Inscrypt 2024

20th China International Conference on Information Security and Cryptology

&

SSR 2024

9th Security Standardisation Research Conference

Program

December 13-16, 2024
Kunming, China

Conference Information

Conference Venue: Lakeview Hall of the Lakeview Hotel Yulongwan Kunming

Registration and Information:

December 13, 13:00－19:00. Lobby of Hotel

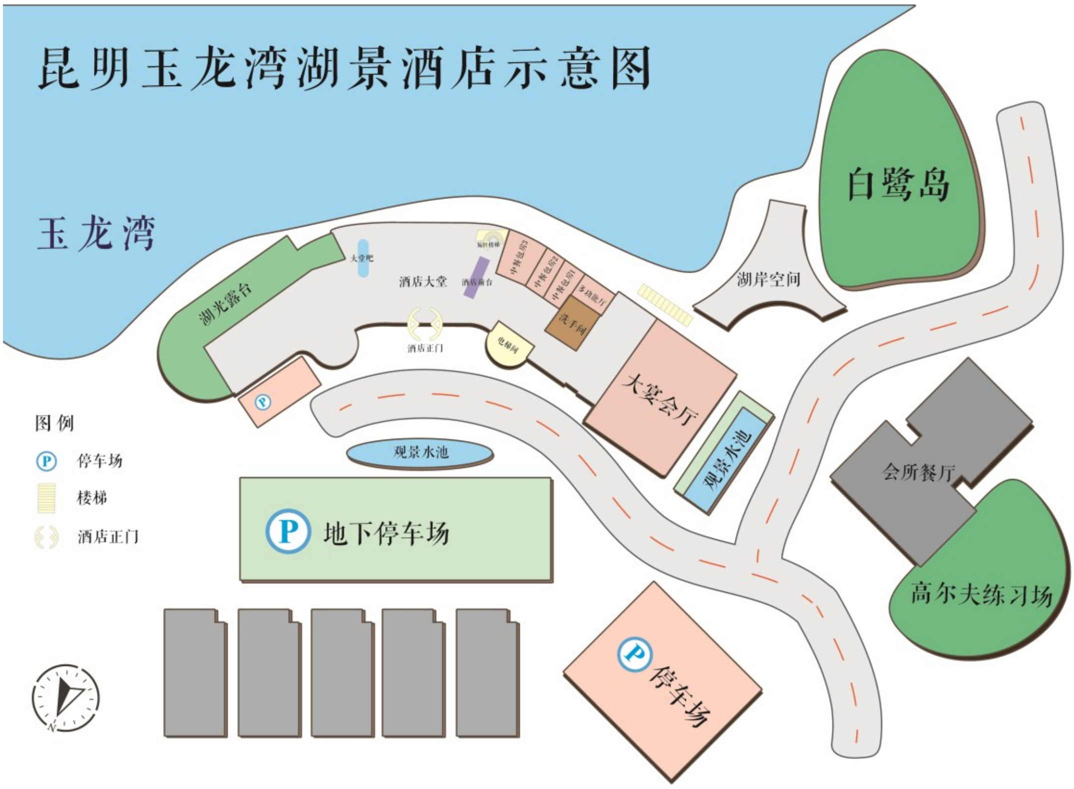
December 14, 07:30－18:00. the Lakeview Hall of Lobby Level (Conference site)

December 15-16, 08:00－18:00. the Lakeview Hall of Lobby Level

Lunches and dinners are served at the All-Day Dinning Restaurant (全日制餐厅) located at the 1A Level of the Hotel.. Tickets for registered participants are in the registration bags. Extra tickets could be purchased at the registration table.

Wifi: Participants may access to the free network at hotel area.

Taxi: Participants may call a taxi by using apps of their cellphone, such as Didi.



Program Sketch

20th China International Conference on Information Security and Cryptology
and
9th Security Standardisation Research Conference

(Inscrypt 2024 & SSR 2024)

December 13 – 16, 2014, Kunming China

Dec 13	14:00-19:00	Conference on site registration	Lobby of the Hotel
	18:00-21:00	Reception	The All-Day Dinning Restaurant of the Hotel
Dec 14	7:00-12:00	Conference on site registration	The Lakeview Hall of Lobby Level
	9:00-9:10	Opening Remarks	The Lakeview Hall of Lobby Level
	9:10-10:10	Invited Talk (I)	
	10:10-10:25	Group Photo	The Hotel Outdoor Lawn
	10:45-12:25	Session 1	The Lakeview Hall of Lobby Level
	12:30-13:30	Lunch	The All-Day Dinning Restaurant of the Hotel
	13:30-15:35	Session 2	The Lakeview Hall of Lobby Level
	15:55-18:25	Session 3	
	18:30-20:00	Dinner	
	20:00-21:00	Rump Session	The All-Day Dinning Restaurant of the Hotel
Dec 15	8:30-9:30	Invited Talk (II)	The Lakeview Hall of Lobby Level
	9:30-10:30	Session 4	
	10:40-12:20	Session 5	
	12:30-13:30	Lunch	The All-Day Dinning Restaurant of the Hotel
	13:30-15:35	Session 6	The Lakeview Hall of Lobby Level
	15:55-18:25	Session 7	
	18:30-21:00	Conference Banquet	The All-Day Dinning Restaurant of the Hotel
Dec 16	8:30-9:30	Invited Talk (III)	The Lakeview Hall of Lobby Level
	9:30-10:30	Invited Talk (IV)	
	10:50-12:30	Session 8	
	12:30-13:30	Lunch	The All-Day Dinning Restaurant of the Hotel
	13:30-15:35	Session 9A	The Lakeview Hall of Lobby Level
		Session 9B/10B	Meeting Room of 1A Level
	15:55-18:25	Session 10A	The Lakeview Hall of Lobby Level
		Session 11B	Meeting Room of 1A Level
	18:30-20:00	Dinner	The All-Day Dinning Restaurant of the Hotel
Dec 17		Tour (only travel agent assistance provided)	

All lectures are in the Lakeview Hotel Yulongwan Kunming（昆明玉龙湾湖景酒店）

Advanced Program

20th China International Conference on Information Security and Cryptology
and
9th Security Standardisation Research Conference
(Inscrypt 2024 & SSR 2024)
Lakeview Hotel Yulongwan Kunming

December 13, 2024	
14:00-19:00	**Conference on site registration**
18:00-21:00	**Reception**
December 14, 2024	
7:00-12:00	**Conference on site registration**
9:00-9:10	**Opening Remarks**
Invited Talk (I) : **Session Chair:**	
9:10-10:10	Black-Box Attacks on Perceptual Hash Functions *Bart Preneel*
10:10-10:25	**Group photo**
10:25-10:45	**Tea Break**
Session 1: AI AND SECURITY **Session Chair:**	
10:45-11:10	Analyzing Decentralized Applications Traffic: A Multimodal Approach Based on GNN and BERT *Haoyang Lu, Rui Zhang and Tong Kong*
11:10-11:35	EditPSM: A New Password Strength Meter Based on Password Reuse via Deep Learning *Yifei Zhang, Zhenduo Hou, Yunkai Zou, Zhen Li and Ding Wang*
11:35-12:00	A Binary Code Similarity Detection Method Based on Cross-Modal Coordinated Representation Learning *Hongyu Yang, Yunlong Wang, Ze Hu and Xiang Cheng*
12:00-12:25	Malware Detection Method Based on Multi-Dimensional Dynamic weighted alpha Image Fusion and Feature Enhancement *Lixia Xie, Chenyang Wei, Hongyu Yang, Ze Hu and Xiang Cheng*
12:30-13:30	**Lunch**
Session 2: SYMMETRIC CRYPTANALYSIS (I) **Session Chair:**	
13:30-13:55	Committing Security of AEAD Based on Stream Cipher *Xueqi Zhu, Yan Jia, Jun Xu and Peng Wang*
13:55-14:20	Integral Attacks Against DIBO Structures: A Low-Complexity Key Extraction Method *Xinming Zhu, Shihui Zheng and Zihao Han*
14:20-14:45	Cube Attacks against Trivium, Kreyvium and ACORN with Practical Complexity *Yanqi Chen, Ting Li and Yao Sun*

14:45-15:10	Improving the Search Algorithm for the Best Differential/Linear Trails of Bit-Permutation-Based Ciphers *Jingsui Weng, Wentao Zhang, Ting Peng and Tianyou Ding*
15:10-15:35	A Note on Neutral Bits for ARX Ciphers from the Perspective of BCT *Jiahao Zhao, Qianqian Yang, Ling Song and Lei Hu*
15:35-15:55	**Tea Break**
Session 3: PUBLIC KEY CRYPTOSYSTEMS (I) AND SECURITY PROTOCOLS **Session Chair:**	
15:55-16:20	On Concrete Security Treatment of Signatures Based on Multiple Discrete Logarithms *George Teseleanu*
16:20-16:45	Solving Modular Linear Equations via Automated Coppersmith and its Applications *Yansong Feng, Zhen Liu, Abderrahmane Nitaj and Yanbin Pan*
16:45-17:10	How to Construct Public Timeline for RSA-formed Time-Lock Cryptography *Huixuan Jin, Cong Peng, Jintao Fu and Min Luo*
17:10-17:35	Permutation Checks via Basis Transformation *Yu Wang*
17:35-18:00	Efficient and Verifiable Multi-Server Framework for Secure Information Classification and Storage *Ziqing Guo, Yaohui Wang, Xuanyu Jin, Xiuhua Wang, Yuanyuan He and Yueyue Dai*
18:00-18:25	Formal Analysis of WAPI Authentication and Key Agreement Protocol *Zhongqi Lv, Hui Li, Haisong Ye, Chi Ma and Jingjing Guan*
18:30-20:00	**Dinner**

December 15, 2024

Invited Talk (II) : Session Chair:	
8:30-9:30	Agility By Design: Cryptography for Evolving Ecosystems *Moti Yung*
Session 4: SECURITY ANALYSIS **Session Chair:**	
9:30-9:55	Attention-based Decompilation through Neural Machine Translation *Ruigang Liang and Ying Cao*
9:55-10:20	DBridger: Discovering Vulnerable Data Sharing Paths in Embedded Firmware *Linyu Li, Lei Yu, Qingli Guo, Ruixuan Zhang, Can Yang, Jun Guan and Xiaorui Gong*
10:20-10:40	**Tea Break**
Session 5: BIG DATA AND CLOUD SECURITY **Session Chair:**	
10:40-11:05	Revocable Registered attribute-based keyword search Supporting Fairness *Zongmin Wang, Qiang Wang, Fucai Zhou and Jian Xu*
11:05-11:30	HiddenStor: A Steganographic Storage System Built on Secret Sharing *Siyuan Ma, Yuewu Wang, Chunjing Kou, Peng Wang, Haotian Shi and Jiwu Jing*
11:30-11:55	ECGRQ-LI: Efficient Conjunctive Geometric Range Query over Encrypted Spatial Data with Learned Index *Mingyue Li and Yuting Zhu*

11:55-12:20	TA-DPDP: Dynamic Provable Data Possession for Online Collaborative System with Tractable Anonymous *Chenchen Wu, Weijing You and Li Xu*
12:20-13:30	**Lunch**
Session 6: PUBLIC KEY CRYPTOSYSTEMS (II) **Session Chair:**	
13:30-13:55	Extended Policy-based Sanitizable Signatures *Ismail Afia and Riham Altawy*
13:55-14:20	Practical Generic Construction of Fully Collision Resistant Chameleon Hash and Instantiations *Siyue Yao, Zhikang Xie and Man Ho Au*
14:20-14:45	Quasi-Linearly Homomorphic Signature for Data Integrity Auditing in Cloud Storage *Futai Zhang, Yichi Huang, Wenjie Yang and Jinmei Tian*
14:45-15:10	Generalized Cryptanalysis of Cubic Pell RSA *Hao Kang and Mengce Zheng*
15:10-15:35	Hierarchical Functional Encryption for Quadratic Transformation *Jun Zhao, Kai Zhang, Junqing Gong and Haifeng Qian*
15:35-15:55	**Tea Break**
Session 7: SYMMETRIC CRYPTANALYSIS (II) AND KEY EXCHANGE Session Chair:	
15:55-16:20	An Automatic Search Method For 4-bit S-box Towards Considering Cryptographic Properties and Hardware Area Simultaneously *Hongtao Hu, Chenhao Jia, Qing Ling, Sijia Gong, Ting Wu and Tingting Cui*
16:20-16:45	Revisiting Truncated Differential Attack from View of Equivalent Propagation Equations: Improved attacks on TWINE and LBlock *Shiqi Hou, Muzhou Li, Kai Hu, Shichang Wang and Bart Preneel*
16:45-17:10	Cryptanalysis of BAKSHEESH Block Cipher *Shengyuan Xu, Siwei Chen, Xiutao Feng, Zejun Xiang and Xiangyong Zeng*
17:10-17:35	Privacy-preserving Certificate-less Authenticated Key Exchange with Key Registration Privacy *Li Duan and Yong Li*
17:35-18:00	An Improved Signal Leakage Attack Against DXL Key Exchange Protocol *Zhiwei Li, Jun Xu and Lei Hu*
18:00-18:25	srCPace: Universally Composable PAKE with Subversion-Resilience *Jiahao Liu, Yi Wang, Rongmao Chen, Xincheng Tang and Jinshu Su*
18:30-21:00	**Conference Banquet**
December 16, 2024	
Invited Talk (III) : Session Chair:	
8:30-9:30	NIST Post-Quantum Cryptography Standardization *Lily Chen*
Invited Talk (IV) : **Session Char:**	
9:30-10:30	Title: *Liqun Chen*

10:30-10:50	**Tea Break**
Session 8: QUANTUM AND POST QUANTUM CRYPTOGRAPHY (I) **Session Chair:**	
10:50-11:15	Quantum Cryptanalysis of Generalized Unbalanced Feistel Structures: Distinguisher and Key Recovery Attack *Boyun Li and Qun Liu*
11:15-11:40	Simplified Periodic Distinguishers Searching: Application to GFS-4F/2F and Twine *Jingwen Chen, Qun Liu, Boyun Li, Jingbo Qiao and Jinliang Wang*
11:40-12:05	Fast Fourier Transform and Gaussian Sampling Instructions Designed for FALCON *Taoyun Wang, Shuaiyu Chen, Lu Li and Weijia Wang*
12:05-12:30	Quantum Public-Key Encryption of Quantum States, and More *Tianshu Shan, Shujiao Cao and Rui Xue*
12:30-13:30	**Lunch**
Session 9A: FOUNDATIONS AND IMPLEMENTATION OF CRYPTOSYSTEMS **Session Chair:**	
13:30-13:55	On the Relationship between Public Key Primitives via Indifferentiability *Shuang Hu, Bingsheng Zhang, Cong Zhang and Kui Ren*
13:55-14:20	Lattice-Based Succinct Mercurial Functional Commitment for Boolean Circuits: Definitions, and Constructions *Hongxiao Wang, Siu-Ming Yiu, Yanmin Zhao, Zoe L. Jiang and Min Xie*
14:20-14:45	From Signature with Re-Randomizable Keys: Generic Construction of PDPKS *Ziyi Li, Ruida Wang, Xianhui Lu, Yao Cheng and Liming Gao*
14:45-15:10	SIMD Optimizations of White-box Block Cipher Implementations with the Self-equivalence Framework *Luoqi Chen, Yufeng Tang, Liangju Zhao and Zheng Gong*
15:10-15:35	When Is Multi-Channel Better Than Single-Channel: A Case Study of Product-Based Multi-Channel Fusion Attacks *Shilong You, Jianfeng Du, Zhu Wang and Aimin Yu*
15:35-15:55	**Tea Break**
Session 10A: WATERMARKING AND PRIVACY-ENHANCING TECHNOLOGIES **Session Chair:**	
15:55-16:20	Dynamic Collusion Bounded Public-Key Watermarking Schemes *Siyuan Yu, Ziqi Zhu, Rupeng Yang and Junqing Gong*
16:20-16:45	A Lossless Relational Data Watermarking Scheme Based on Uneven Partitioning *Wenhao Xu and Hequn Xian*
16:45-17:10	CNNOVZKP: Convolutional Neural Network Model Ownership Verification with Zero-knowledge Proof *Yuhao Lian, Ying Ouyang and Deng Tang*
17:10-17:35	Efficient Privacy-Preserving Data Sharing Mechanisms Against Malicious Senders in Smart Grid *Jiangang Lu, Yunfan Yang, Qinqin Wu, Benhan Li and Mingxin Lu*
17:35-18:00	NEST: Strong Key-Insulated Password-Based Shared-Custodial Blockchain Wallets *Birou Gao, Rui Zhang, Yuting Xiao and Huan Zou*
18:00-18:25	Clustering Coefficient Estimating of Distributed Graph Data based on Shuffled Differential Privacy *Hongfa Ding, Peiwang Fu, Heling Jiang and Xuesong Li*

18:30-21:00	**Dinner**
Session 9B: THE VISION OF MPC AND BLOCKCHAIN STANDARDS **Session Chair:**	
13:30-14:00	The Vision of Multi-Party Computation Technical Standards *Jingqiang Lin and Zhiquan Gao*
14:00-14:30	Vision Paper: Do we need Standardization of Blockchain Consensus? *Zhaoxin Yang, Xiao Sui, Rujia Li, Mingfei Zhang and Sisi Duan*
Session 10B: SECURITY AND PRIVACY PROTECTION IN PRACTICAL APPLICATIONS Session Chair:	
14:30-15:00	Security and Privacy Evaluation of IP Cameras on Shodan *Cheok Ieng Ng and Maryam Mehrnezhad*
15:00-15:30	Limitations of Wrapping Protocols and TLS Channel Bindings: Formal-Methods Analysis of the Session Binding Proxy Protocol *Enis Golaszewski, Edward Zieglar, Alan T. Sherman, Kirellos Abou Elsaad and Jonathan D. Fuchs*
15:30-16:00	**Tea Break**
Session 11B: QUANTUM AND POST QUANTUM CRYPTOGRAPHY (II) **Session Chair:**	
16:00-16:30	SoK: Post-Quantum Key Encapsulation Mechanisms - Security Definitions, Constructions and Applications *Biming Zhou, Yiting Liu, Haodong Jiang and Yunlei Zhao*
16:30-17:00	Scloud+: An Efficient LWE-based KEM Without Ring/Module Structure *Anyu Wang, Zhongxiang Zheng, Chunhuan Zhao, Zhiyuan Qiu, Guang Zeng, Ye Yuan and Xiaoyun Wang*
17:00-17:30	Transitioning to Quantum Secure Encryption Schemes *Shao Huang, Songsong Li, Ying Ouyang and Yanhong Xu*
17:30-18:30	Panel Discussion
18:30-21:00	**Dinner**
December 17, 2024	
Tour (only travel agent assistance provided)	