
يا الله
وعلى الله فليتوكل المتوكلون

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات

بهبود رای گیری اینترنتی با استفاده از ظرفیت های جاوا کارت

مصطفی محمد پور فرد

استاد راهنما:

جناب آقای دکتر دوستاری

استاد مشاور:

جناب آقای دکتر غزنوی

آذر ۱۳۹۲

تقدیم به

پدر و مادرعزیزم

خدای را بسی شاکرم که از روی کرم پدر و مادری فداکار نصیبم ساخته تا در سایه درخت پر بار وجودشان بیاسایم و از ریشه آنها شاخ و برگ گیرم و از سایه وجودشان در راه کسب علم ودانش تلاش نمایم.

والدینی که بودنشان تاج افتخاری است بر سرم و نامشان دلیلی است بر بودنم چرا که این دو وجود پس از پروردگار مایه هستی ام بوده اند دستم را گرفتند و راه رفتن را در این وادی زندگی پر از فراز و نشیب آموختند.

آموزگارانی که برایم زندگی؛ بودن و انسان بودن را معنا کردند

حال این برگ سبزی است تحفه درویش تقدیم آنان....

تشکر و قدردانی

سپاس خدای را که سخنوران در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و دورد بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

بدون شک جایگاه و منزلت معلم، اجّل از آن است که در مقام قدردانی از زحمات بی شائبه ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم.

اما از آنجایی که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تامین می کند و سلامت امانت هایی را که به دستش سپرده اند، تضمین؛ بر حسب وظیفه و از باب " من لم یشکر المنعم من المخلوقین لم یشکر اللّه عزّ و جلّ: "

ازپدر و مادر عزیزم...این دو معلم بزرگوارم... که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از کنار غفلت هایم گذشته اند و در تمام عرصه های زندگی یار و یاوری بی چشم داشت برای من بوده اند؛

از استاد با کمالات و شایسته؛ جناب آقای دکتر **دوستاری** که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این رساله را بر عهده گرفتند؛

از استاد صبور و با تقوا ، جناب آقای دکتر **غزنوی** که زحمت مشاوره این رساله را در حالی متقبل شدند که بدون مساعدت ایشان، این پروژه به نتیجه مطلوب نمی رسید؛

و از اساتید فرزانه و دلسوز؛ جناب آقایان دکتر **حاج سید جوادی** و دکتر **یزدیان** که زحمت داوری این رساله را متقبل شدند؛ کمال تشکر و قدردانی را دارم.

باشد که این خردترین، بخشی از زحمات آنان را سپاس گوید

چکیده

اخیراً رأی گیری اینترنتی به دلیل سرعت، شمارش اتوماتیک، کاهش هزینه، امکان خطای کم، حضور بیشتر در انتخابات و شفافیت زیاد، محبوبیت زیادی کسب کرده است اما چالش های موجود برای پیاده سازی یک سیستم رأی گیری امن قابل توجه هستند. اگر این سیستم ها به دقت طراحی و پیاده سازی نشوند باعث تضعیف شدن اعتماد رای دهندگان به کل فرآیند رای گیری خواهد شد. در این پژوهش یک پروتکل رأی گیری اینترنتی طراحی و پیشنهاد گردیده است که نیازمندیهای امنیتی مطلوب یک سیستم رای گیری را تضمین می کند.

اگرچه سیستم های رأی گیری اینترنتی قابلیت جا بجایی رأی دهنده را با فراهم کردن امکان رأی دادن رأی دهنده با استفاده از کامپیوتر های شخصی فراهم می کنند، اما آنها در مقابل بد افزار ها و حملات پیچیده شبکه ای بسیار آسیب پذیر هستند. ناامن بودن پلتفرم سمت رأی دهنده، یکی از بزرگترین موانع پیاده سازی سیستم های رأی گیری اینترنی می باشد که می تواند به منجر فاش شدن هویت رأی دهنده شود و هم چنین کل فرآیند رأی گیری را تحت تاثیر قرار می دهد. بنابراین، ما جایگزینی را برای پلتفرم ناامن سمت رای دهنده ارائه می کنیم. جاوا کارت ۳ آخرین نسخه جاوا کارت می باشد که می تواند به عنوان وب سرور امن قابل حمل رأی دهنده در نظر گرفته شود. جاوا کارت ۳ می تواند آدرس آیپی بگیرد و به عنوان گره ای از شبکه با گره های دیگر از طریق HTTP/ HTTPS ارتباط برقرار کند. جاوا کارت ۳ می تواند چالش های امنیتی را که بوسیله ناامن بودم کامپیوتر های رأی دهندگان به وجود آمده است را حل کند. بنابراین، در این پژوهش علاوه بر ارائه یک پروتکل امن رأی گیری اینترنتی، برای تضمین امنیت سمت رای‌دهده از ایده جاوا کارت۳ بعنوان جایگزینی امن برای ترمینال‌های رای‌گیری استفاده شده است. هم چنین، پیاده سازیی از پروتکل پیشنهادی نیز با استفاده از جاوا کارت ۳ ارائه شده است.

کلید واژه:

رای‌گیری اینترنتی، جاوا کارت ۳، اجبار، تبانی، تکنولوژی جاوا، پلتفرم ناامن سمت رأی دهنده

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

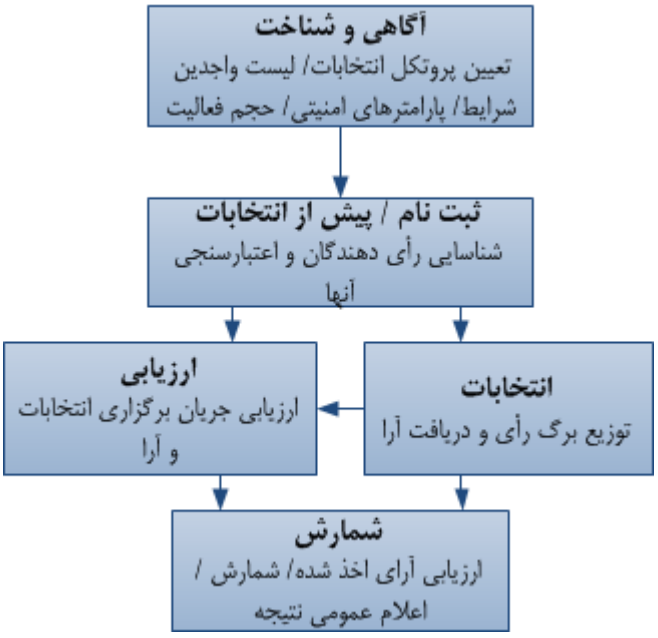
فصل ۱– مقدمه

۱–۱– پیشگفتار

در سال های اخیر، با توسعه زیر ساخت های شبکه در سراسر دنیا، سرویس های الکترونیکی، تعاملات شهروندان با نهادهای دولتی را آسانتر و در عین حال سرعت بخشیده است. رای گیری الکترونیکی یکی از جالب ترین سرویس ها در میان سرویس های الکترونیکی می‌باشد. کارایی، شفافیت، مشارکت و دقت برخی از مزایای رای گیری الکترونیکی می باشد[۱]. رای‌گیری اینترنی که از رای گیری الکترونیکی مشتق شده است، شهروندان را قادر می سازد بدون نیاز به حضور فیزیکی در جایگاه‌های رای‌گیری درانتخابات شرکت کنند. این مهم ترین دستاورد رای گیری اینترنتی می باشد. پیاده‌سازی این موضوع مستلزم آماده‌سازی بسترهای لازم از جمله بکارگیری کارت هوشمند و نظایر آن است.

انتخابات به روش اینترنتی عموماً از مدل شکل ۱ تبعیت می‌کند و تنها با توجه به مسائل مختلف موجود در شرایط برگزاری و برگزار کننده، نحوه پیاده سازی آن متفاوت خواهد بود. می توان مراحل این انتخابات را به شکل زیر بیان کرد:

- آگاهی و شناخت: در این مرحله پروتکل‌ها تعریف شده، لیست واجدین شرایط شرکت در انتخابات استخراج گردیده و پارامترهای امنیتی و حجم فعالیت توسط مراجع قانونی مشخص می‌شود.
- ثبت نام: در این مرحله رأی دهندگان شناسایی و بوسیله مراجع قانونی اعتبار سنجی می‌شوند.
- برگزاری انتخابات: در این مرحله برگ رأی توزیع و واجدین شرایط رأی خود را ارائه می‌نمایند.
- ارزیابی: این مرحله همراه با مرحله قبل آغاز می‌شود و تا پایان انتخاب ادامه دارد در این مرحله سلامت برگزاری انتخابات کنترل می‌شود.
- شمارش: در این مرحله آرا صحت سنجی، شمارش و نتیجه اعلام می‌شود.



شکل ۱ : مدل کلی انتخابات الکترونیکی[۲]

از آنجائیکه رای گیری اینترنتی روی اینترنت انجام می شود و رای دهندگان تحت نظر و کنترل فیزیکی نیستند، پیاده سازی آن باید در مقابل انواع حملات مقاوم باشد تا از نظر رای دهندگان امن فرض شود. سیستم های رای گیری اینترنتی در مقابل دو دسته از حملات آسیپ پذیر هستند. حملات به کلاینت ها / سرور ها و حملات به زیر ساخت های ارتباطی. یکی از مهم ترین مشکلات جاری در طراحی سیستم های رای گیری اینترنتی نا امن بودن پلتفرم سمت رای دهنده می باشد[۳].

آلوده بودن کامپیوترهای سمت رای دهندگان به بد افزار ها[۱] و آسیب پذیری آنها در مقابل حملات مانع بزرگی در پیاده سازی سیستم های رای گیری اینترنتی می باشد[۴, ۵]. حمله کنندگان می توانند از این اسیب پذیری ها استفاده کنند و امنیت سیستم رای گیری را بشکنند. نفوذ به سیستم رای گیری در سمت کلاینت بسیار امکان پذیر تر از سمت سرور می باشد. برای مثال در[۶] حمله کننده به راحتی با هک کردن ماشین سمت رای دهنده توانسته است سیستم رای گیری Helios [۷]را که اولین سیستم رای گیری حسابرسی باز بر پایه وب[۲] بود را بشکند. اکثر پروتکل های پیشنهادی برای رای گیری، پلتفرم سمت رای دهنده را امن فرض می کنند[۸]. این فرضیه، برای تضمین فاش نشدن هویت رای دهنده و تضمین یکپارچگی انتخابات می باشد[۹]. اما از آنجائیکه کامپیوتر ها در مقابل حملات سایبری و بد افزار ها آسیب پذیرند، این فرضیه قابل اجرا نیست. بنابراین برای حل این مشکل ما از جاوا کارت ۳ استفاده نموده ایم که می تواند امنیت مطلوب را در سمت کلاینت برای ما تامین کند.

در این فصل ابتدا به نیازمندی‌ها امنیتی سیستم‌های رای‌گیری الکترونیکی پرداخته می شود. در ادامه، اهداف و مراحل پیاده سازی پژوهش بیان شده و خلاصه ای از آنچه که در این پروژه انجام شده است را مرور می‌کنیم. در انتها عناوین و خلاصه‌ای از محتوای فصول بعد را به اختصار بیان می‌نماییم.

۱-۲- رای گیری اینترنتی و نیازمندی های امنیتی

اگرچه پروتکل های رای گیری الکترونیکی ویژگی‌های بسیار جالبی را ارائه می کند، اما ذات الکترونیکی بودن آنها، به هر حال نگرانی‌های امنیتی را مطرح می‌کند که باید مورد توجه قرار گرفته تا اعتبار انتخابات تضمین گردد. علیرغم این واقعیت که استاندارد مشخصی برای تعیین تمام پیش‌نیازهای امنیتی وجود ندارد، اکثر طرح‌های پیشنهادی در این زمینه بر نیاز های زیر تاکید دارند[۱۰-۱۳]:

۱. قابلیت حرکت[۳]: محدودیتی روی مکان رای دادن برای رای‌دهندگان وجود نداشته باشد.

۲. گمنامی : کسی نتواند رایی را به یک رای دهنده خاص نسبت دهد.

۳. دموکراسی: فقط رای‌دهندگان واجد شرایط می‌توانند رای بدهند (یعنی رای‌دهندگان ثبت‌نام‌شده) و این رای‌دهندگان فقط یک بار می‌توانند رای بدهند.

۴. دقت و صحت: فقط آرای معتبر شمرده شوند. هم‌چنین تغییر، حذف و اضافه کردن رای ممکن نباشد.

۵. اثبات پذیری: اثبات پذیری در دو فرم اثبات پذیری فردی و عمومی بیان می شود:

---

[۱] Malwares

[۲] Web based open audit voting

[۳] Mobility

- عمومی[1]: همه شهروندان می توانند صحت کل انتخابات را بازبینی کنند.
- فردی[2]: هر رای‌دهنده باید بتواند چک کند که رایش به درستی جمع آوری و شمرده شده است.

۶. بی طرف بودن: قبل از اتمام انتخابات رای دهندگان و واحد های انتخاباتی از نتایج آراء اطلاع پیدا نکنند.

۷. رای‌دادن و رفتن[3]: نیازی به مداخله رای‌دهنده در مرحله شمارش نباشد.

۸. مقاوم در برابر تبانی: در این پژوهش تبانی از دو منظر تازه بررسی شده است:

- نقض ویژگی گمنامی و پی بردن به هویت رای دهنده
- رای دادن به جای رای دهنده واجد شرایط اما غائب

۹. مقاومت در مقابل اجبار[4] و خرید و فروش رای: هیچ رای دهند ه ای نتواند اثبات کند که به گونه ای خاص رای داده است. به عبارت دیگر ردیابی رای دهنده امکان پذیر نباشد و رای دهنده نتواند به دیگران ثابت کند که به یک کاندید خاص رای داده است. از انجائیکه در رای گیری اینترنتی رای دهنده می تواند از هر ترمینالی و بدون نظارت واحد انتخاباتی رای دهد، اجبار و خریدو فروش تهدیدات مهمی می باشند.

۱۰. قابلیت شروع دوباره: رای دهنده بتواند فرایند رای گیری را از نقطه ای که وقفه ایجاد شده است پیگیری کند.

۱۱. تنومندی[5] : می تواند از دو جنبه متفاوت بحث شود:

- مقاومت سیستم در برابر نقص ها و شکست ها
- رای دهنده بد خواه نتواند روند انتخابات را برهم زند

۱۲. امنیت پلتفرم سمت رای دهنده: پلتفرم سمت رای دهنده باید کاملا امن باشد تا گمنامی را هنده و صحت ویکپارچگی انتخابات تضمین شود.

۱۳. پیگیری شکایات: یکی از اصلی ترین اصول رای گیری اینترنتی پیگیری شکایت می باشد. از انجائیکه رای گیری اینترنتی به صورت آنلاین انجام می شود، ممکن است بدگمانی و تردید هایی برای رای دهندگان به وجود اید که شاید بر روی اعتماد آنها تاثیر بگذارد. یک راه حل خوب برای بازگرداندن اعتماد استفاده ازمکانیزم ساده پیگیری شکایت برای پاسخ به شکایات رای دهندگان است.

۱۴. کارایی: محاسبات در زمان منطقی قابل انجام باشد.

---

[1] Public verifiability

[2] Individual verifiability

[3] Vote and go

[4] Coercion

[5] Robustness

خرید و فروش رای، تبانی، اجبار، ناامن بودن پلتفرم سمت رای دهنده، بی طرفی از چالش های اصلی رای گیری اینترنتی می باشند که باعث شکست سیستم‌ها و پروتکل‌های رای‌گیری الکترونیکی و اینترنتی می‌شوند. در این پژوهش به این چالش ها پرداخته و راه حل هایی برای آنها ارائه خواهیم کرد.

۱–۳– هدف از انجام پروژه

هدف اصلی این پروژه ارائه سیستم رای گیریی است که ویژگی های ذکر شده در بخش ۲-۱ را تضمین نماید. در بین این ویژگی ها تاکید اصلی ما بر روی امن کردن سمت کلاینت و تضمین ویژگی هایی چون تبانی، اجبار، بی طرفی، خرید و فروش رای است. ناامنی کامپیوترهای رای دهندگان یکی از دلایل اصلی به تعویق افتادن پیاده سازی و استفاده از رای گیری اینترنتی در دنیای واقعی می باشد. . در واقع بدون وجود پلتفرم امن برای رای دهنده، هیچ پروتکلی در پیاده سازی در دنیای واقعی نخواهد توانست امنیت ادعا شده برای سیستم رای گیری پیشنهادی را تامین کند. به صورت خلاصه می توان هدف از انجام پروژه را موارد زیر دانست:

۱. ارائه راه حلی برای امن کردن سمت کلاینت
۲. ارائه یک پروتکل رای‌گیری اینترنتی مقاوم در برابر تبانی، خرید و فروش و و اجبار و بی‌طرفی

۱–۴– ساختار پژوهش

فصل۲:

این فصل، به بررسی انواع روش های رمز نگاری استفاده شده در سیستم های رای گیری الکترونیکی می پردازد. سپس پروتکل های شناخته شده موجود بررسی شده اند و در نهایت به بررسی وضعیت رای گیری الکترونیکی در کشور های مختلف پرداخته شده است.

فصل۳:

در این فصل به معرفی تکنولوژی جاوا کارت و جاوا کارت ۳ می‌پردازیم و کاربردهای این تکنولوژی در حوزه‌های امنیتی را مطالعه و تحلیل می‌نماییم.

فصل۴:

زبان (Java Information Flow (Jif را معرفی و بررسی می کند.

فصل ۵:

به بررسی پروتکل پیشنهادی بر پایه جاوا کارت ۳ و Jif و پیاده سازی و تحلیل آن می پردازد.

فصل ۲–پروتکل های رای گیری الکترونیکی موجود

۲–۱– مقدمه

در این فصل از این پژوهش، به بررسی چند پروتکل پیشنهادی رای گیری الکترونیکی خواهیم پرداخت.

۲–۲– انواع سیستم های رای‌گیری الکترونیکی

اکثر پروتکل های رای گیری اینترنتی پیشین از سه تکتنیک رمزنویسی[۱] برای حل مشکلات امنیتی استفاده می کنند. بنابراین، می توانیم این پروتکل ها را در سه دسته طبقه بندی کنیم: پروتکل هایی که از شبکه های مختلط، رمز نگاری هم ریخت، امضای کور استفاده می کنند.

۲–۲–۱– شبکه های مختلط[۲]

مفهوم شبکه های مختلط برای اولین بار توسط چائوم[۱۴] در سال ۱۹۸۱ مطرح شد. از آن زمان به بعد، برخی از پروتکل های رای گیری پیشنهادی از این روش استفاده کرده اند[۱۵, ۱۶]. این طرح رای گیری بر اساس جایگشت تصادفی رای ها برای تضمین گمنامی در رای گیری می باشد. در این روش یک لیست مرتب از رای ها از طریق شبکه ای از مسئولین[۳]، که هر مسئول لیست را با یک جایشگت مخفی برهم می زند، می فرستد. N سرور M_1، M_2، M_3 و ... هر یک با کلید عمومی خودش E_j وجود دارد. زمانیکه کسی می خواهد رایی را بفرستد، رای فرستاده شده m بار رمز می شود :

$E1\ (E2\ (\ldots E_n\ (m))\ldots)$

و سپس به M_1 فرستاده می شود. M_1 صبر می کند تا تمامی پیام ها برسد.، سپس لایه اول رمز نگاری را حذف می کند و با انجام جایگشتی بر روی آن، آنرا به M_2 می فرستد. این رویه برای همه سرور ها تکرار می شود. سرور نهایی پیام را به گیرینده تحویل می دهد. به هر حال، این سیستم از هزینه بالای ارتباطی و محاسباتی رنج می برد. تاکنون هیچ انتخاباتی بر پایه شبکه های مختلط پیاده سازی نشده است[۱۰].

۲–۲–۲– رمز نگاری همریخت[۴]

در کنار شبکه های مختلط، رمز نگاری همریخت یک روش دیگر برای حفظ ویژگی گمنامی در سیستم های رای گیری اینترنتی می باشد. پروتکل هایی که از رمز نگازی همریخت استفاده کردند بسیار محبوب تر از تکنیک شبکه های مختلط می باشند. رمز نگاری همر یختی اجازه انجام عملیلت پیچیده ریاضی بر روی داده رمز شده را بدون به خطر افتادن الگوریتم رمز نگاری را می دهد. برای مثال، یک شخص می تواند ۲ عدد رمز شده را جمع کند و شخص دیگر می تواند نتیجه را رمز گشایی کند، بدون اینکه قادر به فهمیدن

---

[۱] Cryptographic

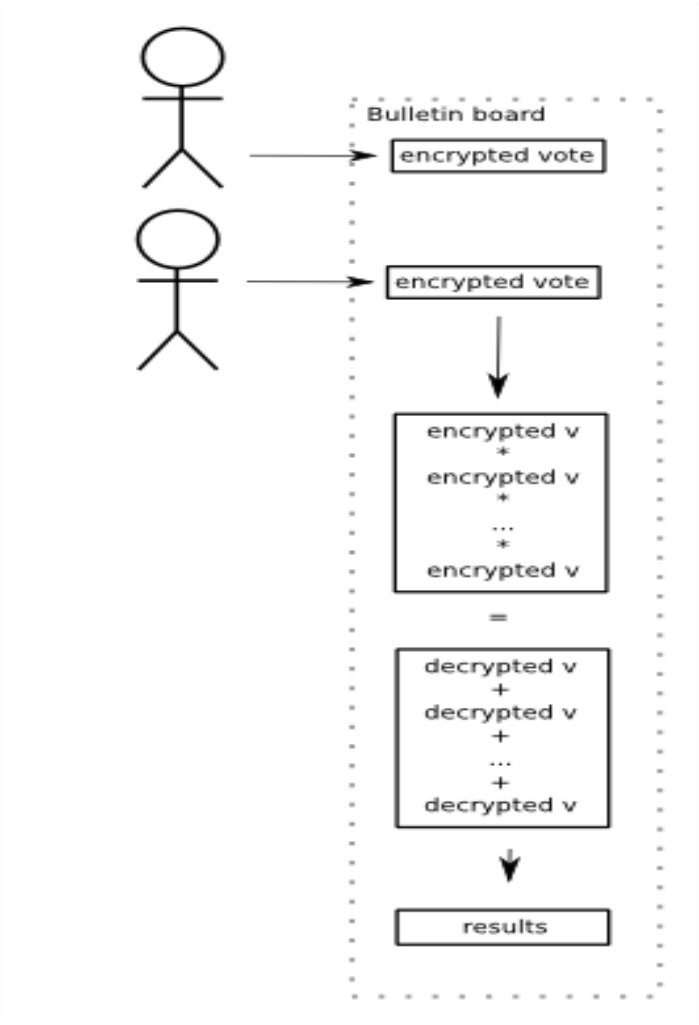
[۲] Mix-net

[۳] Authorties

[۴] Homomorphic Encryption

مقدار واقعی اعداد به صورت جداگانه باشد. فرض کنید اعداد ما ۵ و ۱۰ باشند. که بعد از رمز نگاری به ترتیب به ۱۰ و ۲۰ تبدیل می شوند (عمل رمزنگاری، ضرب در ۲ می باشد). شخص اول اعداد را جمع می کند (۳۰) و به شخص دوم می دهد. شخص دوم با رمز گشایی به عدد ۱۵ ، حاصل جمع اعدا اصلی می رسد بدون اینکه از مقدار هر یک از دو عدد اطلاع داشته باشد.این روش یک خاصیت جالب در رای گیری دارد:

اگر شما رای های رمز شده را با هم ضرب کنید و سپس نتیجه را گرفته و رمز گشایی کنید، همان نتیجه را بدست خواهید که از طریق رمز گشایی همه رای و سپس جمع آنها بدست خواهید آورد. قانون اصلی در این روش اینست که لازم نیست هر رای را رمز گشایی کرده و نتیجه را با استفاده از رای های رمز شده می سازد. از انجائیکه رای ها به صورت فردی رمز گشایی نمی شوند، ویژگی گمنانی تضمین شده است.



شکل ۲: رمز نگاری هم ریختی[۱۷]

اما این روش نیز همانند شبکه های مختلط برای انتخابات با مقیاس بزرگ نامناسب هستند. دلیل آن هزینه های بالای محاسباتی و ارتباطی بالا ناشی از تائید و اثبات اعتبار رای زمانیکه تعداد کاندید ها زیاد باشند، است[۱].

۲-۲-۳- امضای کور

این روش گمنامی را بدون نیاز به اپراتور های پیچیده محاسباتی و هزینه های بالای ارتباطی تضمین می کند. تا کنون پروتکل های زیادی براساس امضای کور پیشنهاد شده اند[۱۳, ۱۸]. برخی از آنها از این

تکنیک برای مخفی کردن محتوای رای و برخی برای مخفی کردن اطلاعات شناسایی رای دهنده استفاده کرده اند. امضای کور به ما این امکان را می دهد که یک شخص پیامی را امضا کند بدون اینکه محتوای آن را بداند.

یک راه ساده برای پیاده سازی امضای کور[1] استفاده از سیستم رمز RSA است. ما از علائم زیر برای توضیح امضای کور استفاده کرده ایم:

- A, B: entity
- m: message
- d: the private key of signer entity
- e, n: the public key
- r: a random number which satisfy gcd*(r,N)* = 1
- s: the signature of m
- r^e mod n: blinding factor

دارنده پیام عدد r را انتخاب می کند. او پیام m را با استفاده از $r^e \bmod n$ کور می کند و سپس پیام کور شده را می فرستد. طرف مقابل با دریافت کردن پیام، امضا شده آن را بر می گرداند.

1. $A \rightarrow B$: $m' \equiv m.r^e \pmod N$
2. $B \rightarrow A$: $s' \equiv (m')^d \bmod N$

با توجه به رابطه ۳، A می تواند امضای s را بدست آورد:

3. $A \rightarrow A$: $s \equiv s'.r^{-1} \bmod N \equiv (m.r^e)^d.r^{-1} \bmod N \equiv (m^d.r^{ed}).r^{-1} \bmod N \equiv (m^d.r).r^{-1} \bmod N \equiv m^d \bmod N$

با توجه به اینکه B از r اطلاعی ندارد نمی تواند از m' به m برسد.

۲-۳- برخی از پروتکل های موجود

در این بخش به بررسی چند پروتکل پیشنهادی شناخته شده برای رای گیری الکترونیکی می پردازیم.

۲-۳-۱- FOO

پروتکل FOO[19] سه عامل اصلی دارد:

- رای‌دهنده(Voter)
- ارزیاب (Validator)
- برگزار کننده(Tallier)

برای درک هر چه بهتر این پروتکل علائم بکار رفته را به ترتیب زیر تعریف می نماییم:

- V (Validator): ارزیاب
- T (Tallier):برگزار کننده
- P (Pollster): رای‌دهنده
- Id: شناسه رای‌دهنده

[1] Blind signature

- b (Ballot): برگ رای
- (e,d): کلید عمومی و خصوصی رای‌دهنده
- (ev, dv): کلید عمومی و خصوصی ارزیاب
- R: فاکتور کورکنندگی
- BB (Bulletin Board): تابلو اعلانات عمومی

فازهای پروتکل FOO به شرح زیر خلاصه می‌شوند. لازم به ذکر است که در پروتکل FOOراجع به نحوه پیاده سازی و ثبت نام رای‌دهندگان مجاز در فاز ثبت‌نام توضیحی داده نشده است و تنها فرض شده است که رای‌دهندگان پیش از انتخابات ثبت‌نام می‌شوند. بدین ترتیب تنها سه فاز رای‌گیری، جمع‌آوری و شمارش آرا در ذیل بیان می‌گردد.

فاز پیش از انتخابات: همچون اکثر پروتکل‌ها در این پروتکل نیز، رأی‌دهندگان در یک مرحله قبل از برگزاری انتخابات، در انتخابات ثبت‌نام کرده و زوج کلید مخصوص انتخابات دریافت می‌نمایند. کلید خصوصی رای‌دهنده تا زمان اتمام انتخابات محرمانه نزد وی می‌ماند. در این پروتکل محدودیتی و یا توضیحی راجع به محل ذخیره کلیدهای رمزنگاری و هم چونین ماژولی که می‌خواهد از این کلیدها استفاده نماید، وجود ندارد.

فاز رای‌گیری:در زمان برگزاری انتخابات رأی‌دهنده، رأیِ خود را با کلید عمومیِ خود، رمز(b^e=B) و کور کرده ($B*R^{ev}$) و پس از امضا با کلید خصوصی ویژه‌ی انتخابات خود، آن را برای سنجش اعتبار به ارزیاب تحویل می‌دهد.

$P \rightarrow V: \quad ((B*R^{ev})+ Id)^d$

ارزیاب علاوه بر کنترل امضا، بررسی می‌کند آیا رای‌دهنده در لیست رأی‌دهندگان مجاز وجود دارد یا خیر، در صورت تایید رأی را امضا کرده و به رای‌دهنده عودت می دهد (ارزیاب فقط کلید عمومی رای‌دهنده را می داند).

$V \rightarrow P: \quad (B*R^{ev})^{dv}$

سپس رای‌دهنده رای را از حالت کور خارج نموده و بدین ترتیب به امضای رای خود توسط ارزیاب دست می یابد.

$(B*R^{ev})^{dv}/R=B^{dv}$

فاز جمع آوری آرا:در این فاز، رای‌دهندگان آرا رمز شده و امضا شده‌ی خود توسط ارزیاب را از طریق یک کانال گمنام‌گر به برگزار کننده تحویل می‌دهند.

$P \rightarrow T: \quad B^{dv}$

برگزارکننده پس از بررسی صحت امضا ارزیاب، آرای رمز شده و امضا شده را در لیستی قرار می‌دهد. این لیست پس از اتمام رای‌گیری در معرض دید همگان قرار می‌گیرد. پس از انتشار این لیست، هر رای‌دهنده، صحت رای منتشر شده (بعد از اتمام انتخابات) در لیست را ارزیابی نموده و در صورت تایید، کلید رمزگشایی ویژه انتخابات خود را از طریق یک کانال گمنام‌گر به برگزار کننده تحویل می‌دهد. وقتی انتخابات به پایان رسید برگزارکننده آرای رمز شده، کلید رمزگشایی و نتیجه را منتشر می نماید. لازم به ذکر است که برگزارکننده برای انتشار آرا از یک تابلو اعلانات عمومی استفاده می‌نماید. با توجه به ساختار پروتکل FOO، مزایا و معایب این پروتکل به شرح ذیل بیان می‌گردد:

پروتکل FOO دارای مزایای زیر می‌باشد:

- سادگی پیاده‌سازی
- تعداد کم اعضای درگیر در پروتکل
- عدم نیاز به پروتکل‌ها و امکانات رمزنگاری پیچیده و دانش تخصصی
- امکان بازرسی فردی و اجتماعی به دلیل استفاده از تابلو اعلانات عمومی
- امکان بررسی صحت انتخابات از طریق تابلو اعلانات عمومی
- تضمین گمنامی در فاز جمع‌آوری و شمارش به دلیل بهره‌گیری از کانال‌های گمنام‌گر
- امکان تبانی ارزیاب و برگزارکننده برای نقض گمنامی رای‌دهنده وجود ندارد. ارزیاب کلید عمومی ویژه انتخابات رای‌دهنده و رای کور شده را دارد، حال آنکه برگزارکننده کلید خصوصی و رای را دارد. لینک بین این دو تنها در اختیار رای‌دهنده می‌باشد.

پروتکل FOO دارای نقاط ضعف اساسی زیر است:

- از آنجاییکه در این پروتکل راجع به نحوه ثبت‌نام رای‌دهندگان مجاز حرفی به میان نیامده است، راجع به تضمین یا عدم تضمین امکان تبانی ثبت‌نام‌گر و ارزیاب برای نقض گمنامی رای‌دهنده نمی‌توان اظهارنظر قطعی کرد. در فاز رای‌گیری بیان شده است که هر رای‌دهنده با استفاده از Id، خود را به ارزیاب معرفی می‌نماید و ارزیاب هم لیستی از Id هایی که هنوز رای نداده‌اند را در اختیار دارد. اما آیا ارزیاب با تبانی با واحد ثبت‌نام‌گر نمی‌تواند به هویت واقعی رای‌هنده دست یابد.
- امکان خرید و فروش رای به دلیل نشان دادن سه مولفه b,B,d در تابلو اعلانات عمومی[۲۰].
- امکان آگاهی از نتیجه انتخابات (به طور نسبی) قبل از اتمام زمان مجاز انتخابات توسط برگزار کننده، وجود دارد.
- امکان پیگیری شکایت پس از انتخابات وجود ندارد. چرا که محتوای واقعی رای در دست رای‌دهنده نبوده و تنها یک رسید در اختیار وی می‌باشد.
- ارزیاب یا مرجع شناسایی آرا به دلیل در دست داشتن لیست رای‌دهندگان مجاز قادر است که به جای رای دهندگان واجد شرایط اما غایب، آرایی (با تولید یک جفت کلید) را معرفی نماید(نقض دموکراسی).
- نقض ویژگی رای دادن و رفتن (رای‌دهنده در مرحله شمارش آرا به خاطر ارائه کلید خصوصی خود دخالت دارد)

این نقاط ضعف باعث شده علی‌رغم نقاط قوت زیاد این پروتکل در مقابل سایر پروتکل‌ها، تمایلی به استفاده از آن در انتخابات اینترنتی وجود نداشته باشد.

Sensus ۲-۳-۲-

کرانور و کایترون[۲۱] در سال ۱۹۹۷ پروتکل Sensus رو ارائه کردند. Sensus از طریق ۳ واحد پیاده سازی می شود:

- رای دهنده P، که علاقه دارد به صورت محرمانه و امن رای دهد.