پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

رمزنگاری خم بیضوی

نگارنده

ستاره نجفی خشنو

استاد راهنما: دکتر امیر قادرمرزی

پایان‌نامه برای دریافت درجه کارشناسی
در رشته علوم کامپیوتر

مرداد ۱۴۰۱

چکیده

رمزنگاری خم بیضوی، حوزه ای از دانش رمزنگاری است که در آن با بکارگیری ساختار جبری خم های بیضوی روی میدان های متناهی سیستم های رمزنگاری کلید عمومی طراحی میشوند. علت کاربرد و اهمیت زیاد این دسته از الگوریتم ها آنست که در مقایسه با پروتکل های رمزنگاری کلاسیک نظیر RSAدر مقابل فراهم ساختن امنیتی برابر نیاز به توان محاسباتی، حافظه ، زمان و هزینه ی کمتری می باشند.

در این گزارش به مطالعه ی ساختار خم های بیضوی و سیستم ها و الگوریتم های ی رمزنگاری مبتنی بر خم بیضوی میپردازیم. در بخش آخر کاربردهای مهم رمزنگاری خم بیضوی بطور مثال در تولید امضای دیجیتال را معرفی می کنیم.

سپاسگزاری

سپاسگزاری

از استاد عزیز و گرانقدر جناب آقای دکتر امیر قادرمرزی که با راهنمایی های خود مرا در انجام این پروژه یاری دادند کمال تشکر را دارم.

پیشگفتار

لزوم به کارگیری سیستم های رمز در دنیای امروز بر کسی پوشیده نیست.رمزنگاری و حفظ اطلاعات محرمانه قدمتی به اندازه ی تمدن دارد. با فراگیرشدن ارتباطات و راه اندازی سیستم های کامپیوتری، مسئله ی امنیت و حفظ اطلاعات از مسائل مهمی است که امروزه مورد توجه بسیاری قرار دارد.همچنین اعتبار پیام های ارسال شده در شبکه های کامپیوتری منوط به آن است که گیرنده اطمینان حاصل کند که پیام ارسال شده از فرستنده بوده و جعلی نمی باشد. رمزنگاری ابزاری برای تامین امنیت و اعتبار اطلاعات و پیام ها در شبکه های کامپیوتری میباشد. تا به امروز الگوریتم های مختلفی برای سیستم های رمز طراحی شده اند. دسته ی مهمی از این الگوریتم ها بر اساس پیچیدگی محاسباتی توابع به کار رفته در سیستم های رمز کلید عمومی می باشند. از طرفی طراحی سیستم هایی که با نیاز به توان محاسباتی پایینتر و مصرف حافظه ی کمتر و طول کلید کوتاه تر امنیت مورد نیاز را تامین کنند از اهمیت به سزایی برخوردار است. رمزنگاری خم بیضوی یک کاندید مناسب برای این هدف میباشد. بطور مثال نشان داده شده است که کلیدی با طول ۴۰۹۶ در سیستم RSA، امنیتی برابر با کلیدی به طول ۳۱۳ بیت در سیستم رمز خم بیضوی دارد. همچنین نشان داده شده است که تولید کلید در این سیستم نسبت به سیستم RSA با سرعت بیشتری امکان پذیر است. علاوه بر این، از کاربردهای مهم رمزنگاری خم بیضوی در تولید امضای دیجیتال است. همچنین در این سیستم های رمزنگاری، ساختار جبری خم بیضوی به کار رفته میتواند در بالا بردن امنیت تاثیرگذار باشد. دسته ای از الگوریتم های کلاسیک که بر پایه ی سختی حل مسئله ی لگاریتم گسسته می باشند، در سیستم های رمز خم بیضوی نیز مورد استفاده قرار می گیرند. از الگوریتم های معروف میتوان به الگوریتم ECDH[1] که در تبادل کلید و الگوریتم ECDSA [2] در امضای دیجیتال اشاره نمود. در این گزارش ابتدا به معرفی مفاهیم مقدماتی رمزنگاری از جمله رمزنگاری کلید خصوصی و کلید عمومی می پردازیم. سپس مطالبی در مورد خم های بیضوی، ساختار گروهی آنها و خم های بیضوی در میدان های متناهی که از اهمیت بالایی در رمزنگاری خم بیضوی برخوردارند بیان خواهیم کرد. در ادامه الگوریتم های کلاسیک را در چارچوب سیستم رمز خم بیضوی می پردازیم و الگوریتم امضای دیجیتال را بیان می کنیم.

[1] Elliptic Curve Diffie–Hellman
[2] Elliptic Curve Digital Signature Algorithm

فهرست مطالب

فصل ۱

مفاهیم پیش نیاز رمزنگاری

پیش از ورود به مبحث رمزنگاری مبتنی بر خم های بیضوی، مفاهیم مقدماتی و الگوریتم های رمزنگاری که همچنین در رمزنگاری مبتنی بر خم های بیضوی استفاده میشوند را در این فصل بیان می کنیم.

رمزنگاری به دو دسته رمزنگاری متقارن و نامتقارن تقسیم میشود. در رمزنگاری متقارن، طرفین با استفاده از کلیدی مشترک داده ها را رمزگذاری و رمزگشایی میکنند. در مقابل آن در رمزنگاری نامتقارن، دو طرف یک کلید عمومی و یک کلید خصوصی مجزا دارند. کلید عمومی را سایر افراد نیز میدانند، در حالیکه کلید خصوصی را تنها هر یک از طرفین میداند. در رمزنگاری نامتقارن فرستنده با استفاده از کلید عمومی گیرنده اطلاعات را رمزنگاری میکند و گیرنده اطلاعات رمزگذاری شده را با استفاده از کلید خصوصی خود رمزگشایی میکند. در ادامه به معرفی الگوریتم های رمزنگاری متقارن و نامتقارن می پردازیم.

۱.۱ الگوریتم های رمزنگاری متقارن

در این دسته از الگوریتم ها فرستنده و گیرنده با استفاده از کلید خصوصی k، اطلاعات را رمزگذاری و رمزگشایی میکنند، بنابراین شرط این دسته از الگوریتم ها آنست که دو طرف این کلید مشترک را بدانند و طرف سوم به آن دسترسی نداشته باشد و همچنین نتواند متن رمزگذاری شده را بدون داشتن کلید خصوصی رمزگشایی کند. این دسته از الگوریتم ها را از این جهت الگوریتم های متقارن نامیده میشوند که فرستنده و گیرنده اطلاعاتی برابر دارند و آن همان کلید خصوصی است. بیان ریاضی این دسته از الگورایتم ها به قرار زیر است:
یک رمزگذاری متقارن از کلیدی مانند K که از فضای کلید های ممکن $\mathcal{K}$ انتخاب شده است برای رمزگذاری پیام خامی مانند m که از فضای پیام های ممکن $\mathcal{M}$ انتخاب شده است استفاده میکند و

حاصل این فرآیند متن رمزگذاری شده c است که به فضای متن های رمزگذاری شده $\mathcal{C}$ تعلق دارد. در اینصورت رمزگذاری را میتوان تابعی مانند زیر در نظر گرفت:

$$e : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$

و بطور مشابه رمزگشایی بصورت تابعی مانند:

$$d : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

خواهد بود. و رابطه ی زیر بین این توابع برقرار است:

$$d(k, e(k, m)) = m \text{ for all } k \in \mathcal{K} \text{ and all } m \in \mathcal{M}$$

در واقع برای هر کلید k تابع رمزگشایی d_k وارون تابع رمزگذاری e_kاست. آنچه که در این الگوریتم ها اهمیت دارد اینست که امنیت بستگی به کلید خصوصی دارد و نه روش رمزگذاری به کار رفته، در اینصورت فرض میشود که طرف سوم توابع رمزگذاری و رمزگشایی را میداند. این مسئله که امنیت سیستم رمزنگاری به کلید خصوصی بستگی دارد و نه روش به کار رفته را اصل کرکهوفس میگویند.
مطالب مربوط به رمزنگاری متقارن را در اینجا به پایان میرسانیم و به بیان الگوریتم های رمزنگاری نامتقارن که در دنیای امروز از کاربرد بیشتری برخوردارند میپردازیم.

۲.۱ الگوریتم های رمزنگاری نامتقارن

یکی از معضلات الگوریتم های رمزنگاری متقارن لزوم وجود راهی ارتباطی بین فرستنده و گیرنده برای تبادل کلید خصوصی بدون آنکه طرف سوم از آن مطلع باشد است. در صورتی که تمام کانالهای ارتباطی بین فرستنده و گیرنده توسط طرف سوم کنترل شود این امر به نظر غیر ممکن میرسد. اما دیفی و هلمن نشان دادند با وجود فرضیاتی این امر تحقق پذیر است.
فرمول بندی ریاضی این دسته از الگوریتم ها به شرح زیر است:
کلید k که در واقع زوج مرتبی مانند (k_{priv}, k_{pub}) است که به ترتیب کلید خصوصی و کلید عمومی نامیده میشوند و از فضای کلیدهای ممکن $\mathcal{M}$ انتخاب شده است و توابع رمزگذاری و رمزگشایی به ازای هر کلید k:

$$e_{k_{pub}} : \mathcal{M} \to \mathcal{C}$$

$$d_{k_{priv}} : \mathcal{C} \to \mathcal{M}$$

در رابطه ی زیر صدق میکنند:

$$d_{k_{priv}}(e_{k_{pub}}(m)) = m$$

سیستم رمزنگاری مبتنی بر این الگوریتم امن است هرگاه محاسبه ی تابع رمزگشایی برای طرف سوم حتی با وجود دانستن کلید عمومی دشوار باشد. دراینصورت تبادل کلید عمومی و متن رمزگذاری شده از طریق یک کانال ناامن در این دسته از الگوریتم ها مانعی ندارد زیرا طرف سوم قادر به رمزگشایی نخواهد بود چرا که برای رمزگشایی به کلید خصوصی نیاز است که تنها در اختیار فرستنده است. آنچه دیفی و هلمن در مقاله ی انقلابی خود در سال ۱۹۷۶ مطرح کردند تعریف سیستم رمزنگاری کلید عمومی بود. از این قرار که تابعی یکطرفه و اطلاعات درب تله از اجزای آن هستند. یک تابع یکطرفه تابعی وارون پذیر است که محاسبه ی خود آن آسان اما محاسبه ی تابع وارون آن دشوار است. دشواری محاسبه ی تابع به معنای آنست که هر الگوریتم شناخته شده ای برای محاسبه تابع از پیچیدگی زمانی بالایی برخودار باشد. منظور از درب تله آن دسته از اطلاعات اضافه ای است که محاسبه ی تابع وارون را آسان میکند. در این دسته از الگوریتم ها با استفاده از الگوریتم های ساخت کلید، کلید عمومی از کلید خصوصی ساخته میشود. تابع رمزگذاری تابعی است که محاسبه ی آن آسان بوده و بر طرف سوم نیز آشکار است. همچنین تابع رمزگشایی برای گیرنده که از کلید خصوصی اطلاع دارد آسان و برای طرف سوم که از آن مطلع نیست دشوار است. توجه به این نکته ضروری است که محاسبه ی وارون تابعی که کلید عمومی را از کلید خصوصی محاسبه میکند باید دشوار باشد. زیرا کلید عمومی جزو اطلاعات عمومی است و کلید خصوصی آن بخشی از اطلاعات درب تله است که محاسبه ی وارون تابع را ساده میکند. لازم به ذکر است که تاکنون تابع یکطرفه ی شناخته شده ای وجود ندارد و در واقع اثبات وجود چنین تابعی معادل حل مسئله ی معروف $\mathcal{P} = \mathcal{NP}$ میباشد. در ادامه الگوریتم های رمزنگاری کلید عمومی را که با این فرض که محاسبه ی وارون توابع موجود دشوار است بیان میکنیم.

۱.۲.۱ مسئله ی لگاریتم گسسته

تعریف ۱.۱. فرض کنید g ریشه ی اولیه برای میدان $\mathbb{F}_p$ باشد و h عضو ناصفری از این میدان باشد. در اینصورت مسئله ی لگاریتم گسسته عبارتست از یافتن x به طوریکه داشته باشیم:

$$g^x \equiv h \pmod{p}$$

x را لگاریتم گسسته ی h در پایه ی g میگویند و آنرا با نماد $\log_g(h)$ نشان میدهند.

تذکر ۲.۱. اگر مسئله ی لگاریتم گسسته دارای جوابی مانند x باشد آنگاه بنا به قضیه ی کوچک فرما به ازای هر k دلخواه $x + k(p-1)$ جوابی برای مسئله ی لگاریتم گسسته است. بنابراین $\log_g(h)$ در همنهشتی $p-1$ تعریف میشود.

صورت کلی تر مسئله ی لگاریتم گسسته که نیازی به فرض آنکه g ریشه ی اولیه نباشد در زیر آمده است.

تعریف ۳.۱. فرض کنید G یک گروه باشد که عمل آنرا با نماد $\star$ نشان دهیم. در اینصورت مسئله ی لگاریتم گسسته برای G چنین تعریف میشود: برای هر دو عضو دلخواه g و h، x را به گونه ای بیابید که

$$\underbrace{g \star g \star g \star g \cdots \star g}_{x \text{ times}} = h$$

۲.۲.۱ الگوریتم دیفی هلمن

این الگوریتم در واقع ابتکاری است که دیفی و هلمن برای رفع مشکل تبادل کلید مشترک در کانال ناامن ارائه دادند. این الگوریتم از سختی مسئله ی لگاریتم گسسته استفاده میکند و به شرح زیر است:

فرستنده و گیرنده روی یک عدد اول بزرگ مانند p و یک عدد ناصفر به پیمانه ی p مانند g توافق میکنند . این مقادیر برای طرف سوم نیز مشخص است. سپس فرستنده و گیرنده به ترتیب اعداد a و b را انتخاب کرده که بر دیگری آشکار نیست و $A = g^a$ و $B = g^b$ را محاسبه میکنند. آنگاه این مقادیر محاسبه شده را تبادل میکنند. فرستنده در ادامه عدد $B^a = g^{ab}$ و گیرنده $A^b = g^{ab}$ را محاسبه میکند که همان کلید مشترک آنها خواهد بود. توجه کنید که مقادیر A و B برای طرف سوم مشخص است زیر از طریق کانال ناامن تبادل شده اند. در اینصورت مسئله ای که طرف سوم با آن مواجه است آنست که با وجود دانستن g^a و g^b مقدار g^{ab} را محاسبه کند. که این مسئله به مسئله ی دیفی_هلمن معروف است و نشان داده میشود که حل آن سخت تر از حل مسئله ی لگاریتم گسسته نیست. بعبارتی طرف سوم با وجود دانستن مقدار g و p، ااگر بتواند مسئله ی لگاریتم گسسته را حل کند آنگاه از g^a و g^b میتواند مقادیر a و b را بدست آورد و در نتیجه مقدار g^{ab} را محاسبه کند.

الگوریتم دیگری که بر پایه ی سختی لگاریتم گسسته است را در ادامه معرفی میکنیم که به الگوریتم الگامال شناخته میشود.

۳.۲.۱ الگوریتم الگامال

الگوریتم الگامال در واقع دنباله ی الگوریتم دیفی_هلمن است که بر پایه ی سختی لگاریتم گسسته است. توجه کنید گه الگوریتم دیفی_هلمن برای تبادل کلید مشترک (رشته ای از بیت های رندوم) به کار میرود، در حالیکه الگوریتم الگامال که در ادامه به بیان آن میپردازیم برای تبادل هر داده ای در یک بستر ناامن به کار میرود.

ابتدا فرستنده یک الگوریتم و یک کلید عمومی از طریق کانال ناامن با گیرنده تبادل میکند. گیرنده با این الگوریتم پیام خود را با کلید عمومی رمزگذاری میکند و تنها فرستنده میتواند توسط کلید خصوصی خود این پیام رمگذاری شده را رمزگشایی کند. در الگوریتم الگامال بر پایه ی لگاریتم

گسسته، فرستنده یک عدد اول بزرگ مانند p که حل مسئله ی لگاریتم گسسته برای آن دشوار است و یک عدد ناصفر مانند g به پیمانه ی p انتخاب میکند. سپس با استفاده از کلید خصوصی خود، عددی مانند a، مقدار g^a را محاسبه کرده و برای گیرنده میفرستد. حال گیرنده توسط کلید عمومی فرستنده پیامی مانند m که عددی بین ۲ و p میباشد را چنین رمزگذاری میکند: ابتدا عدد رندومی مانند k انتخاب میکند که به آن کلید زودگذر گفته میشود چرا که تنها برای رمگذاری یک پیام به کار میرود. سپس گیرنده مقدایر زیر را محاسبه میکند:

$$c_1 \equiv g^k (\mathrm{mod}\, p) \text{ و } c_2 \equiv mA^k (\mathrm{mod}\, p)$$

در اینصورت (c_1, c_2) متن رمزگذاری شده گیرنده است که فرستنده برای رمزگشایی آن بصورت زیر عمل میکند: ابتدا با استفاده از کلید خصوصی خود مقدار $x \equiv c_1^a \pmod p$ و $x^{-1} \pmod p$ را محاسبه میکند و سپس

$$\begin{aligned} x^{-1}.c_2 &\equiv ({c_1}^a)^{-1}.c_2 \pmod p \\ &\equiv (g^{ak})^{-1}.mA^k \\ &\equiv (g^{ak})^{-1}.(m(g^a)^k) \\ &\equiv m \end{aligned}$$

که همان پیام گیرنده است. در اینصورت اگر طرف سوم بتواند مسئله ی لگاریتم گسسته را حل کند با توجه به اینکه مقادیر g و g^a را میداند، میتواند پیام را رمزگشایی کند. نشان داده میشود که اگر طرف سوم راهی برای رمزگشایی پیام در سیستم الگامال داشته باشد، میتواند مسئله ی دیفی‌ـ هلمن را نیز حل کند. در نتیجه با فرض سختی مسئله ی دیفی‌ـ هلمن، سیستم رمزنگاری الگامال امن بنظر میرسد.

۴.۲.۱ الگوریتم حل مسئله ی لگاریتم گسسته

در این بخش الگوریتم هایی که برا یحل مسئله لگاریتم گسسته و در نتیجه الگوریتم های شکستن سیستم های رمزنگاری مبتنی بر لگاریتم گسسته را بیان میکنیم.

اولین الگوریتم، الگوریتم بروت فورس است که به جستجوی تمام فضای حالات ممکن میپردازد. قضیه ی زیر مرتبه ی اجرایی را این الگوریتم را نشان میدهد.

قضیه ۴.۱. فرض کنید G یک گروه باشد و g عضوی از آن با مرتبه ی n باشد. در اینصورت مسئله ی لگاریتم گسسته $g^x = h$ در $\mathcal{O}(n)$ قابل حل است.

کافیست لیستی از توانهای g از ۱ تا $n-1$ تشکیل دهیم و اگر مسئله گاریتم گسسته جواب داشته باشد، h در این لیست ظاهر میشود.

الگوریتم دیگری که برای حل مسئله لگاریتم گسسته بکار میرود توسط شنکس معرفی شد که در ادامه آنرا بیان میکنیم.

قضیه ۵.۱. فرض کنید G یک گروه باشد و g عضوی از آن با مرتبه ی $N > 2$ باشد، در اینصورت الگوریتم زیر مسئله ی لگاریتم گسسته $g^x = h$ را در $\mathcal{O}(\sqrt{N}.\log(N))$ حل میکند.

۱. قرار دهید $n = 1 + \lfloor \sqrt{N} \rfloor$

۲. دو لیست بصورت زیر تشکیل دهید:

$$e, g, g^2, g^3, \ldots, g^n,$$
$$h, h.g^{-n}, h.g^{-2n}, h.g^{-3n}, \ldots, h.g^{n^2}$$

۳. عدد مشترکی بین دو لیست پیدا کنید.

۴. فرض کنید $g^i = hg^{-jn}$ که در گام سوم الگوریتم یافته اید. در اینصورت $x = i + jn$ جوابی برای مسئله لگاریتم گسسته $g^x = h$ است.

قضیه ی فوق نشان میدهد الگوریتم شکستن مسئله ی لگاریتم گسسته از مرتبه ای زمانی کمی بیشتر از $\mathcal{O}(\sqrt{N})$ است. الگوریتم دیگری نیز برای حل مسئله لگاریتم گسسته در حالت خاص توسط پهلیگ ـ هلمن معرفی شده است. برای آشنایی با این الگوریتم به [۱] مراجعه شود.
فصل مقدمات را در اینجا به پایان میرسانیم و در فصلهای بعد به معرفی خم های بیضوی و رمزنگاری خم بیضوی میپردازیم.

فصل ۲

خم بیضوی

۱.۲ تعاریف اولیه

در این فصل به معرفی خم های بیضوی ، بیان ویژگی ها، فرمول بندی ریاضی مربوط به آنها و قضایای مهم میپردازیم.

تعریف ۱.۲. یک خم بیضوی، منحنی ایی است که مجموعه ی نقاط آن در معادله ای به فرم زیر صدق میکنند:

$$y^2 = x^3 + Ax + B$$

معادله ی فوق را معادله ی وایرشتراس مربوط به خم بیضوی می نامند. میگوییم خم بیضوی E روی میدان K تعریف شده است هرگاه A ، B و x از این میدان انتخاب شده باشند.

یادداشت ۲.۲. برای میدان $L \supseteq K$ نقاطی از E که مختصات آنها به این میدان تعلق داشته باشد را با نماد $E(L)$ نشان می دهیم. این مجموعه همچنین دارای نقطه ی ∞ نیز میباشد که در ادامه لزوم وجود این نقطه را توضیح می دهیم:

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L | y^2 = x^3 + Ax + B\}$$

تذکر ۳.۲. در معادله ی وایرشتراس یک خم بیضوی فرض میشود $4A^3 + 27B^2 \neq 0$.
این معادل آنست که معادله ریشه ی مضاعف ندارد. علت آنست که خم های بیضوی که ریشه ی مضاعف دارند برای کاربردهای رمزنگاری مناسب نیستند.

یادداشت ۴.۲. معادله ی تعمیم یافته ی وایرشتراس به فرم زیر است. این معادله ی کلی در حالتی که میدان با مشخصه ی ۲ یا ۳ باشد، کاربرد دارد.

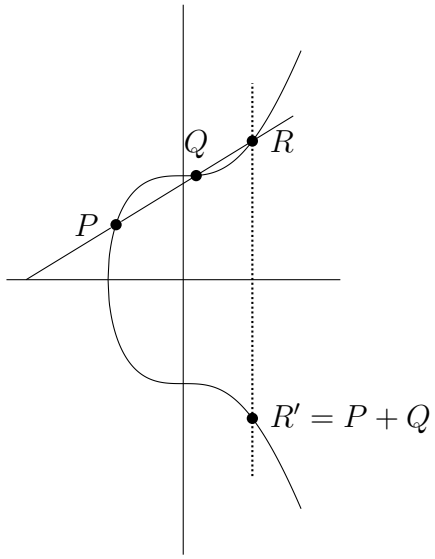
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6$$

در ادامه عمل جمع برای نقاط روی یک خم بیضوی را تعریف میکنیم. مجموعه ی نقاطی که در معادله ی خم بیضوی صدق میکنند با این عمل جمع تشکیل یک گروه آبلی میدهند.

۲.۲ جمع نقاط خم بیضوی

تعریف ۵.۲. فرض کنید P و Q دو نقطه روی خم بیضوی E باشند (شکل ۱.۲) در اینصورت خط گذرنده از این دو نقطه، E را در نقطه ی سومی مانند R قطع میکند. حال بازتاب این نقطه نسبت به محور x ها را بدست آورده و آنرا R' بنامید.تعریف میکنیم:

$$P + Q = R'$$



شکل ۱.۲: جمع نقاط روی خم بیضوی

تذکر ۶.۲. رسم منحنی معنی دار مربوط به خم بیضوی برای هر میدانی امکان پذیر نیست. بنابراین برای چنین میدان هایی برای بدست آوردن حاصل جمع باید از روابط ریاضی که در ادامه به آنها میپردازیم استفاده شود.

با توجه به بیان هندسی جمع دو نقطه روی خم بیضوی، نیاز به بررسی حالتهای مختلف و جزئیات آنها داریم.
در حالتیکه دو نقطه ی $P_1 = (x_1, y_1)$ و $P_2 = (x_2, y_2)$ با یکدیگر متمایز بوده و $x_1 \neq x_2$ باشد، شیب خط L گذرنده از این دو نقطه به راحتی از رابطه ی

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

محاسبه میشود. با جایگذاری معادله ی خط $L : y = m(x - x_1) + y_1$ در معادله ی خم بیضوی و بدست آوردن ریشه های این معادله میتوان مختصات x_3 و با جایگذاری x_3 در معادله ی L، y_3 را بدست آورد

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$
$$0 = x^3 - m^2x^2 + \dots$$
$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

در صورتی که $x_1 = x_2$ و $y_1 \neq y_2$ آنگاه خط گذرنده از P_1 و P_2 موازی محور عمودی است.

در اینجا نقطه ی ∞ که در فصل اول به آن اشاره کردیم راهگشا میباشد. در واقع این نقطه را چنین تعریف میکنیم که روی هر خط عمودی و در هر دو انتهای محور عمودی قرار دارد. همچنین هر دو خط عمودی در این نقطه به یکدیگر می رسند. با توجه به این قرارداد مشخص است که نقطه ی ∞ در دو انتهای محور عمودی یکسان میباشد. برای یک میدان که دارای ترتیب بین اعضا نمیباشد، با استفاده از مختصات تصویری، نقطه ی ∞ را تعریف میکنند. برای مطالعه ی بیشتر به [۲] مراجعه شود.
با توجه به تعریف نقطه ∞ نقطه ی اشتراک دیگر خط عمودی $x = x_1$ با خم بیضوی نقطه ی ∞ میباشد و بازتاب این نقطه نسبت به محور x خود این نقطه است. در نتیجه در این حالت داریم $P_1 + P_2 = \infty$.

حال حالتی را در نظر بگیرید که $P_1 = P_2 = (x_1, y_1)$. هنگامی که دو نقطه ی P_1 و P_2 به یکدیگر بسیار نزدیک باشند، خط گذرنده از آنها، در واقع تقریبی است از یک خط مماس بر منحنی. در اینصورت وقتی دو نقطه یکسان هستند، خط گذرنده از آنها را برابر خط مماس بر منحنی در آن نقطه میگیریم. حال با استفاده از مشتق ضمنی میتوان شیب خط مماس، معادله ی آن و سپس با جایگذاری مانند حالت اول مختصات نقطه ی دیگر را بدست آورد:

$$m = \frac{3x_1^2 + A}{2y_1}$$
$$x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$

توجه کنید که اگر $y_1 = 0$ باشد آنگاه خط مماس عمودی است و داریم $P_1 + P_2 = \infty$.
در نهایت اگر $P_2 = \infty$ آنگاه خط گذرنده از P_1 و ∞ خطی عمودی است که نقطه ی برخورد دیگر آن با خم بیضوی بازتاب P_1 میباشد و در نتیجه داریم $P_1 + \infty = P_1$.

خلاصه ی مطالب فوق را در ادامه بیان میکنیم.

فرض کنید $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ بطوریکه $P_1, P_2 \neq \infty$ نقاطی روی خم بیضوی E باشند. در اینصورت $P_1 + P_2 = P_3 = (x_3, y_3)$ را چنین تعریف میکنیم:

۱. اگر $x_1 \neq x_2$ آنگاه

$$m = \frac{y_2 - y_1}{x_2 - x_1}, x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$$

۲. اگر $x_1 = x_2$ اما $y_1 \neq y_2$ آنگاه $P_1 + P_2 = \infty$

۳. اگر $P_1 = P_2$ و $y_1 \neq 0$ آنگاه

$$m = \frac{3x_1^2 + A}{2y_1}, x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$

۴. اگر $P_1 = P_2$ و $y_1 = 0$ آنگاه $P_1 + P_2 = \infty$

۵. برای هر نقطه ی دلخواه P تعریف میکنیم $P + \infty = P$

قضیه ی مهم زیر نشان میدهد مجموعه نقاط E به همراه عمل جمع تعریف شده تشکیل یک گروه آبلی میدهند.

قضیه ۷.۲. عمل جمع برای یک خم بیضوی در شرایط زیر صدق میکند:

۱. (جابجایی) برای هر دو نقطه ی دلخواه P_1 و P_2 داریم $P_1 + P_2 = P_2 + P_1$

۲. (وجود عضو بی اثر) برای هر نقطه ی دلخواه P داریم $P + \infty = P$

۳. (وجود عضو وارون) برای هر نقطه دلخواه P، نقطه ای مانند P' وجود دارد که $P + P' = \infty$. P' را با نماد $-P$ نشان می دهیم.

۴. (شرکت پذیری) برای هر سه ی نقطه دلخواه P_1، P_2 و P_3 داریم $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$

اثبات. خاصیت وجود عضو بی اثر و عضو خنثی با توجه به تعریف برقرار است. برای خاصیت جابجایی توجه کنید که خط گذرنده از P_1 و P_2 همان خط گذرنده از P_2 و P_1 است. اما اثبات خاصیت شرکت پذیری از پیچیدگی برخوردار است و در اینجا ما به آن نمی پردازیم. برای اثبات به [۲] یا [۳] مراجعه شود. اثبات ارائه شده در [۲] با استفاده از فضاهای تصویری انجام شده است. همچنین میتوان با استفاده از محاسبات جبری با استفاده از روابط معرفی شده حکم را ثابت نمود. □

یادداشت ۸.۲. اگر P نقطه ای روی خم بیضوی و k یک عدد صحیح باشد آنگاه،

$$kp = \underbrace{P + P + \cdots + P}_{k\text{مرتبه}}$$

۳.۲ jـ ثابت

در فصل اول اشاره کردیم که ضرایب A و B در رابطه ی $4A^3+27B^2 \neq 0$ صدق میکنند. مقدار $4A^3+27B^2$ در واقع همان مبیّن چندجمله ای درجه ی سه است که ناصفر بودن آن تضمین میکند که ریشه ها متمایز هستند. حال تعریف jـ ثابت را بیان میکنیم.

تعریف ۹.۲. برای خم بیضوی $y^2=x^3+Ax+B$ ، jـ ثابت E را تعریف کنید

$$j(E)=1728\frac{4A^3}{4A^3+27B^2}$$

قضیه ی مهم زیر نشان میدهد هرگاه دو خم بیضوی دارای jـ ثابت برابر باشند قابل تبدیل به یکدیگر به استفاده از توابع گویا هستند و برعکس. این قضیه یکریختی برای خم های بیضوی را نشان میدهد.

قضیه ۱۰.۲. فرض کنید $E_1 : y^2=x^3+A_1x+B_1$ و $E_2 : y^2=x^3+A_2x+B_2$ دو خم بیضوی با jـ ثابت های j_1 و j_2 باشند. در اینصورت اگر $j_1=j_2$ باشد، آنگاه وجود دارد $\mu \neq 0 \in \overline{K}$[۱] که

$$A_2=\mu^4 A_1$$
$$B_2=\mu^6 B_1$$

و تبدیل $x_2=\mu^2 x_1$ ، $y_2=\mu^3 y_1$ یک معادله را به دیگری میبرد. همچنین هرگاه روابط فوق بین ضرایب دو خم بیضوی برقرار باشد خواهیم داشت $j_1=j_2$.

اثبات. با فرض $A_1 \neq 0$، برای طرف اول μ را به گونه ای انتخاب کنید که $A_2=\mu^4 A_1$. دراینصورت با جایگذاری در روابط jـ ثابت مقدار $B_2=\pm\mu^6 B_1$ بدست می آید. در صورتی که $B_2=-\mu^6 B_1$ آنگاه μ به $i\mu$ تغییر دهید. برای طرف دوم با جایگذاری برابری j_1 و j_2 به آسانی نشان داده میشود. □

تذکر ۱۱.۲. توجه داشته باشید قضیه ی فوق در یک میدان جبری بسته برقرار است. بعبارتی اگر دو خم بیضوی در یک میدان جبری که بسته نباشد، لزوما برقرار نیست. چرا که ممکن است هیچ تابع گویایی با ضرایب انتخاب شده از میدان برای تبدیل دو خم بیضوی وجود نداشته باشد.

[۱] میدان جبری بسته

۴.۲ درون ریختی

منظور از یک درون ریختی E، یک همریختی $\alpha : E(\overline{K}) \to E(\overline{K})$ است که توسط توابع گویا تعریف شده باشد. بعبارت دیگر: $\alpha(P1 + P2) = \alpha(P1) + \alpha(P2)$، و توابع گویایی مانند $R_1(x,y), R_2(x,y)$ وجود دارند که ضرایب آنها از $\overline{K}$ انتخاب شده است و

$$\alpha(x,y) = (R_1(x,y), R_2(x,y))$$

توجه کنید که برای هر زوج $(x,y) \in E(\overline{K})$ میتوان y را با $x^3 + Ax + B$ جایگزین کرد. بنابراین هر تابع گویا بصورت زیر قابل بازنویسی است:

$$R(x,y) = \frac{p_1(x)+p_2(x)y}{p_3(x)+p_4(x)y}$$

که در آن توانهای فرد و زوج y به ترتیب با توابع $p_i(x)$ و $p_j(x)y$ داده شده اند. از طرفی از آنجا که α یک همریختی است داریم $\alpha(x,-y) = -\alpha(x,y)$ و در نتیجه

$$R_2(x,-y) = -R_2(x,y) \text{ ، } R_1(x,-y) = R_1(x,y)$$

بنابراین میتوان فرض کرد $\alpha(x,y) = (r_1(x), r_2(x)y)$.

تعریف ۱۲.۲. فرض کنید $r_1(x) = \frac{p(x)}{q(x)}$، در اینصورت اگر مشتق حداقل یکی از توابع صورت یا مخرج تابع ثابت صفر نباشد، در اینصورت α را درون ریختی جداپذیر می گویند. بعلاوه تعریف میکنیم $\deg(\alpha) = \text{Max}\{\deg p(x), \deg q(x)\}$

مثال ۱۳.۲. فرض کنید خم بیضوی E روی میدان متناهی F_q تعریف شده باشد. در اینصورت نگاشت $\phi_q(x,y) = (x^q, y^q)$ موسوم به نگاشت فروبنیوس یک درون ریختی جداناپذیر برای E میباشد.نگاشت فروبنیوس از اهمیت زیادی در رمزنگاری خم بیضوی برخوردارست.

گزاره ی زیر در اثبات قضیه ی هاسه که در فصل خم های بیضوی در میدان متناهی به آن میپردازیم نقش حیاتی دارد.

گزاره ۱۴.۲. فرض کنید $\alpha \neq 0$ یک درون ریختی جداپذیر برای خم بیضوی E باشد. در اینصورت داریم:

$$deg\ \alpha = \#Ker(\alpha)$$

که در آن $Ker(\alpha)$ هسته ی همریختی $\alpha : E(\overline{K}) \to E(\overline{K})$ میباشد.
اگر α جداپذیر نباشد آنگاه

$$deg\ \alpha > \#Ker(\alpha)$$

در اینجا مقدمات مربوط به خم بیضوی را به پایان می رسانیم. و در فصل آینده در مورد زوج سازی ویل که از مباحث مهم در مطالعه خم های بیضوی است میپردازیم.

فصل ۳

زوج سازی ویل

۱.۳ نقاط پیچش

تعریف ۱.۳. فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است و n عددی صحیح باشد. در اینصورت تعریف می کنیم

$$E[n] = \{P \in E(K) | \, nP = \infty\}$$

برای میدانی که مشخصه ی آن ۲ نیست، $E[2]$ به سادگی قابل تعریف است: قرار دهید $y^2 = (x-e_1)(x-e_2)(x-e_3)$، در اینصورت $2P = \infty$ اگر و تنها اگر خط مماس بر خم بیضوی در این نقطه عمودی باشد. این معادل آنست که $y = 0$. بنابراین داریم:

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

قضیه ۲.۳. فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است و n عددی صحیح باشد. در اینصورت اگر مشخصه ی K بر n بخش پذیر یا صفر نباشد، در اینصورت داریم

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

اگر مشخصه ی K، $p > 0$ باشدو $p|n$ بنویسید $n = p^r n'$ که $p \nmid n'$ در اینصورت

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}'_n \text{ یا } E[n] \simeq \mathbb{Z}'_n \oplus \mathbb{Z}'_n$$

اثبات. برای اثبات رجوع شود به [۲] □

۲.۳ زوج سازی ویل

زوج سازی ویل یکی از ابزارهای اصلی در مطالعه ی خم های بیضوی است. بطور مثال برای اثبات تعداد نقاط روی یک خم بیضوی در یک متناهی، یا حل مسئله ی لگاریتم گسسته برای خم بیضوی کاربرد دارد. در ادامه قضیه زوج سازی ویل را بیان میکنیم. برای اثبات میتوان به [۲] یا [۳] مراجعه شود.

تعریف ۳.۳. فرض کنید E یک خم بیضوی روی میدان K و n عددی صحیح باشد. همچنین فرض کنید مشخصه ی K بر n بخش پذیر نباشد. در اینصورت طبق قضیه ی ۲.۳، $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. در اینصورت

$$\mu_n = \{x \in \overline{K} | x^k = 1\}$$

گروه ریشه های n ام واحد در $\overline{K}$ میباشد. از آنجایی که مشخصه K، بر n بخش پذیر نیست، $x^n = 1$ ریشه ی مضاعف ندارد و در نتیجه μ_n گروهی دوری از مرتبه ی n است. برای ζ که مولد μ_n باشد، میگوییم ζ ریشه ی n ام اولیه ی واحد است.

قضیه ۴.۳. فرض کنید E یک خم بیضوی باشد که روی میدان K تعریف شده است و n عددی صحیح باشد. همچنین فرض کنید مشخصه ی K بر n بخش پذیر نباشد. در اینصورت زوج سازی زیر موسوم به زوج سازی ویل موجود است که در شرایط زیر صدق میکند:

$$e_n : E[n] \times E[n] \to \mu_n$$

۱. e_n برای هر متغیری دوسویه است. بعبارت دیگر:

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

برای هر $S, S_1, S_2, T, T_1, T_2 \in E[n]$

۲. e_n برای هر متغیری غیر منحط است. به این معنا که اگر $e_n(S, T) = 1$ باشد برای هر $T \in E[n]$، آنگاه $S = \infty$ و اگر $e_n(S, T) = 1$ برای هر $S \in E[n]$ آنگاه $T = \infty$.

۳. $e_n(T, T) = 1$ برای هر $T \in E[n]$.

۴. $e_n(T, S) = e_n(S, T)^{-1}$ برای هر $S, T \in E[n]$

۵. $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ برای تمام یکریختی های σ در $\overline{K}$ که برای ضرایب E داشته باشیم $\sigma(A) = A, \sigma(B) = B$

۶. $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{deg(\alpha)}$ برای تمام درون ریختی های جداپذیر α

نتیجه ۵.۳. فرض کنید T_1, T_2 پایه ای برای $E[n]$ باشد. در اینصورت $e_n(T_1, T_2)$ ریشه ی n ام اولیه ی واحد است.

اثبات. فرض کنید $e_n(T_1, T_2) = \zeta$ بطوریکه $\zeta^d = 1$. در اینصورت $e_n(T_1, dT_2) = 1$ همچنین $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ (طبق (۱) و (۳)) حال فرض کندی $S \in E[n]$. در اینصورت a, b موجودند بطوری که $S = aT_1 = bT_2$. در نتیجه داریم:

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1$$

حال از آنجایی که S دلخواه است طبق (۲) خواهیم داشت $dT_2 = \infty$.
از طرفی $dT_2 = \infty$ اگر و تنها اگر $n|d$ که نتیجه میدهد ζ ریشه ی nام اولیه ی واحد است. □

فصل ۴

خم های بیضوی روی میدان متناهی

فرض کنید $\mathbb{F}$ یک میدان متناهی باشد و E یک خم بیضوی باشد که روی این میدان تعریف شده است. در اینصورت تعداد متناهی زوج (x, y) وجود دارند که $x, y \in \mathbb{F}$ باشند. بنابراین $E(\mathbb{F})$ یک گروه متناهی است. در این فصل ویژگی های این گروه از خم های بیضوی را که کاربردهای زیادی در رمزنگاری خم بیضوی دارند بیان میکنیم.

مثال ۱.۴. فرض کنید $y^2 = x^3 + x + 1$ یک خم بیضوی روی میدان $\mathbb{F}_5$ باشد. دراینصورت برای پیدا کردن نقاط روی این خم، به ازای تک تک مقادیر x، مقدار $x^3 + x + 1$ را محاسبه کرده و در صورتی که در پیمانه ی ۵ دارای ریشه ی دوم باشد برای y دو مقدار بدست می آید. در نتیجه به ازای هر x یا دو نقطه روی خم بیضوی خواهیم داشت یا نقطه ای وجود نخواهد داشت. با انجام محاسبات، به مجموعه نقاط زیر میرسیم:

$$E(\mathbb{F}_5) = \{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3), \infty\}$$

قضیه ۲.۴. فرض کنید E یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ باشد در اینصورت داریم:

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad \text{یا} \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

همچنین داریم $n_1 | n_2$

اثبات. از نظریه ی گروه ها میدانیم هر گروه آبلی متناهی یکریخت است با جمع مستقیم گروه های دوری $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \cdots \oplus \mathbb{Z}_{n_r}$ بطوریکه $n_i | n_{i+1}$. از طرفی برای هر i، $\mathbb{Z}_{n_i}$ دارای n_1 عضو از مرتبه ی بخش پذیر بر n_1 است. در نتیجه $E(\mathbb{F}_q)$ دارای n_1^r عضو از مرتبه ی بخش پذیر بر n_1 است. از طرفی طبق قضیه ی ۲.۳ حداکثر n_1^2 عضو با این ویژگی داریم. در نتیجه $r \leq 2$. □

مطالبی که در ادامه بیان می کنیم در اثبات قضیه ی مهم هاسه به کار میروند.

فرض کنید $\mathbb{F}_q$ میدان متناهی باشد و

$$\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,$$
$$x \mapsto x^q$$

نگاشت فربونیوس برای $\mathbb{F}_q$ باشد.. همچنین فرض کنید E خم بیضوی روی $\mathbb{F}_q$ باشد. داریم:

$$\phi_q(x, y) = (x^q, y^q),$$
$$\phi_q(\infty) = \infty$$

لم ۳.۴. فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ باشد و $(x, y) \in E(\mathbb{F}_q)$ باشد. در اینصورت داریم:

۱. $\phi_q(x, y) \in E(\mathbb{F}_q)$

۲. $(x, y) \in E(\mathbb{F}_q)$ اگر و تنها اگر $\phi_q(x, y) = (x, y)$

گزاره ۴.۴. فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ و $n > 1$ باشد.

۱. $Ker(\phi_q^n - 1) = E(\mathbb{F}_q)$

۲. $\phi_q^n - 1$ یک درون ریختی جدا پذیر است و $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$

اثبات. از آنجایی که ϕ_q^n نگاشت فربونیوس برای $\mathbb{F}_{q^n}$ است، گزاره ی (۱) مشابه لم ۳.۴ میباشد. به آسانی میتوان نشان داد که $\phi_q^n - 1$ یک درون ریختی است و در نتیجه طبق گزاره ۱۴.۲ خواهیم داشت $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$ □

قضیه ی مهم زیر موسوم به قضیه ی هاسه که کرانی برای مرتبه ی گروه $E(\mathbb{F}_q)$ میدهد را ثابت کنیم.

قضیه ۵.۴. فرض کنید E یک خم بیضوی روی میدان $\mathbb{F}_q$ باشد. در اینصورت مرتبه ی $E(\mathbb{F}_q)$ در رابطه ی زیر صدق می کند:

$$| q + 1 - \#E(\mathbb{F}_q) | \leq 2\sqrt{q}$$

اثبات. قرار دهید

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1)$$

می خواهیم نشان دهیم $| a | \leq 2\sqrt{q}$
فرض کنید r, s اعداد صحیح باشند بطوری که $\gcd(s, q) = 1$.
آنگاه $\deg(r\phi_q - s) = r^2q + s^2 - rsa$ حال چون $\deg(r\phi_q - s) > 0$ داریم:

$$q(\tfrac{r}{s})^2 - a(\tfrac{r}{s}) + 1 \geq 0$$

از طرفی مجموعه ی اعداد گویا r/s بطوریکه $\gcd(s,q)=1$ باشد در $\mathbb{R}$ چگال است. در نتیجه برای هرعدد حقیقی x داریم:

$$qx^2 - ax + 1 \geq 0$$

بنابراین مبین این چند جمله ای درجه ی ۲ منفی است که معادل آنست که $a^2 - 4q \leq 0$ و بنابراین $| a | \leq 2\sqrt{q}$

□

یادداشت ۶.۴. قضیه ی هاسه در واقع کرانی برای تعداد نقاط روی خم بیضوی در میدان متناهی بدست می دهد. اسکوف [۱] در سال ۱۹۸۵ الگوریتمی ارائه داد که به کمک آن تعداد نقاط روی خم را بطور دقیق محاسبه میکند. برای آشنایی با الگوریتم به [۲] مراجعه شود.

[۱] Schoof

فصل ۵

رمزنگاری خم بیضوی

در این فصل به معرفی سیستم های رمزنگاری مبتنی بر خم بیضوی، به وِیژه سیستم های مبتنی بر مسئله ی لگاریتم گسسته برای خم بیضوی می پردازیم. در ادامه به بیان مطالب مرتبط از جمله امضای دیجیتال میپردازیم. یکی از مزیت های استفاده از خم بیضوی در رمزنگاری آنست که میتوان با صرف حافظه ی کمتری به امنیت برابری با سایر سیستم های رمزنگاری من جمله سیستم رمزنگاری RSA رسید. بطور مثال تخمین زده شده است که کلیدی با ۴۰۹۶ بیت طول امنیتی در سیستم RSA، امنیتی برابر با کلیدی به طول ۳۱۳ بیت در سیستم رمزنگاری خم بیضوی دارد.
الگوریتم هایی که در فصل اول معرفی کردیم در رمزنگاری خم بیضوی نیز به کار میروند. در این فصل صورت تغییر یافته ی این الگوریتم ها با بکارگیری خم بیضوی را بیان می کنیم. در انتها الگوریتم امضای دیجیتال را مطرح می کنیم.

الگوریتم هایی که در فصل اول نیز معرفی کردیم برای خم بیضوی نیز بر پایه ی سختی حل مسئله ی لگاریتم گسسته روی خم بیضوی نیز مطرح میشوند.

مسئله ی لگاریتم گسسته برای خم بیضوی

تعریف ۱.۵. فرض کنید E یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ باشد و همچنین $P, Q \in E(\mathbb{F}_q)$. در اینصورت مسئله ی لگاریتم گسسته خم بیضوی عبارتست از پیدا کردن عدد صحیح n، بطوریکه $Q = nP$.

پیش از آنکه الگوریتم های رمزنگاری خم بیضوی را معرفی کنیم، الگوریتم بروت فورس برای حل مسئله ی لگاریتم گسسته خم بیضوی را بیان میکنیم.

حل مسئله ی لگاریتم گسسته خم بیضوی

برای حل مسئله ی لگاریتم گسسته $Q = nP$، طرف سوم ابتدا اعداد رندوم صحیح $j_1, \ldots, j_r$ و $k_1, \ldots, k_r$ بین ۱ و p را انتخاب میکند. سپس دو لیست زیر را تشکیل میدهد:

$$j_1P, j_2P, j_3P, ..., j_rP$$
$$k_1P + Q, k_2P + Q, k_3P + Q, ..., k_rP + Q$$

حال اگر بین دو لیست عضو مشترکی پیدا کند، بطور مثال $j_uP = k_vP + Q$، $Q = (j_u - k_v)P$، جواب مسئله را بدست می دهد.

۱.۵ الگوریتم دیفی_هلمن خم بیضوی

ابتدا فرستنده و گیرنده روی یک خم بیضوی مانند E روی میدان متناهی $\mathbb{F}_q$ توافق میکنند. همچنین نقطه ای مانند $P \in E(\mathbb{F}_q)$ را که مرتبه ی گروه دوری ایجاد شده توسط آن به اندازه ی کافی بزرگ است انتخاب میکنند. سپس فرستنده و گیرنده به ترتیب اعداد a و b را انتخاب کرده و مقادیر $P_a = aP$ و $P_b = bP$ را محاسبه کرده و با یکدیگر تبادل میکنند. حال فرستنده مقدار $aP_b = abP$ و گیرنده مقدار $bP_a = baP$ را محاسبه میکنند که کلید مشترک آنها خواهد بود. در اینصورت طرف سوم با وجود دانستن E، P_a و P_b باید مقدار abP را بدست آورد. که مشابه مسئله ی دیفی_هلمن برای گروه ضربی $\mathbb{F}_q^\times$ سختی آن معادل سختی حل کردن مسئله ی لگاریتم گسسته است.

مسئله ی تصمیم گیری دیفی_هلمن

تعریف ۲.۵. فرض کنید E، aP، bP، داده شده اند. برای نقطه ی دلخواه $Q \in E(\mathbb{F}_q)$، آیا میتوان مشخص نمود که $Q = abP$ یا خیر.

نشان داده میشود که برای دسته ای از خم ها مسئله ی تصمیم گیری دیفی_هلمن با استفاده از زوج سازی ویل قابل حل است. در این حالت نیازی به حل مسئله ی لگاریتم گسسته نمیباشد.

۲.۵ رمزگذاری مسی_عمورا

الگوریتم این سیستم رمزگذاری که مشابه الگوریتم دیفی_هلمن بر پایه ی سختی مسئله لگاریتم گسسته است به صورت زیر میباشد.

۱. فرستنده و گیرنده روی یک خم بیضوی مانند E روی میدان متناهی $\mathbb{F}_q$ توافق میکنند. قرار دهید $N = \#E(\mathbb{F}_q)$

۲. فرستنده پیام خود را بصورت نقطه ای مانند M روی خم بیضوی نمایش میدهد.

۳. سپس فرستنده عدد صحیحی مانند m_A که $\gcd(m_A, N) = 1$ باشد را انتخاب میکند و مقدار $M_1 = m_AM$ را محاسبه میکند و برای گیرنده میفرستد.

۴. گیرنده عددی مانند m_B که $\gcd(m_B, N) = 1$ را انتخاب کرده و مقدار $M_2 = m_B M_1$ را محاسبه کرده و برای فرستنده ارسال میکند.

۵. حال فرستنده مقدار $M3 = m_A^{-1} M_2$ را محاسبه کرده و برای گیرنده میفرستد.

۶. گیرنده مقدار $M_4 = m_B^{-1} M_3$ را محاسبه کرده که همان پیام فرستنده است.

یادداشت ۳.۵. توجه کنید که $M_4 = m_B^{-1} m_A^{-1} m_B m_A M = m_B^{-1} m_B m_A^{-1} m_A M$ از طرفی چون مرتبه ی گروه برابر N است، k وجود دارد که $m_A^{-1} m_A = 1 + kN$ از طرفی برای هر $R \in E(\mathbb{F}_q)$ داریم $NR = \infty$. بنابراین $m^{-1} A m_A M = (1 + kN)M = M + k\infty = M$ و بطور مشابه $m_B^{-1} m_B M = M$ که نشان میدهد مقدار محاسبه شده در گام ششم الگوریتم همان پیام خام فرستنده است.

حال طرف سوم $E(\mathbb{F}_q)$ و نقاط $m_A M$ و $m_B M$ و $m_B m_A M$ را میداند. قرار دهید $a = m^{-1} A$ و $b = m^{-1} B$ و $P = m_A m_B M$، در اینصورت طرف سوم P، aP و bP را میداند و باید مقدار abP را محاسبه کند. این همان مسئله ی دیفی‌ـ هلمن است.

۳.۵ الگوریتم الگامال خم بیضوی

در این الگوریتم ابتدا گیرنده یک خم بیضوی مانند E روی یک میدان متناهی که مسئله ی لگاریتم گسسته برای $E(\mathbb{F}_q)$ سخت است را انتخاب میکند. سپس نقطه ای مانند P روی خم و عدد صحیحی را انتخاب میکند و مقدار $B = sP$ را محاسبه کرده و برای فرستنده ارسال میکند. توجه کنید که E، $E(\mathbb{F}_q)$ و B کلید عمومی گیرنده و کلید خصوصی است.s حال فرستنده با استفاده از کلید عمومی گیرنده، پیام خود را که بصورت نقطه ای مانند M روی خم بیضوی است چنین رمزگذاری میکند. ابتدا عدد صحیح رندومی مانند k، انتخاب میکند و مقدار $M_1 = kp$ را محاسبه میکند. سپس $M_2 = M + kB$ را محاسبه کرده و (M_1, M_2) را برای گیرنده ارسال میکند. گیرنده متن خام فرستنده را چنین رمزگشایی میکند

$$M = M_2 - sM_1$$

رمزگشایی فوق پیام خام فرستنده را بدست می دهد زیرا:

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M$$

حال طرف سوم با وجود دانستن اطلاعات عمومی گیرنده و نقاط M_1 و M_2 اگر بتواند مسئله لگاریتم گسسته را حل کند، میتواند با استفاده از P و B مقدار s را پیدا کرده و پیام فرستنده را رمزگشایی کند.

۴.۵ الگوریتم امضای دیجیتال

بعنوان مطلب پایانی، الگوریتم امضای دیجیتال مبتنی بر خم بیضوی را بیان میکنیم. فرض کنید فرستنده بخواهد سند ارسالی خود را امضا کند. این سند معمولا یک عدد صحیح است که خروجی یک تابع درهم سازی است که متن اصلی را که ممکن است شامل میلیاردها بیت باشد به یک عدد صحیح نظیر کند. از ویژگی های این تابع درهم سازی میتوان به موارد زیر اشاره کرد:

۱. برای یک پیام m، محاسبه ی $H(m)$، به اندازه ی کافی سریع باشد.

۲. برای هر y دلخواه محاسبه ی m بطوریکه $H(m) = y$ باشد از لحاظ محاسباتی ممکن نباشد.

۳. از لحاظ محاسباتی پیدا کردن دو پیام متمایز m_1 و m_2، بطوریکه $H(m_1) = H(m_2)$ غیر ممکن باشد.

حال به توضیح الگوریتم می پردازیم: فرستنده ابتدا یک خم بیضوی مانند E روی یک میدان متناهی مانند $\mathbb{F}_q$) بطوریکه $\#E(\mathbb{F}_q) = fr$ که در آن r یک عدد اول بزرگ و f یک عدد صحیح کوچک است، انتخاب میکند. سپس یک نقطه ی پایه مانند G در $E(\mathbb{F}_q)$ که مرتبه ی آن r است، انتخاب میکند. سپس عدد صحیحی خصوصی a را انتخاب کرده و مقدار $Q = aG$ را محاسبه میکند. حال فرستنده برای امضای پیامی مانند mبصورت زیر عمل میکند.

۱. عدد صحیح رندومی مانند k که $1 \leq k < r$ انتخاب کرده و مقدار $R = kG = (x, y)$ را محاسبه می کند.

۲. مقدار $s = k^{-1}(m + ax) \pmod r$ را محاسبه میکند.

در اینصورت سند امضا شده (m, R, s) میباشد. حال گیرنده برای اعتبار سنجی امضا چنین عمل میکند:

۱. مقدار $u_1 = s^{-1}m \pmod r$ و $u_2 = s^{-1}x \pmod r$ را محاسبه می کند.

۲. مقدار $V = u_1G + u_2Q$ را محاسبه میکند.

۳. اگر $V = R$ آنگاه امضا را تایید میکند.

چرا که اگر پیام به درستی امضا شده باشد خواهیم داشت:

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R$$

واژه‌نامه فارسی به انگلیسی

کلید عمومی	public key
کلید خصوصی	private key
درب تله	trapdoor
رمزگذاری	encryption
رمزگشایی	decryption
خم بیضوی	elliptic curve
لگاریتم گسسته	discrete logarithm
درون ریختی	endomorphism
نقاط پیچش	torsion points
زوج سازی	pairing
میدان متناهی	finite field

کتاب‌نامه

[1] J. Hoffstein, J. Pipher, J. H. Silverman and J. H. Silverman, An introduction to mathematical cryptography., Springer, vol. 1, 2008.

[2] L. C. Washington. Elliptic Curves: Number Theory and Cryptography. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2003

[3] J. H. Silverman and J. Tate. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992

Abstract

The rapid growth of electronic communication means that issues in information security are of increasing practical importance.Messages exchanged over worldwide publicly accessible computer networks must be kept confidential and protected against manipulation.Electronic business requires digital signatures that are valid in law, and secure payment protocols.Modern cryptography provides solutions to all these problems.
In this report we will study elliptic curve cryptography which is the modern successor of the RSA cryptosystem, since it can provide security equivalent to classical systems like RSA while using fewer bits. For example, it is estimated that a key size of 4096 bits for RSA gives the same level of security as 313 bits in an elliptic curve system.We begin by giving a preliminary on classical crypotographic algorithms, then proceed with the mathematical defnitions of an elliptic curve, its group structure and so on. At last, we will discuss elliptic curve cryptosystems and explain the digital signature algorithm based on elliptic curves.

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

Elliptic Curve Cryptography

Setareh Najafi

Supervisor: Dr. Amir Ghadermarzi

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

Summer 2022