Summarize of ZJU Crypto-School

2023 年 7 月 10 日

CryptoSchool 讲了什么?

课程从零基础开始讲解现代密码学的重要范式–可证明安全。在可证明安全的框架下，深入浅出讲解安全多方计算、通用可组合 (Universal Composability) 安全、不可微分 (Indifferentiability) 安全、黑盒技术、非黑盒技术、简洁非交互式零知识证明、格基密码学等。

主讲人	课程
张秉晟（浙江大学）	可证明安全基础/安全多方计算
Hong-Sheng Zhou（Virginia Commonwealth University）	通用可组合安全
Yi Deng（信工所）	黑盒和非黑盒技术
张聪（浙江大学）	理想模型/不可微分安全
Feng-Hao Liu Washington State University	格密码
胡云聪（上海交通大学）	SNARK

CryptoSchool 讲了什么?

- 视频回放见 B 站“OpenMPC 开放隐私计算”
- 笔记分享见微信公众号“隐私计算研习社”

1 整体介绍

2 可证明安全
- Provable Security Basis
- Universal Composability
- Black-box Reduction
- Indifferentiability

3 安全多方计算

4 NIZK

5 Lattice-based Crypto

6 参考文献

Provable Security

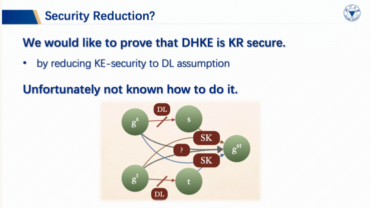
Three Steps of Provable Security:

- Precisely specify threat model
    - Formal model and definition of what security means
- Propose a construction
    - Algorithm, protocol, scheme
- Write a formal proof
    - Formalize the security of Protocol XXX
    - Decide on XXX assumption
    - Provide a proof by reduction

Security Reduction

We would like to prove DHKE is Key Recovery secure

- by reducing to Discrete Logarithm Problem ✗
- by reducing to Computational Diffie-Hellman Problem ✓



We would like to prove DHKE is Indistinguishable (IND) secure

- by reducing to Decisional Diffie-Hellman Problem ✓

Contradistinction

- DL: Given g, g^a, compute a;
- CDH: Given (g^a, g^b), compute g^{ab};
- DDH: Given (g^a, g^b, g^{ab}) and (g^a, g^b, g^u), determine distribution.

DDH≤CDH≤DL

Security Reduction

进一步学习安全规约/可证明可以看郭福春老师的课程

Universal Composability

什么是安全？

- 对于多方安全计算而言，“安全”至少要保障计算各方私有的输入不泄露；
- 对于零知识证明而言，“安全”至少要保障证明方 (Prover) 私有的证明不泄露。
- 更严格地，密码学定义的“安全”指的是不泄露关于私有输入的任何信息（泄露信息量为零)。

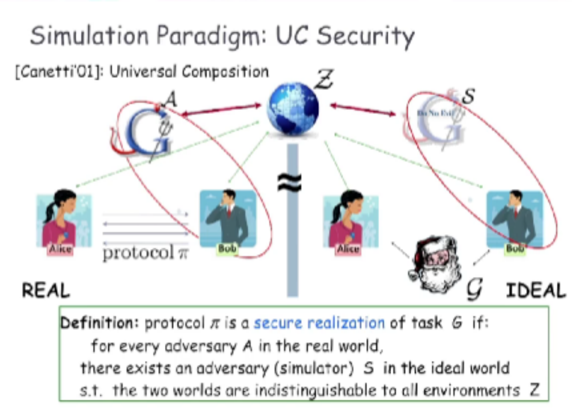
如何证明协议是安全的，参与者确实没有以某种形式泄露秘密呢？

Approach

安全性证明主要有两种，一个是基于属性的，即博弈论的方式来证明安全性；另一种是基于模拟的。

- Property-based (game-based)
  - CPA/CCA-security in encryption
  - Completeness, soundness, zero-knowledge property in ZK proofs
- Simulation-based
  - NIZK
  - Secure Computation

在“Ideal World”中，模拟器没有原始秘密值，如果能找到一种方式“骗过”所有对手，让对手分不清“Real World”和“Ideal World”，则称协议满足“Simulation-Based Security”



More

实例：

- 地图 3 色问题证明
- Schnorr's Protocol

更多资料参考

- Universally composable security: A new paradigm for cryptographic protocols[Can01]
- How to simulate it–a tutorial on the simulation proof technique[Lin17]

What is Black-box Reduction

在当前密码学基础的大部分工作中，密码协议并没有被证明是无条件安全的，相反，它们的安全性被规约为看似较弱或较简单的原语的安全性。

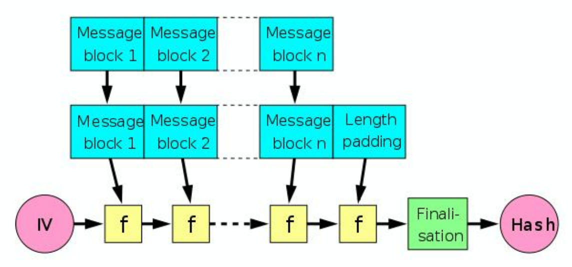
- 如单向函数、伪随机发生器、伪随机函数和签名方案，已经证明一个可以从另一个构建 [HILL99, GGM86, Rom90]。

在很大程度上，这些归约是黑盒的，因为它们仅通过输入-输出行为来考虑原语和/或对手对构造的影响，而不依赖于原语或对手的代码等内部因素 [BBF13]。

- 最早是由 Impagliazzo 和 Rudich[IR89] 提出， Reingold 等人进行了详细分类 [RTV04]:Fully BBR, SemiBBR, Weakly BBR.

Merkle-Damgård Construction

CRYPTO 1989, Merkle 和 Damgård 提出了一种散列函数构造，声称只要函数 f 具有某些理想的性质，所得到的散列函数就保证是抗碰撞的。



'length extension attack'

What is a secure hash function?

Key Point: Collision resistance & Pre-image resistance.

We want hash functions to be **random oracles**.

- 随机预言机是一个完全随机的函数
- 随机函数输出是随机的，而且具有抗碰撞和抗原像性。

为了评估这样的随机函数，提出了 **random oracle model**

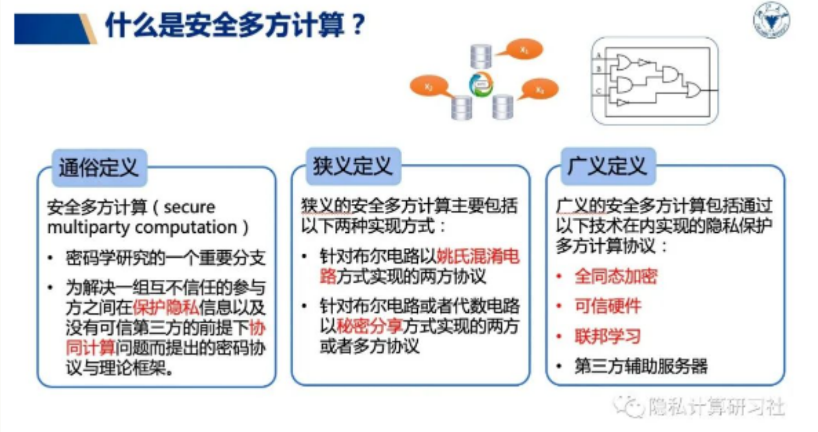
In 2004, Maurer et al. 给出了怎样构建一个随机预言机:

it' s always possible to replace functionality A (e.g., a random oracle) with another functionality B (e.g., an ideal compression function) provided that the following rules are satisfied:

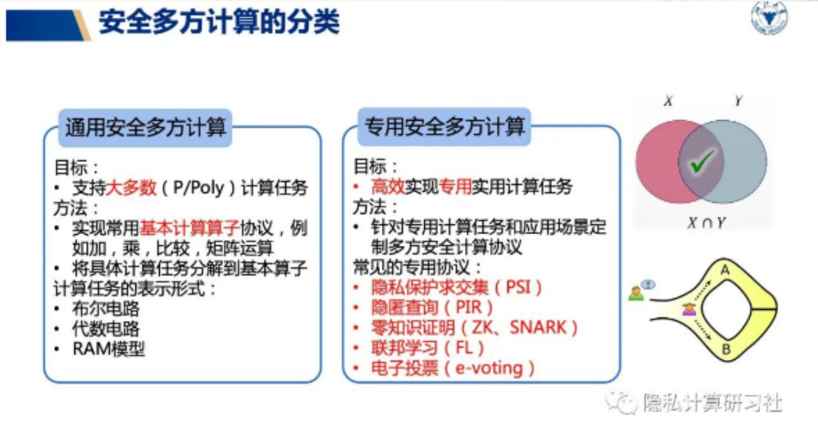
- There exists a way to 'construct' something 'like' A out of B.
- There exists a way to 'simulate' something 'like' B using A.
- An attacker who interacts with constructed A-like thing, B cannot tell the difference (i.e., can' t differentiate it) from A, simulated B-like thing.

参考 Matthew Green's blog

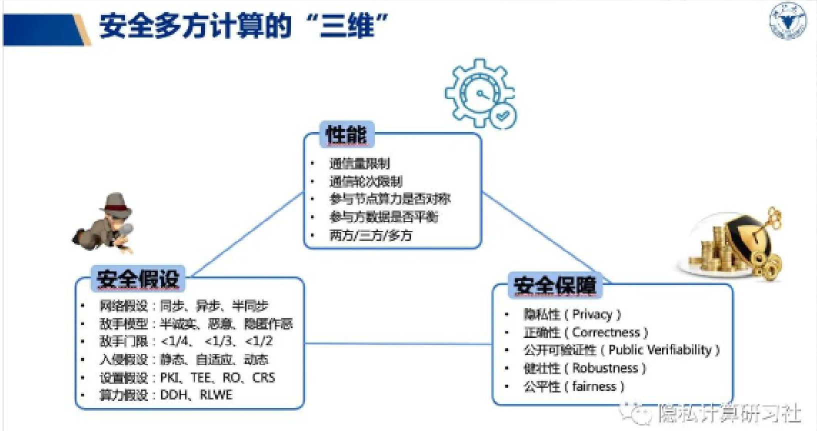
什么是安全多方计算


什么是安全多方计算？
通俗定义
安全多方计算（secure multiparty computation）
• 密码学研究的一个重要分支
• 为解决一组互不信任的参与方之间在保护隐私信息以及没有可信第三方的前提下协同计算问题而提出的密码协议与理论框架。
狭义定义
狭义的安全多方计算主要包括以下两种实现方式：
• 针对布尔电路以姚氏混淆电路方式实现的两方协议
• 针对布尔电路或者代数电路以秘密分享方式实现的两方或者多方协议
广义定义
广义的安全多方计算包括通过以下技术在内实现的隐私保护多方计算协议：
• 全同态加密
• 可信硬件
• 联邦学习
• 第三方辅助服务器
隐私计算研习社

安全多方计算的分类


安全多方计算的分类
通用安全多方计算
目标：
• 支持大多数（P/Poly）计算任务
方法：
• 实现常用基本计算算子协议，例如加，乘，比较，矩阵运算
• 将具体计算任务分解到基本算子
计算任务的表示形式：
• 布尔电路
• 代数电路
• RAM模型
专用安全多方计算
目标：
• 高效实现专用实用计算任务
方法：
• 针对专用计算任务和应用场景定制多方安全计算协议
常见的专用协议：
• 隐私保护求交集（PSI）
• 隐匿查询（PIR）
• 零知识证明（ZK、SNARK）
• 联邦学习（FL）
• 电子投票（e-voting）
X
Y
X ∩ Y
A
B
隐私计算研习社

安全多方计算的“三维”

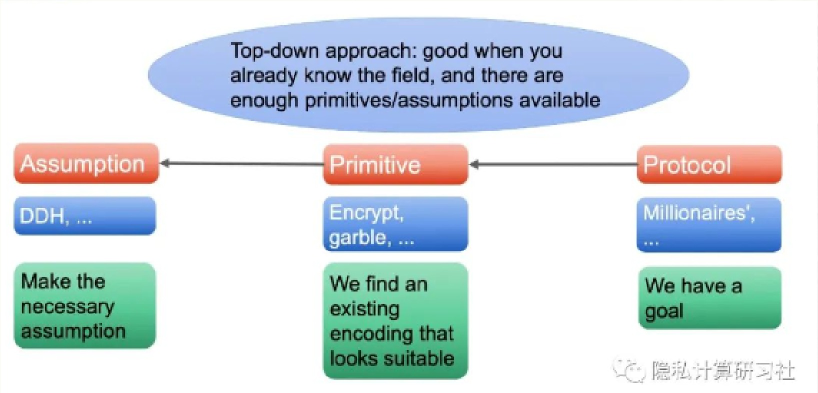

安全多方计算的“三维”
性能
通信量限制
通信轮次限制
参与节点算力是否对称
参与方数据是否平衡
两方/三方/多方
安全假设
网络假设：同步、异步、半同步
敌手模型：半诚实、恶意、隐匿作恶
敌手门限：<1/4、<1/3、<1/2
入侵假设：静态、自适应、动态
设置假设：PKI、TEE、RO、CRS
算力假设：DDH、RLWE
安全保障
隐私性（Privacy）
正确性（Correctness）
公开可验证性（Public Verifiability）
健壮性（Robustness）
公平性（fairness）
隐私计算研习社

协议设计思路

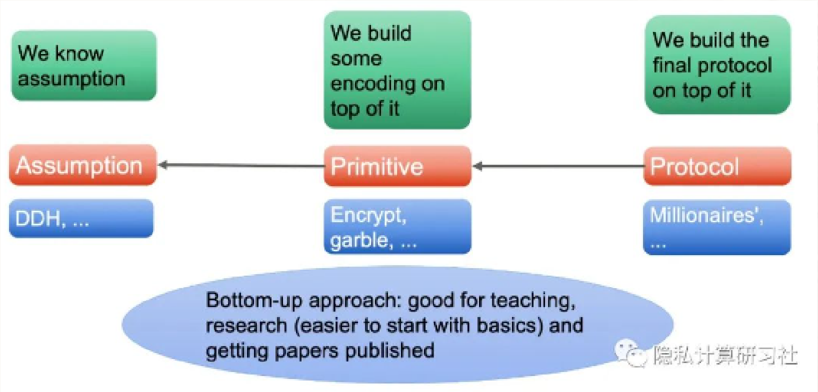
设计思路可以分为自顶向下/自底向上，主要包括三个层次：

- 协议：密码学中的最高层次，如 MPC 协议，PSI 协议等；
- 原语：密码学工具及算法，如加密、数字签名等；
- 假设：任何的协议和原语的安全性都依赖于一些假设，比如求解离散对数问题是困难，求解大整数分解问题是困难。

协议设计思路


Top-down approach: good when you already know the field, and there are enough primitives/assumptions available
Assumption
Primitive
Protocol
DDH, ...
Encrypt, garble, ...
Millionaires', ...
Make the necessary assumption
We find an existing encoding that looks suitable
We have a goal
隐私计算研习社

协议设计思路


We know assumption
We build some encoding on top of it
We build the final protocol on top of it
Assumption
Primitive
Protocol
DDH, ...
Encrypt, garble, ...
Millionaires', ...
Bottom-up approach: good for teaching, research (easier to start with basics) and getting papers published
隐私计算研习社

两方安全计算协议设计

- 基于 Elgamal
- 基于 Lift Elgamal（同态性质）
- Example: Hamming Distance

OT 协议

不经意传输（Oblivious Transfer），也称“茫然传输”，是密码学中的一类协议，实现了发送方将潜在的许多信息中的一个传递给接收方，但对接收方所接收信息保持未知状态。

假设某机构拥有 N 个学校的考研资料，小美想买 A 学校的，但是小美非常在意自己的隐私，不希望向机构泄露自己的目标院校是哪里。因此双方希望这笔交易能够满足以下隐私条件：

- 小美不希望泄露“我准备考 A 学校”这一信息；
- 旅行社只希望出售小美出钱购买的那份资料，而不泄露小美未购买的 N-1 份资料

History of OT

- First related protocol: "Conjugate coding" (1970s)
- Rabin's OT (1981) [Rab05]
- 1-out-of-2 OT, Even et al. (1982) [EGL85]
- 1-out-of-n OT, Brassard et al. (1986) [BCR86]
- Beaver 96 [Bea96]
- IKNP 03 (实用) [IKNP03]
- ……

Basics Construction about OT

- Rabin's OT ⇒ (1,2)-OT
- Random OT ⇒ (1,2)-OT
- (1,2)-OT ⇒ (1,n)-OT
- ……

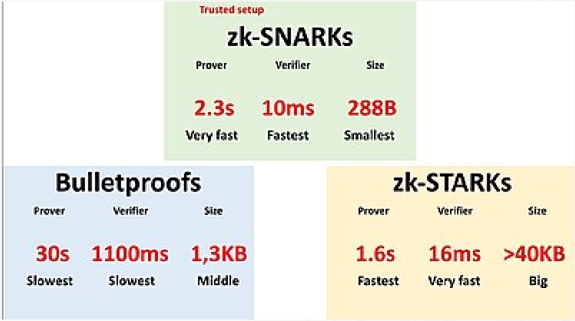
What is NIZK?

Non-interactive zero-knowledge (NIZK) proofs are cryptographic primitives, where information between a **prover** and a **verifier** can be authenticated by the prover, without revealing any of the specific information beyond the validity of the statement itself[GK96].

- Advantage: **Non-interactive**. It is widely used in distributed systems such as blockchain.
- Based on mathematical constructs like elliptic curve / pairing-based cryptography.
- verifiable proofs are **short** and **easily verifiable**.

Famous Protocol

- zk-SNARK, Alessandro Chiesa et al., 2012 [BCCT12]
- Bulletproofs, Benedikt, Boneh et al., 2017 [BBB$^+$18]
- zk-STARK, Ben-Sasson et al., 2018 [BSBHR18]



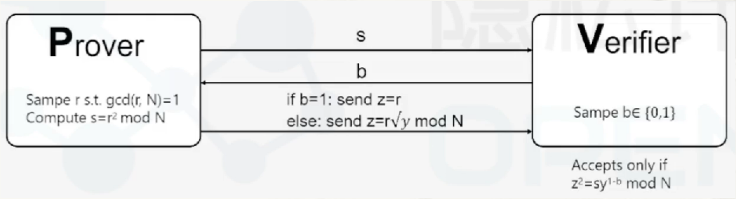
What is zkSNARK

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

- An **argument** system satisfying the following properties:
  - **Zero-knowledge**: the verifier learns nothing from the proof
  - **Succinctness**: the proof size and verification time is subliner to the statement and input
  - **Non-interactive**: A single round protocol
  - **Argument of knowledge**(knowledge soudness): similar to proof of knowledge but the prover is computationally bounded knows the witness.
  - **Completeness** and **Soundness**

Example: QR

$$QR = \{(N, y) : \exists x \ s.t. \ y = x^2 \ mod \ N\}$$



- **Soundness**: If the claim is false, the verifier will accept with probabilty $\leq \frac{1}{2}$. Repeat to decrease the cheating probability.
- **Knowledge Soundness**: the extractor can rewind the prover to obtain r and thus reconstruct $\sqrt{y}$

Why zkSNARK?

- A powerful tool for providing **privacy** and **scalability**
  - zero-knowledge allows the prover to reveal only necessary information
  - succinctness enables efficient outsourcing computation
  - especially useful in decentralized systems
- Examples:
  - private transactions over public blockchains
  - scalablity: proof-based Rollups (zkRollup)
  - Bridging blockchains: proof of consensus (zkBridge)

更多资料请参考安比实验室-零知识证明学习资源汇总

Why Lattice?

Perfect Security e.g. OTP

- impractical

Computational Security e.g. RSA, DL, ECC

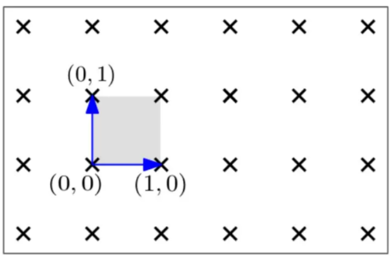
- be challenged with Riemann hypothesis, Quantum computer (e.g. Shor Alg.)...

What are the difficult problems in the post-quantum era?

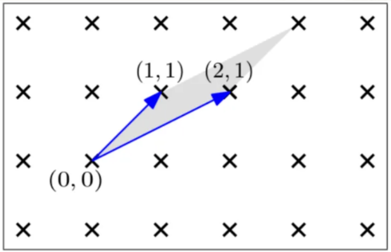
Distinguish between **quantum cryptography** and **post-quantum cryptography**.

What is Lattice

Definition: In linear algebra, a lattice $L \subset \mathbb{R}^n$ is the set of all integer linear combinations of vectors from a basis $\{\mathbf{b_1}, \cdots \mathbf{b_n}\}$ of $\mathbb{R}^n$. In other words, $L = \{\sum a_i \mathbf{b_i} : a_i \in \mathbb{Z}\}$



$\Lambda = \mathbb{Z}^n$



$\Lambda = B \cdot \mathbb{Z}^n : B \in \mathbb{R}^{d \times n}$

SIS Problem

SIS（Short Integer Solution） Problem[Ajt96]

Let $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$, $x = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$

Easy to get x from $Ax = 0$ (via Gaussian elimination)
What if some restrictions are added to x ?

$x_i \in \mathbb{Z}_q^n$ and $\|x\| \leq d$

LWE

LWE (Learning With Errors) Problem[Reg09]

$$\text{Let } A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix}$$

Easy to get x from $Ax = b$ (via Gaussian elimination)
What if we add "noise" to the left side of the equation?

$$Ax + e = b \text{ where } e = \begin{pmatrix} e_1 \\ e_2 \\ \cdots \\ e_n \end{pmatrix}$$

More Info

Daniele Micciancio (UCSD)

COURSE: Lattices Algorithms and Applications

LECTURE

BOOK:Complexity of lattice problems: a cryptographic perspective

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108, 1996.

[BBB+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE symposium on security and privacy (SP)*, pages 315–334. IEEE, 2018.

[BBF13] Paul Baecher, Christina Brzuska, and Marc Fischlin. Notions of black-box reductions, revisited. In *Advances in Cryptology-ASIACRYPT 2013: 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I 19*, pages 296–315. Springer, 2013.

[BCCT12] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 326–349, 2012.

[BCR86] Gilles Brassard, Claude Crépeau, and Jean-Marc Robert. All-or-nothing disclosure of secrets. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 234–238. Springer, 1986.

[Bea96] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 479–488, 1996.

[BSBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive*, 2018.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[GK96] Oded Goldreich and Hugo Krawczyk. On the composition of zero-knowledge proof systems. *SIAM Journal on Computing*, 25(1):169–192, 1996.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In *Annual International Cryptology Conference*, pages 145–161. Springer, 2003.

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 44–61, 1989.

[Lin17] Yehuda Lindell. How to simulate it–a tutorial on the simulation proof technique. *Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich*, pages 277–346, 2017.

[Rab05] Michael O Rabin. How to exchange secrets with oblivious transfer. *Cryptology ePrint Archive*, 2005.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[Rom90] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 387–394, 1990.

[RTV04] Omer Reingold, Luca Trevisan, and Salil Vadhan. Notions of reducibility between cryptographic primitives. In *Theory of Cryptography Conference*, pages 1–20. Springer, 2004.

Best Wishes!