تجزیه و تحلیل تکنیک های رمزنگاری و امنیتی برای ارائه رای گیری الکترونیکی قابل اثبات و سری

چکیده

سیستم های رای گیری الکترونیکی به طور جدایی ناپذیری به تکنیک های رمزنگاری و امنیتی مرتبط هستند. در طول دهه های گذشته، روش های بی شماری برای رویارویی با خطرات ناشی از سیستم های رای گیری الکترونیکی با دقت ریاضی پیشمقوله شده است. بدیهی است که اکثر این آثار به پنهان کاری و اثبات پذیری می پردازند. در این فصل، تکنیک های رمزنگاری و امنیتی با توجه به آن دسته از ویژگی های امنیتی تجزیه تحلیل می شوند که می توانند بر اساس این تکنیک ها ارزیابی شوند، یعنی محرمانه بودن، انصاف، صداقت، و اثبات پذیری. علاوه بر این، ما به طور خلاصه دقت آنها را برای اطمینان از ویژگی های مرتبط تر مانند واجد شرایط بودن و منحصر به فرد مورد بحث قرار می دهیم و تکنیک های رمزنگاری و امنیتی را با توجه به هزینه هایی که همراه با کاربردها در دنیای واقعی می آیند ارزیابی می کنیم. ما این فصل را با خلاصه ای از نتایج ارزیابی نتیجه گیری می نماییم که می تواند به عنوان راهنما برای تصمیم گیران به کار گرفته شود.

واژه های کلیدی : رمزنگاری کاربردی، الزامات رای گیری الکترونیکی، مدل های امنیتی، توانمندی رقبا، تجزیه و تحلیل امنیتی، مطالعه رای گیری الکترونیکی

مقدمه

تاریخچه انتخابات به یونان باستان و روم باستان باز می گردد که در آن شهروندان موقعیت های عمومی انتخاب می کردند. اجرای انتخابات بیش از هزاران سال از نشان دادن دست ها برای پرتاب سنگ و خرده ریز ها به سطل ها تا پر کردن برگه های رای کاغذی و پرتاب آنها را به ظرف های مخصوص مهر و موم شده تغییر کرده است. از دهه ۱۹۶۰، سیستم های الکترونیکی، علاقه عمومی را با توجه به فواید احتمالی انتخابات دقیق، سریع و ارزان به دست آورده اند. سیستم های رای گیری الکترونیکی اولیه به عنوان دستگاه های رای گیری پیاده سازی شدند، از دهه ۱۹۹۰ که

سیستم های رای گیری الکترونیکی از راه دور وارد میدان شدند و تبدیل به یک پیاده سازی امیدوار کننده برای رای گیری غیرحضوری شدند. در سرتاسر این فصل، ما فقط رای گیری از راه دور الکترونیکی را در نظر گرفته و از عبارت رای گیری الکترونیکی به جای یکدیگر استفاده می کنیم.

سیستم های رای گیری الکترونیکی به طور جدایی ناپذیری به تکنیک های رمزنگاری و امنیتی (SNC) برای ارائه انتخابات مخفی، عادلانه و قابل اثبات و همچنین یکپارچگی امنیتی مرتبط می شوند. توجه داشته باشید که روش های SNC در نظر گرفته شده در سراسر این کار از مکانیزم های شناسایی و تصدیق هویت جدا هستند، زمانی که این جهت پژوهش متعامد بر این کار است. با نگاهی به گذشته در بیش از سه دهه تحقیق، طیف گسترده ای از تکنیک های امنیتی و رمزنگاری برای رای گیری الکترونیکی امن وجود دارد. این تکنیک ها به سمت نیازهای خاص تنظیم می شوند و توافق های مختلف در میان ویژگی های متفاوت صورت می گیرد. متاسفانه، مدل امنیتی برای هر یک از ویژگی های امنیتی به وضوح مشخص نیست و یا به روش های مختلف برای روش های مختلف مشخص شده است. این باعث دشوار شدن مقایسه تکنیک های امنیتی و رمزنگاری مختلف پیشمقوله شده برای رای گیری الکترونیکی امن و در نتیجه تصمیم گیری برای نوع خاصی از انتخابات مناسب می شود. این شکاف در این فصل بررسی می شود. در نتیجه، ما از تصمیم گیرندگان در پیدا کردن روش های مناسب SNC برای پیاده سازی رای گیری الکترونیکی با توجه به شرایط انتخاباتی خود حمایت می کنیم.

ما تجزیه و تحلیل خود را بر روی روش های امنیت و رمز نگاری متمرکز می نماییم. به همین طریق، تمرکز بر آن دسته از ویژگی های امنیتی است که این روش ها در حال حاضر می توانند بدون ترکیب آنها با شناسایی و تکنیک های احراز هویت و بدون ساخت کل سیستم رای گیری ارائه دهند. اینها عبارتند از: محرمانه بودن، انصاف، صداقت، و اثبات پذیری . تعاریف سفت و سخت از این ویژگی های امنیتی در یک پروژه بین رشته ای بین دانشمندان حقوقی و فنی استنتاج شده است. این تعاریف در این فصل ارائه شده است. علاوه بر این، ما یک مدل امنیتی مدولار مشترک را توسعه می دهیم تا برای ما استنباط درجه تحقق این ویژگی های برای تکنیک های سفت و سخت SNC را میسر سازد. این مدل شامل یک لیست جامع از قابلیت های رقابتی می شود که از نوشته ها استخراج شده اند. این مدل

امنیتی در این فصل ارائه شده است. ما، پس از آن، تکنیک هاهای به خوبی شناخته شده SNC را برای سیستم های رای گیری الکترونیکی از نوشته ها انتخاب می کنیم و آنها را با توجه به مدل امنیتی خود ارزیابی می کنیم. علاوه بر این، ما به طور مختصر در مورد دقت تکنیک های SNC " برای برآورده سازی ویژگی های امنیتی بیشتر یعنی واجد شرایط بودن و منحصر به فرد بودن که متناظر با تکنیک های شناسایی و تصدیق هویت است و نیز هزینه های به کار بردن این روش در برنامه های کاربردی دنیای واقعی بحث می کنیم.

قبل از رفتن به بخش های اصلی این فصل، ما یک بخش پیش زمینه را اضافه می کنیم. در اینجا، ما کار مرتبط را بررسی می کنیم، یک نمای کلی از اجزای درگیر در فرایند رای گیری الکترونیکی و مقدمات مورد نیاز در باقی مانده این کار را ارائه می دهیم. ما این فصل را با خلاصه ای از کار خود نتیجه گیری می نماییم و به خواننده، جهت تحقیقات آینده را در جامعه رای گیری الکترونیکی نشان می دهیم.

پیش زمینه

بخش اول از این بخش به بررسی متون مرتبط می پردازد و نشان می دهد که کار حاضر در وضعیت فعلی تکنیک های SNC در کجا قرار می گیرد. در بخش دوم، ما به طور کلی اجزای درگیر در فرایند رای گیری الکترونیکی را مطرح می کنیم. پس از آن، مقدمات مورد استفاده در سراسر تجزیه و تحلیل را فراهم کنیم. به طور دقیقتر، این مقدمات، روش های مخفی به اشتراک گذاری، طرح های کدگذاری، طرح های امضای دیجیتال، سیستم های اثبات عدم آگاهی، و چالش Benaloh را پوشش می دهند. خواننده ای که با این مقدمات آشنا باشد، با خیال راحت می تواند از این بخش ها گذر نماید.

کار مرتبط

در این بخش، ما نظر سنجی های مقایسه ای و تجزیه و تحلیل تکنیک های SNC در سیستم های رای گیری الکترونیکی را بررسی نموده و کمک های لازم را از این کارها می گیریم. در (Rjašková، 2002)، نویسنده، مروری جامع بر شکل اولیه رمزنگاری مورد استفاده در رای گیری الکترونیکی را ارائه می دهد و پروتکل های رای گیری رمزنگاری را با زمینه سازی پایه ها برای پروتکل دریافت-آزاد خود بررسی می کند. با توجه به هدف خود، تمرکز

اصلی کار او روی آزادی-دریافت است، یعنی پنهان کاری تحت قابلیت های رقابتی ویژه در حالی که تجزیه و تحلیل ما به انصاف، صداقت رای و اثبات پذیری نیز می پردازد. در (Smith، ۲۰۰۵)، نویسنده مروری جامع بر شکل اولیه و تکنیک های مورد استفاده در رای گیری الکترونیکی رمزنگاری را فراهم می کند. با پرشی به جزئیات زیادی ریاضی، نویسنده، ارائه پیش زمینه فنی برای طرح های رمزنگارانه رای گیری الکترونیکی نظری را هدف قرار می دهد. با این حال، در کار خود، نویسنده روی مسائل رمزنگاری مانند پیچیدگی محاسباتی برای محاسبه عملیات خاص تمرکز می کند. هر دو، شکل اولیه و تکنیک ها، با این حال، در برابر معیارهای قانونی به دست آمده مورد تجزیه و تحلیل قرار می گیرند و نه بر اساس یک مدل امنیتی مشترک. Lambrinoudakis، Tsoumas، Karyda، و Ikonomopoulos (2003) یک مرور کلی را در مورد تکنیک های امنیتی اساسی در سیستم های رای گیری الکترونیکی منتشر نموده اند. طبقه بندی این تکنیک ها و تجزیه و تحلیل آنها، روش های مشخصی را نمی سازد، بلکه با تمرکز روی ارائه یک درک پایه از این پروتکل ها تمرکز می کند. در مقابل کار آنها، فصل ما روی یک رویکرد روش شناختی در طبقه بندی و تجزیه و تحلیل تکنیک های SNC تمرکز می کند که به استفاده از نتایج بدست آمده توسط تصمیم گیرندگان کمک می کند. MacNamara و Iedemska (2012) یک کار مروری در مورد تکنیک های رمزنگاری زمینه ساز سیستم های رای گیری الکترونیکی را ارائه نموده اند. این نویسندگان، امضاهای پنهان، رمزنگاری هموگرافیک، و شبکه های ترکیبی را تجزیه و تحلیل نمودند. با این حال ویژگی های اعلام شده به شدت به تجزیه و تحلیل این تکنیک ها مرتبط نبودند به طوری که تجزیه و تحلیل و نتیجه گیری های نهایی آنها مبهم باقی مانده اند. Mursi، Assassa، Abdelhafez و Samra (۲۰۱۳) اخیراً یک بررسی را منتشر نمودند که در آن تکنیک های امنیتی زمینه ساز سیستم های رای گیری الکترونیکی در مدت کوتاهی ارائه شدند و به طور مقایسه ای مورد تجزیه و تحلیل قرار گرفتند. با توجه به مجموعه گسترده الزامات امنیتی به دست آمده آنها از نوشته ها، تجزیه و تحلیل این تکنیک ها به صورت انتزاعی باقی مانده است. در برابر کار آنها، هدف از این کار، فراهم نمودند مدل های امنیتی از تکنیک های SNC با توجه به این ویژگی ها است که می توانند بر اساس این تکنیک های SNC مورد بررسی قرار گیرند.

اجزاء

معمولا، مقوله های زیر به کلی روند رأی گیری الکترونیکی کمک می نمایند: یک مقوله اعلام شده، یک رای دهنده است، اگر هویت آن در فهرست رای دهنده موجود باشد. مرجع ثبت، مسئول اجازه دادن به رای دهنده واجد شرایط برای رای دادن است. به این ترتیب، مقام مجاز ثبت نام، ثبت انتخاباتی را مقرر میکند. مقام مجاز ثبت کننده، یک نهاد مسئول پردازش رای به منظور ثبت نتیجه انتخابات است. امانت دار کلیدی، یک مقوله اختیاری نگه داشتن یک کلید مخفی است. به طور خاص، مقامات و امنا، اغلب به گونه ای توزیع می شوند که این روند کلی را می توان به مجموعه ای از مقوله ها به منظور ترکیب مدل های امنیتی قوی تر واگذار نمود. سیستم رای گیری الکترونیکی معمولا بر یک جزء بیشتر، یعنی تابلو اعلانات متکی است. این یک جزء سرور است که هر کسی دسترسی خواندن آن را دارد و هر یک از نهادهای مجاز دارای دسترسی نوشتن متناظر است. محیط رای گیری متشکل از سخت افزار و همچنین سیستم عامل و مرورگر مورد استفاده توسط رای دهنده برای شرکت کنندگان خود است.

به اشتراک گذاری سری

به اشتراک گذاری سری، تقسیم یک راز را از هم جدا میسر می سازد به طوری که سهام فردی اجازه نمی دهد تا نتیجه در مورد این راز بازسازی شود، بلکه مجموعه ای از سهام به فرد اجازه می دهد تا بازسازی راز صورت گیرد.

مشخصات

یک طرح به اشتراک گذاری سری یک چندتایی از الگوریتم $(S، R)$ است که در آن S، الگوریتم به اشتراک گذاری و R الگوریتم بازسازی است.

یک طرح به اشتراک گذاری سری ساده را می توان با اپراتور XOR $(\oplus)$ پیاده سازی نمود. فرض کنید یک فروشنده می خواهد راز s را در میان n شرکت کننده به اشتراک بگذارد. بنابراین فروشنده به صورت تصادفی مجموعه $s_1, \dots, s_{n-1}$ را ترسیم نموده و s n را محاسبه می کند به طوری که

$$s = s_1 \oplus \dots \oplus s_{n-1} \oplus s_n$$

فروشنده برای سهامدار i، is را فراهم می کند. اگر همه سهامداران، سهام خود را آزاد کنند، آنها می توانند s را با توجه به تعریف بالا بازسازی کنند. یک نقطه ضعف (در میان دیگران) این روش این است که همه سهام برای بازسازی راز به اشتراک گذاشته شده مورد نیاز است.

به اشتراک گذاری سری Shamir / Feldman

در مقابل ساده ترین شکل به اشتراک گذاری سری، یک آستانه (t, n) به اشتراک گذاری سری، بازسازی راز دارای t سهم را میسر می سازد. در (Shamir، ۱۹۷۹)، فروشنده به صورت تصادفی مقادیر را $r_1, \dots, r_{t-1}$ ترسیم می کند و چندجمله ای با درجه t را به شکل زیر تولید می کند

$$f(x) = s + r_1 x + r_2 x^2 + \cdots + r_{t-1} x^{t-1}$$

فروشنده، سهام کلیدی $(1)\ f$، ...، $(n\ f$) را محاسبه می کند و برای هر شرکت کننده i،سهم او $(i, f(i))$ برای $i \in \{1, \dots, n\}$. فراهم می کند. با توجه به قضیه اساسی جبر، برای یک مجموعه مستقل t از سهام $(i, f(i))$.، چندجمله ای f(x) را می توان با درون یابی لاگرانژ بازسازی نمود:

$$f(x) = \sum_{i=0}^{t-1} f(i) \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

راز s با رابطه $s = f(0)$. ارائه می شود.

طرح Shamir متکی بر یک فروشنده قابل اعتماد است که باید راز را به درستی تقسیم نماید؛ در غیر این صورت سهام فاسد را نمی توان مشخص کرد و تشکیل مجموعه متمایز از سهام t منجر به مقادیر بازسازی شده متمایز می شود. در طرح های به اشتراک گذاری سری قابل اثبات، فروشنده باید اثبات هایی را ارائه نماید که سهام مخفی صادر، بازسازی مخفی را پس از آن میسر می سازد. یک روش برای گسترش طرح Shamir توسط Feldman (Feldman، ۱۹۸۷) ارائه شده است. فرض کنید دو عدد اول بزرگ q، p ارائه می شوند به طوری که

$q|(p-1)$ و یک تولیدکننده g از q. فروشنده پس از تولید چندجمله ای f(x) متعهد این چندجمله ای می شود با نشر

$$g^s \bmod p, g^{r_1} \bmod p, \ldots, g^{r_{t-1}} \bmod p.$$

هر گاه فروشنده، یک سهم را برای یک سهامدار i صادر نماید، این سهامدار می تواند تایید کند که سهم او به روشی درست با کنترل مورد زیر ایجاد شود

$$g^{f(i)} = g^s \cdot g^{r_1 \cdot i} \cdot g^{r_2 \cdot i^2} \cdot \ldots \cdot g^{r_{t-1} \cdot i^{t-1}} \bmod p.$$

در مرحله بازسازی، هر یک از سهامداران، اثباتی را به فروشنده می فرستندبه طوری که تنها سهام درست تولید شده برای بازسازی مخفی استفاده می شوند.

طرح های رمزگذاری

انگیزه پشت طرح های رمزگذاری، رمزگذاری پیام های محرمانه به روشی است که این کد بتوان روی کانال های ناامن به خواننده در نظر گرفته شده این پیام انتقال یابد به طوری که این فرد پس از آن بتواند کد دریافتی را برای به دست آوردن پیام محرمانه رمزگشایی نماید.

مشخصات

به عبارت دیگر، یک طرح رمزگذاری، یک سه گانه از الگوریتم های (G، E، D) است که در آن G یک الگوریتم تولید کلید، E الگوریتم رمزنگاری، و D الگوریتم رمزگشایی متناظر است. طرح های رمزگذاری می توانند نامتقارن و متقارن باشد: در شکل متقارن، کلید رمزنگاری e و کلید رمزگشایی d برابر هستند و در نتیجه برای عموم مردم شناخته شده نیستند، در حالی که طرح های رمزگذاری نامتقارن $e \neq d$ و e برای عموم مردم شناخته شده است. علاوه بر این طرح های رمزگذاری نامتقارن می توانند به طرح های رمزگذاری نامتقارن قطعی و احتمالی طبقه بندی شوند: طرح های قطعی، نقشه پیام های یکسان به متون رمزی یکسان هستند، در برابر طرح های رمزگذاری احتمالاتی که تصادفی بودن را با روش رمزنگاری ادغام می کند به طوری که دو رمزگذاری برای پیام های یکسان

منجر به متون رمزی متمایز می شود. در ادامه این فصل، ما متون رمزی را از پیام m زیر کلید k را با $\{m\}_k^r$ نشان می دهیم که در آن r نشان دهنده تصادفی بودن اختیاری است.

تعداد زیادی از طرح های رمز نگاری وجود دارد که در میان مهم ترین طرح های متقارن، DES (استاندارد رمزگذاری داده ها) و AES (استاندارد رمزگذاری پیشرفته) وجود دارد. اولین و با نفوذ ترین طرح رمزنگاری نامتقارن قطعی نامتقارن RSA (Rivest، Shamir، و Adleman، ۱۹۷۸) و طرح های رمزگذاری احتمالاتی نامتقارن به خوبی تثبیت شده ElGamal (ElGamal، 1985) و Paillier (Paillier، 1999) است. در ادامه این فصل، ما روی طرح های رمزگذاری نامتقارن تمرکز می کنیم همانطور که آنها پایه و اساس بسیاری از سیستم های رای گیری الکترونیکی هستند. طیف گسترده ای از مفاهیم امنیتی، بیانگر امنیت طرح های رمزنگاری نامتقارن است که در میان مهم ترین آنها، غیرقابل تشخیص بودن تحت حمله متن ساده- انتخاب شده (IND- CPA)، غیرقابل تشخیص بودن تحت حمله متن رمزی انتخاب شده غیر انطباقی (IND- CCA)، و غیرقابل تشخیص بودن تحت حمله متن رمزی انتخاب شده تطبیقی (IND- CCA2) قرار دارد.

طرح رمزگذاری ElGamal

در این بخش، ما طرح رمزنگاری ElGamal معرفی شده در (ElGamal، 1985) را تشریح می کنیم. این طرح تبدیل به ارزشی برای سیستم رای گیری الکترونیکی شده است به دلیل اینکه ویژگی های مهم هومومورفیک را ارائه می دهد. رمزنگاری های هومومورفیک اجازه می دهد که عملیات کاربردی در متون ساده انجام شوند که منجر به عملیات های مختلف عملکردی در متن رمزی متناظر می شود. با توجه به دو گروه جبری $(P,\oplus)$ و $(C,\otimes)$، بنابراین ϕ یک نگاشت هومومورفیک بین دو گروه $(P,\oplus)$ و $(C,\otimes)$است اگر برای همه $p_1, p_2 \in P,$ داشته باشیم

$$\phi(p_1 \oplus p_2) = \phi(p_1) \otimes \phi(p_2).$$

همانطور که در زیر مشخص شده، کاراکتر هومومورفیک سیستم های رمزنگاری ElGamal اجازه می دهد تا اجرای تعدادی از عملیات ها مانند رمزگذاری مجدد متون رمزی صورت گیرد.

ایجاد کلید

خروجی الگوریتم تولید کلید، یک p اولیه بزرگ، یک تولیدکننده g برای گروه Z_{p^*} است. علاوه بر این، خروجی این الگوریتم، یک عدد تصادفی $x \leftarrow \{2, \dots, p-2\}$ به عنوان کلید خصوصی و $(g, p, y = g^x \pmod p)$ به عنوان کلید عمومی است.

تولید کلید Feldman مشترک توزیع شده

ما در حال حاضر اقتباسی (Gennaro و همکاران، ۱۹۹۹) از این طرح تولید کلید توزیع معرفی شده در (Feldman، ۱۹۸۷) را ارائه می دهیم. هدف از این طرح، ایجاد یک کلید عمومی مشترک است به طوری که کلید مخفی مربوطه به هر کسی شناخته شده نیست.

۱ . شرکت کننده i، یک چند جمله ای از درجه t را روی Zq تولید می کند

$$p_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,t}x^t,$$

که در آن $a_{i,0}$ نشان دهنده راز به اشتراک گذاشته است. برای هر شرکت کننده j، شرکت کننده i، $x_{i,j} = p_i(j)$ را محاسبه می کند و برای j مقدار آن را فراهم می کند. علاوه بر این، i در pi چند جمله ای تولید شده توسط انتشار مقادیر $X_{i,k} = g^{a_{i,k}}$ برای تمام $0 \le k \le t.$ قرار می گیرد.

۲ . هر شرکت کننده j سهام به دست آمده از همه شرکت کنندگان را با چک کردن این مورد که معادله زیر برآورده شود، بررسی می کند

$$g^{x_{i,j}} = \prod_{k=0}^{t} X_{i,k}^{j_k} \bmod p$$

اگر این معادله برآورده شود، j پذیرفته می شود، در غیر این صورت j یک شکایت را در مورد i منتشر می کند. اگر i توسط بیش از t شرکت کننده متهم ش.ئ و یا اگر i به طور آشکارا از این پروتکل پیروی نکند، i حذف می شود و $a_{i,0}$ ۰ می شود در حالی که $X_{i,0}$ ۱ می شود.

۳ . مقدار عمومی توسط $y = g^a \cdot \prod_{i=1}^{n} X_{i,0} \bmod p$ محاسبه می شود، در حالی که مقدار سری را می توان به عنوان $x = a + \sum_{i=1}^{n} x_{i,0} \bmod p.$ محاسبه نمود. پس از آن رای دهنده قادر به محاسبه مقدار سری است اگر حداقل t از n پیشگو درستی رفتار نمایند.

رمزگذاری

با توجه به یک کلید عمومی (g، p، y)، یک پیام $m \leftarrow \{0, \dots, p-1\}$ با تصادفی بودن $\{2, \dots, p-2\}$ به صورت زیر رمزگذاری می شود:

$$(c_1, c_2) = (g^r, m \cdot y^r) \bmod p$$

اشکار سازی

با توجه به متن رمزی (c 1، c 2) رمزگذاری شده تحت یک کلید عمومی (g، p، y)، پیام m به شرح زیر بازسازی می شود:

$$m = c_2 \cdot c_1^{-x}$$

ویژگی هوموورفیک

طرح رمزگذاری ElGamal، ویژگی مهمی را برای سیستم های رای گیری الکترونیکی برآورده می سازد، یعنی ویژگی هوموورفیک. با توجه به دو متن رمزی ElGamal، معتب $c_i = (g^r, m_1 \cdot y^r)$ و $c_j = (g^s, m_2 \cdot y^s)$ برای پیام های m1,m2، داریم که ci.cj یک متن رمزی معتبر از پیام m1.m2 است که در زیر نشان داده شده است.

$$c = c_i \cdot c_j = (g^r, m_1 \cdot y^r) \cdot (g^s, m_2 \cdot y^s) = (g^{r+s}, m_1 \cdot m_2 \cdot y^{r+s}) \bmod p$$

برای رای گیری الکترونیکی، اضافه کردن پیام ها به جای ضرب آنها می تواند بیشتر مفید باشد. بنابراین، طرح رمزگذاری ElGamal به سمت هوموورفیسم افزودنی گسترش داده می شود. طرح حاصل، ElGamal نمایی نامیده می شود (Cramer، Gennaro از، Schoenmakers، 1997) و در نتیجه متون رمزی به صورت زیر است:

$$(c_1, c_2) = (g^r, g^m \cdot y^r) \bmod p$$

می توان به راحتی دید که ضرب متون رمزی فردی منجر به اضافه شدن متون ساده اساسی می شود.

$$c = c_i \cdot c_j = (g^r, g^{m_1} \cdot y^r) \cdot (g^s, g^{m_2} \cdot y^s) = (g^{r+s}, g^{m_1+m_2} \cdot y^{r+s}) \bmod p$$

لازم به ذکر است که رمزگشایی این متن رمزی فورا به m منجر نمی شود، بلکه به g^m نتیجه می شود. در نهایت، لگاریتم گسسته $g^{m_1+m_2}$ باید محاسبه شود، که تنها برای توان های کوچک امکان پذیر است.

رمزگذاری دوباره

با توجه به متن رمزی $(c_1, c_2) = (g^r, m \cdot y^r) \bmod p$ رمزگذاری شده تحت کلید عمومی (p، g، y) رمز شده، این متن رمزی می تواند دوباره با استفاده از تصادفی بودن $s \leftarrow \{2, \dots, p-2\}$ به روش زیر رمزگذاری شود:

$$(c_1', c_2') = (g^r \cdot g^s, m \cdot y^r \cdot y^s) \bmod p$$

مفهوم رمزگذاری مجدد مجموعه ای از متون رمزی با کلید عمومی مشابه در شیوه ای مستقیم گسترش داده می شود.

رمز شکنی توزیع شده

تاکنون، مفهوم تولید کلید توزیع شده، انتزاعی بوده است. با این حال ثابت شده که این مفهوم از اهمیت زیادی برای برای رمزگشایی توزیع شده برخوردار است. در رمزگشایی توزیع شده، یک متن رمزی به صورت جزئی توسط شرکت

کنندگان رمزگشایی می شود به طوری که رمزگشایی جزئی می تواند برای بازسازی متن بر اساس درونیابی لاگرانژ مورد استفاده قرار گیرد. در نظر بگیرید که $c = (c_1, c_2)$ داده شده باشد. در طول مرحله رمزگشایی، رای دهنده vi، رمزگشایی جزئی خود را محاسبه می کند

$$c_1(i) = c_1^{x_i}$$

و یک اثبات را منتشر می کند که نشان می دهد

$$\log_{c_1} c_1(i) = x_i = \log_g y_i$$

اگر اثبات رای دهنده، اکثریت رای دهنده را متقاعد نکند، به روشی توزیع شده با تکیه بر درون یابی لاگرانژ از سهام متعهد سهام کلید خصوصی رای دهنده vi، آنها تصمیم به بازسازی سهم اعتبار خصوصی خود می گیرند. شرکت کنندگان صادق قادر به بازسازی xi و از این رو $c_1(i) = c_1^{x_i}$. خواهند بود.

زمانی که رمزگشایی های جزئی رای دهنده $c_1(i)$ دسترس باشد، متن ساده توسط عبارت زیر بازسازی می شود

$$m = \frac{c_2}{\prod_{i=1}^{n} c_1(i)}$$

امضاهای دیجیتال

هدف از طرح های امضا، اطمینان از درستی و صحت پیام ها با توجه به فرستنده و همچنین غیر قابل انکار بودن است.

مشخصات

یک طرح امضا؟، یک سه گانه الگوریتم (G، S، V) است که در آن G الگوریتم تولید کلید، S الگوریتم امضا و V الگوریتم تایید است. از قابل توجه ترین ویژگی های امنیتی طرح امضای دیجیتال ، غیرقابل جعل بودن کلی (UU)، غیرقابل جعل بودن انتخابی (SU) و غیرقابل جعل بودن وجودی (EU) .

امضای RSA

تولید کلید : با توجه به دو عدد اول بزرگ p، q، دو مقدار $n = p \cdot q$ و $\varphi(n) = (p-1)$ محاسبه می شود. یک مقدار e با کوپریم $1 < e < \varphi(n)$ برای $\varphi(n)$ به صورت تصادفی انتخاب می شود و d تعیین می شود به طوری که

$$e \cdot d \equiv 1 \bmod \varphi(n).$$

کلید تایید (e, n) و کلید امضا d است .

امضا : با توجه به کلید امضای d ، یک پیام $m < n$ توجه به معادله زیر امضا می شود:

$$s = m^d \bmod n$$

کد : با توجه به کلید تایید (e, n)، امضای s روی پیام m در صورتی معتبر است که معادله زیر برقرار باشد:

$$s^e = m \bmod n$$

امضای پنهان RSA

طرح امضای پنهان RSA در (Chaum 1981) اختراع و امضای استاندارد RSA را گسترش داد

پنهان کننده: پنهانکننده به طور تصادفی عامل پنهان کننده $k \leftarrow Z_n^*$ را انتخاب می کند، پیام m او را پنهان می کند و مقدار مربوطه را

$$b = H(m) \cdot k^e \bmod n.$$

به امضاء کننده می فرستد.

امضا: امضاء کننده این مقدار را با کلید عمومی او علامت گذاری می کند و مقدار مربوطه s' را

$$s' = b^d = (H(m) \cdot k^e)^d = (H(m))^d \cdot k^{ed} = \big(H(m)\big)^d \cdot k \ (\bmod n).$$

به پنهان کننده می فرستد.

باز کردن: پنهان کننده، عامل پنهان کردن را حذف می کند

$$s = \frac{s'}{k} = \frac{\left(H(m)\right)^d \cdot k}{k} = \left(H(m)\right)^d \pmod n$$

و امضای امضاء کننده را در پیام m به دست می آورد. بدون مرحله احراز هویت بیشتر، پنهانکننده می تواند پیام و امضای را منتشر کند. توجه داشته باشید که در مرحله خیره کننده، پیام m باید به منظور جلوگیری از سوء استفاده ها از انعطاف پذیری RSA ریز ریز شود، یعنی یک پنهانکننده مخرب می تواند امضاهای m_1^d, m_2^d را به دست آورد و یک امضای معتبر جدید را برای $m\ 1 * m\ 2$ با توجه به این واقعیت استنباط نماید که

$$(m_1 * m_2)^d = \left(m_1^d * m_2^d\right).$$

سیستم اثبات عدم آگاهی

سیستم های اثبات عدم آگاهی (ZK) از ابزار رمزنگاری برای اثبات اعتبار اظهارات بدون آشکار شدن هر چیزی فراتر از اعتبار این بیانیه است.

مشخصات

یک سیستم اثبات ZK توسط یک چندتایی از الگوریتم های (P، V) ارائه می شود که در آن P ثابت کننده اظهارات و V تصدیق کننده این اظهارات داده شده است. یک سیستم اثبات ZK برای L زبان معین، سه مشخصه را برآورده می سازد: ۱) هر بیانیه معتبر را می توان ثابت نمود (کامل)، ۲) هیچ بیانیه نامعتبری نمی تواند ثابت شود (صحت)، یک تصدیق کننده مخرب، کاری فراتر از اعتبار بیانیه را یاد نمی گیرد (عدم آگاهی) . ما یکی از اثبات های برجسته ZK در سیستم های رای گیری الکترونیکی مورد استفاده قرار می دهیم، یعنی اثبات دانش لگاریتم گسسته، که می تواند برای رد حملات پخش در تولید کلید توزیع شده مورد استفاده قرار گیرد. تعداد زیادی اثبات خاص ZK وجود دارد، به عنوان مثال، اثبات های اثبات شده-تصدیق کننده، اثبات برابری لگاریتم های گسسته، اثبات رمزگذاری ۱ از L ، اثبات فصلی برابری بین لگاریتم های گسسته. ما خواننده علاقه مند را برای اطلاعات بیشتر به (Smith، ۲۰۰۵) ارجاع می دهیم.

اثبات آگاهی از لگاریتم گسسته

در (Schnorr، 1989)، Schnorr یک پروتکل برای اثبات آگاهی از لگاریتم گسسته را اختراع نمود. با توجه به مبنای $g \leftarrow Z_p$، مقدار $y \leftarrow Z_p$، اثبات کننده می خواهد ثابت کند که او l را می داند به طوری که $y = g^l$ که در آن g و y به طور عمومی شناخته شده اند. این پروتکل به طور خلاصه به شرح زیر است :

۱ . ثابت کننده به طور تصادفی $r \leftarrow Z\ p$ را ترسیم می کند و خروجی $a = g^r$ را می گیرد

۲ . تصدیق کننده به طور تصادفی $c \leftarrow Z\ p$ را ترسیم می کند و خروجی c را می گیرد

۳ . ثابت کننده $z = r + l.\ c$ را محاسبه می کند و خروجی z را می گیرد.

۴ . تصدیق کننده چک می کند که ایا $g^z = a \cdot y^c$

چالشBenaloh

در (Benaloh، 2006)، Benaloh یک مفهوم را برای اثبات یکپارچگی رمزگذاری ها در روش اثبات ZK اختراع نمود. فرض کنید یک کاربر قصد دارد پیام m را با کلید رمزنگاری عمومی $k\ p$ با استفاده از طرح رمزگذاری ElGamal در یک سیستم دلخواه به رمز در آورد. بنابراین، با توجه به الگوریتم رمزنگاری، سیستم به طور تصادفی را $r \leftarrow \{2, \dots, p-2\}$ ترسیم می کند و عبارت زیر را محاسبه می کند

$$(c_1, c_2) = (g^r, m \cdot y^r) \bmod p.$$

این سوال مطرح است که چگونه کاربر می تواند مطمئن باشد که با سیستم رمزگذاری شده، مقدار صحیح، به هر حال خروجی به واسطه تعریف برای همه مقادیر ورودی، غیر قابل تشخیص خواهد بود. روش پیشنهادی Benaloh به صورت زیر است: بعد از رمزنگاری m، شده توسط فراهم کردن $H((c_1, c_2))$ برای کاربر سیستم متعهد به فرآیند رمزنگاری می شود. پس از آن کاربر (به طور غیر قابل پیش بینی) تصمیم می گیرد که آیا او ممیزی نماید و یا روند رمزگذاری دستگاه را قبول کند. اگر او تصمیم به ممیزی فرآیند بگیرد، دستگاه تصادفی بودن r را بازمی

گرداند. کاربر می تواند رمز گذاری صحیح را با محاسبه $(c_1', c_2') = (g^r, m \cdot y^r) \bmod p$ به صورت محلی با با کمک یک نهاد خارجی تایید کند و بررسی کند که آیا $H((c_1, c_2)) = H((c_1', c_2'))$. پس از فرآیند راستی آزمایی، رای دهنده دوباره باید تمامی مراحل رمزگذاری را اجرا نماید. اگر کاربر در برخی از نقاط تصمیم در به دست آوردن متن رمز بگیرد، سیستم برای رأی دهنده، (c 1، c 2) و یک امضا بر روی آن را فراهم می کند.

ویژگی های سیستم رای گیری الکترونیکی

انجام انتخابات به طور کلی به محدودیتهای قانونی ملزم خواهد بود. به عنوان مثال، قانون اساسی آلمان، اجرای شش اصل انتخابات همگانی، مستقیم، آزاد، برابر، انتخابات مخفی، و همچنین ماهیت عمومی انتخابات را تجویز می کند. این اصول باید در مشخصات فنی سخت تر در جهت اعمال آنها برای فن آوری رای گیری اصلاح شود. این کار درگفت و گوی میان رشته ای انجام شده است. ما ۱۷ مشخصات فنی را شناسایی نمودیم. برخی از آنها را می توان به طور مستقیم توسط روش SNC، یعنی ویژگی های پنهان کاری ، انصاف، صداقت، و اثبات پذیری رسیدگی نمود، در حالی که دیگران فقط می توانند بر اساس تکنیک های SNC غنی شده با ساز و کارهای شناسایی و احراز هویت مورد بررسی قرار گیرند؛ اینها واجد شرایط بودن و منحصر به فرد می باشند. مشخصات فنی بیشتر تنها می توانند بر اساس سیستم اجرای کامل و سازمانی پیاده سازی شده، مانند قابلیت استفاده و در دسترس بودن سیستم ارزیابی شود. به همین طریق، تمرکز این کار روی محرمانه بودن، انصاف، صداقت، و اثبات پذیری است.

توجه داشته باشید که در تحلیل زیر ما در نظر نمی گیریم که چقدر ارتباط بین رای دهنده و رای او مشخص است که این ارتباط به طور عمده به قالب شناسایی و تصدیق هویت بستگی دارد، یعنی یک رای دهنده که از طریق رمز عبور اثبات صحت می کند، ممکن است به آسانی رمز عبور خود را ارسال نماید، در حالی که یک تصدیق هویت رای دهنده از طریق ID ملی خود نمی تواند انجام شود. از سوی دیگر، با توجه به محرمانه بودن، ما صرفا ارتباط بین رای دهنده و رای او را به عنوان مکانیزم های دقیق مهم، مستقل از شناسایی و تصدیق هویت ، به عنوان مثال با توجه به آدرس IP رای دهنده در نظر می گیریم.

محرمانه بودن، انصاف، صداقت، و اثبات پذیری

محرمانه بودن و عدالت از نزدیک مرتبط هستند و ناشی از یک اصل انتخابات مندرج در بسیاری از قوانین اساسی ملی و بین المللی، یعنی اصل انتخابات سری هستند. در میان اصول دیگر، صداقت از اصول جهانی و برابر انتخابات گرفته شده است. اثبات پذیری از سوی دیگر، پیاده سازی اصل ماهیت عمومی در سطح فنی می باشد. حتی اگر اصل ماهیت عمومی در قوانین اساسی همه کشورهای دموکراتیک " گنجانده نشده باشد، برای سیستم های رای گیری الکترونیکی به دو دلیل دارای اهمیت مرکزی است: اول، سیستم های رای گیری الکترونیکی با خطرات ناشی از دستکاری در مقیاس های بزرگ روبرو هستند (Mercuri، 2002)؛ دوم، این کار ممکن است اعتماد در سیستم رای گیری را افزایش دهد. کار پروژه بین رشته ای ما، ما را به تعاریف زیر هدایت می کند=:

محرمانه بودن : برای هر رای دهنده v که یک رای برای نامزد دلخواه c ریخته، مشخص می کند که رقیب نمی تواند شواهد بیشتری در مورد این واقعیت به دست آورد که آیا رای دهنده c و یا هر انتخاب دیگر c' انتخاب دیگر انتخاب را انتخاب کرده همانطور که او می تواند از علامت نهایی دریافت کند. توجه داشته باشید که انتخاب بستگی به سیستم های انتخاباتی دارد و ممکن است شامل رای دادن به کاندید های متعدد، به عنوان مثال در روش رای گیری مرتبه بندی شده باشد. در این مقاله، ما روی انتخابات یک نامزد تمرکز می کنیم.

انصاف : رقیب می تواند هر گونه شواهد در مورد هر قصد رای را قبل از پایان انتخابات به دست آورد.

صداقت : صداقت از سه زیر خصوصیت تشکیل شده است:

رای به صورت در نظر گرفته شده: نظر رای دهنده مربوط به قصد او است. توجه داشته باشید که رای برای اطمینان از محرمانه بودن با برخی روش ها آماده می شود.

ذخیره شده به صورت رای: نظرسنجی رای دهنده برای جدولبندی به روشی که او رای می دهد ذخیره می شود.

شمارش به صورت ذخیره شده : تمامی آرا به روشی که ذخیره شده اند شمارش می شوند.

اثبات پذیری : در قیاس با تعریف یکپارچگی، اثبات پذیری از سه زیر خصوصیت تشکیل شده است:

نظرسنجی به عنوان در نظر گرفته شده :رای دهنده به صورت جداگانه می تواند اثبات کند که رای او به روش مورد نظر خود در نظر گرفته شده است.

ذخیره شده به عنوان رای :رای دهنده به صورت جداگانه می تواند اثبات کند که رای او برای جدول بندی های به روش مد نظر او ذخیره شده است.

شمارش به صورت ذخیره شده: هر کسی می تواند اثبات کند که تمام آرا به روشی که ذخیره شده اند شمارش می شوند.

دلایل ذکر شده در بالا باید بی عیب باشد، از این رو، امکانی برای رقیب به منظور تولید مدرک برای اظهارات نادرست نباید وجود داشته باشد که از مرحله تایید عبور نماید. در نتیجه، توجه داشته باشید که ما اثبات پذیری را به عنوان قوی ترین شکل از صداقت تعریف می کنیم. در نوشته ها، اثبات پذیری اغلب عنوان اثبات پذیری انتها- به- انتها اشاره می شود، اگر هر سه خصوصیت فرعی اثبات پذیری داده شود.

در عمل، رای دهنده متوسط قادر به بررسی این اثبات ها به صورت دستی نیست، همانطور که این اثبات ها معمولا بر اساس اشکال اولیه پیچیده رمزنگاری نیستند. بنابراین، او نیاز به حمایت دارد. به همین طریق، تأیید را نه توسط رای دهنده که شخصا قادر به بررسی دلایل دستی است، بلکه توسط کسانی تعریف می کنیم که می توانند از سخت افزار/ نرم افزار مستقل به منظور بررسی اثبات ها استفاده کنند. اثبات پذیری فقط در صورتی معین است که سخت افزاری از تولید کنندگان مختلف و نرم افزاری از توسعه دهندگان مختلف ارائه شود چرا که پس از آن رای دهنده می توانید انتخاب کند که کدام تولید کنندگان و کدام توسعه دهندگان مورد اعتماد هستند و از سخت افزار و نرم افزار خود آنها استفاده نماید که در آن نرم افزار شامل سیستم عامل می شود. ما چند مثال برای درک بهتر را در تجزیه و تحلیل بعدی را ارائه می دهیم: پیاده سازی چالش Benaloh (Adida، 2006) در سیستم Helios (Adida، 2008) را در نظر بگیرید : در تئوری، این سیستم خروجی داده های ممیزی را برای ممیزی خارجی فرآیند رمزنگاری میسر می سازد. پیاده سازی استفاده شده در Helios، امکان ارسال داده های ممیزی را جاوا اسکریپت به حسابرسان خارجی ممکن می سازد . زمانی که رای دهندگان فرآیند راستی آزمایی را در محیط رای گیری خود

انجام دهند،اثبات پذیری نظرسنجی به صورت در نظر گرفته شده در این پیاده سازی تضمین نمی شود، به عنوان مثال، محیطی که از آن برای رای دادن استفاده می شود. این محیط رای گیری سخت افزار و همچنین سیستم عامل و مرورگر مورد استفاده توسط رای دهنده را پوشش می دهد. یکی از راه های حصول اطمینان از یکپارچگی به صورت در نظر گرفته شده و بدون پیش فرض های رقابتی در (Karayumak و همکاران، ۲۰۱۱) نشان شده است. نویسندگان، برون سپاری فرآیند ممیزی را از طریق کدهای QR به یک دستگاه خارجی پیشنهاد داده اند، به عنوان مثال، گوشی های هوشمند، به منظور دستیابی به اثبات پذیری رای به صورت در نظر گرفته شده.

ویژگی های و امنیت بیشتر

سیستم های رای گیری الکترونیکی برای از ویژگی های امنیتی بیشتر از محرمانه بودن، انصاف، صداقت، و اثبات پذیری اطمینان حاصل نمایند. علاوه بر این، آنها باید اطمینان حاصل کنند که فقط رای دهنده واجد شرایط می توانند رای معتبر داشته باشد (واجد شرایط بودن) و هر رای دهنده واجد شرایط می توانند دقیقا یک رای معتبر (منحصر به فرد) بدهد. همانطور که اینها تنها می توانند با ترکیب تکنیک های SNC با مکانیزم های شناسایی و تصدیق هویت مربوطه تضمین شوند، این دو ویژگی در تجزیه و تحلیل های اصلی در نظر گرفته نمی شوند. با این حال، همانطور که روش های مختلف SNC باید با مکانیسم های شناسایی و تصدیق هویت های مختلف سازگار باشند، ما یک بحث کلی مختصری از کفایت تکنیک های SNC ' را با توجه به واجد شرایط بودن و منحصر به فرد بودن اضافه می کنیم.

معیارهای ارزیابی

در سراسر این بخش، ما معیارهای ارزیابی را برای تکنیک های SNC مورد استفاده در تجزیه و تحلیل های زیر مشخص می کنیم. به عنوان اولین معیار ارزیابی، ما مدل امنیت زمینه ای تکنیک های SNC و در نتیجه اندازه گیری قدرت تکنیک ها را با توجه به محرمانه بودن، انصاف، صداقت، و اثبات پذیری مشخص می کنیم. رده دوم از معیارهای ارزیابی، کفایت تکنیک های رمزنگاری و امنیتی برای رسیدگی به ویژگی های بیشتر، از جمله ویژگی های امنیت بیشتر، و نیز هزینه را پوشش می دهد.

مدل امنیتی برای ویژگی های امنیتی

مدل امنیتی معیار شامل دو زیر معیار متمایز برای پرداختن به محرمانه بودن، انصاف، صداقت، و ویژگی اثبات پذیری می شود. اولین معیار، مدل رقیب را تعیین می کند که در برابر آن یک تکنیک می تواند محرمانه بودن، انصاف و یکپارچگی را حفظ کند. معیار دوم تجزیه و تحلیل، درجه اثبات پذیری ارائه شده توسط روش مربوطه است.

مدل رقیب

ما مدل های رقیب را توسط یک روش مبتنی بر قابلیت در (Amenaza فن آوری های محدود، ۲۰۰۵) ارائه نموده ایم. در روش مبتنی بر قابلیت، روش SNC به یک نگاشت بین ویژگی ها و مفروضات امنیتی مربوط می شود (خروج از قابلیت های رقابتی) که تحت آن، آن ویژگی ها را می توان تضمین نمود. در نتیجه، رقیب توسط قابلیت های خود در اختیار تعریف می شود.

در مرحله بعد، قابلیت های رقابتی تعیین می شود تا ساخت مدل های رقیب را میسر سازند. قابلیت های رقابتی بر اساس بررسی نوشته ها و ترکیب چندین روش موجود هستند که مدل امنیتی را تعریف می کنند (. Langer، ۲۰۱۰؛ Dolev و yaho، ۱۹۸۱ Carlos و همکاران، ۲۰۱۳). ما قابلیت های رقابتی مشخص شده را در چهار زیر گروه طبقه بندی می کنیم، قابلیت های محاسباتی و زمانبندی مبتنی بر ارتباطات. در پاراگراف های زیر، دسته بندی های مختلف و قابلیت های رقابتی مربوطه را معرفی می کنیم.

قابلیت های مبتنی بر ارتباطات

در اصلی، ارتباط yaho - Dolev و مدل رقیب (Dolev و yaho، ۱۹۸۱) یک رقیب کنترل کننده شبکه بین موجودیت های انتزاعی را در نظر می گیرد. در کار های اخیر (Carlos و همکاران، ۲۰۱۳)، Carlos و همکاران، مدل ارتباطات yaho - Dolev را برای تناسب جشن های امنیتی (از جمله رای گیری الکترونیکی) گسترش می دهند و در نتیجه بین نهادهای انسانی و سیستم های کامپیوتری تمایز قائل می شوند. در سناریوی رای گیری، رقیب ممکن است کانال های شبکه بین سیستم های کامپیوتری (برای مثال اینترنت)، کانال های شبکه بین نهادهای انسانی (به عنوان مثال نامه پستی)، و یا کانال های شبکه بین نهادهای انسانی و سیستم های کامپیوتری (به عنوان

مثال محتوای خواندن رای دهنده بر روی صفحه نمایش و یا تعامل با سیستم های کامپیوتری از طریق تایپ کردن و حرکت موس) را کنترل نماید. با توجه به مدل yaho - Dolev توسعه یافته (. Carlos و همکاران، ۲۰۱۳)، قابلیت برقراری ارتباط بر اساس موارد زیر تعیین می شود:

۱ . رقیب می تواند پیام ها از کانال شبکه بدهد.

۲ . رقیب می تواند پیام را در کانال شبکه بخواند.

۳ . رقیب می تواند پیام ها را در کانال شبکه تزریق نماید.

در سناریوی رای گیری، برای رقیب، تعیین فرستنده یک پیام خاص به منظور نقض مالکیت سیستم رای گیری می تواند کافی باشد. برای پرداختن به این مسئله به اندازه کافی، Langer (Langer، ۲۰۱۰) توانایی برقراری ارتباط را بر اساس موارد زیر مشخص می کند:

۴ . رقیب می تواند فرستنده پیام را در کانال شبکه تشخیص دهد.

۵ . رقیب می تواند استفاده از یک کانال شبکه را اطلاع دهد.

قابلیت های مبتنی بر فساد

اولین مدل قابلیت مبتنی بر فساد، رقیبان قادر به کنترل نهادهای انسانی درگیر در فرآیند انتخابات را مدلسازی می کند. نهاد انسانی خراب شده توسط رقیب به طور کامل تحت کنترل رقابتی است. این نهادهای انسانی ممکن است به عنوان مثال می شود مقامات ثبت کننده یا سهامداران کلیدی باشند، اما رای دهنده، به طور جداگانه در نظر گرفته می شود. بنابراین، قابلیت مبتنی بر فساد در زیر مشخص شده است:

۶ . رقیب می تواند یک نهاد انسانی را خراب کند.

در برابر دیگر سازمان های بشری درگیر در پروسه انتخابات، اذعان می کنیم که رای دهنده به طور کلی برای دفاع در برابر حملات رقابتی با تقلب و رقیب تلاش می کند. این ناشی از این واقعیت است که بدون هر گونه اقدام رقابتی، رای دهنده هیچ انگیزه ای با توجه به قصد واقعی خود به رای دادن ندارد. بنابراین، رقیب نمی تواند به طور کامل رای دهنده را کنترل نماید. با این وجود، رقیب ممکن است برای تاثیر گذاشتن بر رای دهنده با انواع روش ها به منظور

رسیدن به هدف خود تلاش نماید. بنابراین، با توجه به رای گیری الکترونیکی، Langer (۲۰۱۰) این قابلیت ها توسط کانال های جدید شبکه را گسترش داده است اجازه می دهد که مدل های امنیتی ریز مانند کانال های شبکه های غیر مستقیم یا دو طرفه بین رای دهنده و رقیب ظهور یابند.

رقیب ممکن است به منظور تجربه مزایای خاص رای دهنده را به اثبات رای خود برای رقیب متقاعد نماید. این قابلیت ناشی از حملاتی است که در آن رای دهنده در نظر دارد اشیاء به دست آمده در طول فرآیند رای گیری را به منظور اثبات روش رای دادن فرد ارسالنماید (به عنوان مثال به (Adida و Neff، ۲۰۰۹) مراجعه کنید) . بنابراین، Langer (۲۰۱۰) قابلیت مبتنی بر فساد زیر را مشخص می کند :

۷ . رقیب می تواند اشیائی را از یک رای دهنده به دست آورد.

رقیبان نیز ممکن است قادر به فرستادن اشیاء به رای دهنده باشد. اشیاء رقیب ممکن است در پیشبرد مرحله رای گیری به عنوان دستورالعمل پرهیز از انتخابات، امضا برای حملات ایتالیایی به منظور راه اندازی یک حمله تصادفی (به عنوان مثال مراجعه کنید به (Teague، Ramchen، و Naish، 2008)) و یا یک مقدار تصادفی (مراجعه کنید به عنوان مثال برای (Ryan و Teague، ۲۰۰۹)) ارسال شوند. این قابلیت، قدرت رقیب را برای باج خواهی و یا متقاعد کردن رای دهنده در پیشبرد مرحله رای گیری به رای گیری با توجه به قصد رقیب مدلسازی می کند. بنابراین، Langer (۲۰۱۰) قابلیت مبتنی بر فساد زیر را مشخص می کند :

۸ . رقیب می تواند اشیاء را به رای دهنده ارسال کند.

پس از صریح و روشن شدن تمام ظرفیت ها با توجه به نهادهای انسانی، ما در حال حاضر نوع دوم نهادها را در سیستم های رای گیری خود در نظر می گیریم. سیستم های کامپیوتری اغلب به طور مستقیم توسط نهادهای انسانی کنترل نمی شوند و بنابراین مقامات و یا رای دهنده باید از هم جدا شوند. بنابراین، قابلیت مبتنی بر فساد زیر را معرفی می کنیم:

۹ . رقیب می تواند یک سیستم کامپیوتری را خراب کند.

قابلیت های محاسباتی

چند آثار، به عنوان مثال، (Sandler و Wallach، 2008)، به نقاط ضعف رمزنگاری همانطور که آنها ممکن است در چند سال خراب شوند، اذعان می کند. بنابراین سیستم های رای گیری ممکن است با توجه به قدرت محاسباتی رقابتی که در برابر آنها قادر به دفاع از ویژگی های امنیتی خاص هستند، متفاوت باشند. بنابراین، توانایی های زیر مشخص می شود:

۱۰ . رقیب از نظر محاسباتی نامحدود است .

توجه داشته باشید، ما توجه خود را در این فصل به محرمانگی محاسباتی محدود می کنیم و نه اطلاعات نظری. برای ما، زمانی که امنیت اطلاعات نظری به طور کلی همراه با پیش فرض های غیر واقعی می آید، به نظر می رسد این طبیعی ترین است. ما خواننده علاقمند را برای محرمانه بودن اطلاعات نظری در سیستم های رای گیری الکترونیکی به (مورن و Naor، 2007) ارجاع می دهیم.

توانمندی های زمان بندی

علاوه بر این، رقیب ممکن است قابلیت های ذکر شده در بالا را تنها در طول یک مدت زمان محدود داشته باشد. این محدودیت به عنوان مثال توسط حقایقی انگیزش می شود که رقیب ممکن است همه رای دهندگان را به طور همزمان در حال ریختن رای خود مشاهده نکند (به عنوان مثال کانال های شبکه بین رای دهنده و سیستم های کامپیوتری خود)، و ممکن است به طور مداوم دسترسی به کانال های بین نهادهای انسانی نداشته باشد؛ (به عنوان مثال به (Carlos و همکاران، ۲۰۱۳)) نگاه کنید. بنابراین، ما قابلیت های زمان بندی زیر را مشخص می کنیم:

۱۱ . رقیب دارای قابلیت [۱ - ۱۰] در طی یک دوره مشخص از زمان است

درجه اثبات پذیری

ما تکنیک های SNC را با توجه به درجه اثبات پذیری ارزیابی می کنیم آنها می توانند اطمینان حاصل نمایند. به عنوان یک نتیجه از تجزیه و تحلیل یکپارچگی، می توان استنتاج نمود که چند ویژگی فرعی یکپارچگی بدون طرح مفروضات در قابلیت های رقابتی تضمین می شوند. در تحلیل زیر، تمام ویژگی های فرعی تمامیت از اهمیت مساوی برخوردار هستند. بنابراین درجه معیار مدل امنیتی دوم را برای اثبات پذیری توسط یک نسبت به شکل صفر / یک /

دو / سه از سه تعریف کنیم. توجه داشته باشید که ما توجه خود را به اثبات پذیری محاسباتی محدود می کنیم و نه اطلاعات نظری. ما این محدودیت را توسط این واقعیت توجیه می کنیم که تایید معمولا در طی و یا بلافاصله بعد از مرحله رای گیری صورت می یرد، در نتیجه زمان بسیار محدود شده است. علاوه بر این ما به عمد فرض می کنیم که رقیب نمی تواند داده های نوشته شده در تابلو اعلانات را عوض نماید، به عنوان مثال، داده هایی که در تابلو اعلانات نوشته شده است را نمی تواند به صورت غیر آشکار دستکاری نماید. این فرض که توسط این واقعیت توجیه شده است که تابلو اعلانات تحت نظارت مستمر عموم مردم قرار دارد.

معیارهایی برای ویژگی های بیشتر

ما همچنین به طور خلاصه به بررسی رابطه بین تکنیک های SNC با ویژگی هایی می پردازیم که فراتر از محرمانه بودن، انصاف، صداقت، و اثبات پذیری هستند. اول، تکنیک های SNC با توجه به کفایت خود برای پیاده سازی واجد شرایط بودن و منحصر به فرد مورد بحث قرار می گیرند. دوم، ما فرض می کنیم که رای گیری الکترونیکی باید برای فرایندهای دموکراتیک بالاتر باشد، بلکه باید با سیستم های رای گیری معمولی رقابتی تر باشد. بنابراین ما تکنیک های SNC و پیاده سازی شده خود را با توجه به معیار هزینه ، پوشش منابع اداری، معماری و محاسباتی ارزیابی می نماییم. این هزینه ها به شدت به اجرای سفت و سخت شناسایی و تصدیق هویت در محل بستگی دارد. بنابراین، ما این جنبه را برای کار آینده کنار می گذاریم.

تجزیه و تحلیل تکنیک های امنیتی و رمزنگاری

هدف از این بخش، بررسی روش های SNC ایجاد و شناخته شده در سیستم های رای گیری الکترونیکی و ارزیابی آنها با توجه به معیارهای ارزیابی تعریف شده است. در قسمت اول از این بخش، ما به خواننده برخی از اطلاعات پیش زمینه در مورد ساختار این بخش و فرایند انتخاب را ارائه می دهیم. پس از آن، ما از تکنیک های انتخاب شده SNC را توصیف و تجزیه و تحلیل می کنیم.

پیش زمینه

ما با توجه به روش پنهان کاری در محل و در نتیجه مشابه با (Volkamer، 2009) با توجه به مرحله ای (قبل از رای گیری، رای دادن، پس از رای گیری) که در آن ارتباط بین رای دهنده و رای او خراب می شود، تکنیک های SNC را ساختاربندی می نماییم. بنابراین، ما در مرحله اول رای گیری با کد ساده و پیچیده را در مرحله قبل از رای گیری در نظر می گیریم. سپس، روش های امضای پنهان و ورود و خروج رمز شده آنلاین تصادفی را به عنوان محبوب ترین نمایندگان برای مرحله دوم مورد بحث قرار می دهیم. به عنوان نمایندگان مرحله سوم ما ترکیبات و رمزنگاری های هوموورفیک را در نظر می گیریم.

علاوه بر این، ما با دو پروتکل رای گیری، این تکنیک های استاندارد - Civitas (Clarkson, Chong, & Myers, ۲۰۰۸) و دموکراسی نسبتاً خوب را گسترش می دهیم (Ryan و Teague، ۲۰۰۹) – زمانی که هر یک از آنها ترکیبی از دو تکنیک های متفاوت هستند که قبلا ذکر شد.

بر این اساس، ما تکنیک های SNC را از دیدگاه محرمانه بودن تشریح می کنیم و در صورت امکان، این شرح را به سمت اثبات پذیری ارتقا می دهیم.

برای هر یک از روش های SNC توصیف شده، ما مدل امنیتی زمینه ساز پنهان کاری، انصاف، صداقت، و اثبات پذیری را شناسایی می کنیم. توجه داشته باشید، با توجه به نبود فضای کافی، ما مدل امنیت کامل را طرح نمی کنیم، بلکه صرفا توجه خود را به این فرض محدود می کنیم که نیاز به کمترین تعداد از قابلیت های رقابتی مجزا دارد. ما تجزیه و تحلیل را با تجزیه و تحلیل از ویژگی های بیشتر نتیجه گیری می کنیم.

روش های حصول اطمینان از محرمانه بودن در فاز قبل از رای گیری

یک روش به فاز قبل از رای گیری اختصاص داده می شود، اگر تعامل رای دهنده با سیستم رای گیری الکترونیکی هرگز با هویت او در ارتباط نباشد؛ از این رو، رابطه بین رای دهنده و رای انداختن او پیشبرد به مرحله رای گیری خراب می شود. تنها نمایندگان در این گروه از تکنیک ها، طرح های رای گیری مختلف هستند که در این بخش مورد بحث قرار می گیرند. ایده رای دادن کد به کار Chaum (Chaum، 2001) باز می گردد.

توصیف

در مرحله قبل از رای گیری، مقام ثبت نام کتاب کد منحصر به فرد را برای همه رای دهندگان واجد شرایط آماده می کند:کتاب کد شامل کتاب کد ID و یک جدول با سه ستون می شوند که در آن هر کاندیدا یک کد رای گیری و یک کد تصدیق دارد. بعد از تولید از این کتاب ها، مقام مجاز ثبت نام به صورت تصادفی کتاب کد را به رای دهنده اختصاص می دهد و برای مقام مجاز ثبت کننده تمام کتاب کد صادر شده را ارائه می دهد. رای دهنده نباید کتاب کد خود را در محیط رای گیری خود (بلکه به عنوان مثال از طریق نامه پستی) دریافت کند. در نتیجه، ارتباط بین رای دهنده و رای او از قبل در مرحله پیش از رای گیری خراب می شود. در مرحله رای گیری، رای دهنده رای او با ارسال کتاب کد ID و کد رای دهی در کنار نامزد به مقام مجاز ثبت کننده می ریزد. مقام مجاز ثبت کننده دوباره کد را برای شناسایی نامزد انتخاب و ذخیره یک رای برای نامزد تفسیر می کند. پس از آن، مقام مجاز ثبت کننده کد مربوط به رای دهنده را اذعان می کند. در نتیجه، رای دهنده اطمینان حاصل می کند که کد رای گیری او دستکاری نشده و یا توسط سیستم او بر روی کانال های ارتباطی کاهش نیافته است. با ارائه امکان به روز رسانی رای، رای دهنده می توانند کتاب کد ID خود را برای چند رای دادن استفاده کند. در این مورد، رای قدیمی رای دهنده با رای جدید او جایگزین می شود. در مرحله پس از رای گیری، مقام ثبت کننده همه نامزدهای تفسیر شده در تابلو اعلانات را منتشر می کند. این اجازه می دهد تا هر ناظر نتیجه را ثبت کند.

به منظور بهبود درجه اثبات پذیری، VeryVote (Joaquim، Ribeiro,& Ferreira ، ۲۰۰۹) مطرح شده است. این طرح این ایده کد رای دادن را با کدهای MarkPledge (Neff، ۲۰۰۴) ادغام می کند. یک مقام عمومی انتخابات، کتاب کد برای هر رای دهنده را تولید می کند که در آن به هر کاندیدا یک کد رای گیری منحصر به فرد اختصاص داده است. به علاوه، هر کتاب کد دارای کد ویژه اعتراف است، به اصطلاح کد MarkPledge است که در زیر خلاصه شده است. پیش از انتخابات، برای هر رای دهنده، مقام مجاز n -1 رمزگذاری بیت احتمالی ۰ و یک رمزگذاری یک بیتی ۱، نشان داده شده توسط $B\ t\ i\ c\ n$ (0)) و $B\ t\ i\ c\ n\ E$ (1) را تولید می کند. مقام مجاز متعهد می شود که آنها را در تابلو اعلانات همراه با هویت رای دهنده انتشار دهد. پس از آن، یک چالش عمومی $s\ r$ $v\ e$ (که برای استخراج چالش های فردی در مرحله رای گیری مورد استفاده قرار می گیرد) به صورت توزیعی

محاسبه می شود. با توجه به اینکه ویژگی های کدگذاری $B\ i\ t\ E\ c\ n$(1) تا حدی مستقل از چالش باز می شود، در حالی که باز کردن بخشی از $i\ B\ E\ t\ c\ n$ (0) به چالش بستگی دارد. باز کردن جزئی و ساکن رمزگذاری BitEnc(1) به عنوان کد MarkPledge اشاره می شود. پس از اینکه رای دهنده کد رای دهی خود را به مقام مجاز انتخابات می دهد، کد او تفسیر می شود. مقام مرجع BitEnc(1) را به نامزد انتخاب شده و $B\ t\ i\ c\ n\ E$ (0) را به نامزدهای دیگر نسبت می دهد. ترکیبی از نامزدها با رمزگذاری های بیت مورد نظر رای دهنده، مربوط به رای گیری رمزگذاری رای دهنده است. با توجه به چالش های فردی، مقام مجاز تصادفی بودن جزئی مورد استفاده برای تولید مقادیر $B\ t\ i\ n\ E\ c$(0) و BitEnc(1) در رای گیری نشان می دهد. مقام مجاز رمزگشایی جزئی از رای گیری (کدهای تصدیق) را منتشر می کند که دقیقا دریافتی رای دهنده است. نشان دادن مقادیر تصادفی جزئی با ویژگی پنهان کاری، که در (Joaquim، Ribeiro, & Ferreira، ۲۰۰۹) مورد بحث قرار گرفته است تداخل ندارد. رای دهنده به صورت جداگانه می تواند تایید کند که در دریافت عمومی او، کد تصدیق او (MarkPledge) بعد از نامزد انتخابی او به نظر می رسد. علاوه بر این، هر ناظر می تواند تایید کند که مقادیر تصادفی منتشر شده متناظر با چالش است و اینکه رمزگذاری های $i\ B\ t\ E\ c\ n$ (x) متناظر با کدهای ادعا شده ack(x) است، که در میان آنها کد MarkPledge تنها برای مقام مجاز و رای دهنده شناخته می شود. پس از مرحله رای گیری، برگه های رای چاپ شده ناشناخته خواهد ماند و برگه های رای توسط مجموعه ای از امنا رمزگشایی می شود.

در حالی که این بهبود در مورد اثبات پذیری پیچیده است، می توان به بهبود ساده زیر فکر کرد: پس از اینکه رای دهنده کد رای گیری خود را ارائه می دهد، کد اذعان مربوطه نیز در تابلو اعلانات منتشر می شود. پس از مرحله رای گیری، مقام مجاز، هر کد تصدیق را به نامزد مربوطه اختصاص می دهد. تجزیه و تحلیل زیر نشان می دهد که هر دو بهبود به مدل امنیتی مشابه منجر می شوند.

مدل امنیتی

مدل رقیب: در مقابل بسیاری از روش های دیگر SNC ، پنهان کاری در روش رای گیری کد، نه محیط رای گیری و نه کانال های ارتباطی استاندارد بین رای دهنده و مقامات ثبت کننده را به عنوان مواردی قابل اعتماد فرض نمی

کند. تمام اطلاعات که رقیب ممکن است به دست آورد، کنترل کننده محیط است و یا این کانال ارتباطی نمی تواند به انتخاب مربوطه نگاشت شود. از طرف دیگر، باید چنین فرض شود که رقیب نمی تواند کانال بین مقام مجاز ثبت نام و رای دهنده (C2) را بخواند. با این حال، مقام مجاز ثبت نام و ثبت کننده باید برای همکاری نکردن مورد اعتماد باشد چرا که پس از آن مقامات ثبت نام پیگیری می کنند که کدام کتاب کد به رای دهنده ارسال شده است، در حالی که مقام مجاز ثبت کننده می داند که کدام نامزد از کدام کتاب کد انتخاب شده است. توجه داشته باشید که در نسخه بهبود یافته، رقیب فقط نیاز به کنترل مقام مجاز ثبت نام (C6) . در هر دو روش - بهبود ساده و روش VeryVote دارد - مقام مجاز انتخابات / ثبت کننده، عمومی است (وظایف دولتی ممکن است از هم جدا شوند) به طوری که یک مدل رقیب نهایی نمی تواند مورد ارزیابی قرار گیرد. با این حال، هر دو روش بر این واقعیت تکیه دارند که رای دهنده نباید تحت کنترل رقابتی باشد در غیر این صورت او می تواند کتاب کد خود را به رقیب ارسال کند. در نتیجه، او ارتباط بین هویت خود و رای را با توجه به کد اذعان منتشر شده حفظ می کند. از این رو، رقیب باید اطلاعات را از رای دهنده (C7) به دست آورد.

انصاف و عدالت در روش رای گیری کد متکی به رفتار مناسب مقام مجاز انتخابات عمومی (C6) است چرا که این مقام مجاز از رابطه بین کد و داوطلبان اطلاع دارد و علاوه بر این دریافت کدهای انتخاب رای دهنده را دریافت می کند که اجازه می دهد این مقام مجاز نتایج میانی را محاسبه نماید. پس از اینکه رای دهنده کد رای گیری خود را می دهد، کد اذعان مربوطه در تابلو اعلانات منتشر می شود. اگر رای دهنده رای او به رقیب (C7) بدهد، رقیب می تواند از انتخاب رای دهنده اگاه شود و نتیجه میانی را محاسبه نماید.

با توجه به این واقعیت که در مرحله پس از رای گیری، کد اذعان به طور عمومی به نامزدها منسوب می شود، انسجام رای ها به صورت در نظر گرفته شده بر مبنای هر فرضیه ای نیست. با توجه به انسجام ذخیره شده به عنوان رای، یک مقام ثبت نام مخرب (C6) می تواند کتاب کد یکسانی را به رای دهنده بدهد که به طور قابل پیش بینی یک انتخاب را انجام دهد. در آن صورت، کدهای اذعان یک بار منتشر می شود و مقام مجاز ثبت کننده (C6) می تواند

تمامی آرا را با یک کد اذعان دور بیندازد. هیچ نامزد اضافی ذخیره می شود. در نهایت، یکپارچگی ذخیره شده به صورت رای، متکی بر هیچ فرض رقابتی نیست .

درجه اثبات پذیری : تجزیه و تحلیل یکپارچگی نشان می دهد که رای به صورت در نظر گرفته شده و شمارش شده به صورت ذخیره شده قابل اثبات می باشند. در نتیجه، درجه اثبات پذیری دو نفر از سه نفر، برابر است.

ویژگی های بیشتر و معیارهای بیشتر

واجد شرایط بودن و منحصر به فرد بودن به رفتار مناسب مقامات بستگی دارد. رای دهنده ممکن است کتاب کد خود را به رقیب بدهد و در نتیجه واجد شرایط بودن و یا منحصر به فرد بودن را نقض نماید این دلیل که رقیب تمام اطلاعات لازم را برای یک رای به دست می آورد. چسبیده به سیستم های رای گیری معمولی، کانال بین مقام مجاز ثبت نام و رای دهنده ممکن است توسط نامه پستی پیاده سازی شود که ستون اصلی تضمین کننده امنیت اجرا است، از این رو در مرحله قبل از رای گیری، هر رای دهنده نامه ای حاوی کتاب کد تصادفی را دریافت می کند. این ممکن است به هزینه های اداری قابل توجهی منجر شود.

روش های حصول اطمینان از محرمانه بودن در فاز رای گیری

یک روش به مرحله رای گیری اختصاص داده می شود در صورتی که ارتباط بین رای دهنده و رای او به عنوان بخشی از تعامل با سیستم رای گیری الکترونیکی خراب شود. به طور کلی، این تکنیک ها شامل چند فعل و انفعالات رای دهنده با سیستم می شود. نمایندگان این گروه، نشانه های احراز هویت آنلاین تصادفی و روش امضاهای پنهان هستند.

رمز تصدیق تصادفی آنلاین

مفهوم نشانه های احراز هویت تصادفی ممکن است به عنوان یک تفکیک وظایف بین مقام مجاز ثبت نام و ثبت کننده تفسیر شود. نشانه های احراز هویت تصادفی در سیستم رای گیری POLYAS، استفاده می شود که برای انتخابات GI (انجمن علوم کامپیوتر آلمان) (Olembo، Kahlert، Neumann، و Volkamer، 2012) استفاده می شود.

توصیف

در مرحله قبل از رای گیری، مقام ثبت نام، نشانه های تصادفی را برای تمام رای دهندگان واجد شرایط تولید می کند. در مرحله رای گیری، زمانی که رای دهنده واجد شرایط، صحت مقام مجاز ثبت نام را در سراسر مرحله رای گیری اثبات می کند، ID رای دهنده در فهرست رای دهنده مشخص می شود و نشانه تصادفی به رای دهنده بازگردانده می شود. این نشانه رمز تصادفی به سازمان ثبت کننده فرستاده می شود. توجه داشته باشید که تمامی مراحل ثبت نام نیز ممکن آفلاین باشد؛ بنابراین این روش می تواند یک روش پیش از رای گیری باشد و نشانه ها می توانند به طور تصادفی به رای دهنده شبیه به روش رای گیری کد بازگردانده شوند. پس از اینکه رای دهنده رمز هویت تصادفی خود را دریافت کرد، او می تواند انتخاب خود را صورت دهد، و پس از آن رای او به صندوق انداخته می شود. بنابراین، رای دهنده یک چندتایی حاوی رمز خود و انتخاب خود را آماده می کند و این چندتایی را به مقام مجاز ثبت کننده می دهد. سرور آرا را در صورتی را قبول می کند که رمز مرتبط توسط مقامات ثبت نام در هنگام ثبت نام ارسال شود. رای دهنده ممکن است چندین بار رمز خود را به منظور به روز رسانی رای استفاده کند. در مرحله پس از رای گیری، مقام مجاز ثبت کننده نشانه ها را از آرا جدا می کند و نشانه ها را در تابلو اعلانات منتشر می کند. مرجع ثبت نشانه های صادر شده را در تابلو اعلانات منتشر می کند.

می توان بهبود زیر را در نظر گرفت: به منظور ریختن رای v، رای دهنده به طور منحصر به فرد رای خود با تولید یک r عدد تصادفی بزرگ و ریختن یک چندتایی $(v \mid\mid r)$

$$(v||r)$$

به مقام مجاز ثبت کننده شناسایی می کند که در مرحله پس از رای گیری منتشر می شود.

مدل امنیتی

مدل رقیب : اگر رقیب ارتباط بین رای دهنده و این نشانه رمز اختصاص داده را نداند، رقیب ممکن است از آدرس IP برای پی بردن به هویت فرستنده و ایجاد یک لینک بین رای دهنده و رای خود استفاده کند و در نتیجه محرمانه بودن را نقض نماید. از این رو، فرض بر این است که رقیب نمی تواند منشاء پیام ها در کانال بین رای دهنده و

مقامات ثبت کننده (C4) مشخص کند. پنهان کاری در روش رمز احراز هویت تصادفی متکی بر توزیع اعتماد در میان مقام ثبت نام و مجاز ثبت کننده است. اگر هر دو مقامات همکاری کنند، بنابراین ارتباط بین رای دهنده و رای او را می توان ایجاد نمود. این امر منجر به این فرض می شود که رقیب نمی تواند مقام مجاز ثبت نام و ثبت کننده را به طور همزمان (C6) کنترل کند. به خاطر اثبات پذیری، رای ها منحصر به فرد می باشند. بنابراین، باید چنین فرض شود که قبل از مرحله پس از رای گیری (C7 : قبل از بعد از رای گیری) رای دهنده تحت کنترل رقابتی نیست. علاوه بر این، باید چنین فرض شود که رقیب محیط رای گیری (C9) را کنترل نمی کند.

تکنیک نشانه های احراز هویت تصادفی انصاف را با این فرض تضمین می کند که مقام مجاز ثبت کننده، رای منتشر نمی کند، مگر اینکه انتخابات فسخ شده اعلام شود (C6). اگر رقیب قادر به کنترل محیط رای گیری رای دهنده (C9) باشد، می تواند از انتخاب این رای دهنده آگاه شود. در نهایت، اگر رقیب بتواند کانال بین رای دهنده و مقامات ثبت کننده (C2) را بخواند، این رقیب می تواند یک نتیجه میانی را محاسبه نماید.

با توجه به این واقعیت که رای های منتشر شده توسط انسان قابل خواندن هستند، رای به صورت انسجام رای به صورت در نظر گرفته شده به طور ضمنی معین است. مشابه روش قبلی، انسجام رای به صورت ذخیره شده متکی بر چند فرض است همانطور که حمله زیر نشان می دهد : اگر رقیب چند دستگاه رای دهنده ' (C9) و مقام مجاز ثبت کننده (C6)، را کنترل کند، برای رای دهندگان با رای های یکسان می تواند تصادفی بودن یکسان را توسط دستگاه های آنها فراهم نمود. اگر مقام مجاز علاوه بر این تنها یک رای از این رای دهنده را ذخیره و بقیه را باطل کند، یکپارچگی رای به صورت ذخیره شده نقض می شود. این حمله توسط Kusters و 2012) Truderung) به عنوان حمله برخوردی تعریف می شود. چون هر ناظر عمومی می تواند نتیجه نهایی را از رای های ذخیره شده دوباره محاسبه نماید، یکپارچگی شمارش شده به صورت ذخیره شده متکی بر هیچ فرض رقابتی نیست.

درجه اثبات پذیری: تجزیه و تحلیل بالا نشان می دهد که اثبات پذیری رای به صورت در نظر گرفته شده و ذخیره شده معین هستند، در حالی که یکپارچگی رای به صورت ذخیره شده متکی بر عدم وجود چندین قابلیت های رقابتی است، از این رو، دو تا از سه ویژگی های فرعی قابل اثبات است.

ویژگی های بیشتر و معیارهای بیشتر

سه راه برای نقض واجد شرایط بودن و یا منحصر به فرد وجود دارد: اگر رای دهنده پس از دریافت این نشانه رمز خود از انتخابات پرهیز کند، مقام مجاز ثبت کننده ممکن است این نشانه را برای رای دادن از طرف آنها استفاده کند. دوم، مقام مجاز ثبت نام ممکن است نشانه هایی را برای رای دهنده فاقد صلاحیت ارائه کند. سوم، رای دهنده ممکن است نشانه های خود را به رای دهنده فاقد صلاحیت ارائه دهد. این مفهوم روی رمزنگاری پیچیده متکی نیست و نه رای دهنده و نه هیچ مقام نیاز به انجام محاسبات پیچیده ندارد. حتی دستگاه های کم منبع با قابلیت احراز هویت ممکن است برای ذخیره نشانه استفاده شود و آنها را در مرحله رای گیری آزاد نمایند. تنها سه سرور و کارکنان اجرایی برای این سرویس دهنده ها درگیر می شوند که می تواند در هزینه کم ارائه شود.

امضاهای پنهان

در اصل، امضاهای پنهان برای پیاده سازی پول نقد دیجیتال (Chaum، 1981 معرفی شدند) و بعد از آن برای سیستم های رای گیری الکترونیکی (Fujioka، Okamoto، و Ohta، 1992) اعمال شده اند. امضاهای پنهان فرم خاصی از امضای دیجیتال هستند که در آن امضاء کننده، پیام پنهانکننده را بدون دانستن محتوای این پیام پس از احراز هویت موفق علامت گذاری می کند. از این رو، امضای امضاء کننده در این پیام، فرآیند تصدیق هویت مبدا را تایید می کند. قبلاً در سال ۲۰۰۰، یک پیاده سازی ساده از امضای پنهان در کارت های هوشمند برای اجرای انتخابات مجلس دانشجویی در دانشگاه اوسنابروک، آلمان (Klink، 2006) استفاده شد.

توصیف

مشابه با رای گیری کد، روش امضاهای پنهان بر اساس جدایی از رویکرد وظیفه با دو مقام ثبت نام و مقام مجاز ثبت کننده است. سیستم های رای گیری بر اساس امضای پنهان مرحله رای گیری را به یک گام ثبت نام و یک گام رای دادن جدا می کند.

با توجه به (Fujioka، Okamoto، و Ohta، 1992)، یک رای دهنده، انتخاب vi خود را انجام می دهد، این انتخاب را پنهان می کند، رای پنهان را به مرجع ثبت می فرستد و توسط مقام مجاز ثبت نام تایید صحت می شود. مقام مجاز واجد شرایط بودن و نشانه آرای پنهان را در مورد رای دهنده واجد شرایط چک می کند. رای پنهان امضا شده به رای دهنده بازگردانده می شود. رای دهنده رای خود را به گونه ای آشکار می کند که امضا، رای آشکار شده را تایید می کند؛ از این رو رای دهنده رای امضا شده به طور رسمی را به دست می آورد. در مرحله رای گیری، رای دهنده رای امضا شده خود را به مقام مجاز ثبت کننده می دهد. مرجع، صحت امضاء را چک می کند و اگر تایید موفق باشد، رای را ذخیره می کند. در مرحله پس از رای گیری، مقام ثبت کننده تمام داده های معتبر دریافت شده از رای دهنده را با هم با نتیجه در تابلو اعلانات منتشر می کند.

در (Okamoto, 1996; Okamoto, 1997; Xia & Schneider, 2006)، در کنار دیگران، این پروتکل های رای گیری اثبات پذیری را بهبود داده اند. این سیستم متکی بر چند مقامات ثبت نام و ثبت کننده است. در مرحله قبل از رای گیری، رای دهنده یک مقدار تصادفی $a_i \leftarrow Z_q$ را در نظر می گیرد و $h_i = g^{a_i}$. را محاسبه می کند. رای دهنده، انتخاب vi را صورت می دهد و یک عدد تصادفی ri را ترسیم می کند . او مقدار زیر را محاسبه می کند

$$m_i = g^{v_i} \cdot h_i{}^{r_i} \bmod p$$

با استفاده از یک تصادفی بودن ثابت $a\ i$، رای دهنده می تواند $m\ i$ را با راه های مختلفی با تغییر $v\ i$، $r\ i$ محاسبه نماید. تنها محدودیت برای رای دهنده برآورده ساختن معادله زیر است

$$v_i + a_i \cdot r_i \equiv v_i' + a_i \cdot r_i' \bmod q.$$

رای دهنده پس از آن، یک عامل پنهان کننده k را در نظر می گیرد و عبارت زیر را محاسبه می کند

$$x_i = H(m_i||h_i) \cdot k^e$$

رای دهنده، مقدار نشانه پنهان خود را امضا می کند، اعتبار می بخشد و چندتایی $(sig(sk_i, x_i), x_i)$ را به مقام مجاز می فرستد. با توجه به توضیحات بالا، مقام مجاز ثبت نام مقدار xi را به طور پنهان امضا می کند و آن رابه رای دهنده باز می گرداند. رای دهنده به نوبه خود آن را آشکار می کند و عبارت زیر را به دست می آورد

$$s_i = H(m_i||h_i)^d$$

در مرحله رای گیری، رای دهنده $(m_i||h_i, s_i)$ را به تابلو اعلانات ارسال می کند و (m_i, v_i, r_i) را به مقام مجاز ثبت کننده می فرستد. در مرحله پس از رای گیری، مقام ثبت نام لیست چندتایی $\left((sig(sk_1, x_1), x_1), \dots, (sig(sk_k, x_k), x_k)\right)$ را منتشر می کند. مقام مجاز ثبت کننده یک لیست تصادفی از آرا (v 1، ...، k v) را همراه با اثبات ZK منتشر می کند و نشان می دهد که برای هر v i یک mi’ در تابلو اعلانات وجود دارد به طوری که مقام مجاز ri می داند به طوری که $m_i' = g^{v_i} h_i^{r_i}$ بدون آشکار نمودن ارتباط بین viو m’i.

مدل امنیتی

مدل رقیب : پنهان کاری در روش امضای پنهان روی انتقال ناشناس داده ها به مقام مجاز ثبت کننده (C4) متکی می کند. در (Okamoto، 1996؛ Okamoto، 1997)، رای دهنده می تواند تحت کنترل رقابتی باشد، همانطور که رای دهنده می تواند دریافت هایی برای انتخاب های مختلف را با تعویض v_i, r_i تولید کند به طوری که $m_i = g^{v_i} \cdot {h_i}^{r_i} \bmod p$ برآورده شود. با این حال، باید چنین فرض شود که رقیب محیط رای گیری (C9) را کنترل نمی کند، در غیر این صورت رقیب به راحتی می توانید انتخاب رای دهنده و a i را به دست آورد و در نتیجه دریافت های جعلی را تشخیص دهد.

مقام مجاز ثبت کننده دارای دسترسی به نتایج میانی در هر زمان است، از این رو، عدالت متکی بر قابل اعتماد بودن مقام مجاز (C6) است. رقیب نیز نتایج میانی را در صورتی می تواند محاسبه نماید که او قادر به خواندن کانال بین

رای دهنده و مقامات ثبت کننده (C2) باشد. در نهایت، محیط رای گیری تحت کنترل رقابتی می توانید انتخاب (بازدید کنندگان) را در آن محیط (C9) آزاد کند.

پس از اینکه رای دهنده تعهد خود را آشکار کند، او می تواند اعتبار امضا مقام مجاز را بدون محدود کردن رقیب به هر حال بررسی نماید؛ از این رو، تمامیت رای به صورت در نظر گرفته شده با پیش فرض های زیست محیطی ایجاد نمی شود. رای دهنده رای متعهد خود را در تابلو اعلانات منتشر می کند. با این حال، یک حمله شبیه به کد حمله رای گیری ممکن است: اگر مقام مجاز دستگاه های بسیاری از رای دهنده ' (C9) را کنترل کند، او می تواند a_i, r_i را به صورت یکسان برای رای دهنده با رای یکسان انتخاب کند در حالی که همه به یک ورودی در تابلوی اعلانات اشاره می کند . اگر علاوه بر این، تابلو اعلانات با صداقت (C6 یا C9) رفتار کند، این رای دهندگان را $(m_i||h_i, s_i)$ را در تابلو اعلانات پیدا می کنند، در حالی که تنها یک رای ذخیره شده است. بنابراین یکپارچگی ذخیره شده به عنوان رای به عدم حضور قابلیت های رقابتی ذکر شده بستگی دارد. در مرحله پس از رای گیری، مقام ثبت کننده یک لیست از آرا را منتشر می کند و ثابت می کند که هر رای مربوط به دقیقا یک رای غیرمتعهد ذخیره شده در تابلو اعلانات است؛ این کار انسجام به صورت ثبت شده را بدون هر گونه مفروضات تضمین می کند.

درجه اثبات پذیری: تجزیه و تحلیل یکپارچگی بالا نشان می دهد که رای به صورت در نظر گرفته شده و شمارش شده به صورت ذخیره شده قابل اثبات می باشد، از این رو، دو تا از سه ویژگی های فرعی قابل اثبات می باشند.

ویژگی های بیشتر و معیارهای بیشتر

اگر رای دهنده از انتخابات پرهیز کند، مقام مجاز ثبت نام می تواند امضاهای معتبر برای رای های او را صادر نماید و در نتیجه رای معتبر را بیاندازد و در نتیجه واجد شرایط بودن و یا منحصر به فرد را نقض نماید. در ساده ترین روش، امضاهای پنهان روی ثبت نام، یک مقام ثبت کننده، و یک تابلوی اعلانات تکیه می کند. این فرآیند یک مقام مجاز ثبت نام را برای امضای یک آیتم پنهان پیش بینی نموده است در حالی که مقام مجاز ثبت کننده امضا را در مرحله رای گیری تایید می کند؛ وظیفه رای دهنده پنهان و اشکار نمودن ایتم خود است. از این رو تلاش محاسباتی و

تلاش های اداری برای هر دو مقامات و رای دهنده، در سطح پایین قرار دارد و از این رو هزینه ها در حد متوسط هستند.

روش های حصول اطمینان از محرمانه بودن در مرحله پس از رای گیری

تکنیک های مورد بحث در این بخش مشترک هستند، زیرا یک ارتباط بین رای دهنده و رای رمزگذاری شده او وجود دارد، بنابراین، یک رای دهنده معمولا رای رمزگذاری شده خود را همراه با ID خود و یا نام مستعار خود در تابلو اعلانات پست می کند. دو نماینده از این دسته از SnCs، رمزنگاری های هوموورفیک و روش های ترکیبی می باشند.

رمزنگاری هوموورفیک

به جای رمزگشایی رای فردی، اولین مجموع رمزگذاری شده از تمامی آرای رمزگذاری شده محاسبه و سپس این مقدار برای تعیین نتیجه رمزگشایی می شود. این امر در صورتی ممکن است که طرح های رمزگذاری با ویژگی های افزودنی هوموورفیک، مانند طرح نمایی ElGamal (Cramer، Gennaro از، Schoenmakers، 1997) و یا طرح Paillier (Paillier، 1999) در جای خود قرار داشته باشد. روش سیستم رمز هوموورفیک در Helios ۲,۰ اجرا و برای انجام انتخابات رئیس جمهور در دانشگاه de lowin catholique استفاده شده است. یک گزارش تجربی و تجزیه و تحلیل استفاده در دنیای واقعی را می توان در (Adida، پست ، Marneffe de، و Quisquater، 2009) مشاهده نمود.

توصیف

در ساده ترین حالت از رفراندوم (انتخابات بله / خیر)، طرح های رمزنگاری هموگرافیک را می توان به شیوه ای ساده اجرا نمود. نخست رای دهنده i، انتخاب $v_i \in \{0,1\}$ را صورت می دهد و انتخاب خود را با کلید عمومی از طرف امنای کلیدی $k\ p$ رمز گذاری می نماید. به منظور متقاعد شدن در این مورد که رای گیری رمزگذاری شده او شامل آرای او می شود، چالش Benaloh در محل قرار می گیرد. پس از آن رای دهنده، داده های احراز هویت خود

را به رای رمزگذاری شده خود ، به عنوان مثال، با نوشتن نام خود $\{v_i\}_{pk}^{r_i}$ روی تابلو اعلانات متصل می کند. علاوه بر این رای دهنده به منظور جلوگیری از رای دادن رای دهنده مخرب، اثباتی برای اعتبار رای خود فراهم می کند (به عنوان مثال، یک مدرک نشان می دهد که $v_i \in \{0,1\}$). رای دهنده می تواند خود را متقاعد کند که رای او با یک روش بدون تغییر در تابلو اعلانات گذاشته شده است با چک کردن اینکه آیا نام او در کنار رای رمزگذاری شده خود و اثبات متناظر ذخیره شده به نظر می رسد یاخیر.

در مرحله پس از رای گیری، افراد می توانند نتیجه رمزگذاری شده را با ضرب آرای فردی رمز شده محاسبه نمایند.

$$R = \{v_1\}_{pk}^{r_1} \cdot \ldots \cdot \{v_n\}_{pk}^{r_n}.$$

نتیجه را می توان با رمز گشایی محصول R با کلید مخفی متناظر محاسبه نمود، از این رو

$$r = D(sk, R).$$

در نهایت، امنای کلیدی ثابت می کنند که آنها به درستی رمزگشایی شده اند، یعنی که آنها محصول رای رمزنگاری شده را با سهام مخفی مناسب با تولید یک اثبات ZK از رمزگشایی درست بر اساس اثبات ZK برابری لگاریتم گسسته رمزگشایی می نمایند.

مدل امنیتی

مدل رقیب: پنهان کاری سیستم های رمزنگاری هوموروفیک بر اساس قابل اعتماد بودن از افراد کلیدی معتمد است. از این رو، تحت مفروضاتی که آستانه افراد کلیدی معتمد به درستی (C6) رفتار نمایند، آرای فردی رمزگشایی نمی شود و در نتیجه پنهان کاری تضمین می شود. در مرحله رای گیری، رای دهنده فقط رای رمزگذاری شده و اثبات ها را به منظور اثبات پذیری را دریافت خواهد کرد. حتی رای دهنده حمل و نقل کننده این داده ها نمی تواند پنهان کاری را بشکند، چرا که این اطلاعات را نمی توان برای بازسازی انتخاب رای دهنده مورد استفاده قرار داد. علاوه بر این، باید چنین فرض شود که رقیب روی محیط رای گیری (C9) کنترل ندارد، در غیر این صورت انتخاب رای دهنده ممکن است به رقیب فرستاده شود.

تحت این فرض که مجموعه آستانه افراد کلیدی معتمد، قابل اعتماد (C6) است، رمزنگاری هوموورفیک، به دلیل اینکه رای های فردی در هر زمان رمزگشایی نمی شود، عدالت را برقرار می کند. علاوه بر این، محیط رای گیری رای دهنده (C9) به منظور انتخاب آزاد هر رای دهنده و در نتیجه ارائه نتایج میانی نباید تحت کنترل رقابتی باشد.

بدون داشتن فرضیاتی در مورد رفتار رقابتی، رمزنگاری هوموورفیک از یکپارچگی رای به صورت در نظر گرفته شده با توجه به چالش Benaloh، انسجام رای به صورت ذخیره شده با توجه به انتشار رای رمزگذاری شده شناسایی خود ، و یکپارچگی شمارش شده به صورت ذخیره شده با توجه به اثبات ZK برای رمزگشایی درست اطمینان حاصل می کند.

درجه اثبات پذیری : تجزیه و تحلیل یکپارچگی نشان می دهد که روش سیستم رمزگذاری هوموورفیک قابل اثبات است .

ویژگی های بیشتر و معیارهای بیشتر

در روش هوموورفیک، واجد شرایط بودن و منحصر به فرد بودن به شدت به داده های احراز هویت رای دهنده که ط به رای رمزگذاری شده او روش اختصاص داده می شود وابسته است. با توجه به این واقعیت که ساز و کارهای شناسایی و احراز هویت در این کار در نظر گرفته نشده اند، واجد شرایط بودن و منحصر به فرد برای این رویکرد مشخص نشده است. به نظر می رسد که رمزنگاری هوموورفیک برای رای دادن الکترونیکی دچار اشکال مهمی باشد، یعنی تلاش های محاسباتی. به جای ارائه v جمع $vn + \cdots + 1$ برای تمام آرا، رمزگشایی متون رمزی نمایی ElGamal نشان دهنده $g^{v_1+\cdots+v_n}$ است. این تنگنا ممکن است توسط سیستم کارآمدتر Paillier رمزگذاری هوموورفیک غلبه شود. علاوه بر این، رای دهنده نیاز به ارائه شواهدی وجود دارد که آراء او، به صورت آرای معتبر رمزگذاری شده است. پیاده سازی اثبات ZK پیچیده در دستگاه های کم منبع ممکن است مشکل ساز باشد، از این رو هزینه ها در زمان پیاده سازی این روش ممکن است بالا باشد.

ترکیبات

در (Chaum، 1981)، Chaum روش دیجیتالی را برای ترکیب پیام ها به منظور میسر نمودن ارتباطات ناشناس روی شبکه های ارتباطی ناامن اختراع کرد. ترکیبات پروتکل های ارتباطی را در میان مجموعه ای از گره ها پیاده سازی می کند که در آن هر گره دسته ای از پیام های دریافتی را می گیرد، آنها را با توجه به یک جایگشت های مخفی و تصادفی ترکیب می کند، ظاهر آنها را تغییر می دهد (این به زودی مشخص خواهد شد)، و پیام های بی نام را به گره ترکیبی بعدی می فرستد.

با اعمال در سیستم های رای گیری الکترونیکی، ترکیبات برای شکستن پیوند بین رای دهنده و رای رمزگذاری شده او قبل از رمزگشایی رای استفاده می شوند. دو پیاده سازی ترکیبی برجسته هستند: ترکیبات رمزگشایی و ترکیبات رمزگذاری دوباره. با توجه به تاثیر آنها بر سیستم های رای گیری الکترونیکی، در این کار ما صرفا ترکیبات مجدد رمز (ترکیبات رمزگشایی به عنوان مثال در (Clarkson و Myers, ، ۲۰۰۵) استفاده می شود) در نظر می گیریم. اول ترکیب قابل اثبات ترکیبات رمز گذاری مجدد توسط (Sako & Kilian ، ۱۹۹۵) ارائه شد. بسیاری از روش های برای این ترکیبات موثر قابل اثبات ارائه می شوند که در میان آنها ما خواننده را به (Wikström، .D، 2005، Chase و همکاران، ۲۰۱۲) ارجاع می دهیم. این ترکیبات رمز گذاری مجدد قابل اثبات روی استفاده از برنامه رمزگذاری نرم و قابل انعطاف متکی است به عنوان مثال، طرح هایی که رمز گذاری مجدد از متون رمزی را بدون دیدن و تغییر متن موجود میسر می سازد. در (Jakobsson، Juels، و Rivest، 2002)، نویسنده چک کردن تصادفی جزئی را به عنوان روشی برای بهبود بهره وری به طور قابل توجهی پیشنهاد می کند، در حالی که در همان زمان درجه اثبات پذیری ارائه شده کاهش می یابد. این رویکرد مبتنی بر ترکیب، در انتخابات شهرداری نروژی در سال ۲۰۱۱ (Gjøsteen، 2010) مورد استفاده قرار گرفت در حالی که تمام گره ها توسط همان شرکت (OSCE ODIHR /، 2012) ارائه شد.

توصیف

به طور کلی، یک رای دهنده، رای خود را با کلید عمومی از افراد کلیدی معتمد $k\ p$ کدگذاری می نماید. رای دهنده پس از آن داده های احراز هویت خود را به رای رمزگذاری شده خود متصل می کند، به عنوان مثال، با نوشتن

نام خود $\{v_i\}_{pk}^{r_i^1}$ روی تابلو اعلانات . مانند این رویکرد هموморفیک، رای دهنده می تواند خود را متقاعد کند که رای او با توجه به چالش Benaloh در متن رمز کد گذاری شده است. رای دهنده علاوه بر این می تواند خود را متقاعد کند که رای او به روشی بدون تغییر در تابلو اعلانات ذخیره شده است. پس از مرحله رای گیری، رای رمزگذاری شده از ID رای دهنده از هم جدا می شود و سرانجام از طریق ترکیب رمز گذاری مجدد قابل اثبات، همه اطلاعات تولید شده توسط هر گره در تابلو اعلانات منتشر می شود. مجموعه ای از آرای رمزگذاری شده منتشر شده توسط آخرین نقطه ترکیب، رای به رای توسط مجموعه آستانه امنای کلیدی رمزگشایی می شود و در تابلو اعلانات منتشر می شود. پس از آن این آرا شمارش می شود و در نتیجه به چاپ می رسند. در اینجا، هر j گره ترکیبی، رای رمزگذاری شده هر یک از رای دهندگان $\{v_i\}_{pk}^{r_i^{j-1}}$ را با تصادفی بودن اضافی $r_{j1} \dots, r_{jn}$ رمز گذاری مجدد می نماید و نتیجه، تصادفی بودن کلی $r_1^j \dots, r_n^j$ است که یک جایگشت تصادفی را ψ_j ترسیم می کند و انتقال زیر را برای تمامی آرا انجام می دهد:

$$\phi\{v_1\}_{pk}^{r_1^{j-1}}, \dots, \phi\{v_n\}_{pk}^{r_n^{j-1}} \to \psi_j\left(\phi\{v_1\}_{pk}^{r_1^j}\right), \dots, \psi_j\left(\phi\{v_n\}_{pk}^{r_n^j}\right)$$

هر گره ترکیبی باید پردازش صحیح متون رمزی دریافت شده را ثابت کند. بنابراین، هر گره ثابت می کند که متون رمزی ورودی شامل همان متون ساده مانند متون رمزی خروجی بدون متون آشکار ساده می شود. یکی از این روش ها بر اساس پروتکل Pedersen - Chaum (Chaum و Pedersen، ۱۹۹۲) که اجازه می دهد تا یک گره ترکیبی اثبات کند که برای همه $i \in \{1, \dots, n\},\ \psi_j\left(\phi\{v_i\}_{pk}^{r_i^j}\right),$ یک رمزنگاری دوباره $\text{of } \phi\{v_i\}_{pk}^{r_i^j}$ بدون رابطه آشکار است. این اثبات را می توان بر اساس ترکیب ۲ × ۲ اثبات نمود که با OR کردن اثبات ZK برابری لگاریتم گسسته در برابر روش پیشنهادی (Smith، ۲۰۰۵) تحقق می یابد.

مدل امنیتی

مدل رقیب : پنهان کاری متکی بر قابل اعتماد بودن حداقل یک گره ترکیبی است، از این رو، باید چنین فرض شود که همه ترکیبات تحت کنترل رقابتی (C6) نمی باشد. باید چنین فرض شود که مجموعه آستانه افراد کلیدی معتمد، قابل اعتماد (C6) است و آرای رمزگذاری شده که در تابلو اعلانات همراه با نام رای دهنده به چاپ می رسند، رمزگشایی نشده اند. علاوه بر این، محیط رای گیری های مخرب به راحتی پنهان کاری را توسط حمل و نقل انتخاب رای دهنده برای رقیب ، توسط تثبیت اشتباه تصادفی بودن مورد استفاده برای رمزگذاری انتخاب رای دهنده خراب می کند. از این رو، فرض بر این است که رقیب می تواند محیط رای گیری (C9) را کنترل کند.

مشابه با روش سیستم رمزگذاری هوموورفیک، عدالت و انصاف را می توان تحت این فرض تضمین نمود که آستانه افراد کلیدی معتمد، قابل اعتماد (C6) است و محیط رای گیری رای دهنده، قابل اعتماد (C9) است

در قیاس با روش سیستم رمزگذاری هوموورفیک، بدون طرح فرضیات در مورد رفتار رقابتی، روش مبتنی بر ترکیبات از یکپارچگی رای به صورت در نظر گرفته شده با توجه به چالش Benaloh، انسجام رای به صورت ذخیره شده با توجه به انتشار رای رمزگذاری شده شناسایی خود ، و یکپارچگی شمارش شده به صورت ذخیره شده با توجه به اثبات ZK و رمزگشایی درست اطمینان حاصل می کند.

درجه اثبات پذیری : رویکرد مبتنی بر ترکیبات، قابل اثبات است.

ویژگی های بیشتر و معیارهای بیشتر

مشابه با رویکرد هوموورفیک، واجد شرایط بودن و منحصر به فرد نمی تواند بدون جزئیات بیشتر در مورد مکانیسم شناسایی و تصدیق هویت ارزیابی شود. این ترکیبات نیاز به تعداد قابل توجهی از محاسبات برای گره ترکیبی، افراد کلیدی معتمد و همچنین ناظران عمومی (که همچنین ممکن است هر رای دهنده فردی باشد) دارند. در ترکیبات، هر گره ترکیبی باید روی کل مجموعه متون رمزی کار کند و اثبات هایی برای عملکرد صحیح ارائه نماید. به این منظور، ترکیبات رمز گذاری مجدد در میان پر هزینه ترین روش ها برای اطمینان از رازداری در رای گیری الکترونیکی قرار دارد.

ترکیبی از مراحل

در بخش نهایی تحلیل، ما تکنیک هایی را در نظر می گیریم که از محرمانه بودن و اثبات پذیری با ادغام تکنیک های SNC قبلا مورد تجزیه و تحلیل قرار گرفته، اطمینان حاصل می کنند و در نتیجه به مدل امنیتی خاصی می پردازند.

Civitas

در این بخش، ما سیستم Civitas (Clarkson، Chong, & Myers ، ۲۰۰۸) را ارائه می دهیم. Civitas از پنهان کاری در مقابل رقیبان که با رای دهنده ارتباط برقرار می کند و مشاهده رای دهنده در مرحله رای گیری، دفاع می کند. در این سیستم، مقامات ثبت کننده، افراد کلیدی معتمد نیز می باشند.

توصیف

در مرحله قبل از رای گیری، رای دهنده v مجموعه ای از مقامات ثبت نام را اعتبار می بخشد. هر مقام مجاز ثبت نام $i \in \{1, \dots, n\}$ یک سهم به اصطلاح اعتباری س v c_v^i را تولید می کند که پس از آن توسط رای دهنده برای رای دادن استفاده می شود. توجه داشته باشید، که هر اعتبار را می توان برای چند رای به منظور میسر نمودن به روز رسانی رای استفاده نمود. هر مقام مجاز ثبت نام، سهم اعتبار خود را برای رای دهنده v با کلید عمومی $k\ p$ از طرف افراد کلیدی معتمد با استفاده از یک طرح رمزنگاری هموگرافیک ضرب کننده رمز گذاری می کند و در نتیجه v متن رمزی $\{c_v^i\}_{pk}^{r_i}$ را در تابلو اعلانات بعدی برای هویت رای دهنده در فهرست رای دهنده منتشر می کند. مرجع ثبت نام برای رای دهنده c_v^i و اثبات تعیین شده-تصدیق کننده را فراهم می کند (متقاعد نمودن تنها رای دهنده تعیین شده) که نشان می دهد که $\{c_v^i\}_{pk}^{r_i}$ یک رمزنگاری است. در نهایت، رای دهنده اعتبار خود را با ضرب تمام سهام اعتباری دریافت شده از مقامات ثبت نام های مختلف را محاسبه می کند:

$$c_v = \prod_{i \in \{1,\dots,n\}} c_v^i.$$

به این ترتیب، اعتبارات، بخش اول از مکانیسم پنهان کاری اطمینان Civitas را که در فاز قبل از رای گیری اتفاق می افتد، پیاده سازی می نمایند. زمانی که رای دهنده اعتبار خود cv را به دست آورد، می تواند رای خود v v را در مرحله رای گیری با تهیه یک چندتایی از گواهی نامه های رمزگذاری شده و رای رمزگذاری شده

$$\left(\{c_v\}_{pk}^{r_v}, \{v_v\}_{pk}^{r'_v}\right)$$

همراه با دو اثبات ZK نشان دهنده برجستگی رای بدهد و رای دهنده از cv و vv یبه منظور جلوگیری از حملات پخش مجدد آگاهی دارد. این چندتایی در تابلو اعلانات منتشر می شود. در صورت به روز رسانی رای، چندتایی جدید منتشر می شود. در موردی که رای دهنده با یک مجبورکننده مجبور به ارسال اعتبار خود می شود، او می تواند یک سهم اعتبار را جایگزین نماید، به عنوان مثال، $c_{v'}^{1}$ توسط سهم تصادفی c_{r} ، و اعتبار جعلی زیر را تولید نماید

$$c_v^f = c_r \cdot \prod_{i\in\{2,\dots,n\}} c_v^i.$$

بنابراین مجبور کننده می تواند یک رای را با استفاده از c_v^f در تابلو اعلانات منتشر می شود. در مرحله پس از رای گیری، مجموعه آستانه افراد کلیدی معتمد، بخش دوم ساز وکار تضمین پنهان کاری را اجرا می کند: اعتبار های رمزگذاری شده توسط مقامات ثبت نام در مرحله قبل از رای گیری منتشر شده در تابلو اعلانات و اعتبار رمزگذاری در ارتباط با رای تابلو اعلانات، ویژگی زیر را با توجه به طرح رمزگذاری مورد نظر برآورده می سازند:

$$\left\{\prod_{i\in\{1,\dots,n\}} c_v^i\right\}_{pk}^{r} = \prod_{i\in\{1,\dots,n\}} \left\{c_v^i\right\}_{pk}^{r_i}$$

در ادامه، اعتبارنامه رای و گواهی نامه های رمزگذاری شده متشکل از سهام گواهی نامه های رمزگذاری شده ترکیب می شوند. هنگامی که این اعتبار نامه های رمزگذاری ترکیب می شوند، مقام مجاز باید آرا را برای اعتبارات معتبر و به اعتبار جعلی بدون نقض محرمانه بودن شناسایی نماید. بنابراین، مجموعه آستانه توزیع افراد کلیدی معتمد،یک آزمایش هم ارزی متن قابل اثبات را با توجه به (Jakobsson و Juels، 2000) برای هر یک از (ترکیب شده)

اعتبارات در برابر همه (ترکیب شده) اعتبارات معتبر انجام می دهد. اگر یک گواهی نامه رای معتبر نباید، رای مرتبط دور انداخته می شود. در نهایت، رای های مربوط به اعتبارات معتبر به صورت توزیعی و قابل بررسی به صورت ارائه شده در بخش توزیع رمزگشایی ElGamal رمزگشایی می شوند.

مدل امنیتی

مدل رقیب: به منظور دفاع از پنهان کاری در برابر مجبورکننده مشاهده کننده رای دهنده در خلال روند رای گیری، Civitas بر این فرض متکی است که رای دهنده تحت کنترل رقابتی در مرحله قبل از رای گیری قرار نمی گیرد (C7، C8 : قبل از رای گیری). به منظور انتخاب رای در نظر گرفته شده در مرحله رای گیری، باید چنین فرض شود که یک لحظه در مرحله رای گیری وجود دارد که در آن رقیب نمی تواند رای دهنده را کنترل کند. (نه کل مرحله رای گیری C5) در غیر اینصورت، رقیب می تواند از کانال بین رای دهنده و محیط رای گیری خود در طول مرحله رای گیری کامل استفاده نماید. Civitas متکی بر این واقعیت است که حداقل یک مرجع ثبت نام به طور کامل قابل اعتماد (C6) وجود دارد و رقیب نمی تواند کانال ارتباطی بین رای دهنده و مقام مجاز ثبت نام مورد اعتماد (C5) مشاهده نماید. در غیر این صورت، اگر رقیب پس از فاز قبل از رای گیری همه مواد کلیدی از رای دهنده را به دست آورد، رقیب می تواند ارتباط بین رای دهنده و مقام مجاز را رمزگشایی کند و در نتیجه اعتبار واقعی رای دهنده را به دست آورد. علاوه بر آن باید چنین فرض شود که یک مجموعه آستانه افراد کلیدی معتمد به منظور رمزگشایی غیرقانونی آرا، اعتبارات همراه، و / یا اعتبار نامه های معتبر نوشته شده توسط مقامات ثبت نام همراه با نام رای دهنده در نقش رمزگشایی قابل اعتماد انتخاباتی (C6) وجود دارند. در نهایت، سیستم فرض می کند که رقیب محیط رای گیری رای دهنده (C9) کنترل نمی کند ، در غیر این صورت این محیط می تواند انتخاب رای دهنده و یا حتی اعتبار واقعی او را ارسال نماید و در نتیجه محرمانه بودن نقض می شود. در (Neumann و Volkamer، 2012)، Civitas عملا با توجه به پنهان کاری بهبود یافته است. در این نسخه بهبود یافته، مفروضات (C7، C8 : قبل از رای گیری) و (C5) توسط یک مرجع ثبت تحت نظارت نمونه برداری می شوند.

Civitas از عدالت و انصاف توسط یک طرح رمزگذاری آستانه مشابه تکنیک های رمزگذاری و ترکیبات هموморفیک اطمینان حاصل می کن؛ از این رو مجموعه آستانه افراد کلیدی معتمد باید مورد اعتماد باشند (C6) . علاوه بر این، محیط رای گیری مخرب (C9) ممکن است اعتبار واقعی رای دهنده را با اعتبار رای منتشر کند.

Civitas تمامیت به صورت در نظر گرفته شده را با این فرض تضمین می کند که محیط رای گیری قابل اعتماد (C9)با توجه به ذخیره سازی اعتبار واقعی رای دهنده است. از این رو، دستکاری محیط رای گیری می تواند اعتبار رای در نظر گرفته شده اختصاص داده شده به رای دهنده را نامعتبر نماید. Civitas اجازه می دهد تا رای دهنده رای خود را که در تابلو اعلانات ذخیره شده است بررسی نماید، به طوری که یکپارچگی رای به صورت ذخیره شده روی پیش فرض های رقابتی متکی نیست. یکپارچگی شمارش شده به عنوان ذخیره شده بدون محدودیت رقابتی با توجه به اثبات ZK متناظر داده می شود.

درجه اثبات پذیری : همانطور که در بالا نشان داده شده است، Civitas اثبات پذیری ذخیره شده به صورت رای و شمارش شده به صورت ذخیره شده را فراهم می کند؛ از این رو، دو تا از سه ویژگی ها، قابل اثبات می باشد.

ویژگی های بیشتر و معیارهای بیشتر

با این فرض که حداقل نیمی از مقامات ثبت نام قابل اعتماد هستند، رای دهنده فاقد صلاحیت نمی تواند اعتبار (شیرازی، Neumann، Ciolacu، و Volkamer، 2011) را به دست آورد. به بیانی دیگر، رای دهنده می تواند اعتبار واقعی آنها را ارسال نماید و در نتیجه به رقیب اجازه دهد تا از طرف آنها رای دهد. در اصل، این کار با استفاده از اعتبار واقعی و جعلی جلوگیری می شود که نمی تواند توسط رقیب شده توسط پیش فرض های ساخته شده برای پنهان کاری متمایز شود. از این رو، Civitas تمایل به اطمینان از واجد شرایط بودن و منحصر به فرد در تفسیر قوی خاص دارد. Civitas محرمانه بودن را تحت رقیب خاص تضمین می کند و در نتیجه حجم کار محاسباتی بسیار زیادی را برای افراد کلیدی معتمد قرار می دهد. از نظر محاسباتی پرهزینه ترین بخش، حذف رای های غیر مجاز است. مقدار قابل توجهی از کار روی بهبود پیچیدگی مرحله ثبت کننده وجود دارد (Weber، Araujo، و Buchmann، 2007؛ Spycher و همکاران، ۲۰۱۱). علاوه بر این، رای دهنده مسئول بسیاری از محاسبات می

باشد، که از کسب اعتبار سهام توزیع شده و ترکیب اعتبار همراه با تأیید اثباتZK تا آماده سازی رای گیری و اثبات ZK متناظر شروع می شود که نشان دهنده رفتار مناسب رای دهنده است.

دموکراسی خیلی خوب

در این بخش، ما مورد دموکراسی خیلی خوب (PGD) را معرفی می کنیم که (Ryan و Teague، ۲۰۰۹)، ترکیبی از رای گیری کد و ترکیبات است. PGD بر اساس روش رای گیری کد است، اما پنهان کاری را در رابطه با رای دهنده که هدفش، اثبات چگونگی رای دادن است، بهبود می بخشد. توجه داشته باشید، پیشنهادات دیگری وجود دارد - دموکراسی قابل فهم (PUD) پیشنهاد شده توسط Budurushi و همکاران . (۲۰۱۳) - که آن هم ترکیبی از رای گیری کد و ترکیبات است؛ با توجه به این واقعیت است که PUD هنوز به طور گسترده ای در متون علمی مشخص نشده است، ما از تجزیه و تحلیل آن خودداری میکنیم و تصمیم میگیریم تا روی تجزیه و تحلیل PGD تمرکز کنیم.

توصیف

در مرحله قبل از رای گیری، مقام رای گیری، کدهای تصادفی $k \cdot n \cdot (m+1)$ را تولید می کند که در آن k پارامتر کتاب کد اضافه تولید شده برای استفاده در طول فرایند ممیزی است، n تعداد رای دهندگان و m تعداد نامزدها است و هر کد را با کلید عمومی مشترک افراد کلیدی معتمد رمز گذاری می کند. این کدهای رمز شده شامل کدهای رای دهی و کدهای تصدیق می شوند و در تابلو اعلانات نصب می شوند. در زیر، کدهای رمز شده ترکیبی توسط افراد کلیدی معتمد قابل اثبات هستند وP کدهای رمز شده ساخته شده است. هر سطر از P مربوط به کتاب کد تولید شده است و توسط IDکتاب کد، کد های رمز شده برای m نامزد مشخص شده است

$$i, \{c_{i,1}\}_{pk}, \dots, \{c_{i,m}\}_{pk}, \{c_{i,ack}\}_{pk}$$

مرجع ثبت در همکاری با افراد کلیدی معتمد به صورت توزیعی، کتاب کد را رمزگشایی می کند و کتاب کد را در پاکت مهر و موم شده به افسر ارجاع دهنده ارسال می کند. پس از ممیزی کتاب کد تصادفی، افسر بازگشتی به طور تصادفی کتاب کد را به هر رای دهنده واجد شرایط اختصاص می دهد. پس از آن، سفارش کدهای رمز شده را در هر

کتاب کد در جدول P با جایگشت می شود، و نتیجه، جدول Q است. در برابر ترکیبات خالص، جایگشت این ترکیبات باید در مرحله پس از رای گیری برای ثبت نتیجه بازسازی شود. بنابراین، هر امانت دار کلیدی جایگشت را انجام می دهد و کد را در کتاب کد دوباره رمز گذاری می نماید و از نظر هوموورفیک این مقدار جایگشت را به مقدار جایگشت های قبلی در آن کتاب کد می افزاید: از این رو، نتیجه جایگشت φ برای کدهای رمز شده در کتاب کد iدر کتاب کد بدون آنکه کسی از این جایگشت اطلاع داشته باشد ذخیره می شود. بنابراین، پس از جایگشت کتاب کد در P، ردیف ها در جدول Q به دست آمده باید به صورت زیر باشد:

$$i, \{c_{i,\phi(1)}\}_{pk}, \dots, \{c_{i,\phi(m)}\}_{pk}, \{c_{i,ack}\}_{pk}, \{\phi_i\}_{pk}$$

در مرحله رای گیری، رای دهنده سرور رای گیری را اعتبار می بخشد. پس از آن او انتخاب را انجام می دهد و کتاب کد ID خود را با کد رای گیری انتخاب شده به سرور رای گیری می فرستد. سرور رای گیری، کد رای گیری او را رمز گذاری می کند، یک اثبات ZK را برای آگاهی از کد تولید می کند و کد رای گیری رمزگذاری شده را همراه با اثبات ZK در ردیف مربوطه به تابلو اعلانات ارسال می کند. افراد کلیدی معتمد، آزمون هم ارزی متن بین کد رای گیری و کد در کتاب کد را متناظر با جدول Q اجرا میکنند. اگر این تطبیق برقرار باشد، این کد در کتاب کد می را توان در تابلو اعلانات مشخص نمود. در نهایت، کد اذعان مربوطه به صورت توزیعی توسط افراد کلیدی معتمد رمزگشایی می شود و به رای دهنده بازگردانده می شود. در مرحله پس از رای گیری، برای هر سطر شاخص، کد مشخص شده رمزگذاری می شود و به صورت هوموورفیک به مقدار جایگشت رمزگذاری $\{\phi_i\}_{pk}$ اضافه می شود. رمزگذاری حاصل، رمزگذاری شاخص نامزد انتخاب شده است. از این رو، این رمز گذاری ها، به صورت قابل بررسی ترکیب می شود و توسط افراد کلیدی معتمد رمزگشایی می شوند.

مدل امنیتی

مدل رقیب: با توجه به کانال کتاب کد و کانال بین رای دهنده و تابلو اعلانات، هیچ مفروضاتی نباید در مورد محرمانه بودن ساخته شود. حتی یک رای دهنده حمل و نقل کننده کد اذعان خود می تواند رقیب را در مورد انتخاب خود

آگاه نماید، به دلیل این واقعیت که تنها یک کد تصدیق برای کتاب کد او وجود دارد. از این رو، حتی انتشار کد اذعان، محرمانه بودن را نقض نمی کند. حتی یک رقیب کنترل کننده محیط رای گیری می تواند پنهان کاری را نقض نماید. با این حال، اگر سرور رای گیری (C6) هویت رای دهنده را همراه با کد رای دادن او و مقام مجاز ثبت نام (C6) نامزد اختصاص داده شده نشان دهد، محرمانه بودن را نقض کرده است .

مجموعه آستانه افراد کلیدی معتمد نیز باید با توجه به عدالت و انصاف به منظور رمزگشایی ننمودن و تفسیر ننمودن کدهای رای دهی در سراسر مرحله رای گیری (C6) مورد اعتماد باشند.

تمامیت رای به عنوان در نظر گرفته شده متکی بر این واقعیت است که مقام مجاز ثبت نام (C6) و محیط رای گیری (C9) همکاری ندارند. اگر آنها این کار را انجام دهند، محیط رای گیری می تواند تماس مقام مجاز ثبت نام را با کد رای دهندگان متفاوت از کتاب کد خاص برقرار نماید و نه کد رای گیری رای دهنده. یکپارچگی رای به صورت ذخیره شده به دلیل حمله به زیر ارائه نمی شود: اگر یک سرور رای گیری مخرب (C6) کد رای گیری رای دهنده را دریافت کند، می تواند با مرجع ثبت مخرب (C6) برای به دست آوردن کد رای دهی معتبر تماس برقرار نماید . سپس سرور رای گیری با یک کد رای گیری متفاوت ارسال شده توسط رای دهنده اقدام می نماید. اثبات پذیری شمارش به صورت ذخیره شده را با توجه به فرآیند ممیزی جایگشت نامزد و ترکیبات قابل اثبات و رمزگشایی قابل اثبات می توان تضمین نمود.

Ryan (۲۰۱۱) بهبودی را برای اعتماد به مقام مجاز ثبت نام پیشنهاد می کند. در این کار، نویسنده رویکرد تولید و چاپ کتاب کد توزیع شده را ارائه می دهد که اجازه می دهد مقامات ثبت نام توزیع و چاپ و توزیع ارقام فردی کدهای معتبر را برای رای دهنده انجام دهند به طوری که هیچ یک از این مقامات، کد رای دهی کامل را نمی داند است. در نتیجه، تنها باید چنین فرض شود که رقیب روی همه مقامات ثبت نام به طور همزمان (C6) کنترل ندارد.

درجه اثبات پذیری: تجزیه و تحلیل یکپارچگی بالا نشان می دهد که تنها شمارش شده به صورت ذخیره شده قابل اثبات است، از این رو، یکی از سه تا ویژگی های فرعی قابل اثبات است.

ویژگی های بیشتر و معیارهای بیشتر

به منظور میسر نمودن رای دادن رای دهنده فاقد شرایط لازم برای رای، آنها باید کتاب کد معتبر را به دست آورند و سرور رای گیری را تصدیق نمایند. از این رو، اگر مرجع ثبت و سرور رای گیری همکاری داشته باشند، واجد شرایط بودن و منحصر به فرد نقض می شود. علاوه بر این، آستانه افراد کلیدی معتمد غیرقانونی ممکن است کتاب کد را رمزگشایی نماید و آنها را به سرور رای گیری ارسال نماید که یک رای را برای یک کتاب کد پست می کند. مقدار اثبات ZK تولید شده در مرحله قبل از رای گیری و پس از رای گیری، بالا است. علاوه بر این، در طول مرحله رای گیری، مقدار قابل توجهی از ارتباطات میان افراد کلیدی معتمد به منظور اجرای آزمایش هم ارزی متنی توزیع و رمزگشایی کدهای اذعان مناسب برای همه رای دهندگان مورد نیاز است. به این منظور، هزینه محاسباتی PDG نسبتا بالا است.

نتیجه گیری و جهت گیری های آینده

با توجه به طیف گسترده ای از نیازهای خلاف امنیت، رای گیری الکترونیکی، و به طور خاص، رای گیری الکترونیکی از راه دور با روش های امنیتی و رمز نگاری دست به دست می رود. به طور مداوم، به ویژه مفاهیم امنیتی جدید و تکنیک های ارائه شده به صورت خطرات ناشی از پیش فرض های رقابتی حیاتی است. تا به امروز، یک مقدار قریب به اتفاق از آثار در مورد تکنیک های رمزنگاری و امنیتی در سیستم های رای گیری الکترونیکی تمرکز وجود دارد. با این حال، در متون مختلف، از منظر دنیای واقعی (به عنوان مثال، سیاسی تصمیم گیرندگان) دو روند ناامید کننده دیده می شود : اول، مفاهیم امنیت تکنیک های SNC اغلب نسبت به تکنیک های خاص تنظیم می شوند که باعث می شود آنها سخت و یا حتی غیر ممکن شوند . دوم، تکنیک ها به طور کامل در محیط جهان واقعی خود را در نظر گرفته می شوند و عوامل تعیین کننده برای استفاده در دنیای واقعی خود در نظر گرفته می شوند. در نتیجه، این منجر به شکاف اساسی بین دستاوردهای نظری و کاربردهای عملی می شود.

برای پر کردن این فاصله، در این فصل ما پنهان کاری، انصاف، صداقت، و اثبات پذیری را به روشی محدود کننده مشخص کردیم و مدل امنیتی مدولار را ارائه دادیم که ارزیابی این ویژگی ها را میسر می سازد. بر اساس روش ارائه

شده، ما تعدادی از تکنیک های SNC را با توجه به ویژگی های بیشتری که فراتر از ملاحظات امنیتی خالص هستند، یعنی هزینه تجزیه و تحلیل نمودیم. معلوم می شود این معیار برای استقرار در دنیای واقعی از سیستم های رای گیری الکترونیکی ضروری است. در حالی که تمرکز این کار روی رای گیری الکترونیکی از راه دور، بسیاری از تکنیک های مورد بحث در اینجا نیز می توان برای رای گیری الکترونیکی مرکز رای دهی استفاده نمود

بینش های به دست آمده از این کار از نقطه نظر عملی از این دیدگاه جالب است. تفسیر دقیق محرمانه بودن، انصاف، صداقت، و اثبات پذیری در سیستم های رای گیری الکترونیکی اولین اجازه می دهد تا اقدام کنندگان روشی را برای نیازهای خود شناسایی نمایند و نشان می دهد دوم که تکنیک ها و سیستم هایی که اغلب ارائه اثبات پذیری را تفسیر می کنند. به نظر می رسد که روش های طبقه بندی شده برای قبل از رای دادن و رای گیری مرحله مشکلات در تشخیص حذف رای نامشروع مواجه هستند. این ناشی از این حقیقت است که محیط های رای گیری دستکاری شده ممکن است سیستم های کد گذاری مشابه را از انتخاب های یکسان تولید نمایند که رای دهندگان نمی توانند عدم وجود رای های فردی خود را تشخیص دهند. یکی از راه های غلبه بر این اشکال، دخالت رای دهنده در مشخصنمودن ترکیبات رای او، به عنوان مثال، با انتخاب تصادفی مورد استفاده برای رمزگذاری رای است. در این مورد، با این حال باید تاکید کرد که توافق های مهمی در رابطه با پنهان کاری باید ساخته شود چون رای دهنده ممکن است نام خود را به رقیب ارسال نماید. تکنیک های طبقه بندی شده در مرحله پس از رای گیری ظاهرا از این نقطه ضعف رنج می برند. هر چند، در این مورد، حملات خودداری اجباری را می توان اجرا نمود.

به عنوان توصیه آخر، ما تصمیم گیران و کادر فنی درگیر در اجرای رای گیری الکترونیکی را به انجام یک تجزیه و تحلیل تهدید و ریسک با توجه به شرایط انتخاباتی خود به منظور شناسایی روش SNC مناسب برای اجرا تشویق مینماییم. رای گیری کد و بهبود استخراج دموکراسی باید برای تضمین محرمانه بودن و انسجام روی محیط های رای گیری دستکاری شده در آینده با هزینه پیاده سازی کانال امن صورت گیرد. امضاهای پنهان در ابتدا برای سیستم های رای گیری الکترونیکی پیاده سازی شده اند و اثبات شده که برای دستگاه های کم منبع کافی هستند (به عنوان مثال کارت های هوشمند) در حالی که به طور همزمان دسترسی نسبت به عموم مردم را ارائه می دهند.

هر دو رای گیری کد و امضای پنهان با این حال باید اثبات پذیری رای به صورت ذخیره شده را بهبود بخشند. رمزنگاری هوموورفیک و ترکیبات، ارائه دهنده اثبات پذیری هستند و از محرمانه بودن تحت مفروضات معقول اطمینان حاصل می نمایند. با این حال باید توجه داشت که این روش ها هزینه های محاسباتی و اجرایی قابل توجهی دارند و ممکن است در نتیجه نمی توانند برای تمام شرایط انتخابات مناسب باشد. Civitas، پنهان کاری را در مقابل رقیبان به طور فعال موثر بر رای دهنده در مرحله رای گیری و در نتیجه یک سیستم خاص تضمین می کند. اثبات پذیری نمی تواند توسط این سیستم قابل تضمین باشد در حالی که در همان زمان هر دو تلاش های اداری و محاسباتی خسته کننده است. در جدول ۱ ما نتایج حاصل از ارزیابی های خود را به طور خلاصه ارائه نموده ایم.

در آینده، روش های SNC باید به طور کامل در یک چشم انداز سیستماتیک یکپارچه، به طور خاص از جمله ساز و کارهای شناسایی و احراز هویت منسجم شوند. تنها با یکپارچه سازی این مکانیزم به روش SNC، مدل امنیتی دقیق را می توان برای واجد شرایط بودن و منحصر به فرد بودن و برای خصوصیات بیشتر به دست آمده از قانون مانند ناشناس ماندن و پاسخگویی مورد بررسی قرار داد. علاوه بر این، فقط ادغام تکنیک های SNC در سیستم، برآورد هزینه های کلی را میسر می سازد.

علاوه بر این، اصل ماهیت عمومی فراتر از اثبات پذیری خالص است، اما مستلزم آن است که تمام مراحل اصلی فرایند رای گیری باید برای رای دهنده قابل فهم باشد.

صداقت / اثبات پذیری	انصاف	محرمانه بودن	تکنیک ها
رای به صورت در نظر گرفته شده : قابل اثبات ذخیره شده به عنوان رای: رقیب نمی تواند مقام مجاز ثبت نام و مقام مجاز ثبت کننده را به طور همزمان کنترل کند.	رقیب می تواند روی مقام مجاز ثبت نام کنترل داشته باشد. رقیب می تواند اطلاعات را از رای دهنده به دست آورد.	رقیب نمی تواند کانال بین مقام مجاز ثبت نام و رای دهنده را بخواند. رقیب می تواند مقام مجاز ثبت نام را کنترل نماید. رقیب می تواند اطلاعات را از رای دهنده به دست آورد.	کد رای گیری

شمارش شده به صورت ذخیره شده : قابل اثبات			
رای به عنوان در نظر گرفته شده : قابل اثبات ذخیره شده به عنوان رای: رقیب می تواند محیط رای گیری و مقام مجاز ثبت کننده به طور همزمان را کنترل کند شمارش شده به صورت ذخیره شده : قابل اثبات	رقیب نمی تواند کانال بین رای دهنده و مقامات ثبت را بخواند. رقیب نمی تواند مقام مجاز ثبت کننده کنترل کند. رقیب نمی تواند محیط رای گیری کنترل کند.	رقیب نمی تواند منشاء پیام در کانال بین رای دهنده و مقامات ثبت کننده را مشخص کند. رقیب نمی تواند ثبت نام و مقام مجاز ثبت کننده به طور همزمان کنترل کند. رقیب نمی تواند اطلاعات را از رای دهنده قبل از مرحله پس از رای گیری به دست آورند. رقیب نمی تواند محیط رای گیری را کنترل کند.	رمز تصدیق آنلاین تصادفی
رای به عنوان در نظر گرفته شده : قابل اثبات ذخیره شده به عنوان رای : رقیب محیط رای گیری و هیئت مدیره به طور همزمان کنترل نمی شوند. شمارش شده به صورت ذخیره شده : قابل اثبات	رقیب نمی تواند کانال بین رای دهنده و مقامات ثبت کننده به عنوان بخواند. رقیب نمی تواند محیط رای گیری را کنترل کند. رقیب نمی تواند مقام مجاز ثبت کننده کنترل نیست.	رقیب نمی تواند فرستنده پیام را نسبت به مقام مجاز ثبت کننده مشخص نماید. رقیب نمی تواند محیط رای گیری را کنترل کند.	امضاهای پنهان
رای به عنوان در نظر گرفته شده : قابل اثبات ذخیره شده به عنوان رای : قابل اثبات شمارش شده به صورت ذخیره شده : قابل اثبات	رقیب نمی تواند یک مجموعه آستانه افراد کلیدی معتمد را کنترل کند. رقیب نمی تواند محیط رای گیری را کنترل کند .	رقیب نمی تواند یک مجموعه آستانه افراد کلیدی معتمد را کنترل کند. رقیب می تواند محیط رای گیری را کنترل کند.	رمزنگاری هوموورفیک
نظرسنجی به عنوان در نظر گرفته شده : قابل اثبات ذخیره شده به عنوان بازیگران	رقیب نمی تواند یک مجموعه آستانه افراد کلیدی معتمد را کنترل نماید.	رقیب نمی تواند تمام گره ترکیبی را کنترل کند . رقیب نمی تواند یک مجموعه آستانه	ترکیبات

: قابل اثبات شمارش شده به صورت ذخیره شده : قابل اثبات است.	رقیب نمی تواند محیط رای گیری را کنترل کند.	افراد کلیدی معتمد را کنترل کند. رقیب نمی تواند محیط رای گیری را کنترل نماید.	

References

Adida, B. (2006). *Advances in Cryptographic Voting Systems*. Cambridge, MA, USA: Massachusetts Institute of Technology

Adida, B. (2008). Helios: Web-based Open-Audit Voting. In P.C. van Oorschot (Ed.) Proceedings of the 17th conference on Security symposium (pp. 335-348). Berkeley, CA, USA. USENIX Association

Adida, B., Neff, C.A. (2009). Efficient receipt-free ballot casting resistant to covert channels. In D. Jefferson, J.L. Hall, T. Moran (Eds.), Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE) (pp. 11-11). Berkeley, CA, USA. USENIX Association

Adida, B., Pereira, O., De Marneffe, O. Quisquater, J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of Helios, In D. Jefferson and J.L. Hall and T. Moran (Eds.), In Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE) (pp. 10-10). Berkeley, CA, USA. USENIX Association

Amenaza Technologies Limited, Ingoldsby T. R. (2005). Attack Tree-based Threat Risk Analysis.

Benaloh, J. (2006). Simple Verifiable Elections. In USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop (pp. 5-5). Berkeley, CA, USA

Blum, M., Feldman, P., Micali, S. (1988). Non-Interactive Zero-Knowledge and Its Applications. In Proceedings of the 29th annual ACM Symposium on Theory of Computing (pp. 103-112). ACM Press, New York

Budursuhi, J., Neumann, S., Volkamer, M. (2012). Smart Cards in Electronic Voting - Lessons learned from applications in legally binding elections and approaches proposed in scientific papers. In Proceedings of the 5th Conference on Electronic Voting 2012 (pp. 258-271), LNI GI Series, Bonn.

Budurushi, J., Neumann, S., Olembo, M., Volkamer, M. (2013). Pretty Understandable Democracy. In Proceedings of Eighth International Conference on Availability, Reliability, and Security (pp. 198-207). Washington, DC, USA. IEEE Computer Society

Carlos, M., Martina, J., Price, G., Custodio, R. (2013). An updated threat model for security ceremonies. In Proceedings of the 28th Annual ACM Symposium on Applied Computing (pp. 1836–1843). New York, NY, USA. ACM

Chase, M., Kohlweiss, M., Lysyanskaya, A., Meiklejohn, S. (2012). Malleable Proof Systems and Applications. In D. Pointcheval and T. Johansson (Eds.) Advances in Cryptologoy - 2012: Vol. 4886 Lecture Notes in Computer Science (pp. 281-300). Cambridge, UK, Springer

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM, 24*(2), (pp. 84-90). NY, USA.

Chaum, D. (2001). SureVote: Technical Overview. Proceedings of the Workshop on Trustworthy Elections (WOTE '01)

Chaum, D., Pedersen, Pedersen, T.P. (1992). Wallet Databases with Observers. In E.F. Brickell (Ed.), Advances in Cryptology – CRYPTO 1992: Vol. 740 Lecture Notes in Computer Science (pp. 89-105). London, UK, Springer

Chaum, D., van Heyst, E. (1991). Group signatures. In Advances in Cryptology - Eurocrypt 1991: Vol. 547 Lecture Notes in Computer Science (pp. 257-265). Cambridge, UK, Springer

Clarkson, M.R, Chong, S., Myers, A.C. (2008). Civitas: Toward a Secure Voting System. In IEEE Symposium on Security and Privacy (pp. 354-368). Oakland, CA. IEEE Computer Society

Clarkson, M.R., Myers, A.C. (2005): *Coercion-resistant remote voting using decryption mixes*. In Workshop on Frontiers in Electronic Elections

Cramer, R., Gennaro, R., Schoenmakers, B. (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. In Advances in Cryptology - Eurocrypt 1997: Vol. 1233 Lecture Notes in Computer Science (pp. 103-118). Konstanz, Germany. Springer

Dolev, D., Yao, A. (1983). On the security of public key protocols. Technical Report. Stanford, CA, USA.

El Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley, David Chaum (Eds.): Advances in Cryptology – CRYPTO 1984: Vol. 196 Lecture Notes in Computer Science (pp. 10-18). Santa Barbara, California, USA. Springer

Feldman, P. (1987). A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the 28th Annual Symposium on Foundations of Computer Science (pp. 427-438). Washington, DC, USA. IEEE Computer Society

Fiat, A., Shamir, A. (1986). How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Advances in Cryptology - CRYPTO 1986: Vol. 263 Lecture Notes in Computer Science (pp. 186-194), Santa Barbara, CA, USA. Springer

Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T. (1999). Secure distributed key generation for discrete-log based cryptosystems. Journal of Cryptology, 20(1), (pp. 51-83)

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st annual ACM symposium on Theory of computing (pp. 169-178). ACM, NY, USA

Gjøsteen, K. (2010). Analysis of an internet voting protocol. In Cryptology ePrint Archive, Report 2010/380.

Goldreich, O., Kahan, A. (1995). How to Construct Constant-Round Zero-Knowledge Proof Systems for NP. Journal of Cryptology, 9, (pp. 167-190)

Heather, J., Ryan, P.Y.A, Teague, V. (2010). Pretty good democracy for more expressive voting schemes. In D. Gritzalis, B. Preneel, M. Theoharidou (Eds.): Proceedings of European Symposium on Research in Computer Security: Vol. 6345 Lecture Notes of Computer Science (pp. 405-423). Athens, Greece. Springer

Helbach, J. (2008). Code Voting - Ein Verfahren für Aktiengesellschaften? In: Informatik 2008, Vol. 1, (pp. 417–422)

Helbach, J. (2009). Code Voting mit prüfbaren Code Sheets. In S. Fischer, E. Maehle and R. Reischuk (Eds.): GI Jahrestagung 2009. (pp. 1856-1862)

Jakobsson, M., Juels, A. (2000). Mix and match: Secure function evaluation via ciphertexts. In T. Okamoto (Ed.): Advances in Cryptology - ASIACRYPT 2000: Vol. 1976 Lecture Notes of Computer Science (pp. 162-177). London, UK. Springer

Jakobsson, M., Juels, A., Rivest, R.L. (2002). Making mix nets robust for electronic voting by randomized partial checking. In Proceedings of the 11th USENIX Security Symposium (pp. 339-353), Berkeley, CA, USA. USENIX Association

Joaquim, R., Ribeiro, C., Ferreira, P. (2009). VeryVote: A Voter Verifiable Code Voting System. In Ryan, P.Y.A. Ryan, B. Schoenmakers (Eds.): VOTE-ID 2009: Vol. 5767 Lecture Notes in Computer Science (pp. 106-121). Springer

Karayumak, F., Kauer, M., Olembo, M. M., Volk, T. & Volkamer, M. (2011). User study of the improved Helios voting system interfaces. *STAST* (pp. 37-44). IEEE Computer Society

Klink, A. (2006). Cryptographic Voting Protocols: A Prototype Design and Implementation for University Elections at TU Darmstadt. Diploma Thesis. Darmstadt, Germany

Kremer, S., Ryan, M., Smyth, B. (2010). Election verifiability in electronic voting protocols. In D. Gritzalis, B. Preneel, M. Theoharidou (Eds.): Proceedings of European Symposium on Research in Computer Security: Vol. 6345 Lecture Notes of Computer Science (pp. 389-404). Athens, Greece. Springer

Küsters, R., Truderung, T., Vogt, A. (2012). Clash Attacks on the Verifiability of E-Voting Systems. *IEEE Symposium on Security and Privacy* (pp. 395-409), : IEEE Computer Society

Lambrinoudakis, C., Gritzalis, D., Tsoumas, V., Karyda, M. & Ikonomopoulos, S. (2003). Secure Electronic Voting: the Current Landscape. In D. Gritzalis (ed.), *Secure Electronic Voting*, Vol. 7 (pp. 101-122). Springer

Langer, L. (2010). Privacy and verifiability in electronic voting. Ph.D. Thesis. Darmstadt, Germany

Liu, J.K., Wei, V.K., Wong, D.S (2004). Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. In H. Wang, J. Pieprzyk, V. Varadharajan (Eds.): Australasian Conference on Information Security and Privacy, ACISP 2004: Volume 3108 Lecture Notes in Computer Science (pp. 325-335), Springer

Lundin, D. (2010). Component based electronic voting systems. In D. Chaum, M. Jakobsson, R. L. Rivest, P.A. Ryan, J. Benaloh (Eds.) Towards Trustworthy Elections: Vol. 6000 Lecture Notes in Computer Science (pp. 260-273). Springer

MacNamara, K., Iedemska, I. (2012). A Survey of Electronic Voting Schemes. Student Project at University of California.

Mercuri, R. (2002) A Better Ballot Box? IEEE Spectrum, Vol. 39, 2002. IEEE Computer Society

Mitrou, L., Gritzalis, D., & Katsikas, S. (2002). Revisiting legal and regulatory requirements for secure e-voting. *Paper presented at the 16th IFIP International Information Security Conference.* Cairo, Egypt. Kluwer Academics Publisher

Moran, T., Naor, M. (2007). Split-Ballot Voting: Everlasting Privacy with Distributed Trust. In Proceedings of the 14th ACM conference on Computer and communications security. (pp. 246-255), New York, NY, USA. ACM

Mursi, M.F.M, Assassa, G.M.R, Abdelhafez, A., Samra, K.M.A. (2013). On the Development of Electronic Voting. International Journal of Computer Applications, 61(16), 1-11

Naor, M. (1991). Bit Commitment Using Pseudo-Randomness. Journal of Cryptology, 4, 151-158

Naor, M., Pinkas, B. (1999). Oblivious Transfer and Polynomial Evaluation. In Proceedings of the 31st Annual ACM Symposium on Theory of Computing (pp. 245 - 254). ACM Press, New York

Neff, A. (2004): Practical high certainty intent verification for encrypted votes.

Neumann, S., Volkamer, M. (2012). Civitas and the Real World: Problems and Solutions from a Practical Point of View. In Proceedings of Seventh International Conference on Availability, Reliability, and Security (pp. 180-185). Washington, DC, USA. IEEE Computer Society

OASIS Standard (2007): Election Markup Language (EML) Version 5.0 Process and Data Requirements

OSCE/ODIHR (2012). Norway: Internet Voting Pilot Project / Local Government Election / 12 September 2011.

Olembo, M., Schmidt, P., Volkamer, M. (2011). Introducing Verifiability in the POLYAS Remote Electronic Voting System. In Proceedings of Sixth International Conference on Availability, Reliability, and Security (pp. 127-134). Washington, DC, USA. IEEE Computer Society

Olembo, M., Kahlert, A., Neumann, S., Volkamer, M. (2012). Partial Verifiability in POLYAS for the GI Elections. In Proceedings of the 5th Conference on Electronic Voting 2012 (pp. 95-109), LNI GI Series, Bonn.

Organization for the Advancement of Structured Information Standards (2007). Election Markup Language (EML) v5.0

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Advances in Cryptologoy - Eurocrypt 1999: Vol. 1592 Lecture Notes in Computer Science (pp. 223-238). Cambridge, UK, Springer

Pedersen, T.P. (1991). A Threshold Cryptosystem without a Trusted Party. In Advances in Cryptologoy - Eurocrypt 1991: Vol. 547 Lecture Notes in Computer Science (pp. 522-526). Cambridge, UK, Springer

Rivest, R., Shamir, A., Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Journal ACM of Communication, 21, 120-126

Rivest, R., Shamir, A., Tauman, Y. (2001). How to leak a secret. In C. Boyd (Ed.): Advances in Cryptology - ASIACRYPT 2001: Vol. 2248 Lecture Notes of Computer Science (pp. 552-565). Springer

Rjašková, Z. (2002). Electronic Voting Schemes. Diploma Thesis. Bratislava, Slovakia

Rössler, T. (2004). e-Voting: A Survey and Introduction. Technical Report

Ryan, P.Y.A., Teague, V. (2009). Pretty Good Democracy. In B. Christianson, J.A. Malcolm, V. Matyas, and M. Roe (Eds.): Proceedings of the 17th International Workshop on Security Protocols. Vol. 7028 Lecture Notes of Computer Science (pp. 111-130). Springer

Ryan, P. Y. A. (2011). Prêt à voter with confirmation codes. In H. Shacham and V. Teague (Eds.), Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE).

Sako, K., Kilian, J. (1995). Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In L. C. Guillou, J.-J. Quisquater (Eds.): Advances in Cryptology - EUROCRYPT 1995. Vol. 921 Lecture Notes of Computer Science (pp. 393-403). Springer

Sandler, D.R., Wallach, D.S. (2008). The case for networked remote voting precincts. In D. L. Dill and T. Kohno (Eds.) Proceedings of the conference on Electronic voting technology (pp. 6-6). Berkeley, CA, USA, USENIX Association

Schnorr, C. (1989). Efficient Identification and Signatures for Smart Cards. In G. Brassard (Ed.), Advances in Cryptology – CRYPTO 1989: Vol. 435 Lecture Notes in Computer Science (239-252). Springer

Shamir, A. (1979). How to Share a Secret. In Communications of the ACM, 22, pp. 612-613

Shirazi, F., Neumann, S., Ciolacu, I., Volkamer, M. (2011). Robust electronic voting: Introducing robustness in Civitas. In Proceedings of International Workshop on Requirements Engineering for Electronic Voting Systems (pp. 47 -55). IEEE Computer Society

Smith, W. (2005). Cryptography Meets Voting. Technical Report

Spycher, O., Koenig, R., Haenni, R., Schläpfer, M. (2011). *A New Approach Towards Coercion-Resistant Remote E-Voting in Linear Time*. In G. Danezis (Ed.) Proceedings of the 15th International Conference on Financial Cryptography and Data Security. Vol. 7035 Lecture Notes of Computer Science (pp. 182-189). Springer

Teague, V., Ramchen, K., Naish, L. (2008). Coercion-resistant tallying for STV voting. In D. L. Dill and T. Kohno (Eds.) Proceedings of the conference on Electronic voting technology (pp. 15-15). Berkeley, CA, USA, USENIX Association

Volkamer, M. (2009). *Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible Election Authorities* (Vol. 30). Springer

Weber, S., Araujo, R., Buchmann, J. (2007). On coercion-resistant electronic elections with linear work. In Proceedings of Second International Conference on Availability, Reliability, and Security. Vienna, Austria. IEEE Computer Society

Wikström, D. (2005). A Sender Verifiable Mix-Net and a New Proof of a Shuffle. In B. Roy (Ed.): Advances in Cryptology - ASIACRYPT 2005: Vol. 3788 Lecture Notes of Computer Science (pp. 273-292). Springer