JUNMING KE

No.1500, Shunhua Road, Lixia District, Ji'nan, Shandong Province, 250101, P. R. China
+65 87793038, Junmingke1994@gmail.com

EDUCATION

School of Computer Science and Technology, Shandong University *September 2016 - July 2019*
College of Science, Zhejiang University of Technology *September 2012 - July 2016*

TECHNICAL STRENGTHS

Computer Languages JavaScript, MATLAB, GO, Python
Software & Tools HTML, LaTeX, Illustrator, SQL

INTERNSHIP EXPERIENCES

Zhejiang University CAD&CG State Key Laboratory VAG Group May 2015 - August 2016
Internship Research

· 2015.04-2016.02: Crime forecast based on the urban data
Invoking the data interface which provided by Tgram Information Science and Technology Co., Ltd, Hangzhou, extracting partial desensitization data and establishing economic model to predict target groups human behavior every mouth. We finally provide the probability of the prediction and highlight the high risk population to the related supervisor.

· 2016.02-2016.04: Visualization of the urban data mining
Visualization of the resident population, temporary population, the police officers information, the checkpoint information and so on. Meanwhile, the system output the real-time monitoring information, this system was built for related supervisor.

· 2016.04-2016.08: Visual analysis of network information security
This project was cooperated with Chinese Academy of Sciences (CAS). CAS provided the nodes information, including communication node, IP address, and email information. We designed a data analysis system, the system invoke the interface appropriately and using the nodes connecting information to find the adjacent nodes. The system analysis the interested nodes statistical information from both macrocosm and microcosm aspects, in addition to this, the system also provided the variety of interaction patterns.

· Programming with MATLAB, JavaScript, Java, HTML and CSS, including invoke the data interface, build the sites page and design the interaction pattern.

Sansec Inc., China May 2017 - October 2017
Blockchain Application

· Established a web system that supports the data mall application based on the blockchain.
· Configured the application programming interface based on Fabric(original version) and Ethereum(latest version).

Singapore University of Technology and Design(In progress) January 2019 - December 2019
Applied Cryptography

· Under supervisor Pawel Szalachowski(PI) and Jianying Zhou(Co-PI), Conducting blockchain research. Including contingency plans for Bitcoin, the consensus in proof of stake scheme, and the attacks on the Bitcoin.

ACADEMIC PUBLICATION

Lu Junhua, Chen Wei, Ma Yuxin, Ke Junming, Li Zhongzhuan, & Zhang Fan (2017). Recent progress and trends in predictive visual analytics. Frontiers of Computer Science, 11(2), 192-207.
This paper surveyed current progress and trends in predictive visual analytics, and identified the common framework in which predictive visual analytics systems operate, and we also developed a summarization of the predictive analytics workflow.

Wang Hao, Song Xiangfu, Ke Junming, et al. Blockchain and Privacy Preserving Mechanisms in Cryptocurrency[J]. Netinfo Security, 2017(7):32-39. (Chinese)
This paper discusses the working principle of blockchain in cryptocurrency by comparing with the bitcoin system, introduces some typical consensuses mechanisms used in blockchain technology, analyzes the challenges of anonymity and privacy protection in cryptocurrency, and introduces the existing anonymous and privacy protection schemes.

Zhao Shengnan, Jiang Han, Wei Xiaochao, KE Junming, & Zhao Minghao. (2017). An Efficient Single Server-Aided k-out-of-n Oblivious Transfer Protocol. Journal of Computer Research and Development, 54(10), 2215-2223. (Chinese)
In this paper, we propose a service-assisted k-out-of-n OT protocol in single server architecture, which outsources the vast majority of exponentiation operations to the cloud. This scheme is constructed with secret sharing and other fundamental public-key primitives, and it achieves provable security on none-collusion semi-honest model under the Decisional Diffie-Hellamn (DDH) hard problem; meanwhile it ensures data privacy against the cloud server. Besides, a detailed description of scheme construction and security proof is presented in the context.

Junming Ke, Han Jiang, Xiangfu Song, Shengnan Zhao, Hao Wang, Qiuliang Xu. Analysis on the Block Reward of Fork After Withholding, 12th International Conference on Network and System Security 2018.
In this paper, we firstly give a detailed comparation between the BWH and FAW attack, and show the implications behind them. We also consider honest mining to make the analysis of the block reward more clear. We demonstrate the imperfection of FAW in relative reward, reward after the fork and the fork state. Our main finding for FAW attack includes that the reward of victim pool increases faster compared to BWH attack, and for some cases, the attack should adopt honest mining strategy to maximize its reward, therefore, we present an improved FAW strategy, and propose a protocol for the pools manager to resist FAWs attacker. Finally, we discuss the underlying flaws of FAW attack as well as countermeasures to alleviate it.

Liu Yiran, Ke Junming, Jiang Han, Song Xiangfu. Improvement of the PoS Consensus Mechanism in Blockchain Based on Shapley Value. Journal of Computer Research and Development.(Chinese)
Based on the principle of calculating Shapley value in Game Theory, this paper improves the distribution of reward in the mechanism of the PoS consensus mechanism, makes the reward distribution of the nodes participated in the generated block in the PoS mechanism more fair and reasonable, and it can also reverse the social stratification in the blockchain, thus greatly improving the possibility of the new small node gaining the benefit. In addtion, we apply the same ideas in the Ouroboros protocol to improve its revenue distribution algorithm so that it satisfies survivability and durability.

Junming Ke, Qiuliang Xu, Pawel Szalachowsk, Jianying Zhou(2019). IBWH: A Novel Intermittent Block Withholding Attack for Optimal Mining Reward Rate. (Accepted, ISC 2019)
This paper gives a detailed analysis of the dynamic reward of the BWH attacker while considering a more realistic model with the computing power changing incessantly. In the course of analysis, we divided the reward rate into four stages, which indicates distinct periodic reward. We propose a novel

attack called the intermittent block withholding (IBWH) attack and we prove that this attack is optimal in our model. IBWH is a strategy where an attacker influences the reward period time, consequently enlarging the reward rate. Furthermore, in our model, we include the dynamics of the Bitcoin network's computing power, and even with the changing attacker's reward rates, we show that the IBWH's reward rate remains optimal. We consider both the selfish mining attack and the fork after withholding (FAW) attack, and we show that these attacks do not outperform IBWH.

Pawel Szalachowski, Daniel Reijsbergen, Junming Ke, Zengpeng Li (2019). ProPoS: Large-scale Probabilistic Proof-of-Stake Protocol. (On the submission of NDSS 2020)

Junming Ke, Pawel Szalachowski, Jianying Zhou, Qiuliang Xu (2019). Formalize Bitcoin Contingency Plans: A Framework to Evaluate the Breach and Recover the Protocol. (Preparing for FC 2020)

ACADEMIC ACTIVITIES

IET Information Security - Reviewer(2019-)
ChinaCrypt - Organizing Committee(2017)

AWARDS & HONORS

Names	Organizations
School Scholarship(twice)	Shandong University
Annual Appraisal of Advanced Individuals	Shandong University
Mathematical Contest in Modeling Meritorious Winner	COMAP(USA)
School Scholarship(twice)	Zhejiang University of Technology

PERSONAL STATEMENT

I was majored in Information and Computer Science in college, and learned the math foundation courses such as algebra and mathematical analysis. In junior year, I participated in Mathematical Contest in Modeling, which was organized by the Consortium for Mathematics and Its Application, and I was given a Meritorious Winner award for the paper "Eradicating the Ebola". After that, I visited and studied in Computer Aided Design & Computer Graph state key laboratory Visual Analyze Group (VAG), Zhejiang University for one and a half year, under supervisor Prof. Wei Chen (http://www.cad.zju.edu.cn/home/chenwei/). I participated three projects in VAG, such as crime forecast based on the urban data project. This is a data mining project, we analyzed urban data, utilizing economic model and forecasting a given group of human beings behavior. My task was selecting data from Oracle,data selection, data cleaning and programming with SQL.

I was recommended for admission to the School of Computer Science and Technology, Shandong University, under supervisor Prof. Qiuliang Xu(https://www.researchgate.net/profile/Qiuliang_Xu/2). My research focus on Blockchain and Applied Cryptography, and I have accomplished some researches about foundation crypto theory with my classmates, such as improving Oblivious Transmission, surveying blockchain security, improving Proof-of-Stake consensus mechanism in blockchain based on Shapley value and so on.

Now I am working on Blockchain security in iTrust, Singapore University of Technology and Design, with Prof. Jianying(http://jianying.space/) and Prof. Pawel(https://pszal.github.io/).

MISCELLANY

Speaker at the 2018 International Conference on Network and System Security held by the Hong Kong Polytechnic University, August 2018.

Vice Minister of Graduate Student Union, Shandong University, May 2017.

A member of colour guard, Zhejiang University of Technology, December 2013.