بسم اللّه الرّحمن الرّحيم

وزارت علوم، تحقیقات و فناوری

دانشگاه تربیت معلم آذربایجان

دانشکده علوم پایه

پایان نامه

جهت اخذ درجه کارشناسی ارشد

رشته ریاضی محض

عنوان :

دستور محاسبه عمل گروه ژاکوبین خم های فوق بیضوی از گونهٔ ۲

استاد راهنما :

دکتر فرضعلی ایزدی

اساتید مشاور :

دکترقربانعلی حقیقت دوست

دکترمنیره صدقی

پژوهشگر :

مریم شیخی گرجان

شهریور / ۱۳۸۷

تبریز / ایران

تقدیم به

پدر و مادر بزرگوارم

تشکر و قدردانی

با استعانت از خداوند متعال که همواره پشتیبان همگان است، بر خود وظیفه می‌دانم تا از تمامی عزیزانی که راهگشای این پروژه بوده‌اند، تشکر و قدردانی نمایم. امید است که سپاس بی‌دریغ اینجانب را بپذیرند.

استاد بزرگوارم جناب آقای دکتر فرضعلی ایزدی که گنجینه‌های دانش خود را در نهایت صبوری و سخاوت در اختیار اینجانب قرار دادند و مرا در انجام این پروژه همراهی کردند.

دکترمنیره صدقی و دکتر قربانعلی حقیقت دوست که داوری این پروژه را پذیرفتند.

سایر اساتید محترم که در طول دوران تحصیلم افتخار شاگردی ایشان را داشته‌ام.

خانواده عزیزم که یاور و مشوق همیشگی من در زندگی و به ویژه در دوران تحصیلاتم بوده‌اند.

برای تمام این عزیزان، سربلندی و موفقیت و سلامتی در تمام مراحل زندگی آرزو می‌کنم.

مریم شیخی گرجان

فهرست مندرجات

چکیده

گروه ردهٔ ایده‌آل‌های خم های فوق بیضوی می‌توانند در دستگاه‌های رمزنگاری برپایه لگاریتم گسسته مورد استفاده قرار گیرند. در این رساله، فرمول‌های دقیقی برای انجام عمل گروه خم‌های فوق بیضوی از گونهٔ ۲ بیان خواهیم کرد. این فرمول‌ها درحالت کلی برای همه خم‌ها عمومیت داشته ولی برای حصول کمترین تعداد عملیات، حالت‌ها رابرای مشخصه‌های زوج وفرد جداگانه بررسی خواهیم کرد. سه دستگاه مختصات مختلف ارائه خواهیم کرد که برای محیط های متفاوت مناسب هستند، به عنوان مثال درکارت‌های هوشمند بایستی از اعمال معکوس اجتناب کنیم، در حالی که در نرم افزارها تعداد اعمال قابل قبول بایستی محدود باشد. فرمول‌های ارائه شده، برای انجام عمل گروه خم‌های فوق بیضوی گونهٔ ۲ ازلحاظ کاربردی بسیار مفید است. ابتدا عمل گروه خم فوق بیضوی را روی دستگاه مختصات آفین محاسبه می‌کنیم که به یک عمل معکوس نیاز دارد. سپس دستگاه مختصات تصویری را در نظر می‌گیریم که نیازی به عمل معکوس نداشته، ولی به تعداد ضرب‌های بیشتر و یک مختص اضافی نیاز دارد. همچنین یک مختص اضافی هم دارد. در نهایت، دستگاه مختصات جدیدی معرفی نموده والگوریتم‌هایی را بیان می‌کنیم که نشان می‌دهد عمل دوبرابرکردن گروه به طور قابل مقایسه‌ای ساده‌است و نیازی به معکوس ندارد. در این رساله، مقایسه‌ای میان دستگاه‌ها را نیز ارائه خواهیم کرد.

واژه‌های کلیدی: رمزنگاری کلید عمومی، لگاریتم گسسته، خم‌های فوق بیضوی، محاسبات سریع، فرمول‌های دقیق.

پیشگفتار

در سال‌های گذشته، دستگاه‌های رمزنگاری برپایهٔ خم‌های بیضوی بسیار مورد توجه قرار گرفته‌اند، و درحال حاضر قابل استفاده در کاربردهای روزانه می‌باشند، در کارت‌های هوشمند و موبایل به کار رفته‌اند. خم‌های فوق بیضوی توسیعی از خم‌های بیضوی هستند وبطور مشابه می‌توان در دستگاه‌های بالا از آنها استفاده کرد. اخیراً توجه زیادی به استفادهٔ عملی از رمزنگاری فوق بیضوی شده که می‌تواند جایگزینی برای خم‌های بیضوی باشد. رمزنگاری خم‌های فوق بیضوی تمام مزیت های رمزنگاری خم‌های بیضوی را دارد.

یکی از مسائل اساسی در رابطه با استفاده از خم‌های فوق بیضوی، تعداد اعمال مورد نیاز برای انجام عمل گروه خم‌های فوق بیضوی است.

در این رساله، برای دستیابی به سرعت مشابه یا حتی سرعتی بالاتراز خم‌های بیضوی، محاسبات موثر خم‌های فوق بیضوی را مورد بررسی قرار می‌دهیم. تا کنون محاسبات مربوط به عمل گروه خم فوق بیضوی با استفاده از الگوریتم کانتور [1] انجام می‌شد(کانتور برای مشخصه‌های فرد در[2]، کابلیتز[2] برای مشخصه های زوج در[6]). برای یک خم از گونهٔ ثابت، می‌توان مراحل الگوریتم را دقیقاً بیان کرده و با بهینه سازی این مراحل فرمول‌های سریعتری برای جمع و دو برابر کردن بدست آورد. این رساله محتوای مقالات [10]،[11] و [12] رادر بردارد.

در این رساله، فرمول‌های دقیقی برای انجام عمل گروه خم فوق بیضوی از گونهٔ ۲ را بیان کرده و

[1] Cantor

[2] Koblitz

مقایسه‌ای نظری انجام خواهیم داد. در مقالات [1] و [13] مقایسه‌ها به صورت عملی انجام شده‌است، اولین نتایج عملی در مقاله[10] آمده‌است. مطالعه روی خم‌های فوق بیضوی از گونه های بالاتر، از لحاظ کاربردی بسیار ارزنده‌است، چون باعث افزایش سرعت محاسبه مضرب اسکالر می‌شود. در مقالات [3]،[4]،[8] و [15] فرمول‌های دقیقی برای خم‌های فوق بیضوی از گونهٔ ۳ ارائه شده‌است.

یک جمع در دستگاه مختصات آفین به ۲۲ ضرب، ۳ مجذور، و ۱ معکوس نیاز دارد، درحالی که دو برابر کردن، ۲ مجذور بیشتر از جمع لازم دارد.

وضیعت برای خم‌های بیضوی

فرض کنید F_q یک میدان متناهی باشد که در آن $q = p^r$ و p عدد اول است. و $\bar{F}_q$ بستار جبری F_q می‌باشد.

نقاط آفین خم‌های بیضوی، زوج مرتب‌های $(x, y) \in \bar{F}_q^{\,2}$ هستند، که در معادلهٔ

$$C : Y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad a_i \in F_q$$

صدق می‌کند.

هر نقطه (X, Y, Z) که از معادله‌ٔهمگن سازی شدهٔ خم بیضوی بدست می‌آید و متناظر با یک نقطه آفین $(x, y) = (X/Z, Y/Z)$ است، نقطه تصویری نامیده می‌شود. دردستگاه مختصات تصویری، فرمول‌های جمع نقاط دارای عمل معکوس نمی‌باشند.

ایدهٔ بدست آوردن فرمول‌های سریعتر از مختصات تصویری و بدون نیاز به معکوس‌ها، یکی از دلایل ایجاد مختصات تصویری وزن دار می‌باشد. در ساختار خم بیضوی، نقطه (X, Y, Z) که متناظر با $(x, y) = (X/Z^2, Y/Z^3)$ مختصات ژاکوبینی [۳] نامیده می‌شود، در این دستگاه نسبت به دستگاه مختصات تصویری، عمل جمع کمی سخت تر، ولی دو برابر کردن آسان تر است.

در صورتی که فضای نرم افزاری و سخت افزاری محدود نباشد، می‌توان بعضی از محاسباتی را که در روند جمع و دو برابر کردن استفاده می‌شود، را به عنوان مختصات جدید به مختصات قبلی اضافه کرد در این صورت به مختصات (X, Y, Z, Z^2, Z^3) می‌رسیم که مختصات ژاکوبینی چاد نووسکی [۴] نامیده

[۳] Jacobian

[۴] Chudnovsky's Jacobian

می‌شود، عمل جمع و دو برابر کردن دراین دستگاه نسبت به دستگاه مختصات تصویری سریعتر است، ولی در مقایسه با دستگاه مختصات ژاکوبینی معمولی، عمل جمع سریعتر و دو برابر کردن کمی آهسته‌تر است.

به منظور افزایش سرعت دوبرابر کردن، از مختصات اصلاحی کوهن،[۵] یعنی؛ $(X, Y, Z, aZ^۴)$ برای خم‌های بیضوی به شکل $y^۲ = x^۳ + ax + b$ استفاده می‌شود.

وضعیت برای خم‌های فوق بیضوی گونهٔ ۲

در این رساله، سعی می‌کنیم روش های مورد استفاده در خم‌های بیضوی را به خم های فوق بیضوی توسیع دهیم.

اولین بار اسپالک [۶] [16] و کریگر[۷] [7] فرمول‌های دقیق برای خم‌های فوق بیضوی از گونهٔ ۲ مورد مطالعه قرار دادند. هارلی [۸] [5] اولین فرمول‌های دقیق قابل استفاده را برای مشخصه‌های فرد بدست آورد. سپس لنق [۹] [9] آنها را به مشخصه‌های زوج توسیع داد. تاکاهاشی [۱۰] [3] ومیاموتو، دوی، ماتسو، چائو، تیسوچی [۱۱] [14] مستقلاً یک نوع بهینه سازی برای الگوریتم هارلی انجام دادند که برای مشخصه‌های زوج در مقاله [10] توسیع داده شده است.

در همهٔ فرمول‌های ارائه شده حداقل یک معکوس در عمل جمع و دو برابر کردن وجود دارد. در بعضی از محیط‌ها، معکوس‌ها به زمان و فضای زیادی نیاز دارند، که از آن جمله می‌توان به کارت‌های هوشمند اشاره کرد که ضرب‌ها روی آن‌ها بسیار مناسب است، در حالی که تقسیم روی آن‌ها بسیار کند صورت می‌گیرد.

میاموتو، دوی، ماتسو، چائو، تیسوچی [14] تا کنون فقط یک مقاله در زمینه‌ای غیر ازدستگاه مختصات آفین، برای محاسبات مربوط به خم‌های فوق بیضوی از گونهٔ ۲ ارائه کرده‌اند، مقاله [11] با استفاده از

---

[۵] Cohen's modified

[۶] Spallek

[۷] Krieger

[۸] Harley

[۹] lange

[۱۰] Takahashi

[۱۱] Miyamoto,Doi,Matsuo,Chao,Tsujii

روش مشابه، علاوه بر زمان کمتر، میدان‌های متناهی از مشخصهٔ زوج را هم شامل می‌شود.
از جمله کارهای مهم که در زمینهٔ رمزنگاری خم فوق بیضوی انجام شده، کار کیم نگویان [۱۲] در مورد برنامه پیاده شده با استفاده از فرمول‌های تصویری لنق [۱۳] می‌باشد.
این اولین کاربرد از مختصات تصویری معکوس آزاد در یک دستگاه است که نشان می‌دهد خم‌های فوق بیضوی قابل رقابت با خم‌های بیضوی می‌باشند. در ادامه مختصات دیگری را معرفی خواهیم کرد که مختصات جدید نامیده می‌شود، ودرآن مشابه مختصات تصویری، عمل گروه نیاز به معکوس نداشته، و دو برابر کردن‌ها سریعتر هستند.
در مختصات جدید، مشخصه‌های زوج وفرد را بطور جداگانه در نظر می‌گیریم چون به روش‌های بهینه سازی متفاوتی نیاز دارند. محاسبات انجام شده در دستگاه‌های مختلف وهمچنین دستگاه مختصات ترکیبی (مجموعه های مختلفی از مختصات را برای جمع و دو برابر کردن به کار می‌برد.) را با هم مقایسه می‌کنیم.
انتخاب دستگاه مختصات مناسب برای استفادهٔ عملی به ارزش معکوس‌ها نسبت به ضرب‌ها و تعداد پیش محاسبات کاهش یافته بستگی دارد.
این رساله شامل پنج فصل است:
در فصل اول، برخی از تعاریف مقدماتی مربوط به خم های فوق بیضوی والگوریتم کانتور و هارلی بیان شده‌اند. همچنین قضیه نمایش مامفورد [۱۴] آورده شده است، که از قضیه های مهم در مورد خم های فوق بیضوی است.
موضوع فصل دوم، عمل گروه ژاکوبین خم های فوق بیضوی در موارد خاص است، همچنین در این فصل روش های بهینه سازی فرمول های دقیق شرح داده شده است.
فصل سوم، شامل فر مول‌های دقیق برای انجام عمل گروه ژاکوبین در دستگاه مختصات آفین است، در ادامه هر فرمول، تعداد مجذورها، معکوس‌ها و ضرب‌های مورد نیاز برای انجام عمل جمع و دو برابر کردن بیان شده‌است.

---

[۱۲] Kim Nguyen
[۱۳] FameXE
[۱۴] Mumford Representation

در فصل چهارم، ابتدا به معرفی دستگاه‌های مختصات معکوس آزاد، پر داخته شده است، وسپس فر مول های دقیق و تعداد اعمال مورد نیاز برای انجام عمل گروه ژاکوبین در این دستگاه‌ها ارائه شده‌اند. در ابتدای فصل پنجم، مقایسه‌ای نظری بین نتایج بدست آمده در دستگاه‌های مختلف مختصات انجام شده‌است و در ادامه، نحوه محاسبه مضرب اسکالر kD، در میدا ن‌های متناهی از مشخصه فرد بیان شده‌است.

فصل ۱

مقدمه

دراین فصل، برخی تعاریف مقدماتی مربوط به خم‌های فوق بیضوی و سایر مفاهیم مرتبط با آن را مطرح می‌کنیم که در فصل‌های بعدی به کار می‌روند.

۱.۱ مفاهیم مقدماتی

تعریف ۱.۱.۱ فرض کنید F_q یک میدان متناهی از مشخصهٔ p باشد، که در آن p یک عدداول و $q = p^r$، و فرض کنید $\bar{F}_q$ بستارجبری F_q باشد.
معادله دو متغیری

$$C : y^2 + h(x)y = f(x)$$

روی $F_q[x, y]$ را در نظر بگیرید که در آن $f, h \in F_q[x]$ و f یک چند جمله‌ای تکین از درجهٔ $2g + 1$ $(g \geq 1)$، و h یک چند جمله‌ای از درجهٔ حداکثر g است، و علاوه بر این هیچ جوابی مانند $(a, b) \in \bar{F}_q^2$ وجود ندارد که همزمان در معادلهٔ C ومعادلات مشتقات جزئی آن یعنی، $2y + h(x) = 0$ و $h'(x)y - f'(x) = 0$ صدق کند. خم C/F_q که روی F_q تعریف شده‌است، خم فوق بیضوی از گونهٔ

g نامیده می‌شود. خم‌های فوق بیضوی توسیعی از خم‌های بیضوی هستند، خم‌های فوق بیضوی از گونهٔ۱، خم‌های بیضوی نامیده می‌شود.

تعریف ۲.۱.۱ مجموعهٔ

$$C(\bar{F}_q) = \{(a,b)|a,b \in \bar{F}_q, b^2 + h(a)b = f(a)\} \bigcup \{\infty\}$$

نقاط $\bar{F}_q$ ـگویاهای C را نشان می‌دهد، نقطهٔ ∞ را نقطه در بینهایت می‌نامیم، که متناظر با نقطه در بینهایت صفحهٔ تصویری است و در معادلهٔ همگن سازی شده صدق می‌کند.

نگاشت مقابل ساز خم فوق بیضوی، نقطهٔ $p = (a,b)$ را به نقطهٔ $\tilde{p} = (a, -b - h(a))$ تصویر می‌کند و نقطهٔ ∞ را ثابت نگه می‌دارد. $\tilde{p}$ را نقطهٔ مقابل p می‌نامیم. هر گاه $p = \tilde{p}$ ، p نقطهٔ خاص نامیده می‌شود.

مثال ۱.۱.۱ خم

$$C : y^2 + xy = x^5 + 5x^4 + 6x^2 + x + 3$$

روی میدان متناهی F_7، یک خم فوق بیضوی از گونهٔ ۲ می‌باشد، که $h(x) = x$ ، $f(x) = x^5 + 5x^4 + 6x^2 + x + 3$ و داریم :

$$C(\bar{F}_7) = \{\infty, (1,1), (1,5), (2,2), (2,3), (5,3), (5,6), (6,4)\}$$

واضح است که $(6,4)$ یک نقطهٔ خاص خم فوق بیضوی C می‌باشد.

۲.۱ شمارنده‌ها

در این بخش به معرفی شمارنده‌ها وخواص آن‌ها می‌پردازیم سپس ژاکوبین خم فوق بیضوی را معرفی می‌کنیم.

تعریف ۱.۲.۱ شمارندهٔ D، یک فرمول جمعی از نقاط $C(\bar{F}_q)$ به شکل

$$D = \sum_{p \in C(\bar{F}_q)} n_p p$$

است، که در آن $n_p \in \mathbb{Z}$ وتقریباً برای همهٔ نقاط p، $n_p = 0$.

درجهٔ شمارندهٔ D که با نماد $deg(D)$ نشان داده می‌شود، عبارت است از عدد صحیح $deg(D) = \sum_{p \in C(\bar{F}_q)} n_p$.

۱) شمارندهٔ D روی F_q تعریف شده است هر گاه برای هر $\sigma \in Gal(\bar{F}_q/F_q)$، $\sigma(D) = D$.

۲) مجموعهٔ همهٔ شمارنده‌ها که با نماد $\mathbb{D}$ نشان داده می‌شود، با عمل جمع

$$\sum_{p \in C(\bar{F}_q)} n_p p + \sum_{p \in C(\bar{F}_q)} m_p p = \sum_{p \in C(\bar{F}_q)} (m_p + n_p) p$$

تشکیل گروه جمعی می‌دهند.

۳) مجموعهٔهمهٔ شمارنده‌ها از در جهٔ صفر را که با $\mathbb{D}^0$ نشان می‌دهیم، زیر گروهی از $\mathbb{D}$ می‌باشد.

تعریف ۲.۲.۱ برای شمارندهٔ $D = \sum_{p \in C(\bar{F}_q)} n_p p$، تکیه گاه D که با نماد $supp(D)$ نشان داده می‌شود، به صورت زیر تعریف می‌شود:

$$supp(D) = \{p \in C(\bar{F}_q) | n_p \neq 0\}$$

تعریف ۳.۲.۱ حلقه مختصاتی $F_q[C]$، از C روی F_q، یک حلقه خارج قسمتی به شکل

$$F_q[C] = F_q[x, y]/(y^2 + h(x)y - f(x))$$

می‌باشد، که در آن $(y^2 + h(x)y - f(x))$ یک ایده‌آل در $F_q[x, y]$ است.

تعریف ۴.۲.۱ میدان توابع $F_q(C)/F_q$، میدان کسرهای $F_q[C]$ است.

تعریف ۵.۲.۱ برای عضو دلخواه F از میدان توابع $\bar{F}_q(C)/\bar{F}_q$، می‌توان شمارندهٔ F را که با نماد $div(F)$ نشان می‌دهیم، بوسیلهٔ ارزیابی آن در تمام نقاط خم C بدست آورد؛ یعنی $div(F) = \sum_{p\in C(\bar{F}_q)} \nu_p(F)p$ که در آن ν_p، عبارت است از مرتبه صفر تابع F در نقطهٔ p اگر $F(p) = 0$، و یا مرتبه قطب تابع F در نقطهٔ p اگر $F(p) = \infty$. این شمارنده‌ها از درجه صفر هستند و شمارنده‌های اصلی نا میده می شوند، که آن‌ها را با $\mathbb{P}$ نشان می‌دهیم. شمارنده‌های اصلی $\mathbb{P}$ زیر گروهی از شمارنده‌های در جهٔ صفر، یعنی $\mathbb{D}^0$ هستند.

تعریف ۶.۲.۱ گروه خارج قسمتی $J_c(F_q) = \mathbb{D}^0/\mathbb{P}$ را ژاکوبین خم فوق بیضوی C می‌نامیم.

قدم بعدی این است که چگونه عضو های ژاکوبین را به ساده ترین شکل ممکن نمایش دهیم، برای این منظور توجه می‌کنیم که برای تابع $F_a = (x-a)$، خواهیم داشت $div(F_a) = p_a + \tilde{p}_a - 2\infty$ که در آن $p_a = (a,b) \in C(\bar{F}_q)$. بنابراین نمایندهٔ یک رده از شمارنده‌ها را می‌توان با شمارندهٔ

$$D = \sum_{i=1}^{r} p_i - r\infty$$

نمایش داد، که درآن $r \geq 0$، $p_i \neq \infty$ و برای هر $i \neq j$، $p_i \neq \tilde{p}_j$.

تعریف ۷.۲.۱ شمارندهٔ D با شرایط ذکر شده در بالا، یک شمارندهٔ نیمه تحویل یافته نامیده می‌شود. هر گاه $r \leq g$، شمارندهٔ D، یک شمارندهٔ تحویل یافته نامیده می‌شود.

تبصره: مسئله لگاریتم گسسته برای گروه‌های جمعی دلخواه به صورت زیر بیان می‌شود:
برای یک عضو داده شده D از گروه، و عضو F از گروه دوری تولید شده به وسیله D، عدد صحیح k را طوری پیدا کنید که $F = kD$.

ایده‌آل های ماکزیمال $\bar{F}_q(C) = \bar{F}_q[x,y]/(y^۲ + h(x)y - f(x))$ دارای یک پایه شامل دو چند جمله‌ای هستند که چند جمله‌ای اول در $\bar{F}_q[x]$ قرار دارد و دومی به شکل $y - \nu(x)$، که $\nu(x) \in \bar{F}_q[x]$، چون ما به پیمانهٔ یک چند جمله‌ای درجه ۲ بر حسب y کاهش می‌دهیم.
چون خم فقط یک نقطه در بینهایت دارد، ثابت می‌شود که گروه ردهٔ ایده‌آل‌ها (ایده‌آل‌هابه پیمانهٔ ایده‌آل‌های اصلی)، و گروه ردهٔ شمارنده‌ها با هم ایزومورف هستند.
یکی از قضیه های بسیار مهم در زمینهٔ خم‌های فوق بیضوی، قضیه نمایش مامفورد است. که از لحاظ کاربردی بسیار حائز اهمیت می باشد. ویکی از پایه‌های اساسی الگوریتم‌هایی است که بعداً به بیان آن خواهیم پرداخت.

قضیه ۱.۲.۱ (نمایش مامفورد): میدان توابع مربوط به چند جمله‌ای تحویل ناپذیر $y^۲ + h(x)y - f(x)$، که $h, f \in F_q[x]$، $degf = ۲g + ۱$، $degh \leq g$ را در نظر بگیرید. هر ردهٔ ایده‌آل غیر بدیهی بوسیلهٔ ایده‌آل منحصر به فرد $[u(x), y - \nu(x)]$ نمایش داده می‌شود، که $u, \nu \in F_q[x]$، در شرایط زیر صدق می‌کنند:

۱) u یک چند جمله‌ای تکین است.

۲) $deg(\nu) < deg(u) \leq g$

۳) $u | \nu^۲ + \nu h - f$

فرض کنید $D = \sum_{i=۱}^{r} p_i - r\infty$، که در آن $p_i = (a_i, b_i)$، $p_i \neq \infty$ وبرای هر $i \neq j$، $p_i \neq \bar{p}_j$ و $r \leq g$. آنگاه در ردهٔ ایده‌آل متناظر خواهیم داشت، $u = \prod_{i=۱}^{r}(x - a_i)$، و اگر p_i، n_i بار ظاهر شود، آنگاه برای $x = a_i$، داریم:

$$(d/dx)^j[\nu(x)^۲ + \nu(x)h(x) - f(x)]_{x=a_i} = ۰ \qquad ,o \leq j \leq n_i - ۱$$