Cong Zhang | Curriculum Vitae

192 Davidson Road,APT 159,Rutgers,Piscataway,NJ,08854

☎ +215 313 8948 • ✉ congresearch@gmail.com

Undergraduate mathematical science completing the sixth year of a Ph.D degree.Passionate about cryptography, with strong interpersonal skills for working in a team and successfully completing a project.

Education

○ **Rutgers University** — **New Brunswick, NJ**
Ph.D in Computer Science, — *2014–2020*
Major: Cryptography; GPA 3.969/4

○ **Peking University** — **Beijing China**
Master in Software Engineering — *2009–2012*
Major: Information Security; GPA 90.8/100

○ **Shandong University** — **Jinan China**
Bachelor in Science — *2005–2009*
Major: Mathematics and Applied Mathematics; GPA 90.1/100

Research on Security and Cryptography

Research Experience

○ **Indifferentiability in Public Key primitives** — **Princeton Univ**
Visiting student with Prof. Mark Zhandry — *Sep 2018–Present*
This project initiates the research problem of constructing public key primitives, that achieves indifferentiability, based on random oracle model and computational assumptions (double strong-CDH)[1]. In the current state, we extend our technique to generic group model, pairings, multi-linear maps and functional encryption, and explore the equivalence or barriers between each two models.

○ **Blockchain Related research** — **Rutgers Univ**
Research Assistant with Prof. Periklis Papakonstantinou and Prof. Qiang Tang — *Jun 2018–Present*
This project studies various research problems on blockchain related technology, e.g. how to build efficient consensus protocols; how to define proper privacy on blockchain protocols and so forth.

○ **Order Revealing Encryption** — **Princeton Univ**
Visiting student with Prof.Mark Zhandry — *Feb 2017–Present*
This project studies several fundamental problems on order-revealing encryption. We show the evidence that it is impossible to construct an ideal ORE in standard model/Random Oracle model/Generic Group model [3].

○ **Order Preserving/Revealing Encryption** — **Rutgers Univ**
RA with Prof.David Cash, Mark Zhandary, Adam O'Neil and Feng-Hao Liu — *Sep 2015–Jan 2017*
This project studies new leakage profile and privacy notion on order revealing encryption and we introduce a new leakage profile and two new privacy notions for ORE, which is the best leakage profile to the date that only applies bi-linear map [2,4].

- **Functional Encryption** **Columbia Univ**
  Research Assistant with Prof.Allison Bishop *Jun 2015–Sep 2015*
  This project investigate one specific functional encryption, comparison secret key encryption. We give an valid solution using multi-linear map and tribe matrix technique.
- **Leakage-Resilient Encryption** **Hong Kong Univ**
  Research Assistant with Prof.Siu-Ming Yiu *Jan 2012–Jun 2014*
  This project works on variant theoretical topics in leakage-resilient encryption schemes and we applied the dual system techniques to threshold encryption and attribute-based encryption. In my research group, I am a core member and mainly responsible for the design of advanced cryptographic schemes that are useful for real applications and the proof of the schemes.[7,8,9,10,11,12,13]

Research Activities

- Internship at NTT Research hosted by Professor Mark Zhandry, from 10/2019 to 5/2020.
- Research visitor invited by Professor David Wu to University of Virginia, from 4/2019 to 5/2019.
- Research visitor invited by Professor Adam O'Neill to University of Massachusets, from 3/2019 to 4/2019.
- Research visitor invited by Professor Seny Kamara to Brown University, from 11/3/2019 to 13/3/2019.
- Research visitor invited by Professor Dennis Hofheniz to KIT, from 06/2017 to 08/2017.
- Research visitor invited by Professor Dennis Hofheniz to KIT, from 10/2016 to 12/2016.
- Research visitor invited by Professor Mark Zhandry to Princeton University, from 08/2016 to 09/2016.
- Research Visitor invited by Professor Adam O'Neill to the Georgetown University,from 06/2016 to 07/2016.
- Research Visitor invited by Professor Allison Bishop to the Columbia University, from 06/2015 to 08/2015.
- Research Visitor invited by Professor Sherman Chow to the Chinese University of Hong Kong, from 01/2013 to 06/2013.
- External Reviewer of Asiacrypt 2017, 2018, 2019, TCC2017, S&P2017, CCS 2016, AsiaCCS 2013, ACNS 2013, Inscrypt 2013, Provable Security 2013, ICICS2011, 2012.

Talks

- Parameter-Hiding Order Revealing Encryption.
  - Conference talk at ASIACRYPT 2018;
  - ICERM workshop at Brown(2019);
  - Cryptography and Information Security Seminar at Brown(2019);
  - Cryptography and Information Security Seminar at UVA(2019).
- Impossibility of Order Revealing Encryption in Idealized Model.
  - Conference talk at TCC 2018.
- A Ciphertext-Size Lower Bound for Order-Preserving Encryption with Limited Leakage.
  - Conference talk at TCC 2018.
- Multikey Leakage-Resilient Threshold Cryptography.
  - Conference talk at ASIACCS 2013.

Publication

1. Mark Zhandry, **Cong Zhang**: Indifferentiability for Public Key Cryptosystems. In submission to CRYPTO 2020. https://eprint.iacr.org/2019/370.(alphabetical author list)
2. David Cash, Feng-Hao Liu, Adam O'Neill, Mark Zhandry, **Cong Zhang**: Parameter-Hiding Order Revealing Encryption. Proceceing of the 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018):181-210.(alphabetical author list)
3. Mark Zhandry, **Cong Zhang**: Impossibility of Order-Revealing Encryption in Idealized Models. Proceeding of the 16th Annual Theory of Cryptography Conference (TCC 2018): 129-158.(alphabetical author list)
4. David Cash, **Cong Zhang**: A Ciphertext-Size Lower Bound for Order-Preserving Encryption with Limited Leakage. Proceeding of the 16th Annual Theory of Cryptography Conference (TCC 2018): 159-

176.(alphabetical author list)

5. **Cong Zhang**, David Cash, Xiuhua Wang, Xiaoqi Yu,Sherman S. M. Chow: Combiners for Chosen-Ciphertext Security. Proceeding of the 22nd International Computing and Combinatorics Conference (COCOON 2016):257-268.
6. Tsz Hon Yuen, **Cong Zhang**, Sherman S.M. Chow, Siu-Ming Yiu: Related Randomness Attacks for Public Key Cryptosystems. Proceeding of 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015):215-223.
7. **Cong Zhang**, Tsz Hon Yuen, Hao Xiong, Sherman S.M. Chow, Siu-Ming Yiu, Yijun He: Multikey Leakage-Resilient Threshold Cryptography. Proceeding of 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013):61-70.
8. Tsz Hon Yuen, **Cong Zhang**, Sherman S.M. Chow, Joseph Liu: Towards Anonymous Ciphertext Indistinguishability with Identity Leakage. Proceeding of the 7th international conference, provable security (ProvSec 2013): 139-153.
9. Hao Xiong, Tsz Hon Yuen, **Cong Zhang**, Yi-jun He, Siu-Ming Yiu: Attribute Specified IdentityBased Encryption, Proceeding of the 9th Information Security Practice & Experience Conference (ISPEC 2013): 60-74.
10. Hao Xiong, Tsz Hon Yuen, **Cong Zhang**, Siu-Ming Yiu, Yi Jun He: Leakage-resilient certificateless public key encryption. Proceeding of the 1st ACM Asia Public-Key Cryptography Workshop AsiaPKC@AsiaCCS 2013: 13-22.
11. Hao Xiong, **Cong Zhang**, Tsz Hon Yuen, Echo P. Zhang, Siu-Ming Yiu, Sihan Qing: Continual Leakage-Resilient Dynamic Secret Sharing in the Split-State Model. Proceeding of 14th International Conference Information and Communications Security (ICICS 2012): 119-130.
12. Yangwei Li, Qingni Shen, **Cong Zhang**, Pengfei Sun, Ying Chen, Sihan Qing: A Covert Channel Using Core Alternation. Proceeding of The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA Workshops 2012): 324-328.
13. Pengfei Sun, Qingni Shen, Ying Chen, **Cong Zhang**, Anbang Ruan, Liang Gu: Poster: LBMS: load balancing based on multilateral security in cloud. ACM Conference on Computer and Communications Security 2011: 861-864.

In Preparation and Manuscript

- Dov Gordon, Adam O'Neill, Cong Zhang: Relational Preserving Encryption;
- Dennis Hofheinz, Cong Zhang: Compact (H)IBE against Selective Open Attack
- Cong Zhang: Standard IBE does not Imply Indistinguishability under Selective Opening

Honor

2018-2019	Presidential Fellowship of Rutgers University
2017-2018	Presidential Fellowship of Rutgers University
2016-2017	Presidential Fellowship of Rutgers University
2015-2016	Presidential Fellowship of Rutgers University
2014-2015	Presidential Fellowship of Rutgers University
2014-2015	IAB Graduate Fellowship of Rutgers University
2007-2008	Honored Excellent Student First Class Scholarship from Shandong University China
2007-2008	Merit Student from Shandong University China
2006-2007	Honored Excellent Student First Class Scholarship from Shandong University China
2006-2007	Merit Student from Shandong University China
2005-2006	Honored Excellent Student First Class Scholarship from Shandong University China

- 2005-2006 Merit Student from Shandong University China