



۱۵۳۱۹۹ - ۲۰۲۱۵۲۳

دانشگاه یزد
دانشکده مهندسی برق و کامپیوتر
گروه مهندسی کامپیوتر

پایان نامه
برای دریافت درجه کارشناسی ارشد
مهندسی فناوری اطلاعات - شبکه‌های کامپیوتری

**بررسی و بهبود الگوریتم‌های رمزنگاری کلید عمومی
مبتنی بر حلقه‌های چند جمله‌ای کوتاه شده**

استاد راهنما:

دکتر فضل‌ا... ادیب‌نیا

اساتید مشاور:

دکتر کیارش میزانیان

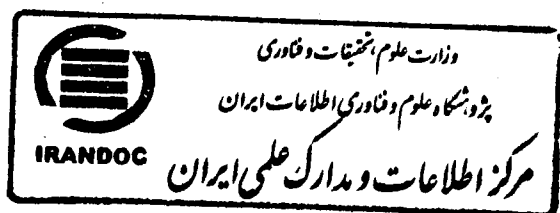
دکتر احمد خادم زاده

پژوهش و نگارش:

نوید باباخانی

۱۳۸۹/۱۲/۱۵

شهریور ماه ۱۳۸۹



۱۵۳۱۹۹



مدیریت تحصیلات تکمیلی

صور تجلسه دفاعیه پایان نامه دانشجوی
دوره کارشناسی ارشد

شناسه: ب/اک/۳۱

کوبیده بابا خانی

دانشجوی کارشناسی ارشد

جلسه دفاعیه پایان نامه تحصیلی آقای کوبیده بابا خانی:

رشته/گرایش: موسیقی مآ و دما (طلسمات سحرزنی) کامپوزیتی

تحت عنوان: "پژوهش و بسط الگوریتم سحرزنی در مآ و دما طلسمات سحرزنی بر حلقه حنیف علما گران مآ"

و تعداد واحد: ۶ در تاریخ ۱۳۸۹/۶/۱۳ با حضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان نامه با نمره: به عدد ۱۸/۷۵ به حروف هجری در صورت

و درجه عالی مورد تصویب قرار گرفت.

عنوان

نام و نام خانوادگی

امضاء

استاد/ استادان راهنما:

دکتر مصطفی الم

ادیب نیا

استاد/ استادان مشاور:

دکتر کیارسی

میرزایی

متخصص و صاحب نظر داخلی:

دکتر مهدی کام

میرام

متخصص و صاحب نظر خارجی:

دکتر فرید

ملکان

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام و نام خانوادگی:

محمد حسن محمد زری

امضاء:

چکیده

ابداع روش‌های رمزنگاری کلید عمومی فصلی جدید را در دانش رمزنگاری گشود و نیازهای اساسی صنعت نوپای کامپیوتر را به زیبایی پاسخ داد. اما متأسفانه بسیاری از سیستم‌های رمزنگاری کلید عمومی در عمل به جهت پیچیدگی‌های محاسباتی و حافظه‌ای، بسیار پر هزینه هستند. در نتیجه محققان بر آن شدند تا سیستم‌های رمز کلید عمومی سریع‌تر و کم‌هزینه‌تری را ابداع نمایند. سیستم رمزنگاری NTRU روشی به نسبت جدید است که به عنوان یک سیستم بسیار سریع معرفی شده و در سال‌های اخیر توجه شایانی به آن شده است. این سیستم نسبت به سایر روش‌های کلید عمومی مرسوم، پیچیدگی محاسباتی کمتری دارد و روال تولید کلید عمومی و خصوصی در آن بسیار ساده است.

سیستم رمز NTRU در حلقه‌ی چندجمله‌ای‌های کوتاه‌شده کار می‌کند و اصلی‌ترین عملیات آن ضرب چندجمله‌ای‌ها بصورت پیمانه‌ای است. برای سرعت بخشیدن به ضرب چندجمله‌ای‌ها روشی به نام ضرب با FFT وجود دارد، اما مشکل آن استفاده از مرتبه‌ی مرکب است که این امر نقص امنیتی بزرگی در آن ایجاد می‌کند.

در این پژوهش، پس از معرفی سیستم NTRU و انجام تحلیل‌های امنیتی روی آن و ذکر پژوهش‌های مشابه دیگر، با توجه به خصوصیت پیمانه‌ای بودن ضرب چندجمله‌ای‌ها در NTRU و با استفاده از روش FFT، روشی به نام ضرب UFFT ارائه داده شده است که کارایی خیلی بهتری نسبت به ضرب معمولی و ضرب FFT دارد. همچنین UFFT راه‌حلی در جهت رفع مشکل استفاده از مرتبه‌ی مرکب برای چندجمله‌ای‌ها معرفی می‌کند.

کلمات کلیدی: رمزنگاری کلید عمومی، حلقه‌ی چندجمله‌ای کوتاه‌شده، ضرب پیچشی، تبدیل فوریه‌ی سریع، مشبکه.

فهرست مطالب

صفحه	عنوان	
۱	مقدمه	۱
۵	سیستم‌های رمزنگاری مبتنی بر شبکه‌ها	۲
۶	۱-۲ تعاریف و مقدمات جبر خطی	
۹	۲-۲ شبکه‌ها، تعاریف و مشخصات اصلی	
۱۲	۳-۲ بردارهای کوتاه در شبکه‌ها	
۱۲	۱-۳-۲ مسئله‌ی کوتاه‌ترین و نزدیک‌ترین بردار	
۱۴	۴-۲ سیستم‌های رمزنگاری مبتنی بر مسائل دشوار شبکه‌ها	
۱۷	۵-۲ سیستم رمزنگاری کلید عمومی GGH	
۱۸	۶-۲ حلقه‌های چندجمله‌ای کوتاه‌شده	
۲۱	۷-۲ سیستم رمزنگاری کلید عمومی NTRU	
۲۱	۱-۷-۲ سیستم رمزنگار NTRU	
۲۶	۲-۷-۲ مسائل ریاضی بنیادی NTRU	
۲۷	۸-۲ NTRU به منزله‌ی یک سیستم رمزنگار شبکه‌ای	
۲۸	۱-۸-۲ شبکه‌ی NTRU	
۳۰	۲-۸-۲ ارزیابی امنیت شبکه‌ی NTRU	
۳۱	مروری بر پژوهش‌های مشابه	۳
۳۲	۱-۳ سیستم رمزنگاری CTRU	
۳۲	۱-۱-۳ نمادها	
۳۳	۲-۱-۳ تولید کلید	
۳۳	۳-۱-۳ رمزنگاری و رمزگشایی	
۳۴	۴-۱-۳ تحلیل امنیت CTRU توسط ابداع‌کنندگان آن	

۲۵.....	سیستم رمزنگاری MaTRU	۲-۳
۳۵.....	نمادها	۱-۲-۳
۳۶.....	تولید کلید	۲-۲-۳
۳۷.....	رمزنگاری و رمزگشایی	۳-۲-۳
۳۸.....	تحلیل امنیت MaTRU	۴-۲-۳
۳۸.....	پیاده سازی سخت افزاری NTRU	۳-۳
۳۹.....	ضرب کننده سخت افزاری و مقیاس پذیر NTRU	۱-۳-۳
۴۱.....	عملیات پشتیبانی شده توسط ضرب کننده سخت افزاری و محدودیت های آن	۲-۳-۳
۴۲.....	شکسته شدن CTRU و معرفی NTRU با اعداد گاوسی	۴-۳
۴۲.....	تحلیل امنیت CTRU و اثبات ناامنی آن	۱-۴-۳
۴۴.....	تحلیل امنیتی NTRU به همراه نتایج محاسباتی	۵-۳
۴۵.....	نتایج محاسباتی زمان بازیابی کلید خصوصی NTRU	۱-۵-۳
۴۷.....	مقایسه NTRU با دیگر سیستم های کلید عمومی	۶-۳
۴۸.....	مقایسه طول کلید	۱-۶-۳
۴۹.....	مقایسه کارایی تولید کلید، رمزنگاری و رمزگشایی	۲-۶-۳
۵۱.....	بهبود سیستم رمزنگاری NTRU	۴
۵۲.....	روش های نمایش چند جمله ای ها	۱-۴
۵۲.....	روش نمایش با ضرایب	۱-۱-۴
۵۳.....	روش نمایش نقطه - مقدار	۲-۱-۴
۵۴.....	ضرب سریع چند جمله ای ها با فرم نمایش با ضرایب با استفاده از FFT	۲-۴
۵۶.....	ریشه های مختلط عدد یک	۱-۲-۴
۵۸.....	تبدیل فوریه ی گسسته	۲-۲-۴
۵۹.....	الگوریتم تبدیل فوریه ی سریع	۳-۲-۴
۶۲.....	معکوس تبدیل فوریه ی گسسته	۴-۲-۴

۶۴	۳-۴ اثبات درستی بکارگیری روش پیشنهادی UFFT در ضرب پیچشی NTRU
۶۶	۴-۴ بررسی امنیتی استفاده از FFT یا UFFT
۶۸	۵-۴ نتایج پیاده‌سازی
۷۵	۵ نتیجه‌گیری و پیشنهادات
۷۶	۱-۵ جمع‌بندی مطالب
۷۸	۲-۵ پیشنهادات
۷۸	۱-۲-۵ محاسبه‌ی احتمال رمزگشایی‌های ناموفق
۷۸	۲-۲-۵ مطالعه و بهبود الگوریتم‌های کاهش شبکه
۷۹	۳-۲-۵ پیاده‌سازی سخت افزاری UFFT
۸۱	ضمائم
۸۱	ضمیمه الف. الگوریتم Babai و استفاده از پایه "خوب" برای حل apprCVP
۸۳	ضمیمه ب. الگوریتم‌های کاهش شبکه
۹۵	واژه‌نامه‌ی فارسی به انگلیسی
۹۹	واژه‌نامه‌ی انگلیسی به فارسی
۱۰۳	منابع

فهرست شکل‌ها

صفحه

عنوان

- شکل ۱-۲ مشبکه‌ی L و ناحیه بنیادی \mathcal{F} ۱۰
- شکل ۲-۲ انتقال‌های \mathcal{F} توسط بردارهای L که \mathbb{R}^n را بطور کامل می‌پوشاند ۱۱
- شکل ۱-۳ ضرب پیچشی دو چندجمله‌ای ۴۰
- شکل ۲-۳ لگاریتم مبنای ۱۰ زمان‌های شکست به ازای $N = 100 \dots 115$ و خط رگرسیون ۴۷
- شکل ۱-۴ نمایی گرافیکی از الگوی ضرب سریع چندجمله‌ای‌ها با استفاده از FFT ۵۵
- شکل ۲-۴ ریشه‌های هشتم مختلط عدد یک ۵۶
- شکل ۳-۴ ضرب پیچشی چندجمله‌ای‌های NTRU با $N = 251$ ۷۰
- شکل ۴-۴ ضرب پیچشی چندجمله‌ای‌های NTRU با $N = 347$ ۷۱
- شکل ۵-۴ ضرب پیچشی چندجمله‌ای‌های NTRU با $N = 503$ ۷۱
- شکل ۶-۴ ضرب پیچشی چندجمله‌ای‌های NTRU با $N = 839$ ۷۲
- شکل ۷-۴ رشد زمان اجرای هر سه روش با افزایش N به ازای ۵۰۰۰ چندجمله‌ای ۷۳
- شکل الف-۱ بکارگیری ناحیه‌ی بنیادی داده شده برای حل CVP ۸۲
- شکل الف-۲ دو پایه‌ی متفاوت برای یک مشبکه ۸۲
- شکل الف-۳ اگر پایه بد باشد الگوریتم Babai بخوبی کار نمی‌کند ۸۳
- شکل ب-۱ v_2^* ، تصویر v_2 بر راستای عمود بر v_1 ۸۴

فهرست جداول

صفحه

عنوان

جدول ۱-۳	تعداد بلوک‌های لازم برای آشکارسازی کلید و زمان صرف شده پنج نمونه به ازای هر اندازه.....	۴۶
جدول ۲-۳	مجموعه پارامترهای NTRU.....	۴۸
جدول ۳-۳	اندازه کلید عمومی در RSA, ECC و NTRU.....	۴۸
جدول ۴-۳	مقایسه‌ی کارایی NTRU و RSA.....	۴۹
جدول ۵-۳	مقایسه‌ی کارایی NTRU و ECC.....	۵۰
جدول ۱-۴	پارامترهای بکار رفته در ارزیابی ضرب چندجمله‌ای‌های NTRU.....	۶۹
جدول ۲-۴	زمان‌های حاصل از ضرب چندجمله‌ای‌ها با سه روش پیاده‌سازی شده.....	۶۹

فهرست علائم اختصاری

Approximate Closest Vector Problem	apprCVP
Approximate Shortest Vector Problem	apprSVP
Block Korkin Zolotarev- Lenstra Lenstra Lovasz	BKZ-LLL
Closest Vector Problem	CVP
Discrete Fourier Transform	DFT
Elliptic Curve Cryptography	ECC
Fast Fourier Transform	FFT
Goldreich Goldwasser Halevi	GGH
Lenstra Lenstra Lovasz	LLL
Nth TRUncated polynomial ring	NTRU
Radio Frequency Identifier	RFID
Rivest, Shamir, Adelman	RSA
Secure Electronic Transaction	SET
Shortest Vector Problem	SVP
Unextended Fast Fourier Transform	UFFT

فصل اول

مقدمه

در سال ۱۹۷۶ با معرفی مفهوم روش‌های رمزنگاری کلید عمومی توسط دیفی و هلمن [10]، فصلی جدید در دانش رمزنگاری گشوده شد و نیازهای اساسی صنعت نو پای کامپیوتر به زیبایی و سادگی پاسخ داده شد. بر پایه‌ی وجود سیستم‌های رمز کلید عمومی بود که مفاهیم و عملیات پایه‌ای دیگری همچون "توزیع کلید"، "امضای دیجیتال"، "گواهی دیجیتال"، "احراز هویت" و به دنبال آن "پروتکل‌های امنیتی" در شبکه‌های کامپیوتری شکل گرفتند و هر نوع ارتباط و کاربرد امن و مطمئنی مانند "تجارت الکترونیک" و "دولت الکترونیک" فراهم شد. استانداردهای عظیمی مانند SET^۱، با توجه به معماری وسیع آن، بدون وجود رمزنگاری کلید عمومی بی‌ارزش و بدون کارایی خواهد بود.

ایده‌ی بنیادی سیستم‌های رمز کلید عمومی وجود "توابع یک‌طرفه"^۲ است. در همین راستا، سیستم‌های بسیاری ابداع شدند که مشهورترین آن‌ها RSA [44]، مبتنی بر مشکل تجزیه‌ی اعداد صحیح^۳ است. همچنین سیستم McEliece [33] مبتنی بر نظریه‌ی کدینگ جبری^۴، سیستم ECC [28] مبتنی بر مسئله‌ی رام نشدنی لگاریتم گسسته‌ی خم‌های بیضوی^۵، گونه‌های مختلفی از سیستم رمزنگاری Matsumoto-Imai [32, 11] مبتنی بر سیستم‌هایی از چندجمله‌ای‌های چند متغیره^۶ و سیستم رمزنگار ElGamal [13] مبتنی بر دشواری لگاریتم گسسته، همه نمونه‌هایی از سیستم‌های رمز کلید عمومی هستند.

متأسفانه بسیاری از این روش‌ها در عمل به جهت پیچیدگی‌های محاسباتی و حافظه‌ای، بسیار پر هزینه هستند. همین پیچیدگی‌هاست که مانع از جایگزین شدن الگوریتم‌های متقارن توسط این الگوریتم‌ها می‌شود. بعلاوه دشواری اجرای بعضی از این الگوریتم‌ها (مانند RSA) از اجرا شدن بهینه‌ی آنها در ابزارهای محاسباتی کم‌توان مانند کارت‌های هوشمند ارزان قیمت، تجهیزات

^۱ Secure Electronic Transaction

^۲ Oneway Function. به بیان ساده، یک تابع یک طرفه، تابعیست که در جهت رفت، محاسبه‌ی بسیار ساده‌ای داشته باشد اما در جهت برگشت (معکوس) بسیار دشوار و در عمل ناممکن باشد.

^۳ Integer Factoring Problem

^۴ Algebraic Coding Theory

^۵ Elliptic Curve Discrete Logarithm

^۶ Multivariable Polynomials

RFID و تلفن‌های همراه جلوگیری می‌کند [5]. در نتیجه محققان بر آن شدند تا سیستم‌های رمزنگار کلید عمومی سریع و جدیدتری را بیابند، علی‌الخصوص سیستم‌هایی که مبتنی بر رده‌ی دیگری از مسائل دشوار ریاضی باشند [23].

در سال ۱۹۹۶، سیستم رمزنگار کلید عمومی NTRU در نشست‌ی در 96 Crypto ارائه شد [22] و اولین مقاله‌ی رسمی آن در سال ۱۹۹۸ در CHES' 98 منتشر گردید [23]. NTRU روشی به نسبت جدید است و به عنوان یک سیستم خیلی سریع معرفی شده که در سال‌های اخیر توجه شایانی به آن شده است. یک مزیت آن در مقایسه با RSA، این است که NTRU به $O(N^2)$ عملیات و طول کلید $O(N)$ نیاز دارد، در حالی که عملیات RSA با $O(N^3)$ انجام شده و طول کلیدی برابر با $O(N^2)$ دارد [5, 23, 34]. علاوه بر آن تولید کلید عمومی و خصوصی در NTRU بسیار ساده‌تر از RSA است و به همین دلیل می‌توان کلیدها را در بازه‌های زمانی کوتاه‌تری استفاده کرد، که این امر امنیت را ارتقا می‌دهد. البته در مقابل این مزایا، معایبی هم موجودند که یکی از آنها وجود رمزگشایی‌های ناموفق^۱ در این الگوریتم است و هیچ اثبات دقیقی بر درستی آن وجود ندارد.

سیستم رمز NTRU در حلقه‌ی چندجمله‌ای‌های کوتاه‌شده $\mathbb{Z}[x]/(x^N - 1)$ کار می‌کند و مسئله‌ی زیربنایی آن دشواری یافتن بردارهای کوتاه در یک سیستم جبری به نام شبکه است. در این پایان نامه که پایه‌ی اصلی آن سیستم رمزنگار NTRU است، پس از معرفی این روش و تحلیل امنیتی آن، راه‌کاری در جهت افزایش سرعت و کارایی آن الگوریتم بیان شده است. در ادامه ساختار پایان نامه توضیح داده می‌شود.

پس از این فصل، که مقدمه‌ای بر رمزنگاری کلید عمومی و بیان اهمیت و ضرورت آن و نیز بیان مسئله (پیچیدگی الگوریتم‌های کلید عمومی حاضر) و چالش‌های آن می‌باشد، در فصل دوم به بررسی سیستم‌های رمزنگاری مبتنی بر شبکه پرداخته می‌شود. در ابتدای فصل تعاریف و پیش زمینه‌های لازم جبر خطی بیان شده و سپس به تعریف شبکه‌ها و مسائل دشوار موجود در آنها و قضایا و الگوریتم‌های لازم پرداخته می‌شود. در نهایت دو سیستم رمز GGH و NTRU ارائه شده و

^۱ Decryption Failure

در مورد جنبه‌های جبری آنها بحث می‌شود. سپس مسائل بنیادی NTRU توضیح داده شده و شبکه‌ی آن بررسی می‌گردد.

در فصل سوم پژوهش‌های انجام شده در زمینه‌ی تحلیل و بهبود NTRU مورد بررسی قرار می‌گیرند. در این فصل دو سیستم CTRU و MaTRU توضیح داده شده و سایر کارهای انجام شده بطور مختصر ارائه خواهد شد.

در فصل چهارم استفاده از تبدیل فوریه‌ی گسسته^۱ در ضرب پیچشی چندجمله‌ای‌های NTRU بررسی شده و با ارائه‌ی یک روش پیشنهادی به نام UFFT، کارایی و سرعت سیستم رمز NTRU بهبود داده می‌شود. در ادامه، ضرب چندجمله‌ای‌ها با روش معمولی، روش FFT و روش UFFT، پیاده سازی نرم افزاری شده و از نظر کارایی مقایسه می‌شوند و در نهایت راه حلی برای مشکل استفاده از FFT و UFFT در ضرب پیچشی چندجمله‌ای‌ها ارائه خواهد شد.

سر انجام در فصل پنجم، به بیان نتیجه‌گیری و جمع‌بندی مطالب مطرح شده در این پایان‌نامه پرداخته و راه‌کارهایی برای آینده و توسعه‌های آتی ارائه خواهد شد.

فصل دوم

سیستم‌های رمزنگاری مبتنی بر شبکه‌ها

۱-۲ تعاریف و مقدمات جبر خطی

فضای برداری. یک فضای برداری V^1 زیرمجموعه‌ای از \mathbb{R}^m است بطوری که:

$$\alpha_1 v_1 + \alpha_2 v_2 \in V \quad \forall v_1, v_2 \in V, \quad \forall \alpha_1, \alpha_2 \in \mathbb{R} \quad (1-2)$$

بطور معادل، یک فضای برداری زیرمجموعه‌ای از \mathbb{R}^m است که تحت عمل جمع و عمل ضرب اسکالر عناصر \mathbb{R} بسته باشد.

ترکیب خطی. فرض کنید v_1, v_2, \dots, v_k عضو فضای برداری V باشند. یک ترکیب خطی^۲ بردارهای v_1 تا v_k برداری به شکل رابطه‌ی (۲-۲) می‌باشد:

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k, \quad \alpha_1, \dots, \alpha_k \in \mathbb{R} \quad (2-2)$$

به مجموعه‌ی تمام ترکیبات خطی به شکل $\{\alpha_1 v_1 + \dots + \alpha_k v_k : \alpha_1, \dots, \alpha_k \in \mathbb{R}\}$ یک پوشش^۳ برای $\{v_1, \dots, v_k\}$ گفته می‌شود.

استقلال خطی^۴. به مجموعه‌ی بردارهای $v_1, v_2, \dots, v_k \in V$ مستقل (خطی) گفته می‌شود هرگاه تنها جواب معادله $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = 0$ این باشد که $\alpha_1 = \alpha_2 = \dots = \alpha_k = 0$. اگر معادله‌ی فوق حداقل با یک α_i غیرصفر، برقرار شود، مجموعه‌ی v_1, \dots, v_k وابسته (خطی) گفته می‌شود.

پایه^۵. یک پایه برای فضای برداری V ، عبارتست از مجموعه بردارهای مستقل خطی v_1, \dots, v_n که پدیدآورنده‌ای برای V باشد. این تعریف را می‌توان بدین صورت بیان کرد که به ازای هر $w \in V$ ، با انتخاب یکتای $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ ، w را می‌توان بصورت ترکیب خطی (۳-۲) نمایش داد:

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n \quad (3-2)$$

گزاره ۱-۲. فرض کنید $V \subset \mathbb{R}^m$ یک فضای برداری باشد،

Vector Space^۱
Linear Combination^۲
Span^۳
Linear Independence^۴
Basis^۵

الف) همواره یک پایه برای V وجود دارد.

ب) هر دو پایه‌ی دلخواهی از V ، دارای تعداد عناصر یکسانی هستند. به تعداد عناصر موجود در هر پایه‌ی V ، بُعد V گفته می‌شود.

ج) فرض کنید v_1, \dots, v_n پایه‌ای برای V باشد و نیز w_1, \dots, w_n مجموعه‌ای از بردارهای موجود در V باشد. هر بردار w_j را می‌توان بصورت ترکیب خطی از v_i ها نوشت:

$$\begin{aligned} w_1 &= \alpha_{11}v_1 + \alpha_{12}v_2 + \dots + \alpha_{1n}v_n \\ w_2 &= \alpha_{21}v_1 + \alpha_{22}v_2 + \dots + \alpha_{2n}v_n \\ &\vdots \\ w_n &= \alpha_{n1}v_1 + \alpha_{n2}v_2 + \dots + \alpha_{nn}v_n \end{aligned} \quad (4-2)$$

می‌توان گفت مجموعه w_1, w_2, \dots, w_n نیز یک پایه‌ی V است اگر و تنها اگر دترمینان ماتریس

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \quad (5-2)$$

برابر با صفر نباشد.

تعریف. فرض کنید $v, w \in V \subset \mathbb{R}^m$ باشد و آن‌دو با استفاده از نقاطشان مشخص شده باشند:

$$v = (x_1, x_2, \dots, x_m), \quad w = (y_1, y_2, \dots, y_m) \quad (6-2)$$

آنگاه ضرب نقطه‌ای v و w از رابطه‌ی (۶-۲) بدست می‌آید:

$$v \cdot w = x_1y_1 + x_2y_2 + \dots + x_my_m \quad (7-2)$$

بعلاوه، دو بردار v و w متعامد^۲ گفته می‌شوند اگر $v \cdot w = 0$ باشد.

طول، یا نرم اقلیدسی^۴ بردار v با $\|v\|$ نشان داده شده و از رابطه‌ی (۸-۲) بدست می‌آید:

$$\|v\| = \sqrt{x_1^2 + x_2^2 + \dots + x_m^2} \quad (8-2)$$

^۱ Dimension

^۲ dot product

^۳ Orthogonal

^۴ Euclidean Norm

توجه داشته باشید که بین نرم اقلیدسی و ضرب نقطه‌ای رابطه‌ی (۹-۲) برقرار است:

$$v \cdot v = \|v\|^2 \quad (۹-۲)$$

تعریف. یک پایه‌ی متعامد برای فضای برداری V ، پایه‌ی v_1, \dots, v_n است بطوریکه:

$$v_i \cdot v_j = 0 \quad \forall j \neq i \quad (۱۰-۲)$$

فرمول‌های بسیار زیادی وجود دارند که اگر برای پایه‌های متعامد بکار برده شوند، بسیار ساده‌تر می‌گردند. به عنوان مثال فرض کنید v_1, \dots, v_n ، یک پایه‌ی متعامد باشد و v یک ترکیب خطی از بردارهای موجود در پایه باشد (یعنی $v = a_1 v_1 + \dots + a_n v_n$)، چون در یک پایه‌ی متعامد رابطه‌ی (۱۰-۲) حاکم است آنگاه:

$$\begin{aligned} \|v\|^2 &= \|a_1 v_1 + \dots + a_n v_n\|^2 \\ &= (a_1 v_1 + \dots + a_n v_n) \cdot (a_1 v_1 + \dots + a_n v_n) \\ &= \sum_{i=1}^n \sum_{j=1}^n a_i a_j (v_i \cdot v_j) \\ &= \sum_{i=1}^n a_i^2 \|v_i\|^2 \end{aligned} \quad (۱۱-۲)$$

در اینجا گونه‌ای از الگوریتم Gram-Schmidt معرفی می‌شود که پایه‌ی متعامدی ایجاد می‌کند.

قضیه ۲-۲. (الگوریتم Gram-Schmidt) فرض کنید v_1, \dots, v_n پایه‌ای برای فضای برداری

$V \subset \mathbb{R}^m$ باشد. الگوریتمی که در ادامه ذکر شده، پایه‌ی متعامد v_1^*, \dots, v_n^* را برای V می‌سازد:

Set $v_1^* = v_1$.

Loop $i = 2, 3, \dots, n$.

Compute $\mu_{ij} = v_i \cdot v_j^* / \|v_j^*\|^2$ for $1 \leq j < i$.

Set $v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{ij} v_j^*$.

End Loop

بعلاوه این دو پایه خاصیت (۱۲-۲) را دارند:

$$\text{Span}\{v_1, \dots, v_n\} = \text{Span}\{v_1^*, \dots, v_n^*\} \quad \forall i = 1, 2, \dots, n \quad (۱۲-۲)$$

۲-۲ شبکه‌ها، تعاریف و مشخصات اصلی

تعریف. فرض کنید $v_1, \dots, v_n \in \mathbb{R}^m$ مجموعه‌ای از بردارهای مستقل خطی باشند مشبکه‌ی L^1 ساخته شده توسط v_1, \dots, v_n مجموعه‌ای از ترکیبات خطی v_1, \dots, v_n با ضرایبی در \mathbb{Z} است:

$$L = \{a_1 v_1 + a_2 v_2 + \dots + a_n v_n : a_1, a_2, \dots, a_n \in \mathbb{Z}\} \quad (۱۳-۲)$$

یک پایه برای L هر مجموعه‌ی مستقل خطی از بردارهایی است که L را تولید می‌کند. هر دو پایه دلخواه L تعداد عناصر یکسانی دارند. بُعد مشبکه‌ی L تعداد بردارهای موجود در هر پایه‌ی L است.

فرض کنید که v_1, \dots, v_n پایه‌ای برای مشبکه‌ی L و $w_1, \dots, w_n \in L$ مجموعه‌ای از بردارهای موجود در L باشد. همانطور که برای فضاهای برداری عمل شد، برای مشبکه‌ها نیز می‌توان هر w_j را بصورت ترکیب خطی از بردارهای پایه‌ی مشبکه نوشت، یعنی:

$$\begin{aligned} w_1 &= a_{11}v_1 + a_{12}v_2 + \dots + a_{1n}v_n \\ w_2 &= a_{21}v_1 + a_{22}v_2 + \dots + a_{2n}v_n \\ &\vdots \\ w_n &= a_{n1}v_1 + a_{n2}v_2 + \dots + a_{nn}v_n \end{aligned} \quad (۱۴-۲)$$

اما در این قسمت چون با مشبکه‌ها کار می‌شود باید توجه داشت که تمام ضرایب a_{ij} ها، اعداد صحیح هستند.

گزاره ۲-۳. هر دو پایه‌ی موجود برای یک مشبکه‌ی L با ماتریسی که درایه‌های صحیح و دترمینان ± 1 دارد بهم مرتبط و وابسته هستند [25].

تعریف. مشبکه‌ی صحیح^۲، مشبکه‌ای است که تمام بردارهای آن مختصات صحیح دارند. بعبارت دیگر مشبکه‌ی صحیح، یک زیرگروه جمعی^۳ از \mathbb{Z}^m به ازای $m \geq 1$ است.

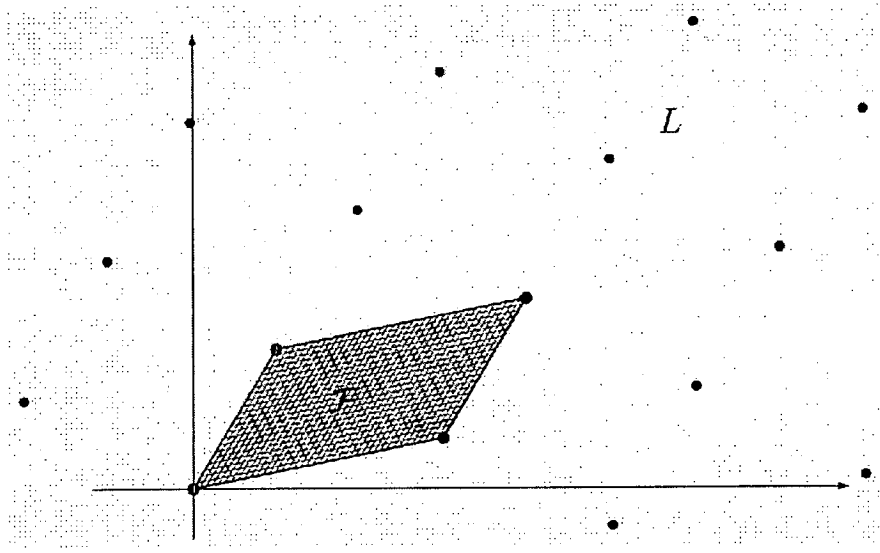
^۱ Lattice

^۲ Integral Lattice

^۳ Additive Subgroup

نکته ۲-۴. اگر $L \subset \mathbb{R}^m$ یک مشبکه با بُعد n باشد، آنگاه یک پایه L را می‌توان بصورت سطرهای یک ماتریس $n \times m$ نوشت. یک پایه جدید می‌تواند از طریق ضرب این ماتریس در یک ماتریس $n \times n$ به نام U که درایه‌های صحیح و دترمینان ± 1 دارد، حاصل شود. مجموعه‌ی چنین ماتریس‌هایی، گروه خطی عمومی^۱ (روی \mathbb{Z}) نامیده شده و با $GL_n(\mathbb{Z})$ نشان داده می‌شود.

یک مشبکه همانند یک فضای برداری است با این تفاوت که یک مشبکه توسط تمام ترکیبات خطی بردارهای موجود در پایه‌ی مشبکه و با استفاده از ضرایب صحیح (به جای استفاده ضرایب حقیقی) ساخته می‌شود. اغلب مفید است که مشبکه را بصورت آرایش منظمی از نقاطش در \mathbb{R}^m در نظر گرفت. به عنوان مثال یک مشبکه در \mathbb{R}^2 در شکل ۱-۲ نشان داده شده است.



شکل ۱-۲ مشبکه‌ی L و ناحیه بنیادی \mathcal{F}

تعریف. فرض کنید L یک مشبکه با بُعد n و v_1, v_2, \dots, v_n پایه‌ی L باشد. ناحیه بنیادی^۲ متناظر با این پایه برای L مجموعه‌ی (۱۵-۲) است که:

$$\mathcal{F}(v_1, \dots, v_n) = \{t_1 v_1 + t_2 v_2 + \dots + t_n v_n : 0 \leq t_i < 1\} \quad (15-2)$$

سطح هاشور زده شده در شکل ۱-۲ یک ناحیه‌ی بنیادی^۲ بعدی را مصور کرده است. گزاره

۵-۲ نشان‌دهنده‌ی دلیلی برای اهمیت مطالعه‌ی نواحی بنیادی در مشبکه‌ها است.

^۱ General Linear Group
^۲ Fundamental Domain