می‌شوند.

۳. مسئول بایگانی کلید عمومی مربوط به خم بیضوی (Q_P, G, p, q) را به BB می‌فرستد.

٤. مسئول تصدیق‌کننده (VA) کلیدهای عمومی و خصوصی مربوط به خود یعنی $k_{VA} \in [1, q-1]$ و $Q_{VA} = k_{VA}.G \ modq$ را محاسبه می‌کند.

٥. اگر رأی‌دهنده V_k دارای حق رأی باشد شماره‌ی id_K^{RA} برای V_k نشان داده می‌شود که این شماره توسط V_k و RA به‌صورت تصادفی تولیدشده‌است. رأی‌دهنده V_k و RA امضای کور $BlindEC$ با شناسه‌ی V_k را اجرا می‌کنند. در پایان این مرحله مقدارهای $BlindEC(id_K^{RA})$ و id_K^{RA} به دست می‌آید.

۳-۲- مرحله‌ی رأی‌گیری

این مرحله شامل فاز وارسی و ریختن رأی است. فاز وارسی توسط یک اثبات صفر دانش غیرتعاملی انجام می‌پذیرد. در طول فاز وارسی، برگه‌ی رأی اثبات‌شده، برگه‌ی رأیی است که توسط سیستم الجمال رمز شده و شامل vG و $vH + c_i^{(k)}$ است که $c_i^{(k)}$ نشان‌دهنده‌ی نامزد i-ام بوده که توسط رأی‌دهنده‌ی V_k انتخاب‌شده است و v یک عدد تصادفی است. در طول فاز اخذ رأی، برگه‌ی رأی رمز شده و قسمت تصادفی فرستاده می‌شوند.

۳-۲-۱- فاز وارسی رأی

۱. ابتدا رأی‌دهنده V_k مقدار $\mathrm{id}_k^{RA} \| \mathrm{BlindEC}\left(\mathrm{id}_k^{RA}\right) \mathrm{mod} p$ را برای VA می‌فرستد. مسئول تصدیق‌کننده، گواهی‌نامه‌ی مجاز شده توسط RA با کلید عمومی‌اش و اینکه V_k قبلاً رأی داده است یا خیر را بررسی می‌کند. اگر V_k قادر به رأی دادن باشد، V_k و VA مقدار تصادفی $\mathrm{id}_k^{VA} \mathrm{mod} p$ که یک شناسه برای فاز وارسی رأی است تولید می‌کند. رأی‌دهنده V_k الگوریتم $\mathrm{BlindEC}$ را برای به دست آوردن شماره‌ی شناسایی خود راه‌اندازی می‌کند و $\mathrm{id}_k^{VA} \| \mathrm{Blind}(\mathrm{id}_k^{VA})$ را به دست می‌آورد. چون در مرحله‌ی وارسی رأی به علت تصادفی کردن، id_k^{RA} و RA مقادیری هستند که آشکار نمی‌شوند، پس کسی با استفاده از id_{VA}^{RA} قادر به ایجاد ارتباط با رأی‌دهنده نیست.

۲. در ادامه V_k، $\mathrm{id}_k^{VA} \| \mathrm{Blind}(\mathrm{id}_k^{VA})$ را از میان یک کانال دوطرفه‌ی گمنام به VA ارسال می‌کند. حال VA امضا را وارسی کرده و اگر رأی‌دهنده‌ی موردنظر قبلاً عملیات مشابه را انجام نداده باشد $\mathrm{z_k} \in \mathrm{Z_q}$ را از میان همان کانال برای رأی‌دهنده می‌فرستد.

۳. در گام بعدی V_k کاندیدای i-ام مطابق $\mathrm{c_i^{(k)}}$ را از میان BB انتخاب می‌کند. برای ایجاد برگه‌ی رأی $\alpha_k, .. \beta_k, \gamma_k \in Z_q^*$ به‌طور تصادفی انتخاب نمونه و به‌طور تصادفی انتخاب نمونه و به‌طور تصادفی انتخاب نمونه و به‌طور تصادفی انتخاب نمونه و y_k و $(\mathrm{G_k}, \mathrm{H_k} + \mathrm{c_i^{(k)}})$ را به‌صورت زیر محاسبه می‌کند.

$$G_k = (\alpha_k + \beta_k).G mod q \quad (۹)$$

$$H_k = (\alpha_k + \beta_k).H mod q \quad (۱۰)$$

$$y_k = (z_k + \gamma_k).G mod q \quad (۱۱)$$

با تصادفی کردن برگه‌ی رأی توسط B_k، دشمن در صورت تبانی با VA چیزی در مورد برگه‌ی رأی نمی‌فهمد. همچنین y_k نیز نقش مهمی در ایجاد خاصیت بدون رسید بودن بازی می‌کند.

٤. مطابق روابط (۱۲) و (۱۳) V_k یک اثبات صفر دانش غیرتعاملی را اجرا می‌کند که در طی آن رأی‌دهنده نشان می‌دهد که رأی‌دهنده برگه‌ی رأی خود را به‌درستی ایجاد کرده‌است به‌طوری‌که او مقدار $\mathrm{c_i^{(k)}}$ را از لیست موجود در BB انتخاب نموده است. او اعداد تصادفی $\mathrm{r_j}, \mathrm{d_j}, \mathrm{w_k} \in \mathrm{Z_q^*}$ را انتخاب کرده که $1 \le \mathrm{j} \le \mathrm{n}$ و $(\mathrm{A}, \mathrm{B}) = (\mathrm{A_1}, \mathrm{B_1}), \ldots, (\mathrm{A_n}, \mathrm{B_n})$ را محاسبه می‌کند $(\mathrm{i} \ne \mathrm{j})$ که در آن $\mathrm{A_i} = \mathrm{w_k}.\mathrm{G} \mathrm{mod} q$ و $\mathrm{B_i} = \mathrm{w_k}.\mathrm{H} \mathrm{mod} q$ برای کاندیدای انتخاب‌شده‌ی i-ام و

$$A_j = r_j.G + d_j.G_k \ \ modq \quad (۱۲)$$

$$B_j = r_j.H + d_j.(H_k + c_i^{(k)} - c_j^{(k)}) modq \quad (۱۳)$$

را برای تمامی کاندیداها به غیر از کاندیدای i-ام $(i \neq j)$ به دست می‌آورد.

۵. سپس رأی‌دهنده مقدار زیر را محاسبه می‌نماید که با این مقدار نیز به چالش کشیده می‌شود:

$$c_k = H(A_1 \| \cdots \| A_n \| B_1 \| \cdots \| B_n \| G_k \| (H_k + c_i^{(k)}) \| G \| H \| id_k^{VA} \| BlindEC(id_k^{VA})) \quad (۱۴)$$

در ادامه $(D,R) = (d_1, r_1), \cdots, (d_n, r_n)$ که در آن برای کاندیدای i-ام:

$$r_i = w_k - (\alpha_k + \beta_k) + d_i \quad (۱۵)$$

$$d_i = c_k - \sum_{j=1, j \neq i}^{n} d_j \quad (۱۶)$$

۶. بعد از محاسبه‌ی تمامی پارامترها V_k یک عدد تصادفی $\tilde{r} \in Z_p$ را انتخاب و $\tilde{r}.G + y_k modq$ را به دست می‌آورد. از این رو رأی‌دهنده V_k، y_k را از دشمن مخفی می‌نماید.

۷. حال V_k برگه‌ی رأی تصادفی و رمز شده و پارامترها را از میان یک کانال دوطرفه‌ی گمنام برای VA ارسال می‌کند:

$$(A,B) G_k (h_k + c_i^{(k)}) c_k (D,R) id_k^{VA} BlindEC(id_k^{VA}) \| (\tilde{r}.G + y_k) \quad (۱۷)$$

به دلیل استفاده از کانال دوطرفه‌ی گمنام، VA هویت شخص فرستنده را نمی‌فهمد.

۸. بعد از دریافت تمامی پارامترهای موردنیاز VA بررسی می‌کند که آیا رأی‌دهند با id_k^{VA} اثبات صفر دانش را انجام داده است. آیا id_k^{VA} به‌طور صحیح امضاشده است و تساوی‌های زیر را محاسبه می‌کند:

$$c_k = \sum_{j=1}^{n} d_j modq$$

$$A_j = r_j G + d_j G_k \ \ modq \qquad j = 1, \ldots, n$$

$$B_j = r_j.H + d_j.(H_k + c_i^{(k)} - c_j^{(k)}) modq \qquad j = 1, \ldots, n$$

اگر id_k^{VA} به‌طور صحیح امضاشده باشد و قبلاً هم بکار نگرفته شده باشد؛ آنگاه رأی‌دهنده‌ی موردنظر استحقاق رأی دادن را دارد. اگر رأی‌دهنده بتواند چندین اثبات صفر دانش را انجام دهد آنگاه او قادر به پردازش چندین برگه‌ی رأی خواهد بود!

۹. اگر وارسی کردن با موفقیت انجام شود آنگاه اجزا تصادفی را به کار بردن $sigGenEC$ امضا می‌کند. VA مقادیر زیر را محاسبه و ارسال می‌کند. لازم به ذکر است که مقادیر زیر از میان کانال دو گمنام برای فرستنده ارسال می‌گردد.

$$sigGenEC(x_{G_k}) = (S_{x,m_1}, R_{x,1}) \quad (۱۸)$$

$$sigGenEC(x_{H_k + c_i^{(k)} + y_k + \tilde{r}.G}) = (S_{x,m_2}, R_{x,2}) \quad (۱۹)$$

$$sigGenEC(x_{y_k + \tilde{r}.G}) = (S_{x,m_3}, R_{x,3}) \quad (۲۰)$$

$$sigGenEC(y_{G_k}) = (S_{y,m_1}, R_{y,1}) \quad (۲۱)$$

$$sigGenEC(y_{H_k + c_i^{(k)} + y_k + \tilde{r}.G}) = (S_{y,m_2}, R_{y,2}) \quad (۲۲)$$

$$sigGenEC(y_{y_k + \tilde{r}.G}) = (S_{y,m_3}, R_{y,3}) \quad (۲۳)$$

۱۰. رأی‌دهنده امضاهای VA را به‌صورت زیر وارسی می‌کند:

$$sigVerEC(S_{x,m_1}, R_{x,1}, x_{G_k})$$
$$sigVerEC(S_{x,m_2}, R_{x,2}, x_{H_k+c_i^{(k)}+y_k+\tilde{r}.G})$$
$$sigVerEC(S_{x,m_2}, R_{x,3}, x_{y_k+\tilde{r}.G})$$
$$sigVerEC(S_{y,m_1}, y_{G_k})$$
$$sigVerEC(S_{y,m_2}, R_{y,2}, y_{H_k+c_i^{(k)}+y_k+\tilde{r}.G})$$
$$sigVerEC(S_{y,m_2}, y_{y_k+\tilde{r}.G})$$

۳-۲-۲- فاز اخذ رأی

۱. رأی‌دهنده اطلاعات را به‌صورت زیر از کانال عمومی به BB می‌فرستد.

$$id_k^{RA} G_k (S_{x,m_1}, R_{x,1}) \| (S_{y,m_1}, R_{y,1}) \left(H_k + c_i^{(k)} + y_k\right) (S_{x,m_2}, R_{x,2}) \| (S_{y,m_2}, R_{y,2}) \quad (۲۴)$$

و $y_k (S_{x,m_2}, R_{x,3}) \| (S_{y,m_2}, R_{y,3})$ از میان کانال گمنام برای VA می‌فرستد. شکل برگه به‌صورت زیر است:

$$c_i^{(k)} + y_k + H_k = (v_i + z_k + \gamma_k + \alpha_k + \beta_k).G \quad (۲۵)$$

که توسط سیستم الجمال به‌دست‌آمده است که در آن z_k توسط VA از میان کانال گمنام فرستاده‌شده است. از این رو مقدار z_k توسط دشمن شناسایی نمی‌شود.

۲. رأی‌دهنده قدرت بررسی رأی خود را در BB دارد. اگر برگه‌ی رأی او مفقود و یا نادرست باشد او می‌تواند طرح دعوی کند.

۳-۳- مرحله شمارش

۱. مسئول تصدیق‌کننده $Y = \sum_{k=1}^{M} y_k \, mod q$ را محاسبه می‌کند و Y را به BB ارسال می‌کند.

۲. بعد از وارسی اعتبار برگه‌ی رأی رمز شده، موارد زیر محاسبه و در BB ظاهر می‌گردد:

$$\Gamma = \sum_{k=1}^{M} G_k \, mod q \quad (۲۶)$$

و

$$\Lambda = \sum_{k=1}^{M} (H_k + c_i^{(k)} + y_k) mod q \quad (۲۷)$$

۳. بعد از محاسبه‌ی $\Lambda - Y$، نتیجه به‌صورت متن رمز شده در BB ظاهر می‌گردد.

۴.)مسئولین همه باهم نتیجه‌ی $t_1 c_1 + \cdots + t_n c_n$ را با اعمال روش رمزگشایی الجمال محاسبه می‌کنند.

۴- خواص به‌دست‌آمده

۱. استحقاق: مسئول وارسی صحت اعتبارنامه‌ی $Blind(id_k^{RA}) \| \mathrm{id}_k^{RA}$ رأی‌دهنده را بررسی می‌کند و بدین‌صورت استحقاق وی احراز می‌شود.

۲. محرمانگی: برای رمز کردن، رأی تصادفی می‌شود، در سیستم الجمال بکار گرفته‌شده، برای رمزگشایی، همه‌ی مسئولین همه باهم باید این کار را انجام دهند. مطابق این طرح رأی‌دهنده‌ی رأی هرگز نمی‌تواند رمزگشایی را انجام دهد. طبق فرض هم حداقل یکی از مسئولین درست‌کار است، لذا رأی‌ها مخفیانه باقی می‌ماند. رأی $c_i^{(k)}$ بدون دانستن y_k استنباط نمی‌شود. چون در طول فاز وارسی رأی، همه‌ی رأی‌ها تصادفی شده‌اند و قابل اتصال به رأی‌دهنده نیستند مسئول وارسی نمی‌داند که

رأی‌دهنده چه رأیی داده است (حتی اگر VA تمامی اطلاعات را از میان BB بداند و یا اثبات صفر دانش را بفهمد).

۳. عدالت: تعیین نتیجه‌ی نهایی انتخابات منوط به رمزگشایی اطلاعات است و این هم فقط در پایان انتخابات و با همکاری سایر مسئولین میسر است.

٤. وارسی عمومی: بعد از اینکه برگه‌ی رأی معتبر تصادفی شده، تائید شد، رأی‌دهندگان رأی‌های رمز شده را به تابلو اعلانات ارسال می‌کنند. لذا تمامی محاسبات انجام‌گرفته در BB توسط هر مشاهده‌کننده‌ای قابل‌بررسی است.

۵. بدون رسید بودن و عدم امکان اجبار: این خاصیت بر این اساس به دست می‌آید که اثبات کافی برای دشمن برای اینکه رأی‌دهنده چه رأیی داده است وجود ندارد. یک دشمن ممکن است $v_i, c_i, \gamma_k, \alpha_k, BlindEC\left(id_k^{RA}\right), id_k^{RA}$ را بداند، در طول فرآیند رأی‌گیری یک رأی‌دهنده مقدار z_k را دریافت و برگه‌ی رأی را رمز می‌کند:

$$Enc_{\alpha_k}(v_i) = (G_k, H_k + c_i^{(k)} + y_k)$$

که

$$c_i^{(k)} + y_k = (v_i + z_k + \gamma_k).G$$

فرض کنید اجبار کننده دارای رأی درخواستی $v_i^* (\neq v_i)$ باشد و z_k را نداند. آنگاه رأی‌دهنده می‌تواند رأی v_i را واریز نماید به‌طوری‌که اجبار کننده برگه‌ی رأی رمز شده در BB را قبول کند. رأی‌دهنده می‌تواند بگوید که مقدار دریافت شده از VA برابر است با:

$$z_k^* = ((v_i + z_k + \gamma_k - v_i^*) - \gamma_k \qquad (۲۸)$$

لذا با به‌کارگیری آن مقدار $(c_i^{(k)})^* + y_k$ که $(c_i^{(k)})^* = v_i^*.G$ بوده به‌صورت زیر است:

$$(v_i^* + z_k^* + \gamma_k).G = (v_i^* + v_i + z_k + \gamma_k - v_i^* - \gamma_k + \gamma_k).G = (v_i + z_k + \gamma_k).G$$

مقدار y_k هرگز در BB ظاهر نمی‌شود و آن در طول زمان رأی‌گیری از میان کانال گمنام برای VA بدون هر شماره‌ی شناسایی فرستاده می‌شود. همچنین VA می‌تواند این وارسی را بررسی کند اما با رأی‌دهنده ارتباط برقرار نمی‌کند. در مقایسه با طرح رأی‌گیری در [۱۷] طرح پیشنهادی دارای این خاصیت مهم است و طرح بیان‌شده در [۱۷] فاقد این خاصیت است و ازاین‌رو باوجود سرعت نسبی بهتر، طرح پیشنهادی با هزینه محاسباتی بیشتر این خاصیت مهم را برآورده می‌سازد.

۵- محاسبه‌ی پیچیدگی

طبق [۱۶] یک خم بیضوی $E(Fq)$ با نقطه‌ی مولد $G \in E(Fq)$ از مرتبه‌ی ۱۶۰ بیتی دارای امنیتی معادل با سیستم ۱۰۲۴ بیتی مبتنی بر تجزیه اعداد است. در جدول شماره ۱ انواع عملگرها و در جدول شماره ۲ پیچیدگی زمانی عملگرهای واقع در گروه خم بیضوی ۱۶۰ بیتی بر اساس عملگر ضرب اعداد معمولی ۱۰۲۴ بیتی بیان‌شده است.

جدول ۱: نمادهای بکار رفته در محاسبه پیچیدگی

تعریف نماد	نماد
پیچیدگی زمانی عملگر ضرب معمولی	$T_{MUL}(p)$
پیچیدگی زمانی جمع معمولی	$T_{ADD}(p)$
پیچیدگی زمانی توان رسانی	$T_{EXP}(p)$
پیچیدگی زمانی معکوس گیری	$T_{INV}(p)$
پیچیدگی زمانی ضرب اسکالر در یک نقطه خم بیضوی	$T_{EC-MUL}(p)$
پیچیدگی زمانی جمع دو نقطه خم بیضوی	$T_{EC-ADD}(p)$

جدول ۲: پیچیدگی زمانی عملگرهای خم بیضوی بر اساس عملگرهای معمولی [۱۶]

پیچیدگی زمانی بر اساس پیچیدگی عملگر ضرب اعداد	پیچیدگی زمانی عملگرهای واحد
$۲۴۰\times T_{MUL}(۱۰۲۴)$	$T_{EXP}(۱۰۲۴)$
ناچیز	$T_{ADD}(۱۰۲۴)$
$۳\times T_{MUL}(۱۰۲۴)$	$T_{INV}(۱۰۲۴)$
$۲۹.۳\times T_{MUL}(۱۰۲۴)$	$T_{EC-MUL}(۱۶۰)$
$۰.۱۲\times T_{MUL}(۱۰۲۴)$	$T_{EC-ADD}(۱۶۰)$
$۰.۰۲۴\times T_{MUL}(۱۰۲۴)$	$T_{MUL}(۱۶۰)$
ناچیز	$T_{ADD}(۱۶۰)$
$۰.۰۷۳\times T_{MUL}(۱۰۲۴)$	$T_{INV}(۱۶۰)$

در جدول شماره ۳ پیچیدگی تمامی مراحل و الگوریتم‌های موجود در این مقاله بر اساس جدول شماره‌ی دو مبتنی بر اعمال یادشده در آن، آورده شده است.

جدول ۳: محاسبه پیچیدگی الگوریتم‌های بکار رفته در طرح پیشنهادی

پیچیدگی زمانی بر اساس پیچیدگی عملگر ضرب اعداد ۱۰۲۴ بیتی	الگوریتم یا مرحله‌ی رأی‌گیری
$۸۳\times T_{MUL(۱۰۲۴)}$	سیستم الجمال هم‌ریخت در خم بیضوی
$(۳۰\times N-۰.۱۲)\times T_{MUL(۱۰۲۴)}$	مولد کلید الجمال با N مسئول
$۳۰\times(N)\times T_{MUL(۱۰۲۴)}$	رمزگشایی الجمال با N مسئول
$۸۹\times T_{MUL(۱۰۲۴)}+complexity\ of\ \ hash\ function$	الگوریتم SigGenEC
$۱۴۸\times T_{MUL(۱۰۲۴)}+complexity\ of\ \ hash\ function$	الگوریتم BlindEC
$(۱۴۸+n\times۲۹.۳)\times T_{MUL(۱۰۲۴)}+complexity\ of\ \ hash\ function$	مرحله احراز هویت با n نامزد
$(۶۸۲+۵۸.۶+n\times۲۳۵.۱۲)\times T_{MUL(۱۰۲۴)}+complexity\ of\ \ hash\ function$	مرحله رأی‌گیری با n نامزد
$(۰.۳۶M+۳۰N)\times T_{MUL(۱۰۲۴)}$	مرحله شمارش آرا با M رأی‌دهنده و N مسئول

۶- نتیجه‌گیری

در این مقاله، بعد از بیان خواص مطلوب یک انتخابات الکترونیکی، پروتکل ایرادشده توسط هوزتی را بر اساس سختی مسئله‌ی لگاریتم گسسته‌ی خم بیضوی تغییر دادیم که از خواص رمزنگاری هم‌ریخت در گروه جمعی خم بیضوی استفاده می‌کند. همچنین این طرح از امضای کور پیشنهادی و امضای دیجیتالی در خم بیضوی استفاده می‌کند. این طرح بدون رسید است لذا در آن امکان فروش رأی منتفی می‌گردد.

مراجع

[1] K. Sampigethaya and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," *computers & security*, vol. 25, no. 2, pp. 137-153, Mar. 2006, doi: 10.1016/j.cose.2005.11.003.

[2] A. Huszti, "A homomorphic encryption-based secure electronic voting scheme," *Publ. Math. Debrecen*, vol. 79, no. 3, pp. 479-496, Jan. 2011, doi: 10.1016/j.cose.2005.11.003.

[3] A. Sghaier, M. Zeghid, C. Massoud and M. Machout, "Design and implementation of low area/power elliptic curve digital signature hardware core," *Electronics*, vol. 6, no. 2, pp. 24-46, Jun. 2017, doi: 10.3390/electronics6020046.

[4] Q. Li, C. Hsu, D. He, KK. Choo and P. Gong, "An identity-based blind signature scheme using lattice with provable security," *Mathematical Problems in Engineering*, vol. 2020, pp. 1-12, May 2020, doi: 10.1155/2020/7528571.

[5] M. Monira, A. Ayman, M. Mazen and H. Hala, "Blind Signature Schemes based on ElGamal Signature for Electronic Voting: A Survey," *International Journal of Computer Applications*, vol. 180, no. 30, pp. 21-28, Apr. 2018, doi: 10.5120/ijca2018916766.

[6] L. Jihong and X. Guozhen, "Remarks on new signature scheme based on two hard problems," Electronics Letters, vol. 34, no. 25, pp. 1-24, Dec. 1998, doi: 10.1049/el:19981657.

[7] H. Mala and N. Nezhadansari, "New blind signature schemes based on the (elliptic curve) discrete logarithm problem," in *ICCKE IEEE*, 2013, pp. 196-201, doi: 10.1109/ICCKE.2013.6682844.

[8] K. Peng, R. Aditya, C. Boyd, E. Dawson and B. Lee, "Multiplicative homomorphic e-voting," in *International Conference on Cryptology in India*, 2004, pp. 61-72, doi: 10.1007/978-3-540-30556-9_6.

[9] H. Jonker, S. Mauw and J. Pang, "Privacy and verifiability in voting systems: Methods, developments and trends," *Computer Science Review*, vol. 10, no. 1, pp. 1-30, Nov. 2013, doi: 10.1016/j.cosrev.2013.08.002.

[10] B. Lee and K. Kim, "Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer," in *International Conference on Information Security and Cryptology*, 2002, pp. 389-406, doi: 10.1007/3-540-36552-4_27.

[11] KR. Iversen, "A Cryptographic Scheme for Computerized General Elections," in *Annual International Cryptology Conference*, 1991, pp. 405-419, doi: 10.1007/3-540-46766-1_33.

[12] C. Park, I. Kazutomo and K. Kaoru, "Efficient anonymous channel and all/nothing election scheme," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1993, pp. 248-259, doi: 10.1007/3-540-48285-7_21.

[13] D. Chaum, "Secret-ballot receipts: true voter-verifiable elections," *IEEE Security & Privacy Magazine*, vol. 2, no. 1, pp. 38-47, Jan. 2004, doi: 10.1109/msecp.2004.1264852.

[14] K. Sako and J. Kilian, "Receipt-free mix-type voting," in *Proceedings of EUROCRYPT95*, 1995, pp. 393-403, doi: 10.1007/3-540-49264-X_32.

[15] AK. AbdulRahim, O. Folorunso and S. Sharma, "An Improved Dynavote E-Voting Protocol Implementation," *International Journal of E-Adoption*, vol. 3, no. 3, pp. 44-61, Jul. 2011, doi: 10.4018/ijea.2011070104.

[16] N. Koblitz, A.J. Menezes and S. Vanstone, "The state of elliptic curve cryptography," *Designs, codes and cryptography*, vol 19, no. 2, pp. 173-193, Mar. 2000, doi: 10.1023/A:1008354106356.

[17] A. Waheed, N. Din, AI. Umar, R. Ullah and U. Amin, "Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves," Mehran University Research Journal of Engineering and Technology, vol. 40, no. 2, pp. 314-322, Apr. 2021, doi: 10.22581/muet1982.2102.06.

زیرنویس‌ها

[1] Eligibility
[2] Privacy
[3] Fairness
[4] Individual and Universal verifiability
[5] Receipt-freeness
[6] Uncoercibility
[7] Andrea Huszti
[8] Correctness
[9] Ompletentss
[10] Soundness
[11] Mix-net
[12] Blind signature
[13] Homomorphic encryption
[14] Registry authority
[15] Bulletin board
[16] Anonymous channel
[17] Elliptic Curve Discrete Logarithm