
بسم الله الرحمن الرحيم

دانشکده‌ی علوم پایه

گروه ریاضی

پایان نامه‌ی دوره‌ی کارشناسی ارشد ریاضی محض

سیستم های رمزنگاری کلید عمومی مبتنی بر مشبکه ها

نگارش: انسیه نجفی

استاد راهنما: دکتر سید حمید حاجی سید جوادی

استاد مشاور: دکتر محمد علی دوستاری

بهمن ۱۳۹۱

چکیده

رمزنگاری، ابزاری مناسب جهت حفاظت اطلاعات در کانال ناامن است. به این منظور، از دو روش رمزنگاری کلید متقارن و رمزنگاری کلید عمومی استفاده می‌شود. شالوده‌ی رمزنگاری به روش کلید عمومی، استفاده از توابع ترپدر یک‌طرفه است. میزان دشواری یافتن معکوس این توابع یا به طور معادل، میزان دشواری مسائل بکار رفته در ساختار آن‌ها، میزان امنیت این توابع را تضمین می‌کند. مشبکه‌ها از جمله منابع مسائل دشوار محاسباتی است که در ساخت توابع یک‌طرفه مورد استفاده قرار می‌گیرد. از آنجا که مشبکه‌ها ساختاری جبری دارند، تغییر در این ساختار بر میزان دشواری این مسائل تاثیرگذار است. هدف از این پایان نامه، بررسی روند بهبود توابع یک‌طرفه مبتنی بر مشبکه‌ها، به کمک ارتقای ساختار جبری آن‌ها می‌باشد. در این تحقیق، ابتدا کاهش‌های انجام شده در مشبکه‌ها روی حلقه‌ی اعداد صحیح مورد بررسی قرار می‌گیرد. پس از آن با جایگزینی حلقه‌ی اعداد صحیح جبری با حلقه‌ی اعداد صحیح، ضریب تقریب، کاهش و در نتیجه امنیت تابع یک‌طرفه افزایش می‌یابد. همین روند، در مشبکه‌های ایدآل نیز بررسی می‌شود. از جمله مزایای بکارگیری مشبکه‌های ایدآل در توابع یک‌طرفه، تبدیل توابع ناکارآمد در مشبکه‌ها به توابع کارآمد در مشبکه‌های ایدآل است. در پایان، روشی برای تولید شبه تصادفی کلید عمومی، با فرض دشواری مسائل مشبکه‌های ایدآل در بدترین حالت، ارائه خواهد شد.

کلمات کلیدی: مشبکه، مشبکه‌ی ایدآل، تابع یک‌طرفه، کاهش از بدترین حالت به حالت متوسط، امنیت اثبات پذیر، میدان اعداد جبری، کوتاه‌ترین بردار، نزدیک‌ترین بردار.

فهرست مطالب

لیست تصاویر

لیست جداول

مقدمه

در دنیای تبادل مجازی اطلاعات، داده‌ها به شکل ۰ و۱ مخابره می‌شوند و در اغلب موارد این داده‌های باینری، توسط هر شخص بخصوص افراد مهاجم، قابل رؤیت است. رمزنگاری روشی برای آشفته نمودن این صفر و یک‌ها است به طوری که استخراج پیام اصلی تنها توسط صاحب پیام یا دریافت کننده‌ی آن میسر باشد. به عمل تبدیل داده‌های باینری بامعنی(متن ساده[۱]) به داده‌های باینری بی‌مفهوم(متن رمز[۲])، *رمزگذاری* و به عمل عکس آن، *رمزگشایی* و به مجموعه‌ی اطلاعات لازم جهت تبدیل متن ساده به متن رمز یا برعکس، کلید گویند. آنچه سبب برتری یک سیستم رمزنگاری نسبت به باقی سیستم‌های رمز می‌شود، میزان امنیت و کارایی آن سیستم است. اگرچه همواره این دو ویژگی را نمی‌توان در یک‌جا جمع نمود. زیرا گاهی امنیت بسیاربالا، سبب عدم کارایی سیستم خواهد شد و یا بالعکس. به‌همین منظور در ساخت سیستم‌های رمزنگاری، هدف، ساخت سیستمی است که در آن، این دو ویژگی به‌طور نسبی برقرار باشد.

اولین سیستم رمزنگاری کلید عمومی در سال ۱۹۷۶ توسط دیفی و هلمن پیشنهاد شد [۱۲]. ایده‌ی اصلی ساخت این سیستم، تابع ترپدر یک‌طرفه بود. بعدها سیستم‌های رمزنگاری کلید عمومی بسیاری بر پایه‌ی توابع یک‌طرفه مطرح شدند که از معروف ترین آن‌ها سیستم‌های RSA، ECC و الجمال[۳] است. توابع یک‌طرفه‌ی بکار برده شده در این سیستم‌ها، مسائل معروفی در نظریه اعداد، مانند تجزیه اعداد و لگاریتم گسسته می‌باشد که البته انتظار می‌رود با بهبود قدرت فرایند، توسعه‌ی محاسبه کوانتوم و توزیع محاسبات، این مسائل قابل حل شوند. در سال ۱۹۹۶، اجتای نشان داد که مسئله‌ی یافتن کوتاه‌ترین بردار در مشبکه‌ها، از حل مسائل نظریه اعداد، دشوارتر است. بدین‌ترتیب با این تحقیقات، دانشمندان امیدوار به ساخت سیستم‌های رمزنگاری بر پایه‌ی این مسائل شدند. از امتیازات سیستم رمزنگاری مبتنی بر مشبکه‌ها امنیت اثبات‌پذیر، سرعت بیشتر، پیچیدگی محاسباتی کمتر و سهولت پیاده سازی سخت افزاری و نرم افزاری آن نسبت به سیستم‌های رمزنگاری کلید عمومی موجود است.

اغلب طرح‌های رمزنگاری مبتنی بر مشبکه، بر پایه‌ی دو مسئله‌ی حالت متوسط، با نام‌های پاسخ صحیح

---

[۱] plain text

[۲] cipher text

[۳] Elgamal

کوتاه [۴] (SIS) و یادگیری همراه با خطا [۵] (LWE) پایه‌گذاری شده‌اند. کاهش این دو مسئله به مسائل دشوار در مشبکه‌ها امنیت آن‌ها را ضمانت می‌کند. مسئله‌ی SIS، نوع خاصی از مسئله‌ی کوله پشتی روی گروه جمعی $\mathbb{Z}_q$ است. هدف این مسئله، به ازای اعداد صحیح و مثبت q و n، یافتن یک ترکیب خطی صحیح و کوچک از n بردار مستقل خطی $a_i \in \mathbb{Z}_q^n$ است به طوری که این ترکیب خطی به پیمانه‌ی q صفر شود. اما در مسئله‌ی LWE، دوتایی‌های $(a_i, b_i \approx \langle a_i, s\rangle) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ به تعداد چندجمله‌ای داده شده است که در آن، $a_i \sim U(\mathbb{Z}_q^n)$ و هر $\langle a_i, s\rangle$ با اضافه کردن یک مقدار تصادفی، به b_i تبدیل می‌شود. هدف از این مسئله، تشخیص توزیع این دوتایی‌ها از دوتایی‌های یکنواخت انتخاب شده از $\mathbb{Z}_q^n \times \mathbb{Z}_q$ می‌باشد.

از جمله طرح‌های رمزنگاری پیشنهادی بر اساس مسئله‌ی SIS، ساخت تابع یک‌طرفه [۴]، ساخت تابع ضدتصادم [۱۷]، طرح‌های تعیین هویت [۴۲، ۲۶، ۲۰] و امضای دیجیتال [۱۵، ۱۱، ۹، ۳۷، ۲۷] است. همین طور بر اساس مسئله‌ی LWE، رمزگذاری کلید عمومی مقاوم در مقابل هر دو حمله‌ی متن اصلی منتخب [۶] [۴۹، ۴۷، ۲۵] و متن رمزشده‌ی منتخب [۷] [۴۸، ۴۴، ۳۷] و رمزگذاری بر پایه‌ی هویت [۱۵، ۱۱، ۱، ۲] ارائه شده است.

از نقاط ضعف این طرح‌های رمزنگاری، ناکارامدی آن‌ها به خاطر زمان محاسبه‌ی بالا و طول زیاد کلید است. یک راه امیدبخش برای نجات از این ناکارامدی ذاتی، استفاده از مشبکه‌هایی است که دارای ساختار جبری خاص هستند. مشیان‌شیو در سال ۲۰۰۲ با الهام از طرح شهودی سیستم رمز NTRU، تابع یک‌طرفه‌ی کارایی را با استفاده از در نظر گرفتن مسئله‌ی SIS در حلقه‌ای خاص، پیشنهاد کرد که دشواری آن حداقل به اندازه‌ی دشواری مسائل مشبکه‌های ایدآل در بدترین حالت است. همین طور، در سال ۲۰۱۲، لایبشوسکی، پیکرت و ریگو، گونه‌ای کارا از مسئله‌ی SIS، را در حلقه‌ی اعداد صحیح جبری معرفی نمودند که دشواری آن حداقل به میزان دشواری بدترین حالت مسائل مشبکه‌های ایدآل است. از جمله مسائل سخت در مشبکه ها دو مسئله یافتن کوتاه‌ترین بردار و نزدیک‌ترین بردار است. سیستم رمز NTRU، از مهمترین سیستم‌های رمزنگاری مبتنی بر مشبکه‌ها است که امنیت خود را از

[۴] Small Integer Solution

[۵] Learning With Error

[۶] chosen-plaintext

[۷] chosen-ciphertext

سختی مسئله‌ی یافتن کوتاه‌ترین بردار بدست می‌آورد. این سیستم در حال حاضر در شرکت های مهمی چون Sony، Intel، NXP و ... مورد استفاده قرار می گیرد. بنابراین با توجه به جدید بودن مشبکه‌ها در زمینه‌های تئوری و عملی، بر آن شدیم با این تحقیق، اندکی با ساختار سیستم‌های رمز مبتنی بر مشبکه آشنا شویم. به این منظور، مفاهیم و تعاریف مورد نیاز را در فصل اول، ارائه نموده‌ایم. در فصل دوم، ابتدا مشبکه‌ها و بعضی مسائل مورد نیاز در آن‌ها تعریف و دشواری آن‌ها بررسی شده است. سپس کاهش‌های انجام گرفته از مسائل دشوار مشبکه در بدترین حالت، به دو مسئله‌ی SIS و LWE به ترتیب بهبود، مورد مطالعه قرار می‌گیرد. در فصل سوم، کاهش‌های انجام گرفته از مسائل دشوار مشبکه‌های ایدآل در بدترین حالت، به دو مسئله‌ی SIS و LWE به ترتیب بهبود و در دو حلقه‌ی اعداد صحیح و اعداد صحیح جبری، مورد کاوش و بررسی قرار می‌گیرد. در آخر، با اثبات شبه تصادفی بودن توزیع LWE روی حلقه‌ی اعداد صحیح جبری، شبه تصادفی بودن کلید عمومی تولید شده در سیستم‌های رمزنگاری بر اساس این مسئله ثابت خواهد شد.

فصل ۱

تعاریف و مفاهیم اولیه

در این فصل به تعریف مفاهیم اولیه در مورد رمزنگاری و امنیت آن، تابع ترپدر و مفاهیم ریاضی و آماری مورد نیاز می‌پردازیم. مطالب این فصل برگرفته از منابع [۳۱]، [۳۹]، [۳۶]، [۴]، [۲۹]، [۴۰] و [۱۲] است.

۱.۱ رمزنگاری به روش کلید عمومی

به‌طورکلی رمزنگاری به دو روش رمزنگاری متقارن و رمزنگاری کلید عمومی انجام می‌شود. تا سال ۱۹۷۶ عملیات رمزنگاری تنها به روش متقارن انجام می‌گرفت، به این صورت که اطلاعات با همان کلیدی رمزگشایی می‌شد که با آن، اطلاعات به شکل رمز درآمده بود. به‌عبارت‌دیگر کلید رمزگذاری و رمزگشایی یکی است یا از روی یکدیگر به راحتی قابل بازیابی است. ازجمله معایب این روش، دشواری انتقال امن کلیدی است که بین دو طرف به اشتراک گذاشته می‌شود، زیرا علاوه بر هزینه‌های قابل توجه، در بعضی موارد این کار امکان‌پذیر نیست. در سال ۱۹۷۶، دیفی و هلمن، یک سیستم رمزنگاری را پیشنهاد کردند که مبنای ساخت آن، تابع یک‌طرفه بود [۱۲]. در این نوع سیستم، هر شخص دارای یک جفت کلید عمومی و خصوصی است که کلید عمومی را به صورت همگانی اعلام کند اما کلید خصوصی را مخفی نگه می‌دارد. بنابراین در تبادل اطلاعات به روش کلید عمومی، هر کس می‌تواند پیام را با کلید عمومی‌شخص مورد نظر رمز نموده، به او بفرستد و دریافت کننده‌ی پیام با کلید خصوصی پیام را از حالت

رمز خارج کند. نکته‌ی جالب در این روش معادل بودن کشف متن اصلی از روی متن رمزشده با یافتن معکوس تابع یک‌طرفه و همچنین معادل بودن محاسبه‌ی کلید عمومی از روی کلید خصوصی با حل یک مسئله‌ی دشوار در ریاضیات است. به‌همین‌جهت، اگرچه کلید عمومی و کلید خصوصی از لحاظ ریاضی به یک‌دیگر مرتبط و جفت منحصربه‌فردند(یعنی برای هر کلید عمومی نمی‌تواند دو کلید خصوصی وجود داشته باشد)، اما اطلاع از کلید عمومی، امنیت کلید خصوصی را مختل نمی‌کند. بنابراین نکته‌ی مهم در سیستم رمزنگاری کلیدعمومی، میزان دشواری یافتن معکوس تابع یک‌طرفه است.

تعریف ۱.۱. منظور از *تابع یک‌طرفه* f، تابعی ازمجموعه‌ی A به مجموعه‌ی B است به‌طوری‌که به ازای هر $x \in A$، یافتن $f(x) \in B$ به سادگی انجام می‌گیرد. اما به ازای هر مقدار تصادفی $b \in B$ یافتن $x \in A$ به طوری که $f(x) = b$ کاری دشوار است. *تابع ترپدر یک‌طرفه*[۱]، یا به اختصار تابع ترپدر، تعریفی مشابه با تابع یک‌طرفه دارد با این تفاوت که با داشتن اطلاعات اضافی درباره‌ی تابع، می توان معکوس آن را به آسانی محاسبه کرد [۱۴].

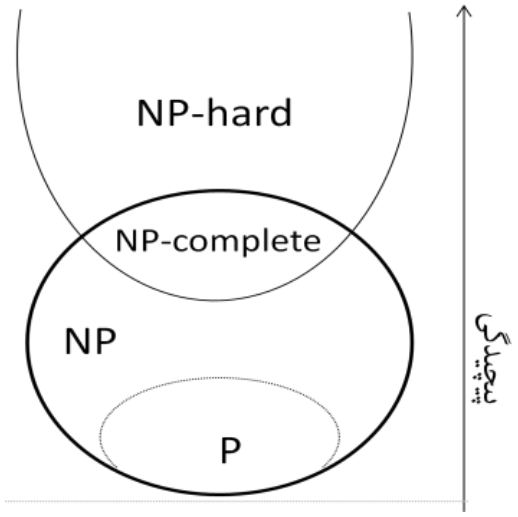
با این تعریف به ذهن می‌رسد که تابع یک‌طرفه امنیت بیشتری را نسبت به تابع ترپدر یک‌طرفه تضمین می‌کند. اما این کار در عمل غیر ممکن است زیرا دریافت کننده‌ی پیام باید بتواند متن رمزشده را به متن ساده تبدیل کند(محاسبه‌ی معکوس تابع یک‌طرفه). این همان رابطه‌ی متضاد بین امنیت و کارایی سیستم‌ها است. ابتکار دیفی و هلمن در ساخت سیستم رمزنگاری، معرفی تابع ترپدر یک‌طرفه بود، تا بتوان به کمک اطلاعات اضافی آن، عمل معکوس را انجام داد. این اطلاعات اضافی، همان کلید خصوصی است که نزد صاحب کلید عمومی، مخفی باقی می‌ماند. قبل از بکارگیری مشبکه‌ها در ساختار سیستم رمزنگاری کلید عمومی، مشهورترین سیستم‌های رمزنگاری کلید عمومی، سیستم رمز RSA و سیستم الجمال بود. این دو سیستم به ترتیب براساس مسائل تجزیه‌ی دو عدد اول بزرگ و لگاریتم گسسته که دو مسئله‌ی دشوار در نظریه‌ی اعداد هستند، بنا نهاده شده است.

---

[۱] trapdoor one-way function

۲.۱ رده‌بندی مسائل محاسباتی ریاضی

همان طور که بیان شد، میزان امنیت تابع ترپدر به میزان دشواری مسئله‌ی معادل با معکوس این تابع برمی‌گردد. در نظریه پیچیدگی، مسائل محاسباتی بنا بر میزان دشواری به رده‌هایی تقسیم می‌شوند که از جمله‌ی آن‌ها، رده‌ی مسائل P و NP است. با یک نگاه کلی می‌توان گفت که مسائل رده‌ی P دسته مسائل آسان و رده‌ی NP دسته مسائل دشوار برای حل است. به‌طور دقیق‌تر، مسائلی در کلاس P قرار می‌گیرند که بهترین الگوریتم‌های معین برای حل آن‌ها، حداکثر در زمانی به طول چندجمله‌ای از طول ورودی قابل حل باشد، اما بهترین الگوریتم برای مسائل NP، الگوریتم‌های نامعین با زمان اجرای حداکثر چندجمله‌ای از طول ورودی است. به‌عبارت دیگر، هیچ الگوریتم زمان‌چندجمله‌ای معین برای چنین مسائلی یافت نشده است. اما در نظریه پیچیدگی، سؤالی که تا به حال بی‌پاسخ مانده این است که آیا P =! NP است؟ البته حدس‌هایی مبنی بر صحت این ادعا وجود دارد [۵۴]. دو رده‌ی دیگر در رده‌بندی مسائل محاسباتی، رده‌ی مسائل NP-complete و NP-hard است. قبل از تعریف این دو رده، دانستن مفهومی به نام *کاهش* ضروری است؛ گوییم مسئله‌ی A به مسئله‌ی B کاهش می‌یابد هرگاه با دانستن پاسخ مسئله‌ی B بتوان در زمان چندجمله‌ای، جوابهای مسئله‌ی A را یافت. از لحاظ شهودی می‌توان گفت هرگاه A به B کاهش یابد آنگاه حل A از B سخت‌تر نیست، زیرا با آگاهی از جواب‌های مسئله‌ی B می‌توان به پاسخ مسئله‌ی A دست یافت. اما مفهوم کاهش در نظریه پیچیدگی، بیش از آن‌که به منظور یافتن پاسخ‌های یک مسئله با جواب‌های نامعلوم به کمک مسئله‌ای با جواب‌های معلوم بکار رود، ابزاری برای اثبات دشواری مسائل است. هرگاه مسئله دشوار A به مسئله‌ی ناشناخته‌ی B کاهش یابد، نتیجه خواهد شد که A دشوارتر از B نیست! به عبارت دیگر با این عمل می‌توان گفت که B حداقل در کلاس دشواری A قرار می‌گیرد. اما مسائل رده‌ی NP-complete یا NPC زیرمجموعه‌ای از رده‌ی NP است، به این صورت که تمام مسائل NP به مسائل NPC کاهش می‌یابد. به عبارت دیگر مسائل NPC از تمام مسائل NP دشوارتر است. اما مسائل NP-hard ، مسائلی هستند که تمام مسائل NP به هر یک از آن‌ها کاهش می‌یابد و اگر ثابت شد که یک مسئله‌ی NP-hard در رده‌ی مسائل NP نیز قرار می‌گیرد، آنگاه آن مسئله حتما NP-complete است. شکل ۱.۱ ارتباط این رده‌ها را با یکدیگر را نشان می‌دهد.



شکل ۱.۱: رابطه‌ی رده‌های پیچیدگی مسائل

۳.۱ امنیت محاسباتی

هر سیستم رمزنگاری دو نوع امنیت را ضمانت می‌کند؛

- امنیت مطلق یا امنیت از دیدگاه نظریه‌ی اطلاعات
- امنیت محاسباتی یا امنیت مشروط

منظور از امنیت مطلق امنیتی است که مهاجم با هر توان محاسباتی قادر به شکستن سیستم رمزنگاری نباشد. چنین امنیتی اصولاً آرمان رمزنگاری متقارن است. سیستم رمزنگاری وان‌تایم‌پد، از جمله سیستم‌های متقارنی است که امنیت مطلق را ضمانت می‌کند. روش کلی این سیستم، تولید کلیدی به طول متن ساده و XOR کلید با متن است. در این روش دریافت کننده‌ی پیام باید کلید رمزگذاری را داشته باشد تا با XOR مجدد کلید، با متن دریافت شده، متن اصلی را بازیابی کند. کاملا تصادفی بودن کلید، امنیت کامل را برای سیستم وان‌تایم‌پد، تضمین می‌کند، اما به خاطر طول کلید در متن‌های طولانی و مشکلات انتقال آن این سیستم در عمل ناکارامد است. اما امنیت محاسباتی، امینت، در مقابل دشمن با توان محاسباتی محدود است [۳۰]. در ساخت سیستم‌های رمزنگاری کلید عمومی، هدف، تأمین امنیت

محاسباتی است. در این صورت اگرچه این سیستم‌ها، در مقابل مهاجم با هر توان محاسباتی امن نیستند، اما در دنیای واقعی، چنین مهاجمی وجود ندارد. در تمام سیستم‌های رمز کلید عمومی، امنیت سیستم، براساس میزان دشواری مسائل مورد استفاده در ساخت تابع ترپدر است.

۴.۱ شکل‌گیری سیستم‌های رمز کلید عمومی بر مبنای مشبکه

تا قبل از سال ۱۹۹۶ قوی‌ترین سیستم‌های رمز کلید عمومی، مانند RSA ، الجمال و...، براساس مسائلی از رده‌ی NP ساخته شدند. اما بتدریج با رشد کامپیوترهای کوانتومی و افزایش سرعت محاسبات، امنیت این سیستم‌ها هرچه بیش‌تر مورد تهدید قرار گرفت. برای مثال در تجزیه‌ی حاصل‌ضرب اعداد اول بزرگ، اعداد با ۵۱۲ بیت که تا دو دهه‌ی قبل تجزیه‌ناپذیر محسوب می‌شدند، تجزیه شدند [۷] .

در سال ۱۹۹۶، اجتای با کاهش تصادفی معکوس تابع ترپدر یک‌طرفه به مسئله‌ای در مشبکه‌ها، ثابت کرد که معکوس نمودن تابع ترپدر، حداقل به اندازه‌ی حل تقریبی از مسئله‌ی SVP در مشبکه‌ها دشوار است [۴] و یک سال بعد، یعنی در سال ۱۹۹۷، نشان داد، SVP در رده‌ی مسائل NP–hard قرار می‌گیرد [۳]. این دو کشف بزرگ اجتای، راه جدیدی را در ساخت سیستم‌های رمز کلید عمومی پیش روی دانشمندان قرار داد. براساس این یافته‌ها، می‌توان در جهت ساخت سیستم‌هایی گام برداشت که شکستن آن‌ها معادل با حل مسئله‌ای در رده‌ی NP–hard باشد. بعلاوه حدس‌های بسیاری مبنی بر این‌که پیشرفت و توسعه‌ی کامپیوترهای کوانتومی تهدیدی برای سیستم‌های رمز کلید عمومی مبتنی بر مشبکه نیست، وجود دارد [۲۴] و [۵۱]. از مهم‌ترین سیستم‌های رمزنگاری مبتنی بر مشبکه، سیستم رمز GGH و NTRU است. جدول ۱.۱ مقایسه‌ای بین این دو سیستم و سیستم رمز RSA انجام می‌دهد.

تعریف ۲.۱. مشبکه، ترکیب صحیحی از بردارهای مستقل‌خطی در $\mathbb{R}^n$ است [۴۲].

از جمله مسائل دشوار در مشبکه، مسئله‌ی *یافتن کوتاه‌ترین بردار* و *مسئله‌ی یافتن نزدیک‌ترین بردار* و یا به اختصار *SVP* و *CVP* در مشبکه است که در رده‌ی مسائل NP–hard قرار می‌گیرند. این دو مسئله، مشبکه‌ها را علاوه بر رمزنگاری، در زمینه‌های دیگر مانند فیزیک، مخابرات و اقتصاد مورد توجه قرار داده است. در بسیاری از این کاربردها یافتن مقدار دقیق پاسخ مسائل لازم نیست، بلکه تنها کافی است تقریبی از این پاسخ‌ها یافت شوند. اما در مورد دشواری تقریب این مسائل چه می‌توان گفت؟

واضح است که هرچه ضریب تقریب بزرگ‌تر باشد، دایره‌ی جواب‌های شدنی بزرگ‌تر و یافتن پاسخ مسئله آسان‌تر است. کشف مهم اجتای، کاهش تصادفی معکوس نمودن تابع ترپدر، به تقریب مسئله‌ی SVP با ضریب تقریب $n^{۸}$ است. اگرچه NP-hard بودن این مسئله‌ی تقریبی، به اثبات نرسیده، اما تاکنون الگوریتم کارایی هم برای حل آن پیدا نشده است. بیش‌تر تلاش‌هایی که بعدها در راستای کار اجتای انجام گرفت یا معطوف به کاهش ضریب تقریب و بدنبال آن افزایش امنیت تابع ترپدر و یا در جهت ارتقای ساختار مشبکه و در نتیجه افزایش کارایی تابع ترپدر بوده است. گرچه گاهی یک بهبود در هر دو زمینه مؤثر واقع شده‌است.

جدول ۱.۱: **مقایسه‌ی سه سیستم رمزنگاری کلید عمومی**

	NTRU	RSA	GGH
سرعت رمزگذاری	$N^{۲}$	$N^{۳}$	$N^{۲}$
سرعت رمزگشایی	$N^{۲}$	$N^{۳}$	$N^{۲}$
طول کلید عمومی	N	$N^{۳}$	$N^{۲}$
طول کلید خصوصی	N	N	$N^{۲}$

۵.۱ توابع ترپدر

اولین تابع ترپدر در مشبکه را اجتای در [۴] معرفی کرد. بعدها مشیان‌شیو معکوس این تابع را به صورت مسئله‌ی یافتن بردار کوتاه یا SIS معادلسازی کرد [۳۹] . تابع ترپدر دیگر را رگیو در سال ۲۰۰۵ پیشنهاد داد و مسئله‌ی معکوس آن را یادگیری همراه خطا یا LWE نامید [۴۹]. این دو مسئله به شکل زیر تعریف می‌شود؛

تعریف ۳.۱. مسئله‌ی یافتن بردار کوتاه $(SIS^{p}_{q,m,\beta})$. به ازای اعداد ثابت و صحیح q و حقیقی β، ماتریس $A \in \mathbb{Z}_q^{n\times m}$ داده‌شده‌است. مسئله، یافتن بردار صحیح و ناصفر $e \in \mathbb{Z}^m$ است به‌طوری‌که $Ae \equiv ۰ \mod q$ و $\| e \|_p \leq \beta$.

تعریف ۴.۱. مسئله‌ی یادگیری همراه با خطا $(LWE_{p,\chi})$. فرض کنیم که $p = p(n) \leq poly(n)$، عددی صحیح و

$$\begin{aligned} \langle s, a_1 \rangle &\approx_\chi b_1 \mod p \\ \langle s, a_2 \rangle &\approx_\chi b_2 \mod p \\ &\vdots \end{aligned}$$

لیستی از تساوی‌ها باشد که در آن $s \in \mathbb{Z}_p^n$، $b_i \in \mathbb{Z}_p$ و $a_i \sim U(\mathbb{Z}_p^n)$ و مستقل از یکدیگر انتخاب شده باشند و همین طور خطا در تساوی‌ها با توزیع احتمالی $\chi : \mathbb{Z}_p \to \mathbb{R}^+$ مشخص شود، به این معنا که برای هر i، $b_i = \langle s_i, a_i \rangle + e_i$ که در آن $e_i \sim \chi(\mathbb{Z}_p)$ و مستقل از یکدیگر انتخاب شده باشد. هرگاه در این تساوی‌ها مقادیر a_i و b_i معلوم و باقی مقادیر نامعلوم باشند، آنگاه مسئله، یافتن مقدار s است.

۶.۱ مفاهیم ریاضی و آماری

۱.۶.۱ فاصله‌ی آماری

از ویژگی‌های توابع یک‌طرفه، کاملا تصادفی بودن خروجی تابع در برد، به ازای توزیع مورد نظر در دامنه است. اما در توابع ترپدر چنین چیزی ممکن نیست. در واقع برای تحلیل امنیت توابع ترپدر به ازای توزیعی که در دامنه اعمال می‌شود، میزان نزدیکی توزیع خروجی به توزیع یکنواخت، مورد بررسی قرار می‌گیرد. محاسبه‌ی فاصله آماری بین دو توزیع، ابزار مناسبی برای این منظور و به طور کلی برای تحلیل کاهش‌ها و الگوریتم‌های احتمالی بشمار می‌رود.

تعریف ۵.۱. فاصله‌ی آماری بین دو متغیر تصادفی گسسته‌ی X و Y روی مجموعه‌ی شمارش‌پذیر A برابر است با

$$\triangle(X, Y) = \frac{1}{2} \sum_{a \in A} |Pr\{X = a\} - Pr\{Y = a\}|.$$

بطور مشابه فاصله‌ی آماری برای دو متغیر تصادفی و پیوسته‌ی X و Y، روی $\mathbb{R}^n$ به ترتیب با توابع چگالی T_1 و T_2، برابر است با

$$\Delta(X,Y) = ۱/۲ \int_{\mathbb{R}^n} |T_۱(r) - T_۲(r)|dr.$$

ازجمله ویژگی‌های فاصله‌ی آماری تأثیر تابع f روی متغیرهای تصادفی است که نمی تواند فاصله‌ی آن‌ها را افزایش دهد. به‌عبارت دیگر

$$\Delta(f(X), f(Y)) \leq \Delta(X,Y).$$

بخصوص این ویژگی، زمانی بکار می‌آید که هرگاه فاصله‌ی دو متغیر تصادفی X و Y، حداکثر $\Delta(X,Y)$ باشد، آنگاه تاثیر الگوریتم روی این دو متغیر، فاصله‌ی آن‌ها را افزایش نخواهد داد. ویژگی مفید دیگر فاصله‌ی آماری محاسبه‌ی کران بالا برای فاصله‌ی دو سری از متغیرهای تصادفی و مستقل $X_۱, X_۲, ..., X_k$ و $Y_۱, Y_۲, ..., Y_k$ است، که به صورت زیر می‌باشد،

$$\Delta((X_۱, X_۲, ..., X_k), (Y_۱, Y_۲, ..., Y_k)) \leq \sum_{i=۱}^{k} \Delta(X_i, Y_i).$$

توضیحات بیشتر در این موضوع را می‌توان در فصل هشتم [۳۱] یافت.

۲.۶.۱ توزیع گاوسی

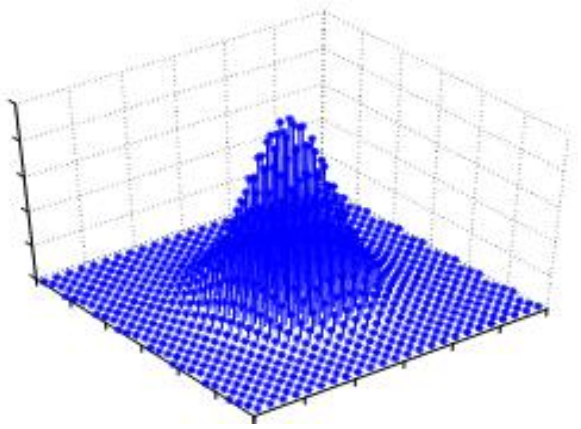
تعریف ۱.۶. برای بردارهای x و c در $\mathbb{R}^n$ و به ازای $s > ۰$ ،

$$\rho_{s,c}(x) = e^{-\pi\|(x-c)/s\|^۲}$$

را اندازه‌ی گاوسی یا تابع گاوسی گویند[۳۹].

از آنجا که $\int_{\mathbb{R}^n} \rho_{s,c}(x)dx = s^n$، پس $\int_{\mathbb{R}^n} \rho_{s,c}(x)/s^n dx = ۱$ و می‌توان $\rho_{s,c}(x)/s^n$ را تابع چگالی احتمال در نظر گرفت.
هرگاه A مجموعه‌ای شمارش‌پذیر باشد، آنگاه $\rho_{s,c}(A) = \sum_{x\in A} \rho_{s,c}(x)$. پس به ازای مجموعه‌ی گسسته‌ی A، توزیع احتمالی گسسته روی A به صورت زیر تعریف می‌شود؛

$$D_{A,s,c}(x) = \frac{\rho_{s,c}(x)}{\rho_{s,c}(A)}.$$



شکل ۲.۱: توزیع گاوسی گسسته

حذف هر یک از اندیس‌های s و c به ترتیب نشان دهنده‌ی مقادیر ۰ و ۱ برای آن‌ها است. شکل ۲.۱ نمایی از توزیع گاوسی گسسته است.

در ادامه، بعضی مفاهیم جبری و جبرخطی مورد نیاز به اختصار بیان شده است.

۳.۶.۱ گروه و حلقه

تعریف ۷.۱. گروه. هرگاه R مجموعه‌ای از اشیا و $\diamond$ عملی دوتایی روی اعضای R باشد، آنگاه در صورت برقراری ۴ ویژگی زیر، $(R, \diamond)$ را گروه نامیم؛

- R نسبت به عمل $\diamond$ بسته باشد
- عمل $\diamond$ روی R شرکت‌پذیر باشد
- R دارای عضو خنثی باشد
- R دارای عضو وارون باشد