丘成桐数学科学中心
YAU MATHEMATICAL SCIENCES CENTER

TSIMF
清华三亚国际数学论坛

互联网和区块链经济学的数学基础

Mathematical Foundations of the Internet and Blockchain Economics

January 6-10, 2025

Room A-103, TSIMF

组织者 ORGANIZERS

Xiaotie Deng(邓小铁), Peking University

Sen Hu(胡森), University of Science and Technology of China

Jing Chen(陈婧), Tsinghua University

Zhiyi Huang(黄志毅), Hong Kong University

Zhan Pang(庞湛), Purdue University

Contents

About

Mathematical Foundations of the Internet and Blockchain Economics
互联网和区块链经济学的数学基础

Date

January 6-10, 2025

Venue

Room A-103, TSIMF

Organizers

Xiaotie Deng(邓小铁), Peking University
Jing Chen(陈婧), Tsinghua University
Sen Hu(胡森), University of Science and Technology of China
Zhiyi Huang(黄志毅), The University of Hong Kong
Zhan Pang(庞湛), Purdue University

Abstract

The topic of this conference is the mathematical foundations of the Internet and blockchain economy. Over the past several decades, the world has witnessed the flourish of the Internet as well as the explosive growth of blockchains. They have connected billions of people and supported a large economy crossing the digital world and the physical world. With its unique properties such as large-scale consensus, trustworthiness and user-programmable smart contracts, blockchains may potentially change the traditional economy and open new avenues for growth and innovation. Mathematical studies have been instrumental to such developments, providing deep insights and solid foundations to many applications. To achieve higher economic goals in these rapidly evolving systems and to guide their sustainable growth, it is crucial to develop rigorous theories and technologies with reliable guarantees. This conference brings together experts from home and abroad in multiple disciplines, such as mathematics, theoretical computer science, game theory, economics, and operations research, to facilitate discussions on the latest developments in the Internet and blockchain economy, identify important mathematical challenges and pave the way for scientific collaborations that will eventually lead to the solutions. The conference provides a platform for attendees to learn about latest results from different domains, while also fosters networking and educational opportunities with their peers and established experts.

Description of the aim

The primary goal of this workshop is to bring researchers from different places together to brain-storm on important challenges in the Internet and blockchain economy. By fusing in-person collaborations on the mathematical aspects of related domains, it will identify new problems, ignite long-term works and eventually solutions with a rigorous theoretical foundation. Indeed, because of the rapid development of Internet and blockchain economy, many exiting solutions are driven by heuristics while solid mathematical modeling and understanding has been lacking, which from time to time causes serious damages to the security and social efficiency of the corresponding economy. The workshop will invite top researchers from both the theoretical front and the application front to share their work and participate in panel discussions and fire-side chats, so as to enhance the mutual understanding among researchers with different pursuits. This way, theoretical studies on Internet and blockchain economy will be able to address pain-points in the industry more directly and lay a solid mathematical foundation for the economy, so as to strengthen the economy's growth in the long run. Also importantly, the workshop will bring together researchers at different career stages, from established experts to graduate-students-to-be, for educational and advisal purposes, which is critical for the healthy and long-term development of related domains.

Schedule

January 6, 2025, Monday

Time 日期	Name 报告人	Title 报告题目
7:30-8:30	Breakfast	
Chair: Jing Chen(陈婧)		
8:50-9:00	Opening	
9:00-9:30	Xiaotie Deng(邓小铁)	Harnessing the Potential of the Digital Economy
9:30-10:00	Yinyu Ye(叶荫宇)	Optimization Algorithm as a Collaborative Game
10:00-10:30	Coffee Break	
Chair: Zhan Pang(庞湛)		
10:30-11:00	Group Photo	
11:00-11:30	Yukun Cheng(程郁琨)	Networked Digital Public Goods Games with Heterogeneous Players and Convex Costs
11:30-12:00	Hanrui Zhang(张涵瑞)	Auction Efficiency in the Autobidding World
12:00-13:30	Lunch	
Chair: Qi Qi(祁琦)		
14:00-14:30	Yiding Feng(冯逸丁)	Beyond Regularity: Simple versus Optimal Mechanisms, Revisited
14:30-15:00	Yuqing Kong(孔雨晴)	Eliciting Informative Text Evaluations with Large Language Models
15:00-15:30	Coffee Break	
Chair:Yukun Cheng(程郁琨)		
15:30-16:00	Zhan Pang(庞湛)	Can Blockchain be a Trust Machine for Supply Chains
16:00-16:30	Qi Qi(祁琦)	Joint Auction in the Online Advertising Market
16:30-17:00	Round Table	
17:00-17:30		
17:30-19:00	Dinner	

January 7, 2025, Tuesday

Time 日期	Name 报告人	Title 报告题目
7:30-8:30	Breakfast	
Chair: Xiaotie Deng(邓小铁)		
9:00-9:30	Juan A. Garay (Zoom)	Truly Permissionless, Fast and Cryptographically Secure Blockchain
9:30-10:00	Jing Chen(陈婧)	Sealed-bid Auctions on Blockchain with Timed Commitment Outsourcing
10:00-10:30	Coffee Break	
Chair: Ron Lavi		
10:30-11:00	Sisi Duan(段斯斯)	Blockchain Security and Economic Incentives
11:00-11:30	Ye Wang(王也)	Flows and Usage of Stable Coins during Crises
11:30-12:00	Yingjie Xue(薛颖杰)	Efficient and Universally Accessible Cross-Chain Options without Upfront Holder Collateral
12:00-13:30	Lunch	
Chair: Minming Li(李闵溟)		
14:00-14:30	Shang-Hua Teng(滕尚华)	Understanding and Characterizing Regularization
14:30-15:00	Ron Lavi	Algorithmic contract theory and contractible contracts
15:00-15:30	Coffee Break	
Chair: Sisi Duan(段斯斯)		
15:30-16:00	Xujin Chen(陈旭瑾)	Competitive Ratios for Online Trading
16:00-16:30	Minming Li(李闵溟)	Fairness in Facility Location Games
16:30-17:00	Round Table	
17:00-17:30		
17:30-19:00	Dinner	

January 8, 2025, Wednesday

Time 日期	Name 报告人	Title 报告题目
7:30-8:30	Breakfast	
Chair:Yuqing Kong(孔雨晴)		
9:00-9:30	Jiheng Zhang(張季恒)	Improving Blockchain Consistency Bound by Assigning Weights to Random Blocks
9:30-10:00	Lu Cao(曹露)	Blockchain-Based Vickrey Auction Protocol for Privacy-Preserving Data Sharing
10:00-10:30	Coffee Break	
Chair:Yurong Chen(陈昱蓉)&Yotam Gafni		
10:30-11:00	Student Rump Session, 5min*19	
11:00-11:30		
11:30-12:00		
12:00-13:30	Lunch	
Free Discussion 13:30-17:30		
18:00-20:00	Banquet	

January 9, 2025, Thursday

Time 日期	Name 报告人	Title 报告题目
7:30-8:30	Breakfast	
Chair: Jing Chen(陈婧)		
9:00-9:30	Man Ho Allen Au(区文浩)	Efficient Zero-Knowledge Arguments For Paillier Cryptosystem and Its Applications
9:30-10:00	Xiapu Daniel Luo(罗夏朴)	Exposing the Invisible: Uncovering Blockchain Vulnerabilities
10:00-10:30	Coffee Break	
Chair:Yingjie Xue(薛颖杰)		
10:30-11:00	Jiasun Li(李家荪)	Bitcoin Mining for Carbon Emission Reduction
11:00-11:30	Jichen Li(李济宸)	Composition of Authenticated Byzantine Agreement under Man-in-middle Attack
11:30-12:00	Group Discussion	
12:00-13:30	Lunch	
Chair: Bo Li(李博)		
14:00-14:30	Zhiyi Huang(黄志毅)	Online Ad Allocation via Relax-and-Round
14:30-15:00	Zhixuan Fang(房智轩)	Incentivizing Truth Exploration and Honest Reporting: A Contract Design Approach
15:00-15:30	Coffee Break	
Chair: Zhiyi Huang(黄志毅)		
15:30-16:00	Yotam Gafni	Recent Developments in the Study of Transaction Fee Mechanisms
16:00-16:30	Yurong Chen(陈昱蓉)	Learning a Stackelberg Leader's Incentive from Optimal Commitments
16:30-17:00	Round Table	
17:00-17:30		
17:30-19:00	Dinner	

January 10, 2025, Friday

Time 日期	Name 报告人	Title 报告题目
7:30-8:30	Breakfast	
Chair: Zihe Wang(王子贺)		
9:00-9:30	Hu Fu(伏虎)	Price Stability and Improved Buyer Utility through Allocation of Prominence
9:30-10:00	Bo Li(李博)	MMS Allocation of Indivisible Chores with Subadditive Valuations and the Fair Surveillance Assignment Problem
10:00-10:30	Coffee Break	
Chair: Hu Fu(伏虎)		
10:30-11:00	Zihe Wang(王子贺)	Competitive Information Design with Asymmetric Senders
11:00-11:30	Weian Li(李维安)	Competition among Mechanism Designers: A Contest-Theoretic Perspective
11:30-12:00	Group Discussion	
12:00-13:30	Lunch	

Titles and Abstracts

Jan 6 Morning

Harnessing the Potential of the Digital Economy

Xiaotie Deng(邓小铁)
Peking University

Effective governance is indispensable for shaping the transformative impact of the rapidly growing digital economy. It is imperative to uphold fairness, ensuring fair competition, accurate valuation of digital assets, stable price dynamics, equitable taxation, and optimization of social welfare within this new economic paradigm.

In the digital marketplace, governance must curtail monopolistic practices and nurture innovation, guaranteeing a level playing field for all participants. Transparent and reliable methods for valuing digital assets are essential, providing clarity and certainty to investors and consumers alike. Price dynamics, influenced by data and network effects, necessitate regulation to ensure fairness, preclude manipulation, and foster stability.

Taxing the digital economy poses unique challenges, and governance must establish a fair and efficient tax system that is consistently applied across borders. Furthermore, governance must ensure that the benefits of the digital economy are widely shared, addressing concerns related to employment and income inequality.

In conclusion, effective and impartial governance is vital for harnessing the potential of the digital economy while promoting equity, fairness, and sustainable development for the community and all stakeholders involved. This report represents our best effort to initiate a comprehensive discussion on the crucial aspects of governing the digital economy, aiming to foster a deeper understanding and collaborative approach towards shaping its future.

Bio: Xiaotie Deng got his BSc from Tsinghua University, MSc from Chinese Academy of Sciences, and PhD from Stanford University in 1989.

He is currently a chair professor at Peking University. He taught in the past at Shanghai Jiaotong University, University of Liverpool, City University of Hong Kong, and York University. Before that, he was an NSERC international fellow at Simon Fraser University. Deng's current research focuses on algorithmic game theo-ry, with applications to Internet Economics and Finance including sponsored search auction, p2p network’s economics such as BitTorrent network, sharing economics, and blockchain.

His other works cover online algorithms, parallel algorithms, and combinatorial op-timization.

He is an ACM Fellow for his contribution to the interface of algorithms and game theory, and an IEEE Fellow for his contributions to computing in partial information and interactive environments, and CSIAM Fellow for his contributions in game theory and blockchain. He is a foreign member of Academia Europaea.

Optimization Algorithm as a Collaborative Game

Yinyu Ye(叶荫宇)
Stanford University

Designing effective optimization algorithms requires adaptivity to the local optimization landscape. In gradient-based methods, such adaptivity often hinges on carefully chosen step sizes. In this talk, we introduce a novel perspective on adaptive algorithm design: we model gradient descent as a collaborative game between a step-size or (hyper-parameter) planner and the optimization landscape executioner. At each iteration, the executioner provides feedback to the planner, and the planner in turn learns to refine the step-size (or hyper-parameter) in an online manner. To illustrate this new viewpoint, we present a family of gradient-based methods that incorporate online step-size or problem-condition planning. These methods guarantee strong convergence with respect to the optimization trajectory and show a significant speedup compared to traditional gradient-based methods in both theory and practice.

Bio: Yinyu Ye, formally the K.T. Li Professor of Stanford University, is now the Visiting Chair Professor of Chinese University of Hong Kong at Shenzhen, Hong Kong University of Science and Technology, and Shanghai Jiao Tong University. His current research topics include Continuous and Discrete Optimization, Data Science and Applications, Numerical Algorithm Design and Analyses, Algorithmic Game/Market Equilibrium, Operations Research and Management Science etc.; and he was one of the pioneers on Interior-Point Methods, Conic Linear Programming, Distributionally Robust Optimization, Online Linear Programming and Learning, Algorithm Analyses for Reinforcement Learning&Markov Decision Process and nonconvex optimization, and etc. He and his students have received numerous scientific awards, himself including the 2006 INFORMS Farkas Prize (Inaugural Recipient) for fundamental contributions to optimization, the 2009 John von Neumann Theory Prize for fundamental sustained contributions to theory in Operations Research and the Management Sciences, the inaugural 2012 ISMP Tseng Lectureship Prize for outstanding contribution to continuous optimization (every three years), the 2014 SIAM Optimization Prize awarded (every three years), etc. According to Google Scholar, his publications have been cited over 62,000 times.

Networked Digital Public Goods Games with Heterogeneous Players and Convex Costs

Yukun Cheng(程郁琨)
Jiangnan University

In the digital age, resources such as open-source software and publicly accessible databases form a crucial category of digital public goods, providing extensive benefits across the Internet. However, the inherent non-exclusivity and non-competitiveness of these public goods frequently result in under-provision, a dilemma exacerbated by individuals' tendency to free-ride. This scenario fosters both cooperation and competition among users, leading to the emergence of public goods games.

This paper investigates networked public goods games involving heterogeneous players and convex costs to explore solutions of Nash Equilibrium (NE) for this problem. In these games, each player can choose her own effort level, representing the contributions to public goods. We employ network structures to depict the interactions among participants. Each player's utility is composed of a concave value component, influenced by collective efforts, and a convex cost component, determined solely by individual effort. To the best of our knowledge, this study is the first to explore a networked public goods game with convex costs.

Our research begins by examining welfare solutions aimed at maximizing social welfare and ensuring the convergence of pseudo gradient ascent dynamics. We establish the presence of NE in this model and provide an in-depth analysis of the conditions under which NE is unique. Additionally, we introduce the concept of game equivalence, which expands the range of public goods games that can support a unique NE. We also delve into comparative statics, an essential tool in economics, to evaluate how slight modifications in the model-interpreted as monetary redistribution-impact player utilities. In addition, we analyze a particular scenario with a predefined game structure, illustrating the practical relevance of our theoretical insights. Consequently, our research enhances the broader understanding of strategic interactions and structural dynamics in networked public goods games, with significant implications for policy design in internet economic and social networks.

Bio: Dr. Yukun Cheng is a professor at the Jiangnan University Business School, and she is also a doctoral advisor. She serves on the editorial boards of several prestigious journals, including the IEEE Open Journal of the Computer Society, Operations Research Transactions, and Blockchain. Prof. Cheng is also a member and secretary of the Blockchain Committee of the China Society for Industrial and Applied Mathematics (CSIAM), as well as the Secretary-General of the Operations Research Society of China and the Deputy Director of the Computational Economics Group of the China Computer Federation (CCF). She is a council member of the Jiangsu Operations Research Society.

Her primary research interests encompass digital economics, algorithmic game theory, combinatorial optimization, and the technology and applications of blockchain. As a project leader and key participant, she has led or contributed to ten national-level research projects. Dr. Cheng has published more than 70 high-level academic papers in top international journals and conferences, including Mathematics of Operations Research, IEEE Transactions on Cloud Computing, IEEE Transactions on Computers, and Theoretical Computer Science. She has also presented at prestigious conferences, such as the TACM Conference on Economics and Computation (EC2022), Financial Cryptography and Data Security (FC 2022), and the International Joint Conference on Artificial Intelligence (IJCAI 2016). She also holds two invention patents. Recognized as a leading academic figure among young scholars in Jiangsu Province's 'Qinglan Project,' Dr. Cheng has received several awards, including the Third Prize for Scientific and Technological Research Achievements from Jiangsu Province in 2021.

Auction Efficiency in the Autobidding World

Hanrui Zhang(张涵瑞)
Chinese University of Hong Kong

Automation has been a major trend in the online advertising industry over the past few years. The idea is that advertisers specify their high-level goals to bidding algorithms provided by the platform, which then bid in ad auctions on behalf of them. These bidding algorithms, often called autobidders, behave differently from quasi-linear utility maximizers -- the latter being the conventional way to model agents in auction design. As a result, commonly used auction mechanisms that are known to be efficient with quasi-linear utility maximizers may not work well with autobidders. In a series of work, we analyze the efficiency (as measured by the price of anarchy) of two auction mechanisms in the autobidding world: first-price auctions (FPA) and generalized second-price auctions (GSP). We also study how other factors -- in particular, the level of sophistication of autobidders and the presence of user costs -- affect auction efficiency.

Bio: Hanrui is an Assistant Professor in Computer Science and Engineering at the Chinese University of Hong Kong. He obtained his PhD from Carnegie Mellon University, and his Bachelor's from Tsinghua University. His research focuses on the intersection of Computer Science and Economics, covering topics such as Ad Auctions and Strategic Machine Learning.

Jan 6 Afternoon

Beyond Regularity: Simple versus Optimal Mechanisms, Revisited

Yiding Feng(冯逸丁)
Hong Kong University of Science and Technology

A large proportion of the Bayesian mechanism design literature is restricted to the family of regular distributions [Mye-81] or the family of monotone hazard rate (MHR) distributions [BMP-63], which overshadows this beautiful and well-developed theory. We (re-)introduce two generalizations, the family of quasi-regular distributions and the family of quasi-MHR distributions.

The significance of our new families is manifold. First, their defining conditions are immediate relaxations of the regularity/MHR conditions (i.e., monotonicity of the virtual value functions and/or the hazard rate functions), which reflect economic intuition. Second, they satisfy natural mathematical properties (about order statistics) that are violated by both original families. Third but foremost, numerous results [BK-96, HR-09, CD-15, DRY-15, HR-14, AHNPY-19, JLQTX-19, FLR-19, GHZ-19, JLTX-20, JLX-23, LM-24] established before for regular/MHR distributions now can be generalized, with or even without quantitative losses.

This talk is based on joint work with Yaonan Jin.

Bio: Yiding Feng is an assistant professor at HKUST IEDA. Previously, he worked as a principal researcher at the University of Chicago Booth School of Business, and postdoctoral researcher at Microsoft Research New England. He received his Ph.D. from the Department of Computer Science, at Northwestern University in 2021. His research focuses on operations research, economics & computation, and theoretical computer science. He was the recipient of the INFORMS Auctions and Market Design (AMD) Michael H. Rothkopf Junior Researcher Paper Prize (second place).

Eliciting Informative Text Evaluations with Large Language Models

Yuqing Kong(孔雨晴)
Peking University

Peer prediction mechanisms motivate high-quality feedback with provable guarantees. However, current methods only apply to rather simple reports, like multiple-choice or scalar numbers. We aim to broaden these techniques to the larger domain of text-based reports, drawing on the recent developments in large language models. This vastly increases the applicability of peer prediction mechanisms as textual feedback is the norm in a large variety of feedback channels: peer reviews, e-commerce customer reviews, and comments on social media. We introduce two mechanisms. These mechanisms utilize LLMs as predictors, mapping from one agent's report to a prediction of her peer's report. Theoretically, we show that when the LLM prediction is sufficiently accurate, our mechanisms can incentivize high effort and truth-telling as an (approximate) Bayesian Nash equilibrium. Empirically, we confirm the efficacy of our mechanisms through experiments conducted on two real datasets: the Yelp review dataset and the ICLR OpenReview dataset. We highlight the results that on the ICLR dataset, our mechanisms can differentiate three quality levels --- human-written reviews, GPT-4-generated reviews, and GPT-3.5-generated reviews in terms of expected scores.

Bio: Yuqing Kong is currently an assistant professor at The Center on Frontiers of Computing Studies (CFCS), Peking University. She obtained her Ph.D. degree from the Computer Science and Engineering Department at University of Michigan in 2018 and her bachelor degree in mathematics from University of Science and Technology of China in 2013. Her research interests lie in the intersection of computer science and economics: information elicitation, aggregation, and the future applications of these areas to machine learning. Her papers were published in several venues include WINE, ITCS, EC, SODA, AAAI, NeurIPS, ICLR, ECCV, IJCAI, WWW, J. ACM.

Can Blockchain be a Trust Machine for Supply Chains

Zhan Pang(庞湛)
Purdue University

Firms in conventional decentralized supply chains often have economic motive to violate compliance, which results in limited trust and inefficiencies. Blockchain technology is seen as a promising trust machine due to its immutability and cryptographic nature. How can blockchain bring trust to a supply chain? How much value can it add to the supply chain? Using a Stackelberg game with asymmetric information, we characterize the strategic interactions between a supplier and a manufacturer or retailer in an untrusted supply chain that may be equipped with blockchain-based traceability. We identify conditions under which blockchain technology can bring both trust and profitability to supply chain. Our analysis sheds new light into the strategic role and value of blockchain for supply chains.

Bio: Zhan Pang is Lewis B. Cullman Rising Star and Professor of Management at Purdue Business School and Purdue Innovation and Entrepreneurship Fellow. His research interests include statistical learning and decision theory, healthcare systems, supply chain risk management, and pricing and revenue management. He is a senior editor for Production and Operations Management and a founding editor of Journal of Blockchain Research.

Joint Auction in the Online Advertising Market

Qi Qi(祁琦)
Renmin University of China

Online advertising is a primary source of income for e-commerce platforms. In the current advertising pattern, the oriented targets are the online store owners who are willing to pay extra fees to enhance the position of their stores. On the other hand, brand suppliers are also desirable to advertise their products in stores to boost brand sales. However, the currently used advertising mode cannot satisfy the demand of both stores and brand suppliers simultaneously. To address this, we innovatively propose a joint advertising model termed “Joint Auction”, allowing brand suppliers and stores to collaboratively bid for advertising slots, catering to both their needs. However, conventional advertising auction mechanisms are not suitable for this novel scenario. In this talk, I will discuss our recent work on joint auctions that can achieve the optimal revenue and guarantee (near-)dominant strategy incentive compatibility and individual rationality.

Bio: Dr. Qi is now a tenured Associate Professor of Gaoling School of Artificial Intelligence, Renmin University of China. She is the Secretary-General of the Computational Economics TC of the China Computer Federation (CCF). She obtained her Ph.D. degree from Stanford University under guidance of Professor Yinyu Ye. Dr. Qi worked at Hong Kong University of Science and Technology before she moved to Renmin University of China. Her publications have appeared in OR, MOR, GEB, EJOR, TR-B, JCSS, etc and conferences including STOC, CCC, KDD, IJCAI, AAAI, NeurIPS, WINE, etc. Her research interests lie generally in the areas of algorithmic game theory, AI and operations research, specifically mechanism and auction design, revenue and social welfare optimization, AI agents, multi-agent systems and their applications in platform economics, online advertising, resource allocation, transportation and sharing economy. She received two US patents on online advertising.

Jan 7 Morning

Truly Permissionless, Fast and Cryptographically Secure Blockchain

Juan A. Garay (Zoom)
Texas A&M University

As a new paradigm for decentralization, the advent of blockchains such as Bitcoin has ignited much excitement, not only for their realization of novel financial instruments, but also for offering alternative solutions to classical problems in fault-tolerant distributed computing and cryptographic protocols. In this talk we focus on the following "trichotomy": Can a proof-of-work-based blockchain simultaneously achieve fast transaction settlement (resp., consensus), in the cryptographic sense (i.e., properties provably achieved except with negligible probability), while relying on trusted set-up assumptions that do not imply participants' authentication? We prove the trichotomy false, by presenting such a construction.
This talk is based on joint work with Aggelos Kiayias and Yu Shen (University of Edinburgh).

Bio: Since Fall '17, Juan Garay is a full professor at Texas A&M University's Computer Science & Engineering Department. Previously, after receiving his PhD in Computer Science from Penn State, he was a postdoc at the Weizmann Institute of Science (Israel), and held research positions at the IBM T.J. Watson Research Center, Bell Labs, AT&T Labs--Research, and Yahoo Research. His research interests include both foundational and applied aspects of cryptography and information security. He is the author of over 190 published works in the areas of cryptography, network security, distributed computing, and algorithms; has been involved in the design, analysis and implementation of a variety of secure systems; and is the recipient of a Thomas A. Edison Patent Award, two Bell Labs Teamwork Awards, an IBM Outstanding Technical Achievement Award, and an IBM Research Division Award. Dr. Garay has served on the program committees of numerous conferences and international panels---including co-chairing Crypto 2013 and 2014, the discipline's premier conference. He is a Fellow of the International Association for Cryptologic Research (IACR).

Sealed-bid Auctions on Blockchain with Timed Commitment Outsourcing

Jing Chen(陈婧)
Tsinghua University

Sealed-bid auctions play a crucial role in blockchain ecosystems. Previous studies have introduced viable blockchain-based sealed-bid auction protocols, leveraging timed commitments for bid encryption. However, a crucial challenge remains: Who should bear the cost of decrypting the timed commitments? In this talk I'll report our recent work in addressing this challenge, which introduces a new timed commitment scheme and a two-sided market to connect bidders and commitment solvers.

Bio: Jing Chen is a professor in the Computer Science Department of Tsinghua University. Her main research interest is theory of computing, in particular algorithmic game theory, mechanism design, and problems related to blockchains. She was Chief Scientist and Head of Theory Research at Algorand Inc, and a faculty member in the Computer Science Department of Stony Brook University. Jing received her bachelor's and master's degrees in computer science from Tsinghua University, PhD from MIT, and was a postdoc at the Institute for Advanced Study, Princeton. She received the NSF CAREER Award for her work on mechanism design.

Blockchain Security and Economic Incentives

Sisi Duan(段斯斯)
Tsinghua University

Blockchain is a distributed system that achieves high availability of the service and integrity of the data. The security properties are preserved by the underlying consensus mechanism, namely Byzantine fault-tolerant protocols. Conventional consensus protocol only considers safety (i.e., something wrong will never happen) and liveness (i.e., something right will eventually happen) as the security properties. However, many permissionless blockchains or cryptocurrencies primarily rely on the incentive mechanism for the system to operate correctly in a public environment. In this talk, I will talk about some of our recent works on incentive mechanisms of blockchains and discuss their relationship with the security of blockchains.

Bio: Dr. Sisi Duan is a researcher at Tsinghua University. She received her Ph.D. from the University of California, Davis in 2014 and her bachelor degree from the University of Hong Kong in 2010. Her research interests include distributed systems security, blockchain, and applied cryptography. Her works have been adopted by many industrial blockchain systems such as Hyperledger Iroha hosted by the Linux Foundation and the mBridge project led by Bank for International Settlements. She has served as the TPC for conferences such as S&P, CCS, and NDSS.

Flows and Usage of Stable Coins during Crises

Ye Wang(王也)
University of Macau

Stablecoins have emerged as a link between the traditional fiat currency system and the cryptocurrency sector. However, they are susceptible to market shocks, which can potentially trigger crises. We construct a novel and unique data set of transaction-level data of eight major stablecoins to comprehensively examine trading activities during stress events within the stablecoin ecosystem. Our study encompasses a sample period that spans four significant crisis events, including the Terra-Luna collapse, the FTX failure, the Binance USD issuance halt, and the Silicon Valley Bank failure which impacted the stablecoin USDC. Our analysis reveals common market patterns across these crises. Although the Terra Luna and FTX shocks affected a broad range of stablecoins and activities, we find that contrary to anecdotal beliefs, these crypto shocks did not result in a systemic flight to safety from stablecoin assets to fiat currencies. Rather, we observe substitution effects between stablecoins, wherein investors pivot from riskier stablecoins to safer alternatives with similar functionalities. We identify a redistribution of stablecoin usage, characterized by outflows from riskier activities towards more secure channels. Our empirical study reveals that the Binance and the Silicon Valley Bank banking stress events primarily affected the particular stablecoin involved (i.e., BUSD and USDC, respectively) with rival stablecoins gaining market share.

Bio: Kanye Ye Wang is an Assistant Professor jointly appointed at the Department of Computer and Information Science and the Department of Finance and Business Economics at the University of Macau. He holds a Ph.D. and an MSc degree from ETH Zurich and a BSc degree from Peking University. Kanye's research focuses on digital economy, blockchain, algorithmic game theory, and information security. He has published numerous academic papers in top conferences and journals such as S&P, CHI, WINE, NDSS, CSCW, IJCAI, WWW, AEA P&P, TCS, JPDC, and JHTR. He has received several awards, including the Best Paper of the Year Award at JHTR 2023, the Best Paper Award at the 2nd Annual CBER Conference, and a Best Paper Nomination at IJTCS-FAW 2023. Kanye has served as an Associate Chair and Program Committee member for conferences such as CHI, CCS, CSCW, WINE, and FC, and is a Young Editorial Board member of the Blockchain journal.

Efficient and Universally Accessible Cross-Chain Options without Upfront Holder Collateral

Yingjie Xue(薛颖杰)
Hong Kong University of Science and Technology (Guangzhou)

Options are fundamental to blockchain-based financial markets, offering essential tools for risk management and price speculation, which enhance liquidity, flexibility, and market efficiency in decentralized finance (DeFi). Despite the growing interest in options for blockchain-resident assets, such as cryptocurrencies, current option mechanisms face significant challenges, including limited asset support, high trading delays, and the requirement for option holders to provide upfront collateral.

In this paper, we present a protocol that addresses the aforementioned issues by facilitating efficient and universally accessible option trading without requiring holders to post collateral when establishing options. Our protocol's universality allows for cross-chain options involving nearly \textit{any} assets on \textit{any} two different blockchains, provided the chains' programming languages can enforce and execute the necessary contract logic. A key innovation in our approach is the use of Double-Authentication-Preventing Signatures (DAPS), which significantly reduces trading latency. Additionally, by introducing a guarantee from the option writer, our protocol removes the need of upfront collateral from holders. Our evaluation demonstrates that the proposed scheme reduces option transfer latency to less than half of that in existing methods. Rigorous security analysis proves that our protocol achieves secure option trading, even when facing adversarial behaviors.

Bio: Dr. Yingjie Xue is currently an Assistant Professor in the FinTech Thrust at the Hong Kong University of Science and Technology (Guangzhou). Her research is focused on blockchain technology and data security. Her work primarily revolves around cross-chain technology, the design of cross-chain transaction protocols, blockchain application protocol design, and issues related to blockchain security and privacy. Dr. Xue's research has been published in leading international conferences and journals, including IEEE TIFS, TPDS, TC, TSC, PODC, ICDCS, and JPDC. She serves as a program committee member for several international conferences, such as ICDCS, INFOCOM, Blockchain, SSS, and IJTCS-FAW, and has acted as a reviewer for authoritative journals including IEEE TON, TDSC, TNSE, and TCC. Dr. Xue earned her Ph.D. in Computer Science from Brown University in May 2023, and she received her Master's degree in Electronic and Communication Engineering and Bachelor's degree in Information Security from the University of Science and Technology of China in 2018 and 2015, respectively.

Jan 7 Afternoon

Understanding and Characterizing Regularization

Shang-Hua Teng(滕尚华)
University of Southern California

The quintessential learning algorithm of empirical risk minimization (ERM) is known to fail in various settings for which uniform convergence does not characterize learning. Relatedly, the practice of machine learning is rife with considerably richer algorithmic techniques, perhaps the most notable of which is regularization. Nevertheless, no such technique or principle has broken away from the pack to characterize optimal learning in these more general settings. The purpose of this work is to precisely characterize the role of regularization in perhaps the simplest setting for which ERM fails: multiclass learning with arbitrary label sets. Using one-inclusion graphs (OIGs), we exhibit optimal learning algorithms that dovetail with tried-and-true algorithmic principles: Occam's Razor as embodied by structural risk minimization (SRM), the principle of maximum entropy, and Bayesian inference. We also extract from OIGs a combinatorial sequence we term the Hall complexity, which is the first to characterize a problem's transductive error rate exactly. Lastly, we introduce a generalization of OIGs and the transductive learning setting to the agnostic case, where we show that optimal orientations of Hamming graphs - judged using nodes' outdegrees minus a system of node-dependent credits - characterize optimal learners exactly. We demonstrate that an agnostic version of the Hall complexity again characterizes error rates exactly, and exhibit an optimal learner using maximum entropy programs.
Joint work (COLT 2024) with Julian Asilis, Siddartha Devic, Shaddin Dughmi, and Vatsal Sharan

Bio: Shang-Hua Teng is a University Professor and Seely G. Mudd Professor of Computer Science and Mathematics at USC. He is a fellow of SIAM, ACM, and Alfred P. Sloan Foundation, and has twice won the Gödel Prize, first in 2008, for developing smoothed analysis, and then in 2015, for designing the breakthrough scalable Laplacian solver. Citing him as, “one of the most original theoretical computer scientists in the world”, the Simons Foundation named him a 2014 Simons Investigator to pursue long-term curiosity-driven fundamental research. He also received the 2009 Fulkerson Prize, 2023 Science & Technology Award for Overseas Chinese from the China Computer Federation, 2022 ACM SIGecom Test of Time Award (for settling the complexity of computing a Nash equilibrium), 2021 ACM STOC Test of Time Award (for smoothed analysis), 2020 Phi

Kappa Phi Faculty Recognition Award (2020) for his book Scalable Algorithms for Data and Network Analysis, 2011 ACM STOC Best Paper Award (for improving maximum-flow minimum-cut algorithms). In addition, he and collaborators developed the first optimal well-shaped Delaunay mesh generation algorithms for arbitrary three-dimensional domains, settled the Rousseeuw-Hubert regression-depth conjecture in robust statistics, and resolved two long-standing complexity-theoretical questions regarding the Sprague-Grundy theorem in combinatorial game theory. For his industry work with Xerox, NASA, Intel, IBM, Akamai, and Microsoft, he received fifteen patents in areas including compiler optimization, Internet technology, and social networks. Dedicated to teaching his daughter to speak Chinese as the sole Chinese-speaking parent in an otherwise English-speaking family and environment, he has also become fascinated with children's bilingual learning.

Algorithmic contract theory and contractible contracts

Ron Lavi
University of Bath

Markets are an ancient tool for allocating goods; but they are also a tool for the allocation of effort. For example, in online labor markets, a freelancer puts in effort to complete tasks delegated to her by the platform's customers. In online advertising, a social-media influencer works to promote several brands. The celebrated principal-agent model, a.k.a. the theory of contract design, studies such issues. When there are multiple principals that simultaneously interact with the agent(s), the model is called ‘common agency’. This is the case, e.g., when a marketing agency bids for ad space on behalf of multiple advertisers, or when platforms like Airbnb act as an agent representing property owners. Classically, contract theory restricts attention to simple objects that describe payments to agents conditioned on their actions or on the obtained outcomes. In this talk I will describe ‘VCG contracts’ which are a type of ‘contractible contracts’ – contracts that can also depend on other contracts. Our main results show that VCG contracts improve the social efficiency relative to classic contracts. Since contractible contracts are reminiscent of smart contracts (and vice versa), a more formal exploration of the connections between the two suggests itself. This talk will be based on a joint paper with Elisheva Shamash.

Bio: Ron Lavi is a reader (associate professor) at the economics department, University of Bath, UK. His research focuses on subjects on the border of economics and computation, mainly algorithmic game theory, auction theory, and the efficient design of economic mechanisms. He completed his doctoral studies in computer science at the Hebrew University, Israel, and his post-doctoral studies at the California Institute of Technology. He was a faculty member at Technion – Israel Institute of Technology during 2006 – 2023, a visiting scholar at UC Berkeley, and a consultant / academic visitor at Google, Microsoft research, and Yahoo! Labs. He has received an outstanding paper award at the 10th ACM conference on Economics and Computation, an Award for Research Cooperation and High Excellence in Science (ARCHES) from the Federal German Ministry of Education and Research, and a Marie-Curie fellowship from the European Commission.

Competitive Ratios for Online Trading

Xujin Chen(陈旭瑾)
Chinese Academy of Sciences

In this talk, we discuss an online trading model featuring homogeneous items, with each seller possessing one item and each buyer demanding one. Both buyers and sellers possess valuations for the items, which are revealed sequentially in a uniformly random order to a central trader. The trader must make an irrevocable decision to trade with an agent (buyer or seller) immediately upon learning their valuation, before the next agent's valuation is revealed.
We examine two versions of this online trading problem. The first seeks to maximize the social welfare of all agents generated by the trading without prior knowledge of the distribution of valuations. For the single-seller case, we present an algorithm that achieves a tight competitive ratio of $4e^2/(e^2+1) \approx 3.523$, improving upon the previous best result of 4.189 [Chen et al., DAM2023]. The second version, assuming the trader knows the i.i.d. valuation distributions of the agents, aims to maximize the trader's gain-from-trade. For the case with an equal number (denoted as n)) of buyers and sellers, we derive a threshold-based algorithm with a competitive ratio of $(2n^2-n)/((n+4^{-n}-1)\cdot(n+1))$, comparable to a previous result of 2 [Correa et al., EC2023].
This is joint work with Xiaodong Hu, Changjun Wang and Qingjie Ye.

Bio: Xujin Chen received her Ph.D degree in Operations Research from Hong Kong University in 2004. She is currently a Professor at Academy of Mathematics and System Science, Chinese Academy of Sciences. Dr. Chen's research interests include Combinatorial Optimization (with an emphasis on polyhedral combinatoric and approximation algorithms), Algorithmic Game Theory (with an emphasis on network games), and Graph Theory (with an emphasis on structural graph theory). Dr. Chen received Excellent Young Scientists Fund of NNSFC, the first place Youth Award of Science & Technology of the Operations Research Society of China, and China Youth Science and Technology Award. She has been selected as a leading talent in science and technology innovation under the National "Ten Thousand Talents Program".

Fairness in Facility Location Games

Minming Li(李闵溟)
City University of Hong Kong

We consider the fairness perspective of facility location games where agents report their information while the mechanism needs to output a facility location that is fair and strategyproof. Various recent works will be discussed along the fairness perspective.

Bio: Minming Li is currently a professor Department of Computer Science, City University of Hong Kong. He received his Ph. D. and B.E. degree in the Department of Computer Science and Technology at Tsinghua University in 2006 and 2002 respectively. His research interests include algorithmic game theory, combinatorial optimization and algorithm design and analysis for scheduling problems.

Jan 8 Morning

Improving Blockchain Consistency Bound by Assigning Weights to Random Blocks

Jiheng Zhang(張季恒)
The Hong Kong University of Science and Technology

Blockchains based on the celebrated Nakamoto consensus protocol have shown promise in several applications, including cryptocurrencies. However, these blockchains have inherent scalability limits caused by the protocol's consensus properties. In particular, the consistency property demonstrates a tight trade-off between block production speed and the system's security in terms of resisting adversarial attacks. As such, this paper proposes a novel method called Ironclad, which improves the blockchain consistency bound by assigning a different weight to randomly selected blocks. We apply our method to the original Nakamoto protocol and rigorously prove that such a combination can significantly improve the consistency bound by analyzing the fundamental consensus properties. This kind of improvement enables a much faster block production rate than the original Nakamoto protocol but with the same security guarantee.

Bio: Jiheng Zhang is the Head of the Department of Industrial Engineering and Decision Analytics at HKUST, where he also holds a joint appointment in the Department of Mathematics. His research interests include Stochastic Modeling and Optimization, Statistical Learning, Numerical Methods, and Algorithms, with applications in Operations Management, Large Communication Networks, and Financial Technology. He serves as an associate editor for several top journals, including Operations Research, Stochastic Systems, and Probability in the Engineering and Informational Sciences. Since 2018, he has been the director of the Elliptic Lab, leading various applied projects with industry partners such as Huawei and Webank. He holds several patents with these industry partners in areas like large-scale production planning and blockchain consensus mechanism design. He earned his Ph.D. in Operations Research from the H. Milton Stewart School of Industrial and Systems Engineering at the Georgia Institute of Technology in 2009. He also holds an M.S. in Mathematics from Ohio State University and a B.S. in Mathematics from Nanjing University.

Blockchain-Based Vickrey Auction Protocol for Privacy-Preserving Data Sharing

Lu Cao(曹露)
Shanghai Institute for Mathematics and Interdisciplinary Sciences(SIMIS)

The integration of blockchain technology with advanced cryptographic techniques has paved the way for fully automated systems that prioritize transparency, privacy, and trustless operation. This work introduces a Blockchain-Based Vickrey Auction Protocol designed to enable privacy-preserving data sharing within decentralized environments. By leveraging cutting-edge cryptographic tools such as zero-knowledge proofs, secure multiparty computation, and threshold cryptography, the protocol ensures bid confidentiality, fairness, and seamless execution. It automates every phase of the auction process—from dataset encryption and bid submission to winner determination and secure data delivery—while guaranteeing robust privacy by disclosing only the winning and second-highest bids. Furthermore, the protocol incorporates controlled access mechanisms, enabling only the verified winner to securely download and decrypt the dataset directly from the blockchain. Key features include tamper-proof auditability, cryptographic scalability, and end-to-end automation, making the system well-suited for applications in AI data marketplaces, government resource allocation, and other high-value data-sharing scenarios. By addressing critical challenges such as scalability, interoperability, and regulatory compliance, this protocol represents a significant step toward revolutionizing secure digital ecosystems.

Bio: Lucy is an Assistant Professor jointly appointed at Fudan University and the Shanghai Institute for Mathematical Sciences. She holds a Ph.D. in Applied Mathematics from the University of Sydney, with a research focus on Mean Field Games, Mechanism Design, and interdisciplinary applications of mathematical sciences. Prior to her current role, Lucy gained extensive teaching experience at the University of Sydney and served as a Postdoctoral Fellow at the Beijing International Center for Mathematical Research, Peking University.

Student Rump Session

Session1

1	Yu Shen(沈俞)	University of Edinburgh
2	Rong Luan(栾蓉)	Nanyang Technological University
3	Feng Luo(罗丰)	The Hong Kong Polytechnic University
4	Haoran Qin(秦浩然)	The Hong Kong Polytechnic University
5	Xinqi Jing(敬新奇)	Academy of Mathematics and Systems Science, Chinese Academy of Sciences
6	Xiyuan Deng(邓茜元)	Academy of Mathematics and Systems Science, Chinese Academy of Sciences
7	Tingting Meng(孟婷婷)	Jiangnan University
8	Zhengyan Deng(邓铮妍)	Jiangnan University
9	Mingfei Zhang(张鸣飞)	Shandong University
10	Xuanzhi Xia(夏暄智)	Tsinghua University

Session2

11	Yan Liu(刘岩)	Renmin University of China
12	Zhicheng Du(杜志成)	Renmin University of China
13	Bingzhe Wang(王炳哲)	Renmin University of China
14	Yuchao Ma(马毓超)	Renmin University of China
15	Ningyuan Li(李宁远)	Peking University
16	Yuejia Dou(窦越嘉)	Renmin University of China
17	Hanbing Liu(刘涵冰)	Renmin University of China
18	Jichen Li(李济宸)	Peking University
19	Yusen Zheng(郑宇森)	Peking University

Jan 9 Morning

Efficient Zero-Knowledge Arguments For Paillier Cryptosystem and Its Applications

Man Ho Allen Au(区文浩)
Hong Kong Polytechnic University

Homomorphic encryption, a groundbreaking cryptographic technique, enables computations on encrypted data without compromising its confidentiality. The Paillier cryptosystem, a well-known example, supports addition of data in its encrypted form, making it a powerful tool for utilizing data while respecting data privacy.

In this talk, we delve into how Paillier encryption can facilitate secure and efficient data aggregation while maintaining data privacy. Furthermore, we introduce our recent advancements in zero-knowledge proofs tailored for the Paillier cryptosystem. These proofs enhance the system's robustness by providing verifiable assurances, thereby safeguarding against malicious adversaries. Our work marks a significant step forward in upgrading the security and trustworthiness of Paillier-based analytics solutions.

Bio: Prof. Man Ho Allen Au is a Professor and Associate Head (Research and Development) in the Department of Computing at The Hong Kong Polytechnic University. He has previously been a faculty member at the University of Hong Kong and the University of Wollongong. His research interests include information security, cryptography, blockchain technology, and their applications. He has published over 200 refereed papers in top journals and conferences, including CRYPTO, ASIACRYPT, ACM CCS, NDSS, IEEE S&P, SIGMOD, SOSP, IEEE TIFS, IEEE TDSC, and others. He received the 2023 BOCHK Science and Technology Innovation Prize (STIP) in FinTech, the 2009 PET runner-up award for outstanding research in privacy-enhancing technologies, and also won ZPrize twice. He has served as a general or program committee chair for several international conferences, including ACM ASIACCS, RAID, SECURECOM, IEEE Blockchain, ISPEC, and PROVSEC, among others. He is an associate editor of IEEE Transactions on Dependable and Secure Computing (TDSC) and Journal of Information Security and Applications (JISA), an advisory board member of ELSP Blockchain, and a member of the Hong Kong Monetary Authority CBDC Expert Group.

Exposing the Invisible: Uncovering Blockchain Vulnerabilities

Xiapu Daniel Luo(罗夏朴)
Hong Kong Polytechnic University

In the fast-paced and continually evolving world of blockchain technology, hidden vulnerabilities can undermine the security and trust that are fundamental to its success. As we delve deeper into this complex technology, it becomes crucial to identify and understand these vulnerabilities to mitigate potential risks. This talk explores the often-overlooked weaknesses in the blockchain ecosystem. Specifically, I will present our recent research findings on identifying and analyzing security vulnerabilities within the Ethereum ecosystem, focusing on their root causes, the resultant effects, and the broader implications for the field.

Bio: Xiapu Luo is a professor at the Department of Computing and the director of the Research

Centre for Blockchain Technology of the Hong Kong Polytechnic University. His research focuses on Blockchain and Smart Contracts Security, Mobile and IoT Security, Network Security and Privacy, and Software Engineering with papers published in top venues. His research led to more than ten best/distinguished paper awards, including ACM CCS'24 Distinguished Paper Award, four ACM SIGSOFT Distinguished Paper Awards in ICSE'24, Internetware'24, ISSTA'22 and ICSE'21, Best DeFi Papers Award 2023, Best Paper Award in INFOCOM'18, Best Research Paper Award in ISSRE'16, etc. and several awards from the industry. He received the BOCHK Science and Technology Innovation Prize (FinTech)'23 for his contribution to blockchain security.

Bitcoin Mining for Carbon Emission Reduction

Jiasun Li (李家荪)
George Mason University

While Bitcoin mining consumes a huge amount of electricity, does it necessarily translate into increased carbon emission? Using an analytical model featuring endogenous renewable energy adoption decisions, we show that with appropriate electricity price policies, the high electricity demand from Bitcoin mining may actually subsidize the capacity building of renewable energy plants and thus lower total carbon emission. A key intuition is that unlike other electricity uses, Bitcoin mining intensity can be elastically dialed up or down without disrupting operations, and thus can replace fuel-based electricity generation as an effective shock absorber for the volatile supply of renewable electricity generation. To corroborate this seemingly counterintuitive result at first sight, we are working on quantifying the potential reductions in carbon emission from introducing Bitcoin mining by calibrating the models with empirical data.

Bio: Dr. Jiasun Li is an associate professor of finance at George Mason University. He received Ph.D. in finance from UCLA Anderson School of Management and B.S. in mathematics from Fudan University (Shanghai, China) prior to joining George Mason. His current research interest is at the intersection of economics and computer science, including blockchain technologies and FinTech applications. His papers analyze node incentives in distributed consensus protocols, crypto tokens' roles in jumpstarting platforms, the industrial organization of cryptocurrency mining pools (and implications for blockchain (de-)centralization and electricity consumption), cryptocurrency mining's (counterintuitive) benefits for emission reduction and renewable energy adoption, factor structures in cryptocurrency returns, forensic analysis on crypto exchanges and on-chain transactions, crypto derivatives, cross-chain communication and interoperability, incentive issues in blockchain scaling solutions, reliability of blockchain explorers, fundamental demand for cryptocurrencies, Web3 participant profiles, and the security design of investment crowdfunding to help investors and entrepreneurs harness "wisdom of the crowd." His other research also covers governance, human-genAI interaction, information economics, market microstructure, mechanism design, the theory of the firm, and traffic control.

Dr Li's research has appeared in leading business/finance journals including Journal of Finance, Review of Financial Studies, and Management Science as well as major computer science conferences/workshops including ACM Web (WWW) and Financial Cryptography (FC), among others. His ongoing research is recognized by the National Science Foundation (NSF) CAREER Award along with many other grants, and his past work has won the Yihong Xia Best Paper Award and Chicago Quantitative Alliance (CQA) academic paper competition along with many other paper prizes. He has taught blockchain technologies to executive, MBA, and undergraduate students, served on the committees of major blockchain conferences such as Financial Crypto, ACM Advances in Financial Technologies, CCS DeFi, and IEEE Crypto Valley, and partnered with the government and private sectors on blockchain economics research. Students in the Master of Management program have voted him the sole recipient of "Faculty of the Year" from the entire faculty.

Dr. Li is a frequent speaker to both academic and practitioner audiences. He has presented at many institutions/events including MIT, Michigan, Northwestern, NYU, UC Berkeley, Yale, National Bureau of Economic Research, IC3, Consensus, the Federal Reserve, U.S. Securities and Exchange Commission, and U.S. Department of Homeland Security National Training Center. A non-technical overview talk on some of his earlier blockchain research at UC Berkeley's Simons Institute for the Theory of Computing can be found here:

https://www.youtube.com/watch?v=5IybadmGPtM&feature=youtu.be

Composition of Authenticated Byzantine Agreement under Man-in-middle Attack

Jichen Li (李济宸)
Peking University

Byzantine Agreement/Generals is a fundamental problem in distributed computing and serves as the foundation for many consensus protocols and MPC (Multi-Party Computation) protocols. To achieve Byzantine Agreement in the plain model, Lamport et al. demonstrated that any protocol can tolerate at most fewer than 1/3 malicious players. They further showed that by augmenting the network with a public-key infrastructure for digital signatures, it is possible to design protocols that are secure against any number of corrupted parties.

However, in real-world scenarios, multiple Authenticated Byzantine Agreement protocols are often executed concurrently with a single common setup. This setup is vulnerable to man-in-the-middle attacks, where the attacker does not corrupt players but can reorder messages within the channel. Our results show that:

(1)Authenticated Byzantine Agreement protocols can notremain secure under parallel composition (even for just two executions) and tolerate (n-1)/2 number of channel attack, even when all players are honest.

(2)We propose a deterministic Authenticated Byzantine Agreement protocols that tolerate (n-2)/2 number of channel attack and remain secure for concurrent composition.

Bio: Jichen Li is a fifth-year PhD student at Peking University, supervised by Prof.
Xiaotie Deng. His research focuses on blockchain, with a particular dedication to analyzing the economic security of existing blockchain protocols using techniques such as game theory, algorithm analysis, and reinforcement learning. His work on blockchain has been accepted by conferences such as ESORICS, WINE, AAMAS, IPDPS and ICDCS.

Jan 9 Afternoon

Online Ad Allocation via Relax-and-Round

Zhiyi Huang(黄志毅)
The University of Hong Kong

We initiate the study of Stochastic Online Correlated Selection (SOCS), a family of online

rounding algorithms for the general Non-IID model of Stochastic Online Submodular Welfare Maximization and its special cases such as unweighted and vertex-weighted Online Stochastic Matching, Stochastic AdWords, and Stochastic Display Ads. At each time step, the algorithm sees the type of an online item and a fractional allocation of the item, then immediately allocates the item to an agent. We propose a metric called the convergence rate that measures the quality of SOCS algorithms in the above special cases. This is cleaner than most metrics in the related Online Correlated Selection (OCS) literature and may be of independent interest. Following this framework, we make progress on numerous problems including two open questions related to AdWords.
This talk is based on a paper published in FOCS 2024 (https://arxiv.org/abs/2408.12524).

Bio: Zhiyi Huang is an Associate Professor of Computer Science at the University of Hong Kong. He works broadly on algorithms, focusing on the role of information and uncertainty in computation. He is interested in algorithms for sequential decision-making under uncertainty (online algorithms), learning based on different forms of information (learning theory), incentivizing self-interested agents to share private information (mechanism design), and disclosing one kind of information while keeping the other confidential (differential privacy).
Zhiyi's research was recognized by several Best Paper Awards, including those from ESA 2024 (Track S), FOCS 2020, and SPAA 2015. He was also the recipient of an Excellent Young Scientists Fund (HK & Macau) by NSFC, an Early Career Award by RGC Hong Kong.

Incentivizing Truth Exploration and Honest Reporting: A Contract Design Approach

Zhixuan Fang(房智轩)
Tsinghua University

In this paper, we study a Principal-Agent problem in which a principal incentivizes an agent by establishing a payment contract that encourages the agent to exert costly effort in exploring the true state of the environment, which is of interest to the principal, and then report the findings. We consider two feedback setups: (1) the true state is ultimately observable by the principal, and (2) only some noisy feedback related to the true state is observable. In the first setup, we demonstrate that the optimal contract is the one that pays the agent only when the report matches the ground truth, and we derive an efficient algorithm to compute this optimal contract. In the second setup, we design a BDD contract and show its approximate optimality with respect to the optimal honest-reporting incentivizing contract, both theoretically and empirically. Furthermore, we introduce a sufficient condition under which the optimal contract encourages honest reporting.

Bio: Zhixuan Fang is a tenure-track assistant professor at the Institute for Interdisciplinary Information Sciences (IIIS) at Tsinghua University, Beijing, China. His research interests are in the design and analysis of multi-agent systems, blockchain and networked systems. He received his Ph.D. degree in computer science from Tsinghua University, China, in 2018, and his B.S. degree in physics from Peking University, China, in 2013.

Recent Developments in the Study of Transaction Fee Mechanisms

Yotam Gafni
Weizmann Institute

To allocate transactions to blocks, cryptocurrencies use an auction-like transaction fee mechanism (TFM). The study of TFMs, initiated by [Lavi, Sattath & Zohar ’17] and consolidated by [Roughgarden ’21], [Chung & Shi ’21], has differed from traditional auction design in requiring more robust guarantees beyond user incentive-compatibility, namely with regards to the miner (auctioneer) and collusion-resistance. I will review some recent results by myself and others w.r.t. the variety of these notions and the types of mechanisms (or impossibilities) they induce.

Bio: Yotam Gafni has received his PhD in Operations Research at Technion, where he was advised by Ron Lavi and Moshe Tennenholtz. He holds a BA in Math and Philosophy from the Hebrew University. Yotam was a research member at SLMath Berkeley’s Fall semester 2023 program for market and mechanism design, and is currently a postdoc at Weizmann institute hosted by Uri Feige and Shahar Dobzinski.

Learning a Stackelberg Leader's Incentive from Optimal Commitments

Yurong Chen(陈昱蓉)
INRIA

Stackelberg equilibria are determined by the payoffs of the leader and the follower. This association makes it possible for one to probe into the leader's incentives from equilibrium samples between the leader and different types of followers. In this paper, we study to what extent one can learn about the leader's payoff information by actively querying the leader's optimal commitments in Stackelberg equilibria. We show that, by using polynomially many queries and operations, one can learn a payoff function that is strategically equivalent to the leader's original payoffs, in the sense that: 1) it preserves the leader's preference over almost all strategy profiles; and 2) it preserves the set of all possible (strong) Stackelberg equilibria the leader may engage in, considering all possible follower types. As an application, we show that the information acquired by our algorithm is sufficient for a follower to induce the best possible Stackelberg equilibrium by imitating a different follower type. To the best of our knowledge, we are the first to demonstrate that this is possible without knowing the leader's payoffs beforehand.

Bio: Yurong Chen is a postdoctoral researcher with the SIERRA team at INRIA Paris, working with Michael I. Jordan. She earned her PhD in Computer Science from Peking University, where she was advised by Xiaotie Deng, and holds a bachelor's degree in Applied Mathematics from the Hua Luogeng Honors Class at Beihang University. Her research focuses on the intersection of learning and game theory, exploring how strategic and learning agents interact. She is a recipient of the Best Student Paper Award at WINE 2022.

Jan 10 Morning

Price Stability and Improved Buyer Utility through Allocation of Prominence

Hu Fu(伏虎)
Shanghai University of Finance and Economics

Platforms design the form of presentation by which sellers are shown to the buyers. This design not only shapes the buyers' experience but also leads to different market equilibria or dynamics. One component in this design is through the platform's mediation of the search frictions experienced by the buyers for different sellers. We take a model of monopolistic competition and show that, on one hand, when all sellers have the same inspection costs, the market sees no stable price since the sellers always have incentives to undercut each other, and, on the other hand, the platform may stabilize the price by giving prominence to one seller chosen by a carefully designed mechanism. This calls to mind Amazon's Buy Box design. We study natural mechanisms for choosing the prominent seller, characterize the range of equilibrium prices implementable by them, and find that in certain scenarios the buyers' surplus improves as the search friction increases.

Bio: Hu Fu is an associate professor at Shanghai University of Finance and Economics, Institute for Theoretical Computer Science. He obtained his PhD in Computer Science from Cornell University, worked at Microsoft Research New England Lab and Caltech as a postdoc, and at University of British Columbia as an assistant professor. His research is mainly on computational problems from economic contexts, and online decision and optimization problems.

MMS Allocation of Indivisible Chores with Subadditive Valuations and the Fair Surveillance Assignment Problem

Bo Li(李博)
Hong Kong Polytechnic University

We study the maximin share (MMS) fair allocation of m indivisible chores to n agents who have costs for completing the assigned chores. It is known that exact MMS fairness cannot be guaranteed, and so far the best-known approximation for additive cost functions is $13/11$ by Huang and Segal-Halevi [EC, 2023]; however, beyond additivity, very little is known. In this work, we first prove that no algorithm can ensure better than $\min\{n, \log m/\log\log m\}$-approximation if the cost functions are submodular. This result also shows a sharp contrast with the allocation of goods where constant approximations exist as shown by Barman and Krishnamurthy [TEAC, 2020] and Ghodsi et al. [AIJ, 2022]. We then prove that for subadditive costs, there always exists an allocation that is $\min\{n, [\log m]\}$-approximation, and thus the approximation ratio is asymptotically tight. Due to the hardness result for general subadditive costs, we turn to study specific subadditive costs, e.g., vertex cover, which is called the fair surveillance assignment problem, and more. For these settings, we show that constant approximate allocations exist.

Bio: Bo Li is an assistant professor in the Department of Computing at The Hong Kong Polytechnic University. Formerly, he was a Postdoctoral Fellow at the University of Oxford and the University of Texas at Austin. He received his Ph.D. in Computer Science from Stony Brook University and B.S. in Applied Maths from Ocean University of China. He is broadly interested in algorithms, AI, and game theory.

Competitive Information Design with Asymmetric Senders

Zihe Wang(王子贺)
Renmin University of China

We consider a competitive information design game in which a number of ex-ante asymmetric senders are competing for a receiver by disclosing information about their respective realizations. Unlike the setting with symmetric senders where a symmetric equilibrium always exists, the equilibrium may not exist under the asymmetric setting. Using the idea of discrete approximation and passing to the limit, we show that if there is no mass point in the senders' priors, then an equilibrium always exists. We next establish the necessary and sufficient conditions for the equilibrium structure. Our characterizations strictly generalize the symmetric equilibrium conditions provided in the symmetric environment studied in previous works. We then use the characterized equilibrium structure to solve the equilibrium for a general two-sender game along with providing a computational method of computing it.

Bio: Zihe Wang received his bachelor's degree from Tsinghua Institute of Interdisciplinary Information in 2011. In 2016, he received his Ph.D. from the Institute of Interdisciplinary Information, Tsinghua University. He is currently an assistant professor at the Gaoling School of Artificial Intelligence. In particular, his interests include the computation of Nash equilibria in games, designing mechanisms to achieve the goals of the mechanism designer.

Competition among Mechanism Designers: A Contest-Theoretic Perspective

Weian Li(李维安)
Shandong University

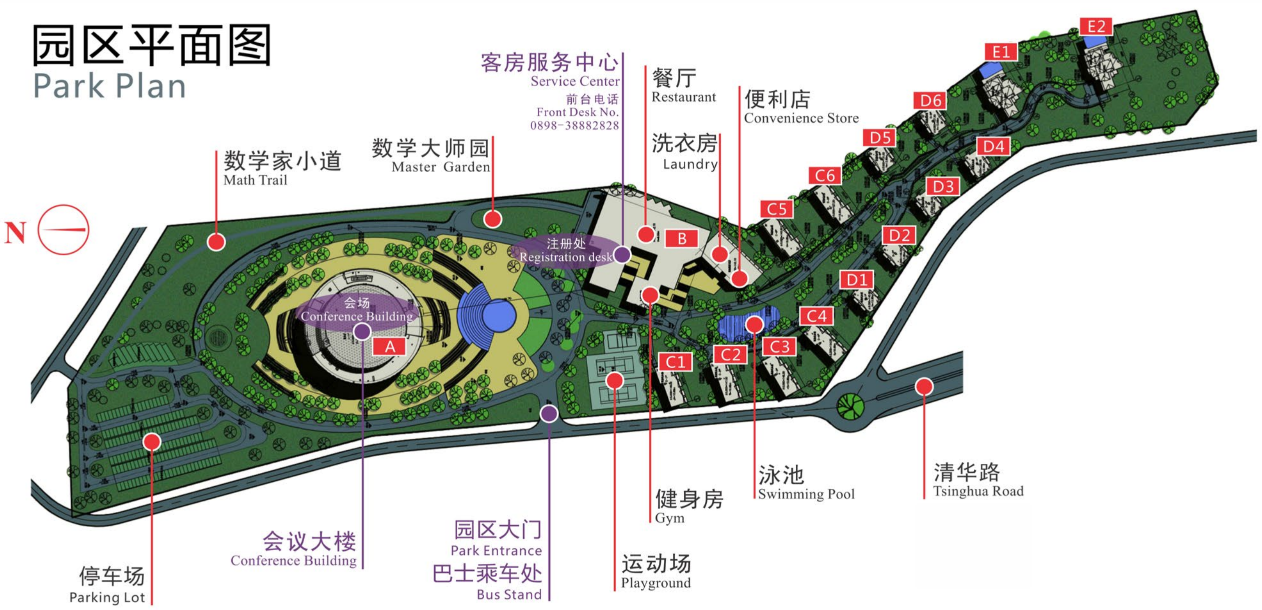
Game theory studies how players optimize strategies to maximize utility, often focusing on outcomes such as Nash equilibria. Mechanism design extends this framework by exploring how designers optimize game rules to achieve desired objectives. This talk mainly discusses strategic interactions among multiple mechanism designers, examining the outcome of their competition.
Using contest theory as a foundation, we develop a two-stage game model. In the first stage, contest designers compete by setting contest configurations, and in the second stage, contestants pursue the prizes by optimizing their strategies. We investigate the characterization and computation of key concepts, including best responses and equilibria, offering insights into competition among mechanism designers.

Bio: Weian Li is an associate researcher at the School of Software, Shandong University. He obtained his Ph.D. from the Hong Kong University of Science and Technology in 2021. Before joining Shandong University, he was a postdoctoral researcher at the Center on Frontiers of Computing Studies, Peking University. His research focuses on economics and computation, particularly algorithmic game theory, mechanism design, and Internet economics. His work has been published in several conferences and journals, including WINE, KDD, AAAI, TCS, and COCOON.

The facilities of TSIMF are built on a 23-acre land surrounded by pristine environment at Phoenix Hill of Phoenix Township. The total square footage of all the facilities is over 29,000 square meter that includes state-of-the-art conference facilities (over 10,000 square meter) to hold many international workshops simultaneously, two reading rooms of library, a guest house (over 10,000 square meter) and the associated catering facilities, a large swimming pool, gym and sports court and other recreational facilities.

Management Center of Tsinghua Sanya International Forum is responsible for the construction, operation, management and service of TSIMF. The mission of TSIMF is to become a base for scientific innovations, and for nurturing of innovative human resource; through the interaction between leading mathematicians and core research groups in pure mathematics, applied mathematics, statistics, theoretical physics, applied physics, theoretical biology and other relating disciplines, TSIMF will provide a platform for exploring new directions, developing new methods, nurturing mathematical talents, and working to raise the level of mathematical research in China.

About Facilities



Registration

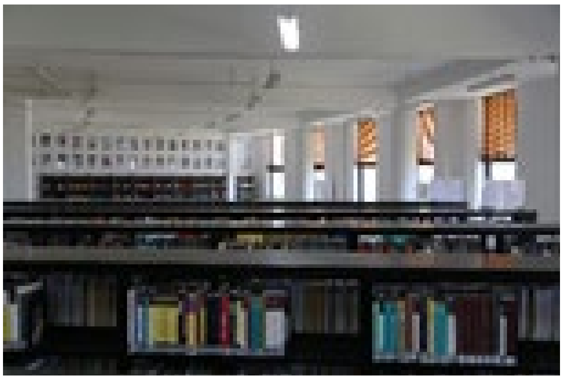
Conference booklets, room keys and name badges for all participants will be distributed at the front desk. Please take good care of your name badge. It is also your meal card and entrance ticket for all events.

Guest Room

All the rooms are equipped with: free Wi-Fi (Password:tsimf123), TV, air conditioning and other utilities.

Family rooms are also equipped with kitchen and refrigerator.

Library



Opening Hours: 09:00am-22:00pm

TSIMF library is available during the conference and can be accessed by using your room card. There is no need to sign out books but we ask that you kindly return any borrowed books to the book cart in library before your departure.

In order to give readers a better understanding of the contributions made by the Fields Medalists, the library of Tsinghua Sanya International Mathematics Forum (TSIMF) instituted the Special Collection of Fields Medalists as permanent collection of the library to serve the mathematical researchers and readers.

So far, there are 271 books from 49 authors in the Special Collection of Fields Medalists of TSIMF library. They are on display in room A220. The participants are welcome to visit.

Restaurant

All the meals are provided in the restaurant (Building B1) according to the time schedule.

Breakfast	07:30-08:45
Lunch	12:00-13:30
Dinner	17:30-19:00

Laundry

Opening Hours: 24 hours
The self-service laundry room is located in the Building(B1).

Gym

Opening Hours: 24 hours
The gym is located in the Building 1 (B1), opposite to the reception hall. The gym provides various fitness equipment, as well as pool tables, tennis tables etc.

Playground

Playground is located on the east of the central gate. There you can play basketball, tennis and badminton. Meanwhile, you can borrow table tennis, basketball, tennis balls and badminton at the reception desk.

Swimming Pool

Please enter the pool during the open hours, swimming attire and swim caps are required, if you feel unwell while swimming, please stop swimming immediately and get out of the pool. The depth of the pool is 1.2M-1.8M.
Opening Hours: 13:00-14:00 18:00-21:00

Free Shuttle Bus Service at TSIMF

We provide free shuttle bus for participants and you are always welcome to take our shuttle bus, all you need to do is wave your hands to stop the bus.

Destinations: Conference Building, Reception Room, Restaurant, Swimming Pool, Hotel etc.

Contact Information of Administration Staff

Location of Conference Affairs Office: Room 104, Building A
Tel: 0086-898-38263896
Conference Affairs: Shouxi He 何守喜
Tel:0086-186-8980-2225
Email: heshouxi@tsinghua.edu.cn

Location of Accommodation Affairs Office: Room 200, Building B1
Tel: 0086-898-38882828
Accommodation Manager: Ms. Li YE 叶莉
Tel: 0086-139-7679-8300
Email: yel@tsinghua.edu.cn

IT
Yuanhang Zhou 周远航
Tel: 0086-133-6898-0169
Email: 13368980169@163.com

*Reception duty hours: 7:00-23:00, chamber service please call: 0086-38882828 (exterior line) 80000 (internal line)
*Room maintainer night duty hours: 23:00-7:00, if you need maintenance services, please call: 0086-38263909 (exterior line) 30162 (internal line)

Director Assistant of TSIMF
Kai CUI 崔凯
Tel/Wechat: 0086- 136-1120-7077
Email :cuik@tsinghua.edu.cn

Director of TSIMF
Prof.Xuan GAO 高瑄
Tel: 0086-186-0893-0631
Email: gaoxuan@tsinghua.edu.cn

清华大学三亚国际论坛管理中心 | 三亚清华数学论坛管理中心
Tsinghua Sanya International Mathematics Forum (TSIMF)

☎ 0086-898-38882828
0086-898-38883896
FAX 0086-898-38883895
tsimf@tsinghua.edu.cn
✉ 572000
https://www.tsimf.cn
海南省三亚市天涯区清华路 100 号，清华三亚国际数学论坛
No.100, Tsinghua Road, Tianya District, Sanya, Hainan, P. R. China.