Chen Qian

Mobile: (+47) 40485379 · **E-Mail:** chen.qian@ntnu.no

Personal Website: http://qianchen92.github.io/

Work experience

Post-Doc Norwegian University of Science and Technology (NTNU), Norway 2019.10-

- **Host:** Jiaxin Pan

Internship École Normale Supérieure de Lyon (ENS Lyon), France 2016.03-2016.09

- **Host:** Benoît Libert
- **Result:** Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts. (PKC 2017)

Internship NTT Secure Platform Laboratories, Japan 2015.05-2015.09

- **Host:** Mehdi Tibouchi
- **Result:** Universal Witness Signatures. (IWSEC 2018)

Internship Univ Rennes 1, France 2014.05-2014.09

- **Host:** Pierre-Alain Fouque
- **Result:** Study of cryptographic algorithm and cryptanalysis.
  - Fault Attacks on Efficient Pairing Implementations. (AsiaCCS 2016)
  - Binary Elligator Squared. (SAC 2014)

Education

Ph.D. in Cryptography, Univ Rennes 1, France 2016.09 - 2019.10

- **Supervisors:** Pr. Pierre-Alain Fouque, Pr. Benoît Libert
- **Co-supervisor:** Dr. Adeline Roux-Langlois
- **Dissertation:** Lossy trapdoor primitives, zero-knowledge proofs and applications.

Master in Computer Science ENS Rennes/Université Paris Diderot, France, 2015.09 - 2016.09

- **MPRI:** Joint computer science research master program by University Paris Diderot, École Polytechnique and École Normale Supérieure (ENS Paris/Lyon/Cachan/Rennes).
- **Honor:** Summa cum Laude (top 2%)

Magister in Computer Science ENS Rennes/Univ Rennes 1, France 2014.09 - 2015.09

- **Honor:** Summa cum Laude (top 2%)

Bachelor in Computer Science ENS Rennes/Univ Rennes 1, France 2013.09 - 2014.09

- **Honor:** Summa cum Laude (top 2%)

Bachelor in Mathematics ENS Rennes/Univ Rennes 1, France 2013.09 - 2014.09

- **Honor:** Magna cum Laude (top 5%)

Classe Préparatoire Lycée du Parc, France 2011.09 - 2013.09

- **Discipline:** MPSI-MP* (Mathematics Physics with Computer Science)
- **Program:** Joint program by French and Chinese Ministry of Education: 50 Chinese high school students in French preparatory class for Grand Écoles.
- **Honor:** Summa cum Laude (top 2%)

Publication list

In cryptography, authors are usually listed alphabetically by their surnames.

- Jiaxin Pan, Chen Qian, and Magnus Ringerud:
  Signed Diffie-Hellman Key Exchange with Tight Security.
  Cryptographers' Track at the 2021 edition of RSA Conference, **CT-RSA 2021**.

- Balthazar Bauer, Georg Fuchsbauer, and Chen Qian:
  Transferable E-cash: A Cleaner Model and the First Practical Instantiation.
  24th International Conference on Practice and Theory in Public-Key Cryptography, **PKC 2021**.
- Benoît Libert, Chen Qian:
  Lossy Algebraic Filters with Short Tags.
  22nd International Conference on Practice and Theory in Public-Key Cryptography, **PKC 2019**.
- Benoît Libert, Thomas Peters Chen Qian:
  Logarithmic-Size Ring Signatures with Tight Security from the DDH Assumption.
  23rd European Symposium on Research in Computer Security, **ESORICS 2018**.
- Chen Qian, Mehdi Tibouchi, Rémi Géraud:
  Universal Witness Signatures.
  13th International Workshop on Security, **IWSEC 2018**.
- Benoît Libert, Thomas Peters, Chen Qian:
  Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts.
  20th IACR International Conference on Practice and Theory in Public-Key Cryptography, **PKC 2017**.
- Pierre-Alain Fouque, Chen Qian:
  Fault Attacks on Efficient Pairing Implementations.
  11th ACM on Asia Conference on Computer and Communications Security, **AsiaCCS 16**.
- Diego F. Aranha, Pierre-Alain Fouque, Chen Qian, Mehdi Tibouchi, Jean-Christophe Zapalowicz:
  Binary Elligator Squared.
  21st International Conference on Selected Areas in Cryptography, **SAC 14**.

Research Grants

- European H2020 Prometheus Project. (Participated as a Ph.D. Student)
- Plan to submit: Chinese National Science Fund for Excellent Young Scholars 2022.

Reviewer Experience

- IACR International Conference for Cryptography: Crypto (2021, 2019), Eurocrypt (2021), Asiacrypt (2021, 2020, 2019), PKC (2020, 2019, 2018), TCC (2021, 2020)
- Journal: IET Information Security, SCN (2018)

Invited Talks

- **Conference talks:** PKC'19, ESORICS'18, PKC'17, AsiaCCS'16.
- **Invited Talk:** ENS Lyon 2018 Monthly Lattice Meeting.
- **Student Presentation:** LatinCrypt 2015.

Teaching Experience

Provable Security for Master/Ph.D. Students @ NTNU, Norway 2020 - 2021

- **Role:** Joint Lecturer
- This course introduces the advanced cryptography for Master and Ph.D. students. The main topic consists of the concept of security proof and construction of cryptographic primitives including public encryption, signature scheme etc.

Provable Security for Master/Ph.D. Students @ NTNU, Norway 2019 - 2020

- **Role:** Lecturer
- This course introduces the advanced cryptography for Master and Ph.D. students. The main topic consists of the concept of security proof and construction of cryptographic primitives including public encryption, signature scheme etc.

Basic Algorithm, for first year Bachelor students @ Univ Rennes 1, France 2018 - 2019

- **Role:** Teaching Assistant
- This course introduces the basic algorithms and Java programming language to the first year Bachelor students.

Functional Programming, for third year Bachelor Students @ National Institute of Applied Sciences of Rennes (INSA Rennes), France 2018 - 2019

- **Role:** Teaching Assistance

- This course introduces the basic concept of functional programming and λ-calculus. We also teach the students how to program with the functional programming language OCaml.

Basic Algorithm, for first year Bachelor students @ Univ Rennes 1, France 2017 - 2018

- **Role:** Teaching Assistant
- This course introduces the basic algorithms and Java programming language to the first year Bachelor students.

Computer System, for third year Bachelor Students @ Univ Rennes 1, France 2016 - 2017

- **Role:** Lecturer
- This course introduces the basic computer file system, including the disk storage, how the system store and read data etc.

Language Skills

- Chinese (Native)
- English (Nearly Native)
- French (Nearly Native). Learning French since junior high school (Nanjing Foreign Language School).