درس رمزنگاری مشبکه‌مبنا

(Lattice-based Cryptography)

(کد درس: ۲۵۸۲۳- گروه ۱)

نیم‌سال اول ۰۲-۱۴۰۱

نوع درس: نظری	**۳ واحد**
پیش نیاز: رمزنگاری **۲۲۸۱۴ / ۲۵۱۶۵**	**هم نیاز ندارد**
مقطع: تحصیلات تکمیلی	**اولین نیم‌سال ارائه شده: ۲-۹۳-۹۲**
گروه مخابرات (گرایش رمز)	**مدرس: ترانه اقلیدس** teghlidos@sharif.edu Homepage:sharif.edu/~teghlidos

اهداف درس:

بیان ضرورت رمزنگاری پساکوانتومی، آشنایی با ساختار رمزنگاری کلید عمومی مشبکه‌مبنا به عنوان جایگزینی برای رمزنگاری کلید همگانی مبتنی بر نظریه اعداد، توابع چکیده ساز برخورد تاب مشبکه مبنا، امضای دیجیتال مشبکه مبنا و مقایسه‌ی سامانه‌های مشبکه مبنا با سامانه‌های رمز متعارف از دیدگاه امنیت و کارآیی.

جلسات هفتگی درس:

زمان: روزهای شنبه و دوشنبه از ساعت ۱۰:۳۰ تا ۱۲:۰۰
مکان: ساختمان آموزش-کلاس ۲۰۸

معرفی درس

کاربرد مشبکه‌ها در رمزنگاری کلید عمومی اولین بار توسط Ajtai (بخوانید آیتای) در سال ۱۹۹۶ مطرح شد. از آن زمان تا کنون پیشرفت‌های بسیاری در این زمینه حاصل شده است. کاربرد مشبکه در سامانه‌های امنیت اطلاعات از سامانه‌های رمز کلید عمومی گرفته تا توابع چکیده‌ساز گسترش یافته است. در رمزنگاری مشبکه‌مبنا سامانه‌ها امنیت خود را از سختی حل مسائل مشبکه اخذ می‌کنند. مسائل یافتن کوتاهترین بردار و نزدیک‌ترین بردار در مشبکه از مسائل سخت به شمار می‌روند که تا کنون الگوریتمی، چه از نوع عادی (کلاسیک) و چه از نوع کوانتومی، برای حل آن‌ها در زمان معقول (چندجمله‌ای) ارائه نشده است. رمزنگاری

مبتنی بر مسائل نظریه اعداد، مانند تجزیه اعداد بزرگ و لگاریتم گسسته، که با الگوریتم‌های کوانتومی حل پذیرند، به تدریج جای خود را به رمزنگاری پساکوانتومی می‌دهد. ازاین‌رو، رمزنگاری مشبکه‌مبنا به عنوان یکی از انواع رمزنگاری‌های پساکوانتومی برای مقابله با تهدید الگوریتم‌های کوانتومی پیشنهاد شده است. همچنین سامانه‌های رمز مشبکه‌مبنا به دلیل سرعت زیاد اجرا نسبت به سامانه‌های رمز مبتنی بر نظریه اعداد برتری دارند.

در این درس به معرفی مشبکه و مسائل سخت مربوط به آن و نیز کاربردهای مشبکه در سامانه‌های رمز کلید عمومی، توابع چکیده‌ساز و امضای رقمی می‌پردازیم.

سر فصل‌های درس:

مقدمه ای بر مشبکه‌ها:

- تعاریف اولیه مشبکه، تعامد سازی گرام-اشمیت، کمینه‌های متوالی، قضیه مینکوفسکی.
- مسائل سخت در مشبکه‌ها: مسئله کوتاهترین بردار، مسئله نزدیکترین بردار.
- الگوریتم‌های تقریبی در حل مسائل سخت مشبکه‌ها: پایه کاهش یافته، الگوریتم کاهش پایه LLL، الگوریتم تقریبی CVP در بعد n.
- مشبکه q-ary و الگوریتم‌های یافتن کوتاهترین بردار.

رمزنگاری مشبکه‌مبنا:

- توابع چکیده‌ساز برخوردتاب،
- رمزنگاری‌های کلید عمومی Ajtai، GGH و NTRU.
- رمزنگاری مبتنی بر یادگیری همراه با خطا (LWE)،
- امضای رقمی مشبکه‌مبنا.

منابع:

1. Micciancio, Daniele, and Goldwasser Shafi. *Complexity of lattice problem: A cryptographic perspective.* The Kluver Intl. Series, Springer, 2002.

2. Bernstein Daniel J., Johannes Buchmann, and Erik Dahmen, *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 2008.

3. Hoffstein Jeffrey, Pipher Jill, Silverman Joseph H, *An Introduction to Mathematical Cryptography*, Chapter 6, Springer, 2008.

4. Galbraith Steven D., *Mathematics of Public Key Cryptography*, Part IV, Cambridge University Press, 1st Ed., 2012.

ارزیابی

۱- تمرینات درسی: ۳ نمره.

۲- حضور در کلاس: ۱ نمره.

۳- پروژه درس (گزارش و ارائه با اسلاید): ۳+۳ نمره.

۴- امتحان میان ترم: ۴ نمره.

۵- امتحان پایان ترم: ۶ نمره.

مشاوره

روزهای سه‌شنبه از ساعت ۱۶:۰۰ تا ۱۷:۰۰ با تعیین وقت قبلی.

تاریخ‌های مهم!

جلسه آغازین کلاس: دوشنبه ۱۴۰۱/۰۷/۲۸.

امتحان میان ترم: پنج‌شنبه ۱۴۰۱/۰۹/۰۳. ساعت ۹-۱۲

امتحان پایان ترم: طبق تقویم معاونت آموزشی دانشگاه: ۱۴۰۱/۱۰/۲۶، ساعت ۱۵.

جلسه پایانی کلاس: دوشنبه ۱۴۰۱/۱۰/۰۵.

ارائه سمینار نهائی دانشجویان (با نمایش اسلاید): شنبه ۱۴۰۱/۱۰/۱۰. ساعت ۹:۰۰ تا ۱۲:۰۰

تحویل گزارش نهائی پروژه (به‌صورت کتبی): شنبه ۱۴۰۱/۱۱/۰۸.