多方零知识证明系统的设计与实现

硕士学位答辩

崔泓睿
上海交通大学
2022 年 1 月 10 日

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目录

第 1 节

课题研究问题背景

第 1 节

课题研究问题背景

第 1 小节

问题背景

多方借贷问题

公司

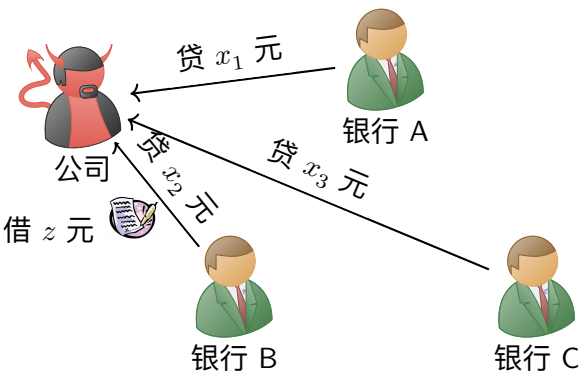
银行 A

银行 B

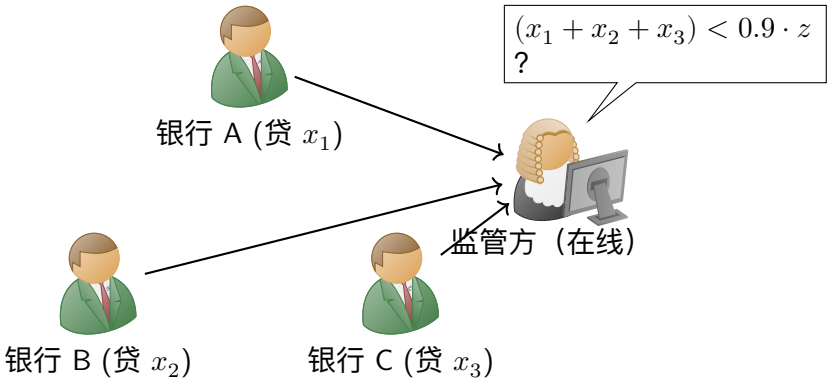
银行 C

多方借贷问题

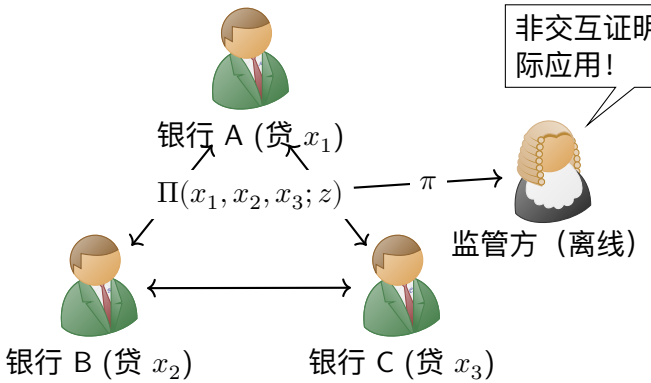
多方借贷问题



多方借贷问题



多方借贷问题



第 1 节

课题研究问题背景

第 2 小节

功能刻画

多方零知识证明

对于 $\mathcal{NP}$ 关系的证明功能

$$\mathcal{F}^{\mathsf{mpzk}}(\underbrace{x_1,\ldots,x_m}_{m\ \text{证明方}};\ \underbrace{y}_{1\ \text{验证方}}) \mapsto \mathcal{R}(x_1,\ldots,x_m;y)$$

其中 $\mathcal{R}$ 定义了一个 $\mathcal{NP}$ 关系

多方零知识证明

对于 $\mathcal{NP}$ 关系的证明功能

$$\mathcal{F}^{\mathsf{mpzk}}(\underbrace{x_1,\ldots,x_m}_{m\ \text{证明方}};\ \underbrace{y}_{1\ \text{验证方}}) \mapsto \mathcal{R}(x_1,\ldots,x_m;y)$$

其中 $\mathcal{R}$ 定义了一个 $\mathcal{NP}$ 关系

- 当 $m=1$，退化为传统零知识定义
- 若验证方只需广播随机数，我们可以通过 FS/BCS 转换实现 RO 模型下的非交互证明[1-2]

第 2 节

国内外研究进展

第 2 节

国内外研究进展

第 1 小节

多方计算下的零知识

多方计算 + 零知识

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

完备性结论下的解决方案

- 可以在通用多方计算协议下计算函数 $\mathcal{F}^{\text{mpzk}}$
- GCZK 的构造遵循此框架[3-5]

多方计算 + 零知识

完备性结论下的解决方案

- 可以在通用多方计算协议下计算函数 $\mathcal{F}^{\text{mpzk}}$
- GCZK 的构造遵循此框架[3-5]

讨论

- 缺点：无法使用通用转换实现非交互证明

多方计算 +zk-SNARK

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

使用进阶构造

多方计算框架下，多个证明方可以分布式地运行 zk-SNARK 的证明电路

多方计算 +zk-SNARK

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

使用进阶构造

多方计算框架下，多个证明方可以分布式地运行 zk-SNARK 的证明电路

讨论

- 假设协议有 3 轮消息 (a, c, z)
- 若直接输出 (a, c, z)，需要多方计算某种哈希函数
- 若分解为 MPC1$(\vec{w}, x) \mapsto (a, \vec{s})$，$c = H(a)$，MPC2$(\vec{w}, x, c, \vec{s}) \mapsto z$ 则需要保证 MPC1/2 之间的一致性

第 2 节

国内外研究进展

第 2 小节

公开可验证的多方计算

公开可验证的多方计算

功能非常相似的原语

- PV-MPC 允许任意外部参与方验证计算过程的正确性
- 这一性质满足多方零知识的需求

公开可验证的多方计算

功能非常相似的原语

- PV-MPC 允许任意外部参与方验证计算过程的正确性
- 这一性质满足多方零知识的需求

不足之处

然而现有工作存在显著缺陷

- Baum 等人的工作依赖公告板—不可篡改的广播，无法由标准假设蕴含[6-7]
- Schoenmakers 与 Veeningen 的工作依赖大多数节点诚实来保证隐私性[8]

第 2 节

国内外研究进展

第 3 小节

分布式零知识

分布式的零知识证明

秘密分享形式的证明实例

- Boneh 等人在 2019 年提出了“秘密分享数据上的零知识”[9]
- 在他们的定义下，单个证明方持有完整的 x，而多个验证方持有分享数据 $(x_1, \ldots, x_n)$
- 这一原语主要用来提升多方计算的安全性[10]

分布式的零知识证明

秘密分享形式的证明实例

- Boneh 等人在 2019 年提出了“秘密分享数据上的零知识”[9]
- 在他们的定义下，单个证明方持有完整的 x，而多个验证方持有分享数据 $(x_1, \ldots, x_n)$
- 这一原语主要用来提升多方计算的安全性[10]

结论

- 除了格式接近，与我们需要的功能均没有明显关联

第 3 节

基于头脑模拟的多方零知识

第 3 节

基于头脑模拟的多方零知识

第 1 小节

基础定义

NP 关系

$\mathcal{NP}$ 关系的电路定义

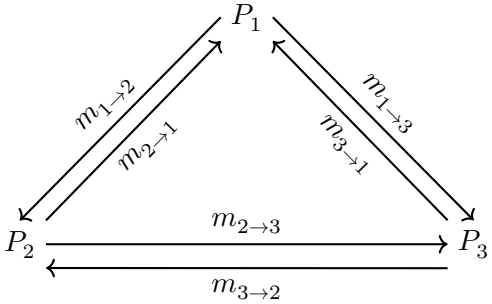
我们用电路模型刻画 $\mathcal{NP}$ 关系：$\mathcal{R}(x,w)=C(x,w)$，其中 $C:\{0,1\}^*\to\{0,1\}$ 为验证电路

扩展的验证电路

对于一个给定的验证电路 C，我们定义作用在 w 的扩展上的验证电路 $C^{\mathsf{ext}}(x,w_1,...,w_n)=C(x,\sum w_i)$

多方计算

考虑三方计算布尔电路 $C(x_1, x_2, x_3)$



$P_1 : x_1 \qquad V_1$

$P_2 : x_2 \xrightarrow{\text{MPC}} V_2$

$P_3 : x_3 \qquad V_3$

- 定义“视图”$V_i := (x_i, r_i, m_{*\to i})$
- 正确性：$P(V_i) = C(x_1, x_2, x_3)$
- 安全性：$V_i \approx \mathsf{Sim}(x_i, C(x_1, x_2, x_3))$

第 3 节

基于头脑模拟的多方零知识

第 2 小节

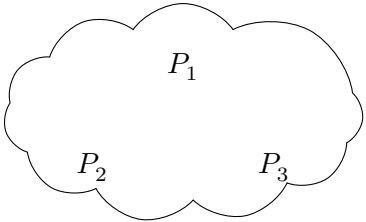
通用构造

传统头脑模拟框架

证明方

验证方

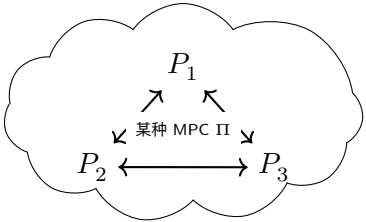
传统头脑模拟框架



证明方

验证方

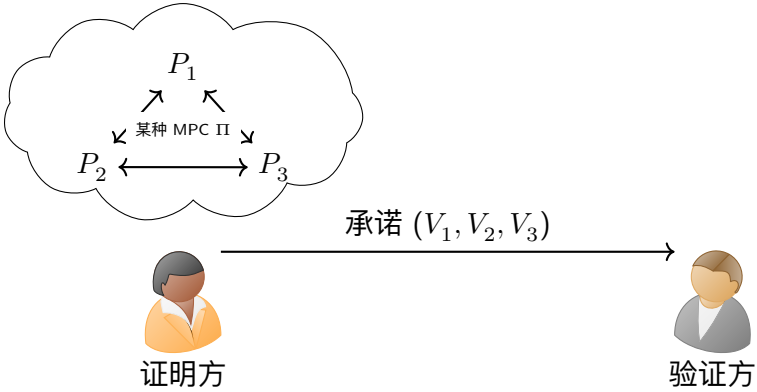
传统头脑模拟框架



证明方

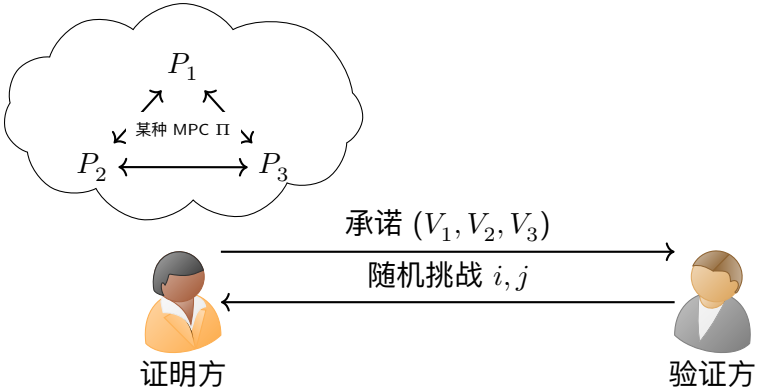
验证方

传统头脑模拟框架



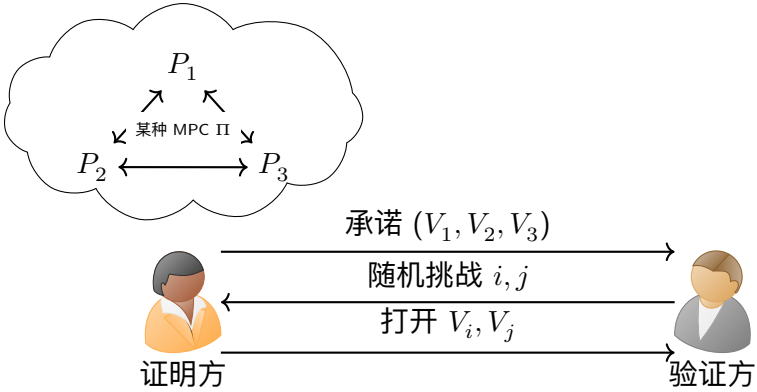
- 承诺可以由单向函数假设蕴含

传统头脑模拟框架



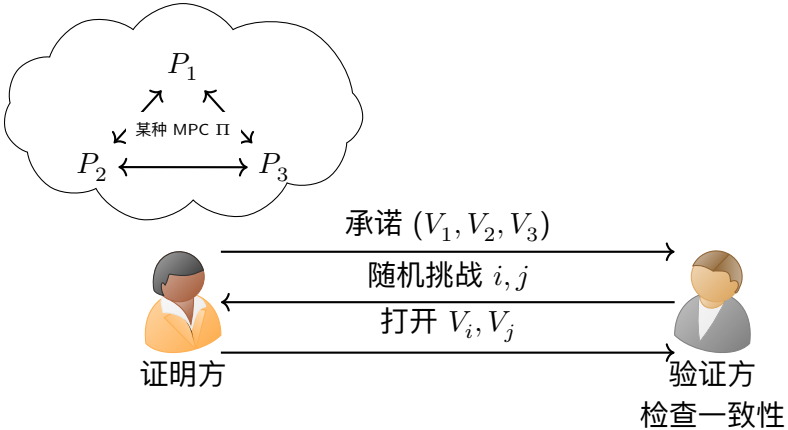
- 承诺可以由单向函数假设蕴含
- 随机挑战的不可预测性保证证明的可靠性

传统头脑模拟框架



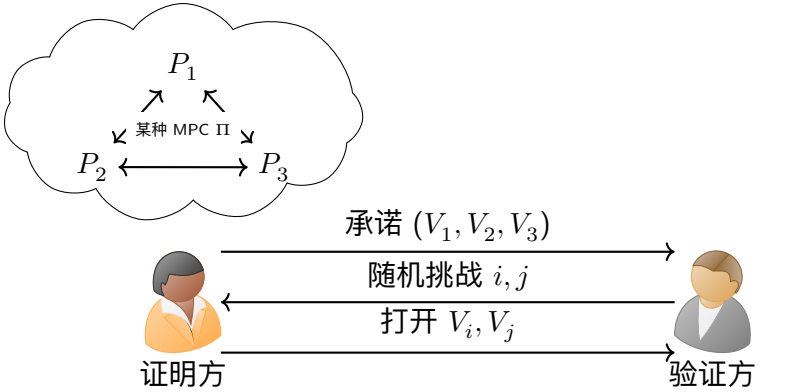
- 承诺可以由单向函数假设蕴含
- 随机挑战的不可预测性保证证明的可靠性
- 一致性检查通过模拟 P_i, P_j 实现

传统头脑模拟框架



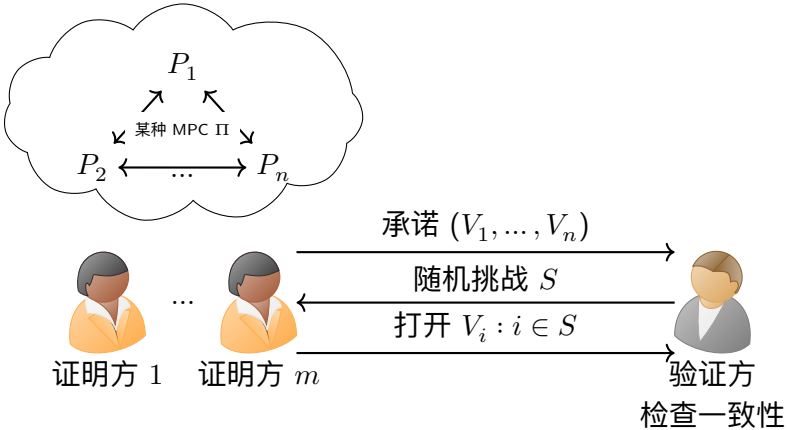
- 承诺可以由单向函数假设蕴含
- 随机挑战的不可预测性保证证明的可靠性
- 一致性检查通过模拟 P_i, P_j 实现

传统头脑模拟框架



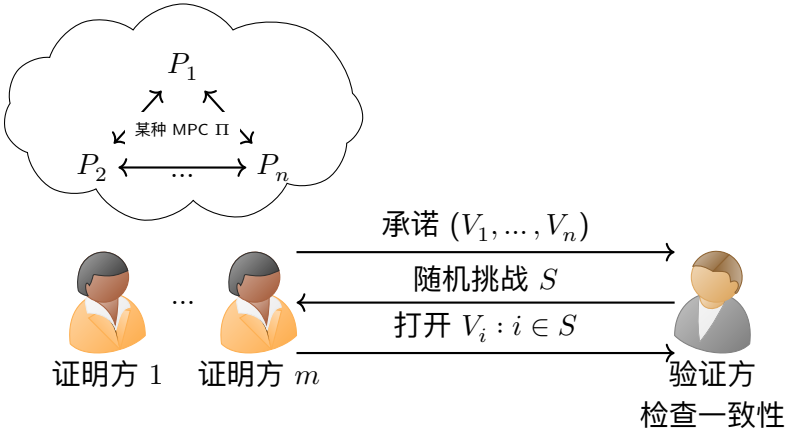
- 承诺可以由单向函数假设蕴含
- 随机挑战的不可预测性保证证明的可靠性
- 一致性检查通过模拟 P_i, P_j 实现
- 定理（IKOS[11]）：假设单向函数存在，多方计算蕴含了 $\mathcal{NP}$ 关系的零知识证明

扩展证明方数量



- 证明方可以通过交互产生 $V_1, ..., V_n$

扩展证明方数量



- 证明方可以通过交互产生 $V_1, ..., V_n$
- 可以使用 Fiat-Shamir 完成非交互转换

第 3 节

基于头脑模拟的多方零知识

第 3 小节

代码实现与实验结果

实验环境

测试的证明关系：

- $\mathcal{R}^{\mathsf{hash}}(y;(x_1,x_2))$: $y = \mathsf{SHA256}(x_1 \oplus x_2)$
- $\mathcal{R}^{\mathsf{comp}}((y,h_1,h_2);((x_1,r_1),(x_2,r_2)))$:

$$\underbrace{y < (x_1 + x_2)}_{\text{32 位整数}} \wedge h_1 = \mathsf{SHA256}(x_1||r_1) \wedge h_2 = \mathsf{SHA256}(x_2||r_2)$$

- $\mathcal{R}^{\mathsf{sum}}(y;(x_1,...,x_8))$: $y = \underbrace{x_1 + ... + x_8}_{\text{32 位整数}}$

实验结果

- 使用半诚实版本的 GMW 协议实现了内部协议 Π
- 验证方打开每个证明方的两个虚拟视图来检查一致性

关系	$\mathcal{R}^{\mathsf{hash}}$	$\mathcal{R}^{\mathsf{comp}}$	$\mathcal{R}^{\mathsf{sum}}$
电路规模	94,302/22,528	189,450/45,312	1,821/288
参与方数量	2×3	2×3	8×3
可靠性等级	2^{-40}	2^{-40}	2^{-40}
重复次数	70	70	70
证明时间	109min	223min	26min31s
验证时间	23.7s	50.0s	1.44s
证明长度	4.0MB	8.0MB	1.3MB

第 4 节

总结

课题总结

在本次课题研究中实现了以下目标：

- 在大数据背景下的实际应用中提炼出新的密码原语
- 根据多方计算得到了一种通用构造，并进行了优化
- 针对基础的通用构造给出了代码实现，验证了可行性

第 I 部分

附录

参考文献

参考文献 I

[1] FIAT A, SHAMIR A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]//ODLYZKO A M. LNCS: CRYPTO'86: vol. 263. [S.l.]: Springer, Heidelberg, 1987: 186-194. DOI: 10.1007/3-540-47721-7_12.

[2] BEN-SASSON E, CHIESA A, SPOONER N. Interactive Oracle Proofs[C]// HIRT M, SMITH A D. LNCS: TCC 2016-B, Part II: vol. 9986. [S.l.]: Springer, Heidelberg, 2016: 31-60. DOI: 10.1007/978-3-662-53644-5_2.

[3] JAWUREK M, KERSCHBAUM F, ORLANDI C. Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently[C]//SADEGHI A R, GLIGOR V D, YUNG M. ACM CCS 2013. [S.l.]: ACM Press, 2013: 955-966. DOI: 10.1145/2508859.2516662.

参考文献 II

[4] FREDERIKSEN T K, NIELSEN J B, ORLANDI C. Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge[C]//OSWALD E, FISCHLIN M. LNCS: EUROCRYPT 2015, Part II: vol. 9057. [S.l.]: Springer, Heidelberg, 2015: 191-219. DOI: 10.1007/978-3-662-46803-6_7.

[5] HEATH D, KOLESNIKOV V. Stacked Garbling for Disjunctive Zero-Knowledge Proofs[C]//CANTEAUT A, ISHAI Y. LNCS: EUROCRYPT 2020, Part III: vol. 12107. [S.l.]: Springer, Heidelberg, 2020: 569-598. DOI: 10.1007/978-3-030-45727-3_19.

参考文献 III

[6] BAUM C, DAMGÅRD I, ORLANDI C. Publicly Auditable Secure Multi-Party Computation[C]//ABDALLA M, PRISCO R D. LNCS: SCN 14: vol. 8642. [S.l.]: Springer, Heidelberg, 2014: 175-196. DOI: 10.1007/978-3-319-10879-7_11.

[7] BAUM C, ORSINI E, SCHOLL P, et al. Efficient Constant-Round MPC with Identifiable Abort and Public Verifiability[C]//MICCIANCIO D, RISTENPART T. LNCS: CRYPTO 2020, Part II: vol. 12171. [S.l.]: Springer, Heidelberg, 2020: 562-592. DOI: 10.1007/978-3-030-56880-1_20.

参考文献 IV

[8] SCHOENMAKERS B, VEENINGEN M. Universally Verifiable Multiparty Computation from Threshold Homomorphic Cryptosystems[C]//MALKIN T, KOLESNIKOV V, LEWKO A B, et al. LNCS: ACNS 15: vol. 9092. [S.l.]: Springer, Heidelberg, 2015: 3-22. DOI: 10.1007/978-3-319-28166-7_1.

[9] BONEH D, BOYLE E, CORRIGAN-GIBBS H, et al. Zero-Knowledge Proofs on Secret-Shared Data via Fully Linear PCPs[C]//BOLDYREVA A, MICCIANCIO D. LNCS: CRYPTO 2019, Part III: vol. 11694. [S.l.]: Springer, Heidelberg, 2019: 67-97. DOI: 10.1007/978-3-030-26954-8_3.

参考文献 V

[10] BOYLE E, GILBOA N, ISHAI Y, et al. Efficient Fully Secure Computation via Distributed Zero-Knowledge Proofs[Z]. Cryptology ePrint Archive, Report 2020/1451. https://eprint.iacr.org/2020/1451. 2020.

[11] ISHAI Y, KUSHILEVITZ E, OSTROVSKY R, et al. Zero-knowledge from secure multiparty computation[C]//JOHNSON D S, FEIGE U. 39th ACM STOC. [S.l.]: ACM Press, 2007: 21-30. DOI: 10.1145/1250790.1250794.

谢谢