امضای دیجیتال مقاوم کوانتومی بر اساس همسانی های بین خم های سوپرسینگولار

مصطفی قربانی

استاد راهنما: دکتر حسن دقیق

امنیت بیشتر سیستم های رمزنگاری کلید عمومی که امروزه استفاده می‌شود بر اساس مسائل سخت ریاضیاتی همچون مساله تجزیه اعداد و لگاریتم گسسته می‌باشد. با این حال کامپیوترهای کوانتومی قادر خواهند بود این دو مساله سخت در کامپیوترهای کلاسیک را به طور موثری حل کنند که تهدیدی جدی برای رمزنگاری مدرن خواهد بود.

رمزنگاری پساکوانتومی ، مطالعه سیستم های رمزنگاری کلاسیک می‌باشد که در برابر حملات کوانتومی ایمن باقی می‌مانند. تاکنون چندین سیستم پیشنهادی برای رمزنگاری پسا کوانتومی کاندید شده اند ، از جمله رمزنگاری های مشبکه مبنا ، کد مبنا ، هش مبنا و همین طور رمزنگاری چندمتغیره.

اخیرا سیستم رمزنگاری بر اساس همسانی های بین خم های سوپرسینگولار توسط جائو و همکارانش در [۲] معرفی شده است که این سیستم رمزنگاری شامل پروتکل تبادل کلید ، اثبات دانش صفر هویت و همچنین رمزنگاری کلید عمومی می‌باشد. همسانی ها به دلیل اندازه کلید کوچک و همچنین پیاده سازی موثر آن [۱، ۳] جز کاندیدهای تبادل کلید پسا کوانتومی می‌باشند. چندین طرح احراز هویت بر مبنای همسانی ها ارائه شده است که ما در این پایان نامه قصد داریم به بررسی طرح امضای دیجیتال که قویا غیرقابل جعل در برابر حمله متن انتخاب شده [1] در مدل اوراکل

[1] unforgeable under chosen message attack

تصادفی کوانتومی هستند [۶] بپردازیم. در ادامه به بررسی امضای دیجیتال غیرقابل انکار [۴] و همچنین امضای دیجیتال غیرقابل انکار کور [۵] خواهیم پرداخت.

طرح امضای معرفی شده ، بوسیله اجرای یک انتقال عمومی اثبات دانش صفر هویت ارائه شده در [۲] به دست می‌آید. در سیستم های کلاسیک (قدیمی) رمزنگاری ، امنیت امضای دیجیتال از طریق اثبات دانش صفر تعاملی [2] با اعمال مدل انتقالی فیات_شمیر [3] قابل پیاده سازی بود. اما برای امنیت درمدل های کوانتومی نیاز به طرحی جدید نیاز شد که به تازگی مدل انتقال آنره [4] ارائه شده است که ما برای طرح پیشنهادی خود از این مدل استفاده خواهیم کرد.

رمزنگاری همسانی_مبنا

با داشتن دو خم بیضوی E_1 و E_2 در میدان متناهی F_q با مرتبه q ، یک همسانی ϕ عبارت است از یک نگاشت جبری از خم بیضوی E_1 به خم بیضوی E_2 که

$$\phi(x,y)=\Big(\frac{f_1(x,y)}{g_1(x,y)},\frac{f_2(x,y)}{g_2(x,y)}\Big)$$

چنان که $\phi(\infty)=\infty$. (f_1,f_2,g_1,g_2 چندجمله ای های دو متغیره و ∞ عنصر همانی روی خم بیضوی می‌باشد). به طور معادل ، یک همسانی یک نگاشت جبری؟؟ .دو خم بیضوی E_1 و E_2 را روی $\mathbb{F}_q$ همسان گوییم اگر و تنها اگر یک همسانی بین آنها وجود داشته باشد. قضیه ای معروف به قضیه تیت [5] بیان می کند دو خم E_1 و E_2 همسان هستند اگر و تنها اگر :

$$\#E_1(\mathbb{F}_q)=\#E_2(\mathbb{F}_q)$$

با داشتن یک همسانی $\phi=E_1\to E_2$ از درجه n ، همسانی $\hat{\phi}:E_2\to E_1$ از درجه n وجود خواهد داشت که :

$$\phi o\hat{\phi}=\hat{\phi}o\phi=[n]$$

که $[n]$ یک نگاشت چندبرابر کردن و همسانی $\hat{\phi}$ دوگان همسانی ϕ می‌باشد.

[2] intractive zero-knowledge proof

[3] Fiat-Shamir transform

[4] Unrah

[5] Tate Theorem

برای هر عدد طبیعی n ، زیرگروه $E[n]$ را به صورت زیر معرفی می‌کنیم :

$$E[n] = \{P \in E(\bar{\mathbb{F}}_q) : nP = \infty\}$$

به عبارت دیگر ، $E[n]$ هسته نگاشت n برابر کردن بستار جبری $\bar{\mathbb{F}}_q$ روی میدان $\mathbb{F}_q$ می‌باشد.؟؟؟ گروه $E[n]$ با گروه $(\mathbb{Z}/n\mathbb{Z})^{۲}$ (که n و q نسبت به هم اول اند) یکریخت می‌باشد.

حلقه درون ریختی $End(E)$ را مجموعه ای از تمام همسانی ها از خم E به خودش روی بستار جبری $\bar{\mathbb{F}}_q$ از میدان $\mathbb{F}$ می‌نامیم. حلقه درون ریختی همراه با عمل جمع گروه و عمل ترکیب تشکیل یک گروه می‌دهد. اگر $dim_{\mathbb{Z}}(End(E)) = ۲$ باشد آنگاه خم بیضوی E را یک خم معمولی گوییم و اگر $dim_{\mathbb{Z}}(End(E)) = ۴$ آنگاه خم بیضوی E را سوپرسینگولار می نامیم. دو خم بیضوی همسان یا هر دو معمولی اند یا هر دو سوپرسینگولار هستند.

همسانی $\phi : E_۱ \rightarrow E_۲$ را جداپذیر گوییم هرگاه ؟؟؟ یک ویژگی مهم یک همسانی جداپذیر آن است که اندازه هسته یک همسانی برابر با درجه همسانی می‌باشد . طبق الگوریتم ولو هر تولید کننده هسته یک همسانی منحصر به فرد تولید خواهد کرد.

گراف همسانی

یک گراف ℓ ـ همسانی گرافی است که راس های آن خم های بیضوی همریخت و بین دو خم $E_۱$ و $E_۲$ یک یال وجود دارد اگر وتنها اگر یک ℓ ـ همسانی بین این دو خم وجود داشته باشد. در خم های سوپرسینگولار ، گراف ℓ ـ همسانی گراف متصل است. با داشتن دو راس متفاوت از این گراف پیدا کردن مسیری با اندازه ثابت یک مسئله سخت منظور می‌شود که این سختی مسئله در طراحی سیستم های رمزنگاری همسانی مبنا مورد استفاده قرار می‌گیرد.

اثبات دانش صفر [۶]

برای بیان مفهوم اثبات دانش صفر لازم است دو شخصیت را معرفی کنیم ، پگی [۷] به عنوان

[6] Zero Knowledge Proof
[7] Peggy

یک اثبات کننده [8] و ویکتور [9] به عنوان یک تاییدکننده. [10] به طور رسمی ، یک سیستم اثبات دانش صفر یک رویه است که طی آن پگی ، ویکتور را متقاعد می‌کند که به یک حقیقت معین اشراف دارد بطوریکه هیچ اطلاعات اضافی نسبت به دانش خود در اختیار ویکتور قرار نمی‌دهد تا خود ویکتور نتواند به عنوان یک مدعی دیگران را متقاعد کند که به حقیقت مورد بحث اشراف دارد.در نگاه اول این طور به نظر می‌رسد که با داشتن سیستم های رمزنگاری موجود هیچ شانسی برای ارائه این چالش وجود ندارد. برای مثال پگی (در نیویورک) چگونه می‌تواند ویکتور (در کالیفرنیا) را متقاعد سازد که رنگ خانه اش قرمز است بدون اینکه عکسی از خانه خود برای ویکتور ارسال کند؟ و همچنین اگر پگی عکس خانه خود را برای ویکتور ارسال کند آنگاه ویکتور این قابلیت را خواهد داشت که به دیگران اثبات کند که رنگ خانه پگی را می‌داند!

در عمل ، یک سیستم اثبات دانش صفر (تعاملی) به این شکل است که چندین مرحله ارتباط به صورت چالش و پاسخ بین پگی و ویکتور برقرار می‌شود. در یک مرحله از این ارتباط ویکتور چالشی را برای پگی ارسال می‌کند و پگی متناسب با آن چالش یک پاسخ ارائه می‌دهد و سپس ویکتور با ارزیابی این پاسخ اگر متقاعد شود آنگاه پاسخ را می‌پذیرد و در غیر اینصورت آن را رد می‌کند. پس از طی چندین مرحله مشخص از این پرسش و پاسخ ، یک اثبات دانش صفر خوب مقدار y که ویژگی $\mathcal{P}$ را دارد؟؟ دو ویژگی زیر را برآورده می‌کند :

- تمامیت[11]
اگر پگی صادق باشد و رازی داشته باشد که بخواهد ویکتور را متقاعد کند که راز را می‌داند و همچنین اگر ویکتور نیز صادق باشد آنگاه این پروتکل به درستی انجام می‌پذیرد.

- صداقت[12]
اگر پگی رازی برای اثبات نداشته باشد ولی خواهان آن باشد که ویکتور را به اشتباه متقاعد کند که راز را می‌داندُ این عمل با احتمال بسیار زیادی غیرممکن است(شانس این عمل خیلی خیلی کم می‌باشد).

[8] Prover
[9] Victor
[10] Verifier
[11] Completeness
[12] Soundness

- دانش صفر[13]

در حین انجام این پروتکل هیچ اطلاعات اضافی توسط پگی نباید فاش شود تا ویکتور نتواند بعد از اتمام این اثبات خود در نقش یم اثبات کننده در مقابل دیگران باشد.

مثال پگی دو عدد اول بزرگ p و q را انتخاب و $N(= p \times q)$ را منتشر می‌کند. وظیفه پگی این است که عدد مشخصی مانند y را که در میدان N مربع است را به ویکتور ثابت کند به نحوی که هیچ اطلاعات اضافی را برای ویکتور افشا نکند تا ویکتور نتواند با این اطلاعات خودش در نقش یک اثبات کننده برای y باشد. در این صورت y مربعی در میدان N است اگر پگی عامل های N را بداند و در نتیجه می‌تواند ریشه مربعی برای y همچون x به دست آورد :

$$x^{۲} \equiv y \pmod N$$

در هر مرحله ، پگی و ویکتور مراحل زیر را انجام می‌دهند :

۱. پگی یک عدد تصادفی r را در میدان N انتخاب کرده و مقدار s را به طریق زیر محاسبه و برای ویکتور ارسال می‌کند :

$$s \equiv r^{۲} \pmod N$$

۲. ویکتور به طور تصادفی یک مقدار $\beta \in \{۰, ۱\}$ انتخاب و β را برای پگی ارسال می‌کند.

۳. پگی عدد زیر را محاسبه و برای ویکتور ارسال می‌کند :

$$z \equiv \begin{cases} r \pmod N & if\ \beta = ۰, \\ xr \pmod N & if\ \beta = ۱ \end{cases} \qquad (۱)$$

۴. ویکتور ، $z^{۲} \pmod N$ را محاسبه و بررسی زیر را انجام می‌دهد :

$$z^{۲} \equiv \begin{cases} s \pmod N & if\ \beta = ۰, \\ ys \pmod N & if\ \beta = ۱ \end{cases} \qquad (۲)$$

اگر جواب true باشد ، ویکتور جواب پگی را می‌پذیرد و در غیر اینصورت آن را رد می‌کند.

[13] Zero knowledge

پگی و ویکتور این مراحل را n بار (که عدد نسبتا بزرگی است، به طور مثال ۸۰ بار) تکرار می‌کنند. اگر تمام پاسخ های پگی مورد قبول واقع شود آنگاه ویکتور اثبات پگی (که y مربعی در میدان N) را می‌پذیرد (قانع می‌شود که پگی اثبات را می‌داند) در غیر اینصورت اثبات را نمی‌پذیرد.

انواع اثبات

- اثبات تعاملی

  در این نوع اثبات نیاز به یک ارتباط دوطرفه بین ادعاکننده و اثبات کننده می‌باشد و برای هر ارتباط ادعاکننده با اثبات کننده متفاوت باید ارتباط دوطرفه مجزایی برقرار شود.

- اثبات غیر تعاملی

  در این نوع اثبات نیازی به ارتباط بین ادعا کننده و اثبات کننده نیست و بنابراین ادعای یک راز می‌تواند توسط هر اثبات کننده ای ارزیابی شود.

پروتکل فیات شمیر[۱۴]

پروتکل فیات شمیر تکنیکی در رمزنگاری است که می‌توان یک امضای دیجیتال بر اساس پروتکل دانش صفر تعاملی که ویژگی سکه عمومی [۱۵] را دارد ، معرفی کرد. در واقع اگر اثبات تعاملی ، یک پروتکل احراز هویت باشد آنگاه نسخه غیرتعاملی آن می‌تواند به عنوان یک امضای دیجیتال استفاده شود. در واقع پروتکلی که فیات-شمیر معرفی کرده اند این است که با تکنیکی از یک اثبات دانش تعاملی با فرض یک ویژگی معین به یک اثبات دانش صفر غیرتعاملی می‌رسیم که با این پروتکل می‌توان یک انضای دیجیتال طراحی کرد.

تذکر. در واقع از اثبات دانش تعاملی برای طراحی پروتکل های احراز هویت و از اثبات دانش غیرتعاملی برای طراحی یک سیستم امضای دیجیتال استفاده می‌شود.

در ادامه برای معرفی کامل تر این پروتکل مثال آورده شده است :

مثال. اثبات دانش صفر تعاملی بر اساس مسئله لگاریتم گسسته

[14]Fiat-Shamir heuristic

[15]public-coin

۱. پگی می‌خواهد ویکتور را متقاعد کند که x را می‌داند :

$$y \equiv g^x \pmod q$$

که y و g و میدان q عمومی‌اند.

۲. پگی یک عدد تصادفی ${\mathbb{Z}_q}^* \ni v$ را انتخاب و $t = g^v$ را محاسبه و برای ویکتور ارسال می‌کند.

۳. ویکتور یک عدد تصادفی ${\mathbb{Z}_q}^* \ni c$ انتخاب و برای پگی ارسال می‌کند.

۴. پگی $r = v - cx$ را محاسبه و r را برای ویکتور ارسال می‌کند.

۵. ویکتور تساوی زیر را بررسی می‌کند :

$$t \equiv g^r g^c \pmod q$$

اگر طرف دوم را باز کنیم ، داریم :

$$g^r g^c = g^{v-cx} g^{xc} = g^v = t$$

نکته. اگر در مرحله سوم از یک اوراکل تصادفی غیرتعاملی استفاده کنیم آنگاه طرح اثبات تعاملی ما به یک طرح اثبات غیرتعاملی تبدیل می‌شود که برای رسیدن به این منظور می‌توانیم از تابع هش استفاده کنیم :

۱. پگی می‌خواهد ویکتور را متقاعد کند که x را می‌داند :

$$y \equiv g^x \pmod q$$

که y و g و میدان q عمومی‌اند.

۲. پگی یک عدد تصادفی ${\mathbb{Z}_q}^* \ni v$ را انتخاب و $t = g^v$ را محاسبه و برای ویکتور ارسال می‌کند.

۳. پگی $c = H(g, y, t)$ را محاسبه می‌کند که $H()$ یک تابع هش می‌باشد.

۴. پگی $r=v-cx$ را محاسبه می‌کند و زوج (t,r) به عنوان اثبات نظر گرفته می‌شود.(چنانکه r توانی از g باشد در پیمانه $q-1$ محاسبه می‌شود).

۵. هرکسی می‌تواند $t=g^r g^c$ را بررسی کند.

البته در طرح امضای دیجیتال معرفی شده در پایان نامه از پروتکل آنره [16] برای ساخت یک اثبات دانش غیرتعاملی از اثبات دانش تعاملی نظیر آن استفاده می‌کنیم ، که در ادامه به تشریح این پروتکل می‌پردازیم و چون خود این پروتکل از پروتکل زیگما [17] بهره می‌برد بنابراین توضیح مختصری در ادامه آمده است.

پروتکل زیگما (Σ)

مفهوم پروتکل زیگما را با یک مثال نشان می‌دهیم :

p را عددی اول و q را عاملی از $p-1$ در نظر می‌گیریم. همچنین g عنصری از مرتبه q در $\mathbb{Z}_p^*$ می‌باشد.در ادامه اثبات کننده $\mathcal{P}$ ، یک عدد تصادفی $w \leftarrow_R \mathbb{Z}_q$ را انتخاب می‌کند و $h \equiv g^w \pmod p$ را منتشر می‌کند.تاییدکننده $\mathcal{V}$ ، چندتایی (p,q,g,h) را دریافت می‌کند((p,q,g,h) عمومی اند). پس از دریافت بررسی می‌کند که اعداد p,q اعدادی اول هستندو همچنین بررسی می‌کند که آیا g,h از مرتبه‌ی q هستند یا خیر؟ . از آنجا که فقط یک زیرگروه از مرتبه‌ی q در $\mathbb{Z}_p^*$ وجود دارد بنابراین بدیهی است که $h \in < g >$ و در نتیجه همواره یک مقدار w وجود دارد که $h=g^w$ (دلیل این امر به این دلیل است که در یک گروه از مرتبه عدد اول تمام عناصر به غیر از عنصر همانی مولدند و درنتیجه g یک مولد خواهد بود). با این اوصاف دلیلی وجود ندارد که ثابت کننده $\mathcal{P}$ حتما از w آگاه باشد.

پروتکل اشنور یک راه خیلی موثر ارائه می‌کند تا اثبات کننده $\mathcal{P}$ ، تاییدکننده $\mathcal{V}$ را متقاعد سازد که مقدار یکتای $w \in \mathbb{Z}_q$ را که $h \equiv g^w \pmod p$ می‌داند:

پروتکل اشنور (بر اساس مسئله لگاریتم گسسته)

- ورودی عمومی : اثبات کننده و تاییدکننده هر دو مقادیر (p,q,g,h) را می‌دانند.

[16] Unruh Construction
[17] Zigma Protocol

- ورودی خصوصی : اثبات کننده ، مقدار $w \in \mathbb{Z}_q^*$ را در اختیار دارد که : $h \equiv g^w \pmod p$

- پروتکل :

۱. اثبات کننده $\mathcal{P}$ ، مقدار تصادفی r ($r \leftarrow_R \mathbb{Z}_q$) را انتخاب و $a \equiv g^r \pmod p$ را برای تاییدکننده $\mathcal{V}$ ارسال می‌کند.

۲. تاییدکننده یک چالش تصادفی e ($e \leftarrow_R \{۰, ۱\}^t$) را برای اثبات کننده ارسال می‌کند (که t ثابت با شرط $۲^t < q$)

۳. اثبات کننده مقدار $z \equiv r + ew \pmod q$ را برای تاییدکننده ارسال می‌کند.

۴. تاییدکننده بررسی می‌کند که آیا $g^z \equiv ah^e \pmod p$ (با این دانش که p و q اعداد اولند و g و h هر دو از مرتبه q هستند) ودر نتیجه اگر عبارت بالا برقرار بود آنگاه اثبات پذیرفته و در غیر اینصورت آن را رد می‌کند.
توجه :

$$(g^z \equiv g^{r+ew} \equiv g^r.g^{ew} \equiv a.(g^w)^e \pmod q) \equiv a.h^e \pmod p$$

مراجع

[1] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In *Annual International Cryptology Conference*, pages 572–601. Springer, 2016.

[2] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[3] Amir Jalali, Reza Azarderakhsh, and Mehran Mozaffari Kermani. Efficient implementation of supersingular isogeny-based diffie-hellman key exchange on arm. 2017.

[4] David Jao and Vladimir Soukharev. Isogeny-based quantum-resistant undeniable signatures. In *International Workshop on Post-Quantum Cryptography*, pages 160–179. Springer, 2014.

[5] M Seshadri Srinath and Venkatachalam Chandrasekaran. Isogeny-based quantum-resistant undeniable blind signature scheme. *IACR Cryptology ePrint Archive*, 2016:148, 2016.

[6] Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In *International Conference on Financial Cryptography and Data Security*, pages 163–181. Springer, 2017.