高级密码组件及其应用
教学大纲

陈宇
山东大学
cycosmic@gmail.com

课程信息

课时/学分: 32/2

课程属性: 专业选修课

主讲教师： 陈宇

中文名称: 高级密码组件及其应用

英文名称： Advanced Cryptographic Primitives and Their Applications

教学目的、要求
本课程重点介绍理论密码学中的高级密码组件, 旨在使学生精通若干高级密码组件 (包括各类高级单向函数、程序混淆和受限伪随机函数、不可延展非交互式证明、哈希证明系统等) 的概念和构造, 并掌握其在公钥密码学中的重要应用。本课程旨在帮助学生在《理论密码学》课程之上进一步拓宽加深密码理论基础, 追踪科研前沿进展.

预修课程: 理论密码学 (强烈建议选课同学课前阅读相关参考文献)

主要内容

第一讲: 公钥加密简介 (学时:3+1) [NS09, DFMV13, Wee16]

- 公钥加密的 KEM-DEM 构造方法
- 公钥加密的传统安全
- 超越传统语义安全: 抗泄漏安全、抗篡改安全、消息相关密钥安全

第二讲: 高级单向函数 I(学时:3+1) [PW08, CQX18]

1. 有损陷门函数的概念、构造
2. 有损陷门函数的应用
3. 有损陷门函数的重要扩展

第三讲: 高级单向函数 II(学时:3+1) [RS09, KMO10]

1. 相关积陷门单向函数的概念与构造
2. 自适应单向陷门函数的概念与构造
3. 自适应单向陷门函数的应用

第四讲: 非交互式零知识证明及其应用 (学时:3+1) [NY90, DDN91, Sah99]

1. Naor-Yung 双重加密范式
2. Dolev-Dwork-Naor 构造
3. 不可延展非交互式零知识证明及其应用

第五讲: 哈希证明系统及其应用 (学时:3+1) [CS02, QL13, Wee16]

1. 哈希证明系统的定义及构造
2. 哈希证明系统在 CCA 安全中的应用
3. 哈希证明系统在 KDM 安全和抗泄漏安全中的应用

第六讲: 可提取哈希证明系统及其应用 (学时:3+1) [Wee10]

1. 可提取哈希证明系统的定义及构造
2. 可提取哈希证明系统在 CCA 安全中的应用
3. 自适应单向陷门关系

第七讲: 程序混淆与受限伪随机函数 (学时:3+1) [BGI$^+$01, BW13, SW14]

1. 程序混淆的概念与构造
2. 受限伪随机函数的概念
3. 程序混淆与受限伪随机函数的应用

第八讲: 可公开求值伪随机函数 (学时:3+1) [CZ14, CWZ18]

1. 可公开求值伪随机函数的概念与构造

2. 可公开求值伪随机函数的应用

3. 可穿孔可公开求值伪随机函数及其在抗泄漏密码学中的应用

参考文献

[BGI$^+$01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18. Springer, 2001.

[BW13] Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In *Advances in Cryptology - ASIACRYPT 2013*, volume 8270 of *LNCS*, pages 280–300. Springer, 2013.

[CQX18] Yu Chen, Baodong Qin, and Haiyang Xue. Regularly lossy functions and their applications. In *Topics in Cryptology - CT-RSA 2018*, pages 491–511, 2018.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *Advances in Cryptology - EUROCRYPT 2002*, pages 45–64, 2002.

[CWZ18] Yu Chen, Yuyu Wang, and Hong-Sheng Zhou. Leakage-resilient cryptography from puncturable primitives and obfuscation. In *Advances in Cryptology - ASIACRYPT 2018*, pages 575–606, 2018.

[CZ14] Yu Chen and Zongyang Zhang. Publicly evaluable pseudorandom functions and their applications. In *9th International Conference on Security and Cryptography for Networks, SCN 2014*, pages 115–134, 2014.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *STOC*, pages 542–552. ACM, 1991.

[DFMV13] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, and Daniele Venturi. Bounded tamper resilience: How to go beyond the algebraic barrier. In *Advances in Cryptology - ASIACRYPT 2013*, volume 8270 of *LNCS*, pages 140–160. Springer, 2013.

[KMO10] Eike Kiltz, Payman Mohassel, and Adam O'Neill. Adaptive trapdoor functions and chosen-ciphertext security. In *Advances in Cryptology - EUROCRYPT 2010*, pages 673–692, 2010.

[NS09] Moni Naor and Gil Segev. Public-key cryptosystems resilient to key leakage. In

Advances in Cryptology - CRYPTO 2009, volume 5677 of *LNCS*, pages 18–35. Springer, 2009.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the 22th Annual ACM Symposium on Theory of Computing, STOC 1990*, pages 427–437. ACM, 1990.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008*, pages 187–196, 2008.

[QL13] Baodong Qin and Shengli Liu. Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter. In *Advances in Cryptology - ASIACRYPT 2013*, volume 8270 of *LNCS*, pages 381–400. Springer, 2013.

[RS09] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. In *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009*, volume 5444 of *LNCS*, pages 419–436. Springer, 2009.

[Sah99] Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS 1999*, pages 543–553. ACM, 1999.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Symposium on Theory of Computing, STOC 2014*, pages 475–484. ACM, 2014.

[Wee10] Hoeteck Wee. Efficient chosen-ciphertext security via extractable hash proofs. In *Advances in Cryptology - CRYPTO 2010*, volume 6223, pages 314–332, 2010.

[Wee16] Hoeteck Wee. Kdm-security via homomorphic smooth projective hashing. In *Public-Key Cryptography - PKC 2016*, volume 9615 of *LNCS*, pages 159–179. Springer, 2016.