دانـــشگاه یـــزد
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 چندجمله‌ای کوتاه شده

استاد راهنما:
دکتر فضل ا... ادیب‌نیا

اساتید مشاور:
دکتر کیارش میزانیان
دکتر احمد خادم زاده

پژوهش و نگارش:
نوید باباخانی

شهریور ماه ۱۳۸۹

بسمه تعالی

مدیریت تحصیلات تکمیلی	صورتجلسه دفاعیه پایان نامه دانشجوی دوره کارشناسی ارشد	شناسه: ب/ک/۳

جلسه دفاعیه پایان نامه تحصیلی آقای/ خانم: کوید بابا خانی — دانشجوی کارشناسی ارشد

رشته/گرایش: مهندسی فناوری اطلاعات گرایش شبکه های کامپیوتری

تحت عنوان: "بررسی و بهبود الگوریتم های رمزنگاری کلید عمومی مبتنی بر خلقه های چند جمله ای گسسته"

و تعداد واحد: ۶ در تاریخ ۱۳۸۹/۶/۱۵ باحضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان‌نامه با نمره: به عدد ۱۸/۷۵ به حروف هجده و هفتاد و پنج صدم و درجه عالی مورد تصویب قرارگرفت.

عنوان	نام و نام خانوادگی	امضاء
استاد/ استادان راهنما:	دکتر محمد اصل اریب نیا	
استاد/ استادان مشاور:	دکتر کیارش میرانیان	
متخصص وصاحبنظر داخلی:	دکتر مهدی آقا	
متخصص و صاحبنظر خارجی:	دکتر فریبا ملک	

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام ونام خانوادگی: علیرضا محمدزاده

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

عنوان | صفحه

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

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[1]، 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[2]" است. در همین راستا، سیستم‌های بسیاری ابداع شدند که مشهورترین آن‌ها RSA [44]، مبتنی بر مشکل تجزیه‌ی اعداد صحیح[3] است. همچنین سیستم McEliece [33] مبتنی بر نظریه‌ی کدینگ جبری[4]، سیستم ECC [28] مبتنی بر مسئله‌ی رام نشدنی لگاریتم گسسته‌ی خم‌های بیضوی[5]، گونه‌های مختلفی از سیستم رمزنگاری Matsumoto-Imai [32, 11] مبتنی بر سیستم‌هایی از چندجمله‌ای‌های چند متغیره[6] 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

---

[1] Secure Electronic Transaction

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

[3] Integer Factoring Problem

[4] Algebraic Coding Theory

[5] Elliptic Curve Discrete Logarithm

[6] 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 Crypto' 96 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 حالی‌که 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[1] 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 مشبکه 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 مشبکه پرداخته می‌شود. در ابتدای فصل تعاریف و پیش زمینه‌های لازم جبر خطی بیان شده و سپس به تعریف مشبکه‌ها و مسائل دشوار موجود در آنها و قضایا و الگوریتم‌های لازم پرداخته می‌شود. در نهایت دو سیستم رمز GGH و NTRU ارائه شده و

---

[1] Decryption Failure

در مورد جنبه‌های جبری آنها بحث می‌شود. سپس مسائل بنیادی NTRU توضیح داده شده و مشبکه‌ی 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[1] 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.

---

[1] Discrete Fourier Transform

فصل دوم

سیستم‌های رمزنگاری مبتنی بر مشبکه‌ها

۲-۱ تعاریف و مقدمات جبر خطی

فضای برداری. یک *فضای برداری*[۱] V زیرمجموعه‌ای از $\mathbb{R}^m$ است بطوری که:

$$\alpha_1 \mathrm{v}_1 + \alpha_2 \mathrm{v}_2 \in V \quad \forall \mathrm{v}_1, \mathrm{v}_2 \in V \ , \ \forall \alpha_1, \alpha_2 \in \mathbb{R} \qquad (۲-۱)$$

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 $\mathrm{v}_1, \mathrm{v}_2, \dots, \mathrm{v}_k$ عضو فضای برداری V باشند. یک *ترکیب خطی*[۲] بردارهای v_1 تا v_k برداری به شکل رابطه‌ی (۲-۲) می‌باشد:

$$\mathrm{w} = \alpha_1 \mathrm{v}_1 + \alpha_2 \mathrm{v}_2 + \cdots + \alpha_k \mathrm{v}_k \ , \ \alpha_1, \dots, \alpha_k \in \mathbb{R} \qquad (۲-۲)$$

به مجموعه‌ی تمام ترکیبات خطی به شکل $\{\alpha_1 \mathrm{v}_1 + \cdots + \alpha_k \mathrm{v}_k \ : \ \alpha_1, \dots, \alpha_k \in \mathbb{R}\}$، یک پوشش[۳] برای $\{\mathrm{v}_1, \dots, \mathrm{v}_k\}$ گفته می‌شود.

استقلال خطی[۴]. به مجموعه‌ی بردارهای $\mathrm{v}_1, \mathrm{v}_2, \dots, \mathrm{v}_k \in V$ *مستقل (خطی)* گفته می‌شود هرگاه تنها جواب معادله $\alpha_1 \mathrm{v}_1 + \alpha_2 \mathrm{v}_2 + \cdots + \alpha_k \mathrm{v}_k = 0$، این باشد که $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. اگر معادله‌ی فوق حداقل با یک α_i غیرصفر، برقرار شود، مجموعه‌ی $\mathrm{v}_1, \dots, \mathrm{v}_k$ وابسته (خطی) گفته می‌شود.

پایه[۵]. یک *پایه* برای فضای برداری V، عبارتست از مجموعه بردارهای مستقل خطی $\mathrm{v}_1, \dots, \mathrm{v}_n$ که پدیدآورنده‌ای برای V باشد. این تعریف را می‌توان بدین صورت بیان کرد که به ازای هر $\mathrm{w} \in V$، با انتخاب یکتای $\alpha_1, \dots, \alpha_n \in \mathbb{R}$، w را می‌توان بصورت ترکیب خطی (۲-۳) نمایش داد:

$$\mathrm{w} = \alpha_1 \mathrm{v}_1 + \alpha_2 \mathrm{v}_2 + \cdots + \alpha_n \mathrm{v}_n \qquad (۲-۳)$$

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

---

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

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*[1] 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_iها نوشت:

$$\begin{aligned} w_1 &= \alpha_{11}v_1 + \alpha_{12}v_2 + \cdots + \alpha_{1n}v_n \\ w_2 &= \alpha_{21}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{2n}v_n \\ &\vdots \\ w_n &= \alpha_{n1}v_1 + \alpha_{n2}v_2 + \cdots + \alpha_{nn}v_n \end{aligned} \tag{۴-۲}$$

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

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \tag{۵-۲}$$

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:

$$v = (x_1, x_2, \dots, x_m) \quad , \quad w = (y_1, y_2, \dots, y_m) \tag{۶-۲}$$

آنگاه ضرب نقطه‌ای[2] v و w از رابطه‌ی (۲-۷) بدست می‌آید:

$$v \cdot w = x_1y_1 + x_2y_2 + \cdots + x_my_m \tag{۷-۲}$$

بعلاوه، دو بردار v و w *متعامد*[3] گفته می‌شوند اگر $v \cdot w = 0$ باشد.

طول، یا *نرم اقلیدسی*[4] بردار v با $\|v\|$ نشان داده شده و از رابطه‌ی (۲-۸) بدست می‌آید:

$$\|v\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_m^2} \tag{۸-۲}$$

---

[1] Dimension

[2] dot product

[3] Orthogonal

[4] Euclidean Norm

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

$$\mathrm{v} \cdot \mathrm{v} = \|\mathrm{v}\|^2 \tag{۹-۲}$$

تعریف. یک *پایه‌ی متعامد* برای فضای برداری V، پایه‌ی $\mathrm{v}_1, \dots, \mathrm{v}_n$ای است بطوریکه:

$$\mathrm{v}_i \cdot \mathrm{v}_j = 0 \quad \forall j \neq i \tag{۱۰-۲}$$

فرمول‌های بسیار زیادی وجود دارند که اگر برای پایه‌های متعامد بکار برده شوند، بسیار ساده‌تر می‌گردند. به عنوان مثال فرض کنید $\mathrm{v}_1, \dots, \mathrm{v}_n$، یک پایه‌ی متعامد باشد و v یک ترکیب خطی از بردارهای موجود در پایه باشد (یعنی $\mathrm{v} = a_1\mathrm{v}_1 + \cdots + a_n\mathrm{v}_n$)، چون در یک پایه‌ی متعامد رابطه‌ی (۲-۱۰) حاکم است آنگاه:

$$\begin{aligned} \|\mathrm{v}\|^2 &= \|a_1\mathrm{v}_1 + \cdots + a_n\mathrm{v}_n\|^2 \\ &= (a_1\mathrm{v}_1 + \cdots + a_n\mathrm{v}_n) \cdot (a_1\mathrm{v}_1 + \cdots + a_n\mathrm{v}_n) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j (\mathrm{v}_i \cdot \mathrm{v}_j) \\ &= \sum_{i=1}^{n} a_i^2 \|\mathrm{v}_i\|^2 \end{aligned} \tag{۱۱-۲}$$

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

قضیه ۲-۲. (الگوریتم Gram-Schmidt) فرض کنید $\mathrm{v}_1, \dots, \mathrm{v}_n$ پایه‌ای برای فضای برداری $V \subset \mathbb{R}^m$ باشد. الگوریتمی که در ادامه ذکر شده، پایه‌ی متعامد $\mathrm{v}_1^*, \dots, \mathrm{v}_n^*$ را برای V می‌سازد:

Set $\mathrm{v}_1^* = \mathrm{v}_1$.

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

Compute $\mu_{ij} = \mathrm{v}_i \cdot \mathrm{v}_j^* / \|\mathrm{v}\|^2 \qquad for\ 1 \le j < i.$

Set $\mathrm{v}_i^* = \mathrm{v}_i - \sum_{j=1}^{i-1} \mu_{ij}\mathrm{v}_j^*$.

End Loop

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

$$\mathrm{Span}\{\mathrm{v}_1, \dots, \mathrm{v}_n\} = \mathrm{Span}\{\mathrm{v}_1^*, \dots, \mathrm{v}_n^*\} \quad \forall\, i = 1,2, \dots, n \tag{۱۲-۲}$$

۲-۲ مشبکه‌ها، تعاریف و مشخصات اصلی

تعریف. فرض کنید $v_1, \dots, v_n \in \mathbb{R}^m$، مجموعه‌ای از بردارهای مستقل خطی باشند مشبکه‌ی[۱] L *ساخته شده* توسط $v_1, \dots, v_n$ مجموعه‌ای از ترکیبات خطی $v_1, \dots, v_n$ با ضرایبی در $\mathbb{Z}$ است:

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

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:

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

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.

---

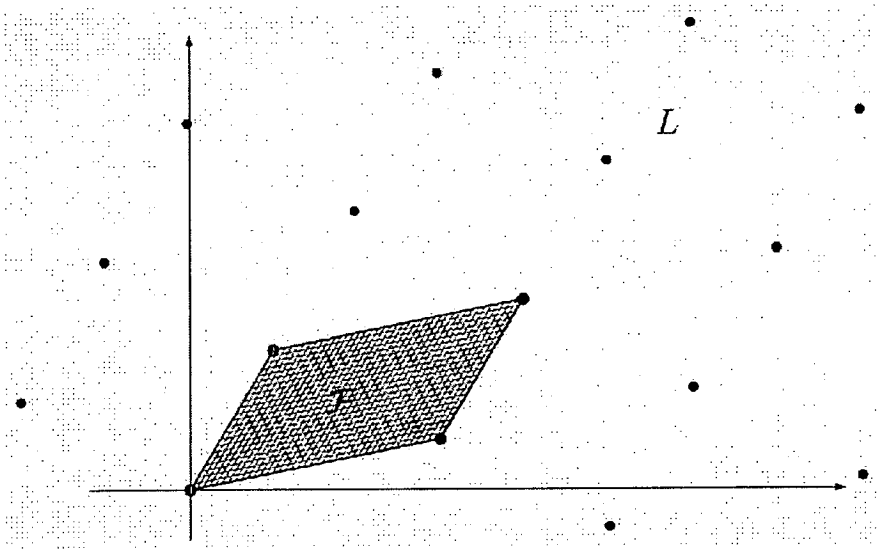
۱ Lattice

۲ Integral Lattice

۳ Additive Subgroup

نکته ۲-۴. اگر $L \subset \mathbb{R}^m$ یک مشبکه با بُعد n باشد، آنگاه یک پایه‌ی 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 $\mathrm{GL}_n(\mathbb{Z})$ 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 ۲-۱ نشان داده شده است.



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

تعریف. فرض کنید L یک مشبکه با بُعد n و $\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_n$ پایه‌ی L باشد. *ناحیه بنیادی*[۲] متناظر با این پایه برای L، مجموعه‌ی (۲-۱۵) است که:

$$\mathcal{F}(\mathrm{v}_1, \ldots, \mathrm{v}_n) = \{t_1\mathrm{v}_1 + t_2\mathrm{v}_2 + \cdots + t_n\mathrm{v}_n \ : \ 0 \le t_i < 1\} \qquad (۱۵\text{-}۲)$$

سطح هاشور زده شده در شکل ۲-۱ یک ناحیه‌ی بنیادی ۲ بعدی را مصور کرده است. گزاره ۲-۵ نشان‌دهنده‌ی دلیلی برای اهمیت مطالعه‌ی نواحی بنیادی در مشبکه‌ها است.

---

[۱] General Linear Group

[۲] Fundamental Domain