قطب علمی رمز

بسم الله الرحمن الرحیم

دانشگاه صنعتی شریف

مقدمه ای بر رمزنگاری کد مبنا

ترانه اقلیدس

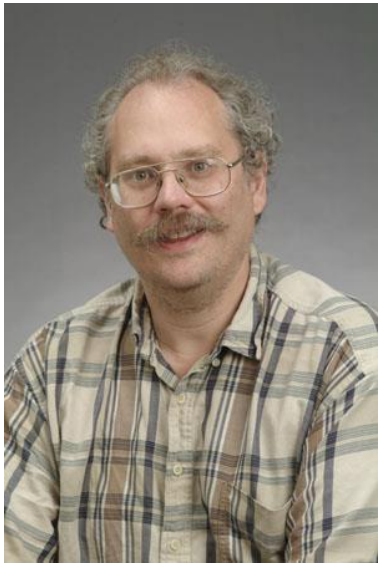
پژوهشکده الکترونیک– دانشگاه صنعتی شریف

teghlidos@sharif.edu

فهرست مطالب

تاریخچه

Robert J. McEliece
رمزنگاری کلید عمومی کدمبنا ۱۹۷۸



Peter W. Shor
الگوریتم کوانتومی برای تجزیه اعداد صحیح ۱۹۹۴

انگیزه

- کامپیوترهای کوانتومی سامانه های رمزنگاری مبتنی بر نظریه اعداد از قبیل RSA، El-Gamal و ECC را می شکنند. (الگوریتم Shor در سال ۱۹۹۴)
  - باید به دنبال راه های جدید باشیم.
  - شاید از اکنون دیگر امنیت نداریم. ذخیره داده های رمزشده توسط مهاجمین برای رمزگشایی در آینده!

- رمزنگاری پساکوانتومی با سامانه های رمزی سر و کار دارد، که
  - در کامپیوترهای مرسوم اجرا می شوند.
  - در برابر کامپیوترهای کوانتومی امن هستند.

انگیزه

- **چرا از هم اکنون نگران تهدید کامپیوترهای کوانتومی باشیم؟**
  - چرا به استفاده از RSA و ECDSA ادامه ندهیم؟ زمانی که کامپیوترهای کوانتومی بزرگ ساخته شوند، به استفاده از McEliece روی آوریم.
- به سه دلیل مهم توجه بخشی از جامعه رمزنگاری به رمزنگاری پساکوانتومی جلب شده است:
  - نیاز به زمان برای
    - بهبود کارآیی رمزنگاری پساکوانتومی،
    - اطمینان از رمزنگاری پساکوانتومی،
    - بهبود استفاده از رمزنگاری پساکوانتومی.
- بدون اقدام کنونی، در صورت نیاز فوری به رمزنگاری پساکوانتومی در آینده ای نزدیک، سال های بحرانی تحقیقات را از دست داده ایم.

رمزنگاری کوانتومی

- رمزنگاری کوانتومی یا "توزیع کلید کوانتومی" : گسترش یک کلید کوتاه به اشتراک گذاشته شده به یک رشته نامتناهی مشترک کاربردی.
- **پیش نیاز رمزنگاری کوانتومی**
  - دانش طرفین ارتباط (کاربران) از کلید مخفی غیر قابل پیشگویی.
- **نتیجه رمزنگاری کوانتومی**
  - افزایش طول رشته خروجی (به طور خطی) بر حسب زمانی که طرفین ارتباط روی رمزنگاری کوانتومی صرف می کنند.
- این توصیف از رمزنگاری کوانتومی شبیه به رمز جریانی است، ولی جزئیات رمزنگاری کوانتومی کاملاً متفاوت از جزئیات رمز جریانی است.
- اگر رمزنگاری کوانتومی به طور کامل پیاده سازی شود، آنگاه امنیت آن از قوانین پذیرفته شده عام مکانیک کوانتومی پیروی می کند.

مقایسه رمزنگاری پساکوانتومی با رمزنگاری کوانتومی

رمزنگاری پساکوانتومی، در حالت کلی، عنوان کاملاً متفاوتی از رمزنگاری کوانتومی است:

رمزنگاری پسا کوانتومی حوزه وسیعی از ارتباطات امن، از عملیات کلید مخفی، امضاهای کلید عمومی و رمزگذاری کلید عمومی تا عملیات سطح بالا مانند رأی گیری الکترونیکی امن را پوشش می دهد.	**رمزنگاری کوانتومی** تنها یک کار انجام می دهد: گسترش یک کلید مخفی به اشتراک گذاشته شده کوتاه به کلید مشترک بلند.
رمزنگاری پسا کوانتومی، شامل سامانه هایی است که امنیت آن ها اثبات شده است یا حدس زده می شود که امن هستند.	**رمزنگاری کوانتومی** سامانه های حدسی را رد می کند–با این پرسش که چگونه آلیس و باب می توانند به طور امن یک راز (کلید رمزنگاری) را تسهیم کنند.
رمزنگاری پسا کوانتومی نیازی به هیچ سخت افزار جدیدی ندارند.	**رمزنگاری کوانتومی** نیازمند سخت افزار شبکه جدیدی است، که در حال حاضر برای اکثر کاربران اینترنتی بسیار (به طور امکان ناپذیری) گران است.

رمزنگاری پساکوانتومی

- نمونه هایی از طرح های رمزنگاری پساکوانتومی:
  - رمزنگاری کدمبنا (McEliece)
  - رمزنگاری مشبکه مبنا (NTRU)
  - رمزنگاری مبتنی بر چکیده ساز (طرح درخت چکیده ساز Merkle)
  - رمزنگاری مبتنی بر معادلات درجه دوم چندمتغیره (HFE)

رمزنگاری کدمبنا

- رمزنگاری کدمبنا یکی از نامزدهای برجسته در رمزنگاری پساکوانتومی است.
- استفاده از کدهای تصحیح خطا برای دستیابی به امنیت،
  - امنیت بر اساس مسائل سخت نظریه کدینگ.
- بهترین حملات به سامانه های رمز کدمبنا، از جمله McEliece، به صورت مستقیم از الگوریتم های کدگشایی کدهای خطی استفاده می کنند.
- مسائل کدگشایی مبتنی بر سندروم و کدگشایی کدهای عام از دسته مسائل NP-hard هستند.
- به دست آوردن انواع سامانه های رمزنگاشتی از قبیل توابع چکیده ساز، رمزهای جریانی، احراز اصالت، امضای دیجیتال، طرح های تسهیم راز، مولدهای اعداد تصادفی و رمزگذاری (متقارن و همگانی).

رمزنگاری کدمبنا

- اولین سامانه رمزنگاری کدمبنا: طرح رمزگذاری کلید همگانی McEliece در سال ۱۹۷۸.
  - تا کنون هیچ حمله ای که نشان از تهدید جدی به این سامانه باشد، حتی روی یک کامپیوتر کوانتومی، شناخته نشده است.

- مزیت های سامانه های رمز کد مبنا:
  - سرعت زیاد،
  - سادگی پیاده سازی،
  - قابلیت استخراج انواع مختلف اولیه‌های رمزنگاری (Primitives).

مراجع

- Bernstein D. J., Buchmann J., Dahmen E., “Post-Quantum Cryptography,” Springer 2009, ISBN: 978-3-540-88701-0, e-ISBN: 978-3-540-88702-7.

با تشکر از توجه شما!