پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

خم‌های بیضوی فوق منفرد در رمزنگاری

نگارنده

پارسا تسبیح‌گو

استاد راهنما: دکتر مرتضی محمدنوری

پایان‌نامه برای دریافت درجه کارشناسی
در رشته علوم کامپیوتر

تاریخ: اردیبهشت ۱۴۰۲

چکیده

هدف این پروژه آشنایی با رمزنگاری بر اساس ایزوژنی‌های خم‌های بیضوی فوق‌منفرد می‌باشد. در این پروژه ابتدا به معرفی مفاهیم مقدماتی خم‌های بیضوی و بطور ویژه بخش‌هایی که در رمزنگاری خم‌های بیضوی کاربرد دارند می‌پردازیم. سپس خم‌های بیضوی را از نگاه هندسه جبری بررسی می‌کنیم و مسائل محاسباتی مبتنی بر ایزوژنی‌های میان این خم‌ها را معرفی می‌کنیم.
در فصل دوم سیستم تبادل کلید SIDH را به عنوان یکی از نمونه‌های رمزنگاری مبتنی بر ایزوژنی بررسی می‌کنیم و نگاهی بر پتانسیل رمزنگاری مبتنی بر ایزوژنی برای رمزنگاری پساکوانتوم می‌کنیم.

سپاسگزاری

سپاسگزاری

این پروژه به عنوان پروژه پایانی جهت دریافت مدرک کارشناسی علوم کامپیوتر از دانشگاه تهران تهیه شده.
استاد راهنما این پروژه دکتر مرتضی محمد نوری از دانشکده ریاضی و علوم کامپیوتر دانشگاه تهران بوده‌اند و صمیمانه از ایشان سپاس گذارم که قبول زحمت کردند.
همچنین دکتر شهرام خزایی از دانشکده علوم ریاضی دانشگاه صنعتی شریف من را در پیشبرد این پروژه راهنمایی کردند از همین رو از ایشان نیز کمال تشکر را دارم.

پیشگفتار

در دنیای امروز که تقریبا همه ارتباطات از طریق کانال‌های الکترونیک انجام می‌شود حفظ امنیت چنین کانال‌هایی چالشی بسیار مهم است که توسط رمزنگاری مدرن امکان پذیر است.
هنگامی که برای اولین بار ایده رمزنگاری نامتقارن یا کلید عمومی در ۱۹۷۰ توسط جیمز الیس [۱] مطرح شد این امکان فراهم شد که دو نفر که هیچگاه یکدیگر را ملاقات نکرده‌اند و به هیچ کانال ارتباطی خصوصی دسترسی ندارند، بدون هیچ دانش خصوصی از پیش معین، پیام‌هایی مبادله کنند که هیچ فرد دیگری نتواند آن‌ها را بخواند و متوجه شود. البته الیس نتوانست ایده خود را پیاده‌سازی کند. اما طولی نکشید که ویتفیلد دیفی [۲] و مارتین هلمن [۳] در سال ۱۹۷۶ نخستین پروتکل تبادل کلید نامتقارن را به طور عمومی منتشر کردند. پس از انتشار این پروتکل امکان امنیت دیجیتال بوجود آمد و اکنون انسان‌ها می‌توانستند سیستم‌های ارتباطی بسازند که امنیت آن‌ها تضمین شده بود.
البته که لازم به ذکر است که این تضمین امنیت نسبی است. شانون [۴] نشان داد که ساختن سیستم رمزنگاری کاملا امن امکان پذیر نیست. اما ما می‌توانیم امنیت را در سطح کاربردی تعریف کنیم و به آن دست یابیم.
امنیت کاربردی معمولا همان چیزی است که در مقالات حوزه رمزنگاری به آن امنیت محاسباتی می‌گویند. در حالت ساده شده می‌توان امنیت محاسباتی را اینگونه تعریف کرد: **هیچ ماشین محاسبه‌گری** موجود نیست که بتواند در زمان معقول (معمولا زمان چندجمله‌ای) با **احتمال غیر ناچیز** امنیت سیستم رمزی مورد نظر را شکست دهد.
کلمات مهم در این تعریف **هیچ ماشین محاسبه‌گری** و **احتمال غیر ناچیز** هستند. در زمانی که الگوریتم‌های که امروزه آن‌ها را می‌شناسیم و استفاده می‌کنیم مثل Diffie-Hellman Key Exchange و RSA ارائه شدند، همه ماشین‌های محاسباتی شناخته شده کامپیوترهای کلاسیک (باینری) بودند، لذا قید هیچ ماشین محاسبه‌گر تنها باید برای این نوع کامپیوترها صادق می‌بود. که چنین بود، یعنی اعتقاد عموم دانشمندان این حوزه این بود که حل مسائلی همچون تجزیه اعداد

[۱] James H. Ellis
[۲] Whitfield Diffie
[۳] Martin Hellman
[۴] Claude Shannon

طبیعی یا محاسبه لگاریتم گسسته با کامپیوترهای کلاسیک در زمان چندجمله‌ای و با احتمال غیر ناچیز ممکن نیست (در حالی که همچنان اثباتی برای این ادعا موجود نیست). اعتقاد به سختی حل این مسائل برای اثبات امنیت الگوریتم‌های نام‌برده شده و خیلی از الگوریتم‌های دیگر کافی بود و تضمین امنیتی که پیشتر از آن صحبت کردیم از همین اعتقاد بدست می‌آمد.

امروز با اینکه همچنان اعتقاد به سختی حل این مسائل نقض یا اثبات نشده اما این اعتقاد دیگر برای تضمین امنیت الگوریتم‌های کلاسیک رمزنگاری کافی نیست و دلیل این شرایط معرفی کامپیوترهای کوانتومی است. همانطور که گفتیم قید **هیچ ماشین محاسبه‌گر** مهم است. با پیدایش محاسبات کوانتومی و نوع جدیدی از ماشین‌های محاسبه‌گر موجود شدند که می‌توانستند امنیت الگوریتم‌های رمزنگاری را بشکنند.

و این اتفاق افتاد. پیتر شور [۵] در سال **۱۹۹۴** الگوریتمی کوانتومی برای یافتن دوره تناوب توابع متناوب با مقادیر صحیح ارائه کرد، که این الگوریتم با ترکیب شدن با روش‌هایی از نظریه اعداد که سال‌ها قبل دانسته شده بودند می‌توانست مسئله تجزیه اعداد طبیعی را در زمان بسیار کوتاه و با احتمال بسیار بالا حل کند. لذا الگوریتم‌های رمزنگاری که امنیت آن‌ها مبتنی بر سختی مسئله لگاریتم گسسته یا تجزیه اعداد بودند در برابر مهاجمی با کامپیوتر کوانتومی امن نیستند.

در نتیجه این انقلاب در دنیای رمزنگاری دانشمندان به دنبال الگوریتم‌های جدیدی برای رمزنگاری بودند و از آنجا که قضیه شانون مبنی بر عدم وجود سیستم کاملا امن همچنان برقرار است، پس باید به دنبال مسائلی باشیم که حل آن‌ها برای کامپیوترهای کوانتومی علاوه بر کامپیوترهای کلاسیک دشوار باشد تا با استفاده از آن‌ها سیستم های رمزی جدید و امن در برابر مهاجم کوانتومی بسازیم.

کاندیداهای متعددی برای چنین مسائلی مطرح شدند، رایج‌ترین این مسائل، مسائل مرتبط با مشبکه [۶] هستند. اما از آن‌جا که سختی این مسائل اثبات شده نیستند خوب است الگوریتم‌هایی مبتنی بر مسائل دیگری نیز داشته باشیم تا در صورت نیاز بتوانیم از آن‌ها استفاده کنیم. یکی از گزینه‌های جایگزین مناسب برای ساختن الگوریتم‌های رمزنگاری پساکوانتومی، مسائل مرتبط با ایزوژنی‌ها بطور ویژه ایزوژنی‌های میان خم‌های بیضوی فوق منفرد هستند. نام رمزنگاری ایزوژنی فوق منفرد از همین‌رو انتخاب شده است [۷].

در این پروژه ابتدا خم‌های بیضوی را معرفی می‌کنیم و چندی از خواص آن‌ها را مطالعه می‌کنیم و با خم‌های فوق منفرد آشنا می‌شویم. سپس به بررسی نوع خاصی از توابع میان این خم‌ها که ایزوژنی نام دارند می‌پردازیم.

در ادامه به کاربرد این مفاهیم در رمزنگاری می‌پردازیم و با یکی از اصلی‌ترین الگوریتم‌هایی که از این مفاهیم برای ساخت سیستم‌های رمزی استفاده می‌کند آشنا می‌شویم، تعدادی از مسائل سخت محاسباتی مربوط به خم‌های فوق منفرد را می‌بینیم و در نهایت در مورد پروتکل‌های اثبات هیچ‌ـ

[۵] Peter Shor
[۶] Lattice
[۷] Super Singular Isogeny Cryptography

دانشی برای این مسائل بحث می‌کنیم.

برای دنبال کردن مطالب این پروژه آشنایی مقدماتی با نظریه گروه‌ها، هندسه جبری (یا خم‌های بیضوی) و اثبات‌های تعاملی و هیچ‌ـدانشی مورد نیاز است. برای مطالعه اثبات‌هایی که در متن به آن‌ها اشاره شده ممکن است دانش بیشتری از نظریه اعداد، هندسه جبری و نظریه گراف مورد نیاز باشد.

فهرست مطالب

فصل ۱

مفاهیم مقدماتی

۱.۱ خم‌های بیضوی

۱.۱.۱ تعریف خم بیضوی به عنوان خم جبری

خم بیضوی نوعی خم جبری تصویری[۱] هموار[۲] با جینوس[۳] یک است.
خم‌های بیضوی که روی میدان k با مشخصه[۴] غیر از ۲ یا ۳ تعریف شده باشند را می‌توان با معادله به فرم Weierstrass مشخص کرد.

$$Y^{۲}Z = X^{۳} + aXZ^{۲} + bZ^{۳} \tag{۱.۱}$$

این معادله یک خم تصویری در $\mathbb{P}^{۲}(k)$ و نقطه در بی‌نهایت آن در چارت آفین XY نقطه $\mathcal{O} = (۰ : ۱ : ۰)$ است.

متداول است که معادله ۱.۱ را با قرار دادن $x = X/Z$ و $y = Y/Z$ در فرم آفین نوشت:

$$y^{۲} = x^{۳} + ax + b \tag{۲.۱}$$

طبق تعریف خم بیضوی باید هموار باشد لذا، باید غیر تکین [۵] باشد. این شرط برای خم‌ها در فرم Weierstrass معادل است با $۴a^{۳} + ۲۷b^{۲} \neq ۰$.

---

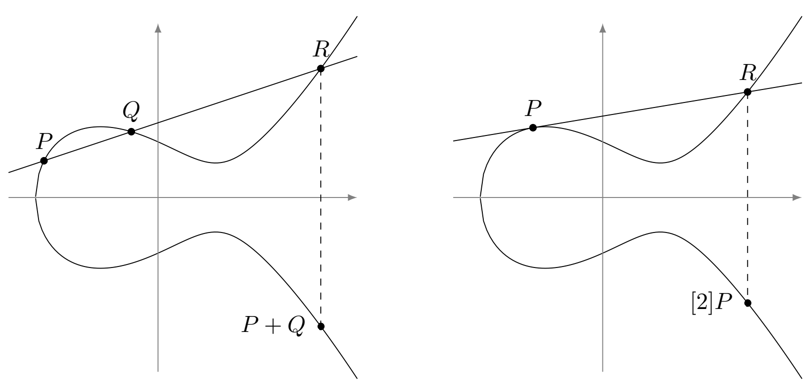
[۱] projective
[۲] smooth
[۳] genus
[۴] characterisitc
[۵] non-singular

۲.۱.۱ ساختار گروه روی خم‌های بیضوی

خم‌های بیضوی توسط معادلات درجه ۳ در فضا تصویری [۶] مرتبه ۲ تعریف می‌شوند در نتیجه طبق قضیه بزو [۷] [۳] هر خط هر خم بیضوی را در دقیقا ۳ نقطه قطع می‌کند. با استفاده از این حقیقت می توانیم ساختار گروه بر روی یک خم بیضوی دلخواه تعریف کنیم.

تعریف ۱.۱ (ساختار گروه روی خم‌های بیضوی)**.** *برای تعریف ساختار یک گروه روی یک خم بیضوی کافیست حاصل عمل گروه را برای هر دو نقطه دلخواه مشخص کنیم.*
فرض کنیم P و Q دو نقطه دلخواه (نه لزوما متمایز) روی خم E هستند، می‌دانیم خط گذرنده از P و Q خم E را در دقیقا ۳ نقطه قطع می‌کند، نقطه سوم را R می‌نامیم. $-R$ را قرینه نقطه R نسبت به محور x در نظر می‌گیریم و تعیف می‌کنیم $P+Q=-R$.
توجه کنیم که قرینه نقطه R نسبت به محور x را می توان به شیوه دیگری معرفی کرد: خط موازی محور y که از R می‌گذرد در چارت آفین XY خم E را در ۲ نقطه قطع می‌کند، یکی R است و تقاطع دیگر را $-R$ در نظر می‌گیریم. نقطه تقاطع سوم که در چارت XY دیده نمی‌شود نقطه در بینهایت $\mathcal{O}$ است.

می‌توان بررسی کرد که در این تعریف حاصل جمع نقاط تقاطع هر خط با خم برابر $\mathcal{O}$ است. همچنین $\mathcal{O}$ عضو خنثی عمل گروه (جمع) است، از این رو $\mathcal{O}$ و ۰ را به عنوان نمادهای معادل استفاده می‌کنیم.



شکل ۱.۱: نمایش عمل جمع و ضرب اسکالر روی نقاط یک خم بیضوی

---

[۶] Projective space
[۷] Bezout's Theorem

با استفاده از این تعریف جمع می‌توانیم ضرب نقاط در اعداد طبیعی را تعریف کنیم:

$$\begin{cases} [n]P = P & n = ۱ \\ [n]P = P + [n-۱]P & n \geq ۲ \end{cases}$$

۳.۱.۱ زیرگروه‌های پیچشی [۸]

برای هر $m \in \mathbb{N}$ همه نقاط مثل P روی خم بیضوی E که $[m]P = ۰$ با عمل جمع گروه تشکیل یک گروه می‌دهند. این گروه را زیرگروه پیچشی مرتبه m می‌نامیم و با $E[m]$ نمایش می‌دهیم. فرض کنیم خم E روی میدان k با مشخصه p تعریف شده باشد، آنگاه:

- اگر $p \nmid m$ آنگاه، $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^۲$.
- اگر $m = p^i$ آنگاه، $\begin{cases} E[p^i] \simeq (\mathbb{Z}/p^i\mathbb{Z}) \\ E[p^i] \simeq \{\mathcal{O}\} \end{cases}$. حالت اول را خم بیضوی معمولی[۹] و حالت دوم را خم بیضوی فوق منفرد[۱۰] می‌گوییم.

۲.۱ نگاشت‌ها بین خم‌های بیضوی

در این بخش به بررسی نگاشت‌ها بین خم‌های بیضوی که خواص جبری (به عنوان گروه) و هندسی (به عنوان واریته تصویری) آنها را حفظ می‌کنند می‌پردازیم.
می‌توان بررسی کرد که تنها نگاشت‌هایی که چنین شرایطی را دارند به فرم $(x, y) \to (u^۲x', u^۳y')$ هستند که $u \in \bar{k}$. چنین نگاشتی یک یکریختی بین خم‌های $y^۲ = x^۳ + au^۴x + bu^۶$ و $(y')^۲ = (x')^۳ + ax' + b$ تعریف می‌کند.

۱.۲.۱ حلقه توابع

تعریف ۲.۱. *خم C را یک واریته تصویری تعریف شده توسط $f(x, y, z) = ۰$ که $f(x, y, z) \in k[x, y, z]$ در نظر می‌گیریم. $k(C)$ همه توابع گویا به فرم $\frac{g}{h}$ هستند که:*

- *$f \in k[x, y, z]$ و $g \in k[x, y, z]$ همگن و هم درجه هستند.*

---

[۸] Torsion Subgroups
[۹] Oridinary Elliptic Curve
[۱۰] Super Singular Elliptic Curve

- $h \nmid f$ *معادلا* $h \notin (f)$.
- $\frac{g_1}{h_1} = \frac{g_2}{h_2} \iff g_1h_2 - g_2h_1 \in (f)$

توجه کنیم که $C(k)$ نقاط گویا روی C هستند و نباید با $k(C)$ اشتباه شوند.
مجموعه $k(C)$ با اعمال جمع و ضرب ساختار حلقه پیدا می کند. عضو خنثی جمع تابع ثابت ۰ و عضو خنثی ضرب تابع ثابت ۱ است.

تعریف ۳.۱ (تابع منظم در یک نقطه)**.** *$\alpha \in k(C)$ را دلخواه در نظر می‌گیریم. می‌گوییم α در نقطه $P \in C(\bar{k})$ منظم یا تعریف شده است اگر و تنها اگر $g, h \in k[x, y, z]$ چنان موجود باشند که $\alpha = \frac{g}{h}$ و $h(P) \neq 0$.*

۲.۲.۱ ایزوژنی[11]

تعریف ۴.۱ (نگاشت گویا)**.** *تابع $\phi : C_1 \to C_2$ را یک نگاشت گویا گوییم اگر ϕ به صورت $(\phi_1, \phi_2, \phi_3) \in \mathbb{P}^2(k(C_1))$ باشد که برای هر $P \in C_1(\bar{k})$ که $\phi_1(P)$ و $\phi_2(P)$ و $\phi_3(P)$ همگی تعریف شده و دست‌کم یکی از آنها ناصفر باشد، داشته باشیم:*
$$(\phi_1(P), \phi_2(P), \phi_3(P)) \in C_2(k)))$$
همچنین می‌گوییم phi در نقطه P تعریف شده است، اگر و تنها اگر $\lambda \in k(C_1)^*$ چنان موجود باشد که $\lambda\phi_1$ و $\lambda\phi_2$ و $\lambda\phi_3$ همگی در نقطه P تعریف شده باشند و دست‌کم یکی از آنها ناصفر باشد.

تعریف ۵.۱ (مورفیسم[12])**.** *نگاشت گویایی که روی همه خم تعریف شده باشد را مورفیسم گوییم.*

قضیه ۶.۱. *اگر C_1 خم تصویری هموار باشد آنگاه، هر نگاشت گویا تعریف شده روی C_1 مثل $\phi : C_1 \to C_2$ (مستقل از C_2) یک مورفیسم است.*

نتیجه ۷.۱. *هر نگاشت گویا روی یک خم بیضوی یک مورفیسم است.*

تعریف ۸.۱ (یکریختی خم‌های تصویری)**.** *خم‌های تصویری C_1 و C_2 را یکریخت گوییم اگر و تنها اگر یک مورفیسم وارونپذیر مثل $\phi : C_1 \to C_2$ موجود باشد به طوری که $\phi^{-1} o \phi$ تابع همانی روی C_1 و $\phi o \phi^{-1}$ تابع همانی روی C_2 باشد.*

تذکر ۹.۱. *ممکن است نگاشت گویا بین دو خم را روی میدانی بجز میدان تعریف خم‌ها تعریف کنیم. برای مثال ممکن است C_1 و C_2 روی میدان k تعریف شده باشند اما نگاشتی گویا بین آنها روی $\bar{k}$ تعریف کنیم. به همین صورت ممکن است مورفیزم‌ها و ایزومورفیزم ها نیز روی میدانی متفاوت تعریف شوند.*

[11] Isogeny
[12] Morphism

قضیه ۱۰.۱. *هر مورفیزم روی خم‌های تصویری پوشا یا ثابت است.*

تعریف ۱۱.۱ (ایزوژنی)**.** *یک مورفیزم پوشا تعریف شده بین دو خم بیضوی مثل $\phi : E_1 \to E_2$ که یک همریختی گروهی ($E_1(\bar{k}) \to E_2(\bar{k})$) باشد را یک ایزوژنی گوییم.*

تذکر ۱۲.۱. *در صورتی که مشخص نشده باشد، تنها ایزوژنی‌های تعریف شده روی میدان k را در نظر می‌گیریم.*

قضیه ۱۳.۱. *هر مورفیزم بین دو واریته آبلی [13] که عضو خنثی را به عضو خنثی ببرد، یک همریختی گروهی است.*

نتیجه ۱۴.۱. *نگاشت گویا $\phi : E_1 \to E_2$ یک ایزوژنی است اگر و تنها اگر، ثابت نباشد و $\phi(\circ_{E_1}) = \phi(\circ_{E_2})$.*

با توجه به تعریف یکریختی خم‌های تصویری و ایزوژنی خم‌های بتضوی، می‌توان گفت که خم‌های E_1 و E_2 یکریخت هستند اگر و تنها اگر، ایزوژنی های $\phi_1 : E_1 \to E_2$ و $\phi_2 : E_2 \to E_1$ چنان موجود باشند که ترکیب آنها تابع همانه باشد.

تعریف ۱۵.۱. *فرض کنیم E خم بیضوی باشد که معادله آن در فرم آفینی $y^2 = x^3 + ax + b$ است. تابع j را چنین تعریف می‌کنیم:*

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \tag{3.1}$$

قضیه ۱۶.۱ (j-invariant)**.** *خم‌های بیضوی E_1 و E_2 تعریف شده روی میدان k، روی $\bar{k}$ یکریخت هستند اگر و تنها اگر، $j(E_1) = j(E_2)$.*

۳.۲.۱ حلقه درون‌ریختی [14]

تعریف ۱۷.۱ (درون‌ریختی)**.** *یک مورفیزم از خم بیضوی E به خودش که عضو خنثی را به خودش می‌برد یک درون‌ریختی می‌نامیم.*

تعریف ۱۸.۱. *یک درون‌ریختی که یکریختی هم باشد، خودریختی می‌نامیم.*

تذکر ۱۹.۱. *هر درون‌ریختی بجز نگاشت ثابت صفر، یک ایزوژنی است.*

تعریف ۲۰.۱. *مجموعه همه درون‌ریختی‌ها با اعمال جمع و ترکیب توابع یک حلقه تشکیل می‌دهد. این حلقه را حلقه درون‌ریختی خم بیضوی E می‌نامیم و با $End(E)$ نمایش می‌دهیم.*

[13] Abelian Variety
[14] Endomorphism Ring

۴.۲.۱ فرم استاندارد ایزوژنی‌ها

برای سادگی در نمادگذاری و بعضی تعریف‌ها مربوط به ایزوژنی‌ها در این بخش یک فرم استاندارد برای نوشتن آنها معرفی می‌کنیم و در ادامه به برسی بعضی از این خواص می‌پردازیم.

تعریف ۲۱.۱. *فرض کنیم E_1 و E_2 خم‌های بیضوی باشند و $\alpha : E_1 \to E_2$ یک ایزوژنی بین آنها باشد.* $u, v, s, t \in k[x]$ *چنان موجود هستند که* $v \perp u$ *و* $t \perp s$ *و* $\alpha = (\frac{u(x)}{v(x)} + \frac{s(x)}{t(x)}y)$

قضیه ۲۲.۱. *مجموعه ریشه‌های $v(x)$ و $t(x)$ در $\bar{k}$ یکسان است.*

همه نقاط آفین $(x, y, 1) \in E_1(\bar{k})$ در هسته [۱۵] ایزوژنی $\alpha : E_1 \to E_2$ دقیقا نقاطی هستند که $v(x) = 0$ و $t(x) = 0$ که α این نقاط را به $\mathcal{O}$ (نقطه در بی‌نهایت) می‌برد. علاوه بر این نقاط آفین، $\mathcal{O}$ هم در هسته α قرار دارد که در چارت آفین XY دیده نمی‌شود.

$$ker(\alpha) = \mathcal{V}(v(x)) \cup \{\mathcal{O}\} \qquad (۴.۱)$$

تذکر ۲۳.۱. *هسته ایزوژنی α زیرگروهی متناهی از $E_1(\bar{k})$ است و نقاط ناصفر آن با واریته آفین تولید شده توسط $v(x)$ در تناضر هستند.*

تعریف ۲۴.۱ (درجه ایزوژنی)**.** *فرض کنیم $\alpha : E_1 \to E_2$ یک ایزوژنی باشد. می‌دانیم می‌توان α را به صورت $\alpha = (\frac{u(x)}{v(x)} + \frac{s(x)}{t(x)}y)$ نوشت. درجه α را بیشینه درجه $u(x)$ و $v(x)$ تعریف می‌کنیم.*

$$deg(\alpha) = max\{deg(u), deg(v)\} \qquad (۵.۱)$$

تعریف ۲۵.۱ (ایزوژنی جداشدنی [۱۶])**.** *فرض کنیم $\alpha : E_1 \to E_2$ یک ایزوژنی باشد. می‌دانیم می‌توان α را به صورت $\alpha = (\frac{u(x)}{v(x)} + \frac{s(x)}{t(x)}y)$ نوشت. می‌گوییم α جداشدنی است اگر و تنها اگر، مشتق $\frac{u(x)}{v(x)}$ ناصفر باشد. در غیر این صورت α را جدانشدنی می‌نامیم.*

قضیه ۲۶.۱. *اگر α ایزوژنی جداشدنی باشد آنگاه،*

$$deg(\alpha) = |ker(\alpha)| \qquad (۶.۱)$$

۳.۱ خم‌های بیضوی روی میدان‌های متناهی

در این بخش خم‌هایی را بررسی می‌کنیم که روی میدان‌های متناهی تعریف شده اند. فرض کنیم E خم‌بیضوی تعریف شده روی F_q باشد و $q = p^m$.
از آنجا که نقاط گویا متناهی هستند، روشن است گروه $E(k)$ نیز متناهی است در نتیجه همه اعضا آن مرتبه متناهی دارند و پیش از این ساختار زیرگروه‌های پیچشی را بررسی کردیم.

[۱۵] Kernel
[۱۶] Seprable Isogeny

۴.۱ گراف ایزوژنی[۱۷]

در این بخش به معرفی ساختار گراف ایزوژنی می‌پردازیم. همان طور که در بخش‌های قبلی صحبت شد خم‌های بیضوی به کلاس‌های یک ریختی (در بستار جبری میدان محل تعریف خم‌ها) افراز می‌شوند که می‌توان هر کلاس را با مقدار ناوردا-j خم‌های آن مشخص کرد. همچنین خم‌های بیضوی به کلاس‌های ایزوژنی افراز می‌شوند که بین خم‌های درون هر کلاس، ایزوژنی وجود دارد و هر دو خم دارای ایزوژنی در یک کلاس ایزوژنی قرار می‌گیرند.

قضیه ۲۷.۱. *همه خم‌های فوق منفرد در یک کلاس ایزوژنی قرار دارند.*

تعریف ۲۸.۱ (گراف ایزوژنی)**.** *برای هر j که مقدار ناوردا-j یک کلاس یکریختی از خم‌های بیضوی است یک راس در نظر می‌گیریم و بین رئوس j_1 و j_2 به ازای هر ایزوژنی بین این دو کلاس یکریختی (در حد یکریختی) یک یال قرار می‌دهیم.*
اگر میدان تعریف خم‌ها را k در نظر بگیریم گراف حاصل را گراف ایزوژنی خم‌های بیضوی تعریف شده روی k می‌نامیم و با $\mathcal{IG}_k$ نشان می‌دهیم.

می‌توان زیرگراف‌های مختلفی از $\mathcal{IG}_k$ در نظر گرفت؛ مثلا زیرگراف ایزوژنی‌های جداشدنی که تنها یال‌های متناظر با ایزوژنی‌های جداشدنی را شامل می‌شود یا زیرگراف خم‌های فوق منفرد که تنها رئوس متناظر با خم‌های فوق منفرد را شامل می‌شود.
در این پروژه زیرگراف خم‌های فوق منفرد و ایزوژنی‌های جداشدنی مورد توجه ما است، این زیرگراف را گراف ایزوژنی‌های جداشدنی خم‌های فوق منفرد می‌نامیم.

تعریف ۲۹.۱ (گراف رامانوجان)**.** *گراف منتظم-d n راسی G با مقادیر ویژه $d = \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ ، را دارای خاصیت رامانوجان گوییم اگر و تنها اگر، $\lambda_i \leq 2\sqrt{d-1}$ برای هر $2 \leq i \leq n$.*

گراف‌های رامانوجان بهترین گراف‌های گسترش دهنده[۱۸] هستند، یکی از خواص گراف‌های گسترش دهنده این است که با این که تعداد یال‌های کمی دارند، بین هر دو راسی مسیری کوتاه وجود دارد. از این رو گراف‌های رامانوجان برای ساخت اولیه‌های رمزنگاری گزینه مناسبی هستند زیرا می‌توان با داشتن اطلاعات مناسب مسیری کوتاه بین راس‌های دلخواه پیدا کرد اما بدون داشتن این اطلاعات یافتن چنین مسیری سخت است.

قضیه ۳۰.۱. *گراف ایزوژنی‌های جداشدنی خم‌های فوق منفرد رامانوجان است.*

---

[۱۷] Isogeny Graph
[۱۸] Expander Graph

فصل ۲

رمزنگاری مبتنی بر ایزوژنی

در این فصل به معرفی پروتکل دیفی-هلمن ازوژنی‌های فوق منفرد می‌پردازیم. این پروتکل از این‌رو دیفی-هلمن نام گرفته که تا حدی مشابه پروتکل دیفی-هلمن عمل می‌کند. پروتکل دیفی-هلمن استاندارد از گذرهای تصادفی روی گراف ساخته شده توسط یک گروه دوری استفاده می‌کند، در حالی که پروتکل SIDH از گذرهای تصادفی روی گراف ایزوژنی‌های جداشدنی خم‌های فوق منفرد استفاده می‌کند.

۱.۲ پروتکل تبادل کلید SIDH [۱]

۱.۱.۲ صورت پروتکل SIDH

تعریف ۱.۲ (SIDH)**.** *فرض کنیم پارامترهای عمومی چنین تعیین شده‌اند، عدد اول p به فرم $p = l_1^{e_1} \times l_2^{e_2} \times f \pm 1$ بطوری که l_1 و l_2 اعداد اول کوچک هستند و $l_1^{e_1}$ تقریبا هم‌اندازه $l_2^{e_2}$ است. همچنین میدان مورد نظر ما $\mathbb{F}_{p^2}$ است [۱].*
خم بیضوی فوق منفرد E را به عنوان نقطه شروع در نظر می‌گیریم. می‌دانیم که $E(\mathbb{F}_{p^2})$ دارای زیرگروه‌های پیچشی $E[l_1^{e_1}]$ و $E[l_2^{e_2}]$ است، پایه‌های $\{P_1, Q_1\}$ و $\{P_2, Q_2\}$ را برای زیرگروه‌های $E[l_1^{e_1}]$ و $E[l_2^{e_2}]$ انتخاب می‌کنیم (یعنی $E[l_i^{e_i}] =< P_i, Q_i >$).
می‌دانیم برای ایزوژنی‌های جداشدنی دانستن کرنل معادل با دانستن خود ایزوژنی است. در SIDH دانش خصوصی آلیس و باب به ترتیب ایزوژنی‌های $\phi_A : E(\mathbb{F}_{p^2}) \to E_A(\mathbb{F}_{p^2})$ و $\phi_B : E(\mathbb{F}_{p^2}) \to E_B(\mathbb{F}_{p^2})$ با درجات $l_1^{e_1}$ و $l_2^{e_2}$ هستند.
از آن‌جا که درجه ایزوژنی‌های جداشدنی با اندازه کرنل آن‌ها برابر است برای ساختن کلیدهای

[۱] Super-Singular Isogeny Diffie Helman

خصوصی تصادفی کافی است نفر i مقادیر $n_i, m_i \in \mathbb{Z}/l_i^{e_i}\mathbb{Z}$ را بصورت تصادفی انتخاب کند و ایزوژنی که کرنل آن توسط نقطه $K_i = [n_i]P_i + [m_i]Q_i$ ساخته می‌شود را کلید خصوصی خود قرار دهد. به این ترتیب کلید خصوصی هر نفر می‌تواند هر یک از ایزوژنی خصوصی او، کرنل آن ایزوژنی یا n_i و m_i باشد. همچنین توجه کنیم که $Ker(\phi_{AB}) = \phi_B(Ker(\phi_A))$ و $Ker(\phi_{BA}) = \phi_A(Ker(\phi_B))$.

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_{AB}"] \\
E_B \arrow[r, "\phi_{BA}"'] & E_{AB}
\end{tikzcd}$$

شکل ۱.۲: دیاگرام خاصیت جابه‌جایی تاثیر ایزوژنی‌ها روی خم بیضوی اولیه E [۱].

پس از این‌که آلیس تصویر کلید خصوصی باب E_B را دریافت کند، باید E_{AB} را محاسبه کند، به عبارت دیگر باید $Ker(\phi_{AB})$ را محاسبه کند. از طرفی می‌دانیم $Ker(\phi_{AB}) = \phi_B(Ker(\phi_A))$ پس کافی است $\phi_B(Ker(\phi_A))$ را محاسبه کند. اما برای این کار نیاز است آلیس مقدار ϕ_B را برای نقاطی محاسبه کند. توجه کنیم که $Ker(\phi_A) =< [n_1]P_1+[m_1]Q_1 >$ و از آن‌جا که ϕ_B یک هم‌ریختی گروهی است لذا کافی است آلیس مقادیر $\phi_B(P_1)$ و $\phi_B(Q_1)$ را بداند و متقابلا باب مقادیر $\phi_A(P_2)$ و $\phi_A(Q_2)$ را بداند. به این ترتیب آلیس می‌تواند چنین محاسبه کند:

$$Ker(\phi_{AB}) = \phi_B(Ker(\phi_A)) =< \phi_B([n_1]P_1 + [m_1]Q_1) >=< [n_1]\phi_B(P_1) + [m_1]\phi_B(Q_1) > .$$

به این ترتیب آلیس و باب به دو خم بیضوی یک‌ریخت دست می‌یابند که در نتیجه یک j-ناوردا دارند و می‌توانند از $j(E_{AB}) = j(E_{BA})$ به عنوان کلید مشترک خود استفاده کنند.

۲.۱.۲ نگاهی عمیق‌تر به پروتکل SIDH

تذکر ۲.۲. *می‌توان پروتکل $SIDH$ را به این صورت تعریف کرد. گراف‌های G_A و G_B را به ترتیب زیرگرافی از گراف ایزوژنی‌های جداشدنی فوق منفرد با یال‌های ایزوژنی‌های درجه l_1 و l_2 در نظر می‌گیریم. لذا این گراف‌ها راس‌های یکسان اما یال‌های (کاملا) متفاوت دارند.*
کلید خصوصی آلیس یک گذر تصادفی به طول e_1 در G_A و کلید خصوصی باب یک گذر تصادفی به طول e_2 در G_B است. حال توجه کنیم که برای ایزوژنی‌های جداشدنی درجه و اندازه کرنل آن‌ها برابر است، به عبارت دیگر اگر آلیس یک گذر به طول e_1 در G_A انتخاب کند آن‌گاه معادل آن گذر یک زیر گروه دوری مثل $< A >$ از $E[l_1^{e_1}]$ انتخاب کرده و در نتیجه یک ایزوژنی $\phi_A : E \to E/ < A >$ از درجه $l_1^{e_1}$ انتخاب کرده، که همان صورت قبلی پروتکل $SIDH$ را بدست می‌دهد.

۳.۱.۲ مسائل سخت مبتنی بر ایزوژنی

تعریف ۳.۲ (مسئله ایزوژنی عمومی)**.** *برای $j, j' \in \mathbb{F}_{p^2}$ در صورت وجود ایزوژنی $\phi : E \to E'$ را چنین بیابید که $j(E) = j$ و $j(E') = j'$.*
به زبان دیگر ادعا سختی این مسئله یعنی یافتن ایزوژنی بین دو خم بیضوی دلخواه دشوار است.
توجه کنیم که تصمیم‌گیری وجود ایزوژنی ساده است؛ ایزوژنی موجود است اگر و تنها اگر $|E(\mathbb{F}_{p^2})| = |E'(\mathbb{F}_{p^2})|$

تعریف ۴.۲ (مسئله SIDH محاسباتی)**.** *برای عدد اول p داده شده به فرم $p = l_1^{e_1} \times l_2^{e_2} \times f \pm 1$، خم بیضوی فوق منفرد E_0 و نقاط $\{P, Q\}$ پایه زیرگروه پیچشی $l_2^{e_2}$، فرض کنید $\phi : E_0 \to E_1$ یک ایزوژنی درجه $l_1^{e_1}$ باشد. $(E_1, \phi(P), \phi(Q))$ داده شده، ایزوژنی $\psi : E_0 \to E_1$ از درجه $l_1^{e_1}$ را چنان پیدا کنید که $\psi(P) = \phi(p)$ و $\psi(Q) = \phi(Q)$.*
به عبارت دیگر ادعا سختی این مسئله یعنی با داشتن کلید عمومی پروتکل $SIDH$ نمی‌توان کلید خصوصی متناظر آن را بدست آورد.
توجه کنیم که فرض سختی این مسئله رد شده است و پروتکل $SIDH$ امن نیست و حمله $GPST$ [۶] می‌تواند کلید خصوصی را بازیابی کند.

تعریف ۵.۲ (مسئله تصمیمی ضرب خم‌های فوق منفرد DSSP [2])**.** *فرض کنیم $\phi : E_0 \to E_1$ یک ایزوژنی از درجه $l_1^{e_1}$ باشد، در مسئله DSSP می‌خواهیم میان توزیع‌های زیر تمایز دهیم:*

- *$D_0 = (E_2, E_3, \phi')$ به طوری که زیرگروه دوری G از مرتبه $l_2^{e_2}$ از $E_0[l_2^{e_2}]$ موجود است که $E_2 = E_0/G$ و $E_3 = E_1/\phi(G)$ و $\phi' : E_2 \to E_3$ یک ایزوژنی درجه $l_1^{e_1}$ است.*
- *$D_1 = (E_2, E_3, \phi')$ به طوری $|E_2| = |E_0|$ و $\phi' : E_2 \to E_3$ از درجه $l_1^{e_1}$ است.*

بطور شهودی این مسئله بیان می‌کند که با داشتن چهار راس و یال پائینی یک مربع ایزوژنی مشابه شکل ۵.۲ نمی‌توان به سادگی فهمید آیا یال‌های عمودی معتبری برای این مربع موجود است یا خیر.

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_{AB}"] \\ E_B \arrow[r, "\phi_{BA}"'] & E_{AB} \end{tikzcd}$$

شکل ۲.۲: نمونه‌ای از یک مربع ایزوژنی. یال‌های افقی ایزوژنی‌های درجه $l_1^{e_1}$ و یال‌های عمودی ایزوژنی‌های درجه $l_2^{e_2}$ هستند[۱].

[2] Decisional Supersingular Product problem

فصل ۳

اثبات هیچ-دانشی برای مسائل ایزوژنی

در این فصل قصد داریم پروتکلی بسازیم که به صورت هیچ-دانشی [1] به طرف مقابل اثبات کند که اثبات‌گر یک ایزوژنی بین دو خم فوق منفرد دلخواه در دست دارد (طبق مطالب فصل اول می‌دانیم دانش یک ایزوژنی معادل با دانش هسته آن است).
در طول این فصل در صورت عدم تعیین مشخص فرض می‌کنیم p عددی اول به فرم $p = l_1^{e_1} \times l_2^{e_2} \times f \pm 1$ است و E_0 خمی بیضوی و فوق منفرد است که $|E_0(\mathbb{F}_{p^2})| = (l_1^{e_1} \times l_2^{e_2} \times f)^2$.

۱.۳ De Feo-Jao-Plut : پروتکلی ساده اما ناصحیح

در این پروتکل کلید خصوصی نقطه‌ای مثل $K_\phi \in E_0(\mathbb{F}_{p^2})$ از مرتبه $l_1^{e_1}$ است. که یک ایزوژنی مثل $\phi : E_0 \to E_1 = E_0 / < K_\phi >$ از مرتبه $l_1^{e_1}$ را معین می‌کند. فرض کنیم $E_0[l_2^{e_2}] =< P_0, Q_0 >$ آنگاه پارامترهای عمومی SIDH می‌تواند (p, E_0, P_0, Q_0) و کلید عمومی $(E_1, \phi(P_0), \phi(Q_0))$ باشند. تعامل میان اثبات‌کننده و بررسی‌کننده به این صورت عمل می‌کند:

۱. اثبات کننده یک نقطه تصادفی مثل K_ψ از مرتبه $l_2^{e_2}$ انتخاب می‌کند. توجه کنیم که می‌توان K_ψ را به صورت $K_\psi = [a]P_0 + [b]Q_0$ نوشت زیرا $< P_0, Q_0 >$ همان زیرگروه پیچشی مرتبه $l_2^{e_2}$ است.
در ادامه اثبات‌کننده خم‌های $E_2 = E_0 / < K_\psi >$ و $E_3 = E_1 / < \phi(K_\psi) = E_0 / < K_\psi, K_\phi >$ را تشکیل می‌دهد و برای بررسی‌کننده ارسال می‌کند. شکل ۱ رابطه ایزوژنی میان خم‌های تشکیل شده را نشان می‌دهد:

[1] Zero-knowledge

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi"] \arrow[d, "\psi"'] & E_1 \arrow[d, "\psi'"] \\
E_2 \arrow[r, "\phi'"] & E_3
\end{tikzcd}
$$

شکل ۱.۳: روابط ایزوژنی میان خم‌ها در پروتکل De Feo-Jao-Plut [۵]

۲. بررسی‌کننده به طور تصادفی بیت b را از میان بیت‌های ۰ یا ۱ را انتخاب می‌کند و برای اثبات کننده ارسال می‌کند.

۳. در این مرحله ایده این پروتکل مشابه ایده پروتکل اثبات یکریختی گراف‌ها است.
اگر $b = 0$، آنگاه اثبات‌کننده a و b را برای بررسی‌کننده ارسال می‌کند. به این ترتیب بررسی‌کننده می‌تواند $K_\psi = [a]P_0 + [b]Q_0$ و $K'_\psi = [a]\phi(P_0) + [b]\phi(Q_0)$ را محاسبه کند و اطمینان حاصل کند که اثبات‌کننده واقعا ایزوژنی‌های ψ و ψ' را می‌داند.
در صورتی که $b = 1$، آنگاه اثبات کننده $K'_\psi = \psi(K_\phi)$ را برای بررسی‌کننده ارسال می‌کند. به این ترتیب بررسی‌کننده می‌تواند به سهولت ایزوژنی ϕ' را محاسبه کند و اطمینان حاصل کند که اثبات‌کننده یک ایزوژنی بین E_2 و E_3 می‌داند.

به این ترتیب اگر پروتکل صادقانه اجرا شود در هر مرحله بررسی‌کننده قانع می‌شود که اثبات‌کننده یک ایزوژنی از مرتبه درست بین E_0 و E_1 می‌داند. زیرا:

$$\hat{\psi}' o \phi' o \psi = [l_2^{e_2}]\phi \tag{۱.۳}$$

دشوار نیست که بررسی کنیم این پروتکل هیچ‌ـدانشی است همچنین طبق معادله ۱.۳ شرط تمامیت [۲] نیز برقرار است.
لذا چالش این پروتکل در اثبات صحت [۳] آن است. در نگاه اول بنظر می‌رسد که احتمال تقلب

[۲] Completeness
[۳] Soundness

اثبات کننده در هر مرحله مقداری ثابت و اکیدا کمتر از ۱ است، اما این مشاهده نادرست است.
برای بحث مفصل در مورد صحت این پروتکل بخش‌های ۲.۴ و ۳.۴ از [۵] را ببینید.

۲.۳ ساخت پروتکل هیچ‌ـدانشی

در این بخش تلاش می‌کنیم برای گزاره‌ای طبیعی اما ضعیف‌تر از دانش کلید خصوصی SIDH یک پروتکل صحیح و امن بسازیم.
گزاره مورد بحث رابطه زیر است:

$$R_{weakSIDH} = \{(\phi, E_\phi) | \phi : E_۰ \to E_\phi \text{ and } \phi \text{ degree is } l_۱^{e_۱}\} \qquad (۲.۳)$$

۱.۲.۳ پروتکلی صحیح اما ناامن

در ابتدا پروتکلی می‌سازیم که امن است اما نشتی اطلاعات دارد و به زبان دیگر امن یا هیچ‌ـدانشی نیست.
این پروتکل تلاش می‌کند تا مشکل صحت پروتکل DJP [۴] را رفع کند، اما رفع این مشکل موجب نشت اطلاعات می‌شود.
پارامترهای عمومی را $(p, l_۱, l_۲, e_۱, e_۲, E_۰)$ قرار می‌دهیم. کلید خصوصی همانند قبل یک نقطه از مرتبه $l_۱^{e_۱}$ و ایزوژنی متناظر آن است. در این پروتکل برخلاف پروتکل DJP پایه‌ای برای زیرگروه پیچشی مرتبه $l_۲^{e_۲}$ را به عنوان کلید عمومی در نظر نمی‌گیریم.
تعامل میان اثبات‌کننده و بررسی‌کننده به این ترتیب است:

تعهد [۵]

- نقطه K_ψ را از مرتبه $l_۲^{e_۲}$ به تصادف از خم $E_۰$ انتخاب می‌کنیم.
- ایزوژنی $\psi : E_۰ \to E_۲$ را تشکیل می‌دهیم. توجه کنیم که درجه این ایزوژنی $l_۲^{e_۲}$ است.
- پایه $< P_۲, Q_۲ >$ را به طور تصادفی برای $E_۲[l_۲^{e_۲}]$ انتخاب می‌کنیم.
- قرار بده $K'_\phi = \psi(K_\phi)$ و ایزوژنی $\phi' : E_۲ \to E_۳$ را محاسبه می‌کنیم.
- مقادیر $P_۳ = \phi'(P_۲)$ و $Q_۳ = \phi'(Q_۲)$ را محاسبه می‌کنیم و $(E_۲, P_۲, Q_۲, E_۳, P_۳, Q_۳)$ را برای بررسی‌کننده ارسال می‌کنیم.

پس از مرحله تعهد مشابه پروتکل DJP دیاگرام ایزوژنی‌ها میان خم‌های $E_۰$، $E_۱$، $E_۲$ و $E_۳$ ساخته می‌شود.

---

[۴] De Feo-Jao-Plut
[۵] Commitment

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi"] \arrow[d, "\psi"'] & E_1 \arrow[d, "\psi'"] \\
E_2 \arrow[r, "\phi'"] & E_3
\end{tikzcd}
$$

توجه کنیم که تفاوت این پروتکل با پروتکل DJP تا اینجا این است که نقاط انتخاب شده روی خم E_2 و متعاقبا E_3 تصادفی هستند و از پیش‌تصویر آن‌ها اطلاعاتی موجود نیست.

چالش [6] در این مرحله بررسی‌کننده بیت b را به تصادف از $\{0, 1\}$ انتخاب می‌کند و برای اثبات‌کننده ارسال می‌کند.

پاسخ [7]

- اگر $b = 0$، آنگاه $\hat{\psi}$ (ایزوژنی دوگان ψ) را محاسبه می‌کنیم و سازنده کرنل آن را $K_{\hat{\psi}}$ می‌نامیم. می‌دانیم $K_{\hat{\psi}} \in E_2[l_2^{e_2}]$ ، لذا $c, d \in \mathbb{Z}_{l_2^{e_2}}$ چنان موجودند که، $K_{\hat{\psi}} = [c]P_2 + [d]Q_2$. (c, d) را برای بررسی‌کننده ارسال می‌کنیم.
- اگر $b = 1$، آنگاه $K_{\phi'}$ را برای بررسی‌کننده ارسال می‌کنیم.

بررسی [8] اگر $b = 1$،

- بررسی می‌کنیم که $K_{\phi'}$ از مرتبه $l_2^{e_2}$ باشد و روی خم E_2 قرار داشته باشد.
- ایزوژنی $\phi' : E_2 \to E_3'$ را محاسبه می‌کنیم و بررسی می‌کنیم که $E_3 = E_3'$ و $(\phi'(P_2), \phi'(Q_2)) = (P_3, Q_3)$.

اگر $b = 0$،

- قرار می‌دهیم $K_{\hat{\psi}} = [c]P_2 + [d]Q_2$ و $K_{\hat{\psi}'} = [c]P_3 + [d]Q_3$ سپس بررسی می‌کنیم که $K_{\hat{\psi}}$ و $K_{\hat{\psi}'}$ از مرتبه $l_2^{e_2}$ باشند و به ترتیب روی خم‌های E_2 و E_3 باشند.
- ایزوژنی‌های $\hat{\psi} : E_2 \to E_0'$ و $\hat{\psi}' : E_3 \to E_1'$ را محاسبه می‌کنیم و بررسی می‌کنیم که $E_0 = E_0'$ و $E_1 = E_1'$.

[6] Challenge
[7] Response
[8] Verification

۲.۲.۳ اثبات دانش [۹]

می‌خواهیم نشان دهیم این پروتکل صحت ۲ـ ویژه[۱۰] دارد. فرض کنیم دو رونوشت [۱۱] با چالش‌های متفاوت مثل $\alpha = (com, ۰, resp)$ و $\beta = (com, ۱, resp')$ از این پروتکل بدست آمده است. نشان می‌دهیم با در دست داشتن این دو رونوشت می‌توان کلید خصوصی اثبات‌کننده را بدست آورد.
با استفاده از α می‌توانیم (c, d) و در نتیجه $\hat{\psi}$ و $\hat{\psi}'$ را بدست آوریم، سپس با استفاده از β می‌توانیم ϕ' را بدست آوریم. حال سه یال از یک مربع ایزوژنی را داریم و می‌توانیم یال چهارم که همان ϕ است را محاسبه کنیم.
لذا این پروتکل یک اثبات دانش برای یک ایزوژنی درجه $l_1^{e_1}$ بین دو خم بیضوی فوق منفرد دلخواه است.

تذکر ۱.۳. *دشوار نیست که ببینیم این پروتکل نمی‌تواند به بررسی‌کننده ثابت کند که نقطه (P_1, Q_1) تصویر نقطه (P_0, Q_0) تحت ایزوژنی ϕ است. یک دلیل شهودی آن است که در هیچ جای این پروتکل از (P_1, Q_1) استفاده نشده است. برای بحث مفصل‌تر در این مورد به بخش ۲.۵ [۵] مراجعه کنید.*

۳.۲.۳ امن کردن پروتکل

در پروتکل ۱.۲.۳ هنگامی که بیت چالش $b = ۰$، اثبات‌کننده ایزوژنی‌های $\hat{\psi}$ و $\hat{\psi}'$ را به بررسی‌کننده می‌دهد آنگاه بررسی کننده مقادیر $\phi(\hat{\psi}(P_2)) = \hat{\psi}'(P_3)$ و $\phi(\hat{\psi}(Q_2)) = \hat{\psi}'(Q_3)$ را دارد، در نتیجه با احتمال بالا می‌تواند پس از تعداد ثابتی تکرار این پروتکل عمل ϕ روی $E.[l_2^{e_2}]$ را بدست آورد. این به این معنی است که نشت اطلاعات صورت می‌گیرد. اطلاعات دیگری نیز در این پروتکل نشت می‌کند که باعث ناامن شدن آن می‌شوند که ما به آن‌ها نمی‌پردازیم، می‌تواند برای بررسی دقیق‌تر تحلیل نشت اطلاعات این پروتکل بخش ۳.۵ [۵] را ببینید.
برای رفع مشکل نشتی اطلاعات چالش $b = ۰$ را به دو قسمت تقسیم می‌کنیم و از یک‌دیگر جدا می‌کنیم تا نیاز نباشد اثبات‌کننده هم‌زمان $\hat{\psi}$ و $\hat{\psi}'$ را منتشر کند. همچنین برای چالش $b = ۱$ یک ضریب تصادفی به $K_{\phi'}$ اضافه می‌کنیم تا شبیه‌سازی آن ساده‌تر شود.
همچنین در ساخت این پروتکل از پروتکل تعهد [۱۲] Comit استفاده می‌کنیم که بطور آماری پایبندکننده [۱۳] و بطور محاسباتی مخفی‌کننده [۱۴] است.

Proof of Knowledge[۹]
2-special soundness[۱۰]
transcript[۱۱]
scheme Commetment[۱۲]
Binding Statistically[۱۳]
Hiding Computationally[۱۴]

تعهد [۱۵]

- $(E_۲, P_۲, Q_۲, E_۳, P_۳, Q_۳)$ را مشابه پروتکل ۱.۲.۳ می‌سازیم، ایزوژنی ψ را نیز بطور مشابه محاسبه می‌کنیم.
- یک سازنده برای کرنل $\hat{\psi}$ محاسبه می‌کنیم و آن را $K_{\hat{\psi}}$ می‌نامیم.
- از آن‌جا که $E_۲[l_۲^{e_۲}] =< P_۲, Q_۲ >$ پس $c, d \in \mathbb{Z}_{l_۲^{e_۲}}$ چنان موجود هستند که $K_{\hat{\psi}} = [c]P_۲ + [d]Q_۲$.
- تعریف می‌کنیم $com_L = (E_۲, P_۲, Q_۲)$ و $com_R = (E_۳, P_۳, Q - ۳)$
- مقادیر r_L, r_R, r را بطور تصادفی انتخاب می‌کنیم و $(C_L = Comit(com_L, r_L), C_R = Comit(com_R, r_R), C = Comit(c, d, r))$ را برای بررسی‌کننده ارسال می‌کنیم.

چالش [۱۶] در این مرحله بررسی‌کننده بیت bرا بطور تصادفی از $\{۱-, ۱, ۰\}$ انتخاب می‌کند و برای اثبات‌کننده ارسال می‌کند.

پاسخ [۱۷]

- اگر $b = ۱$،
$K_{\phi'}$ را مشابه پروتوکل ۱.۲.۳ محاسبه می‌کنیم، سپس $u \in \mathbb{Z}^*_{l_۱^{e_۱}}$ را بطور تصادفی انتخاب می‌کنیم و قرار می‌دهیم $K'_{\phi'} = [u]K_{\phi'}$. سپس $(com_L, r_L, K'_{\phi'}, com_R, r_R)$ را برای بررسی‌کننده ارسال می‌کنیم.
- اگر $b = ۰$،
(com_R, r_R, c, d, r) را برای بررسی‌کننده ارسال می‌کنیم.
- اگر $b = -۱$،
(com_L, r_L, c, d, r) را برای بررسی‌کننده ارسال می‌کنیم.

بررسی [۱۸]

- اگر $b = ۱$، بررسی می‌کنیم که C_L و C_R تعهدهای درستی باشند. و در ادامه مشابه پروتکل ۱.۲.۳ عمل می‌کنیم.
- اگر $b = -۱$،
بررسی می‌کنیم که C_L و C تعهدهای درستی باشند. سپس با استفاده از c, d نقطه $K_{\hat{\psi}}$ را محاسبه می‌کنیم و در ادامه ایزوژنی $\hat{\psi} : E_۲ \to E'_.$ را محاسبه می‌کنیم و بررسی می‌کنیم که $E'_. = E_.$.

Commitment[۱۵]
Challenge[۱۶]
Response[۱۷]
Verification[۱۸]

- اگر $b = 0$،
مشابه حالت قبل بررسی می‌کنیم که C_R و C تعهدهای درستی باشند. سپس $K_{\hat{\psi}'}$ را محاسبه می‌کنیم و ایزوژنی $\hat{\psi}' : E_3 \to E'_1$ را بدست می‌آوریم و بررسی می‌کنیم که $E_1 = E'_1$

می‌توان نشان داد که پروتکل ۳.۲.۳ دارای خاصیت SHVZK [19] است. در نتیجه طبق لم هایبرید گلدرایخ [20]، میکالی [21]، ویگدرسن [22] [۲] این پروتکل پس از k مرتبه تکرار همچنان SHVZK است. همچنین می‌توان برای این پروتکل شبیه‌ساز [23] ساخت (به بخش ۳.۵ از [۵] مراجعه کنید) در نتیجه این پروتکل ZK است.
در فصل ۶ از [۵] با تغییر جزئیاتی از پروتکل ۳.۲.۳ اثباتی برای رابطه SIDH نیز ارائه شده است.

$$R_{SIDH} = \{(\phi, E_\phi, (P_1, Q_1)) | \phi : E_0 \to E_\phi \text{ and } \phi \text{ is degree } l_1^{e_1} \text{ and } (\phi(P_0), \phi(Q_0)) = (P_1, Q_1)\} \quad (۳.۳)$$

به این ترتیب یک Σ-پروتکل برای مسئله SIDH بدست می‌آید که با استفاده از تبدیل فیات-شمیر [24] می‌توان یک اثبات هیچ-دانشی غیر تعاملی [25] در مدل اراکل تصادفی [26] برای مسئله SIDH ساخت.

[19] Special Honest Verifier Zero Knowledge
[20] Goldreich
[21] Micali
[22] Wigderson
[23] Simulator
[24] Transform Fiat-Shamir
[25] Proof Zero-Knowledge Non-Interactive
[26] Model Oracle Random

Bibliography

[1] Luca De Feo. Mathematics of isogeny based cryptography. 2017.

[2] Oded Goldreich. *Foundations of Cryptography.* Cambridge University Press, 2003.

[3] Klaus Hulek. *Elementary Algebraic Geometry.* Student Mathematical Library. American Mathematical Society, 2003.

[4] John T. Tate Joseph H. Silverman. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer, 2nd edition, 2015.

[5] Steven D. Galbraith Lukas Zobering Luca De Feo, Samuel Dobson. Sidh proof of knowledge. 2022.

[6] Petit Ti Samuel Dobson, Steven D. Galbraith. On the security of supersingular isogeny cryptosystems. *Advances in Cryptology – ASIACRYPT 2016*, 2016.

[7] Joseph H. Silverman. *The Arithmatic of Elliptic Curves.* Graduate Texts in Mathematics. Springer, 2nd edition, 2008.

[8] Douglas B. West. *Introduction to Graph Theory.* 2nd edition, 1995.

Abstract

The purpose of this article is to study Super Singular Isogeny based cryptography. Firstly we introduce the fundumentals of elliptic curves with an emphasis on the properties useful to cryptography. Then we discuss elliptic curves from an algebraic geometrical point of view and introduce some of the computational problems that arise in this field.
In the second chapter we study the SIDH protocol as an instance of isogeny-based cryptography and discuss isogeny-based cryptography's potential for post quantum cryptography.

College of Science
School of Mathematics, Statistics, and Computer Science

Super Singular Elliptic Curves in Cryptography

Parsa Tasbihgou

Supervisor: Prof. Morteza Mohammad Noori

A thesis submitted in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science

2023