钱宸

手机：(+47) 40485379 · 邮箱：chen.qian@ntnu.no

个人网页:http://qianchen92.github.io/

职业经历

博士后，挪威科技大学 (NTNU), 挪威 2019.10-

- **Host**：Jiaxin Pan

实习, 里昂高等师范 (ENS Lyon), 法国 2016.03-2016.09

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

实习, 日本电信电话, 安全实验室 (NTT Secure Platform Laboratories), 日本 2015.05-2015.09

- **Host**：Mehdi Tibouchi
- **科研成果**：Universal Witness Signatures. (IWSEC 2018)

实习, 雷恩第一大学 (Univ Rennes 1), 法国 2014.05-2014.09

- **Host**：Pierre-Alain Fouque
- **科研成果**:
  - Fault Attacks on Efficient Pairing Implementations. (AsiaCCS 2016)
  - Binary Elligator Squared. (SAC 2014)

教育背景

雷恩第一大学/里昂高等师范，法国，Univ Rennes/ENS Lyon 1，博士 2016.09 - 2019.10

- **导师**: Pr. Pierre-Alain Fouque, Pr. Benoît Libert
- **合作导师**: Dr. Adeline Roux-Langlois
- **题目**: Lossy trapdoor primitives, zero-knowledge proofs and applications.

雷恩高等师范/巴黎大学，法国，ENS Renns/ University of Paris，硕士二年级 2015.09 - 2016.09

- **MPRI**：由巴黎大学 (University of Paris)，法国高等师范集团 (École Normale Supérieure), 综合理工大学 (École Polytechnique) 共同举办的法国理论计算机领域最具盛名的硕士项目。
- **毕业荣誉**：Summa cum Laude （最高等荣誉, 前 2%）

雷恩高等师范/雷恩第一大学，法国，ENS Rennes/Univ Rennes 1，硕士一年级 2014.09 - 2015.09

- **学科**：计算机科学
- **毕业荣誉**：cum Laude （高等荣誉, 前 10%）

雷恩高等师范/雷恩第一大学，法国，ENS Rennes/Univ Rennes 1，学士 2013.09 - 2014.09

- **学科**: 计算机科学
- **毕业荣誉**：cum Laude （高等荣誉, 前 10%）

雷恩高等师范/雷恩第一大学，法国，ENS Rennes/Univ Rennes 1，学士 2013.09 - 2014.09

- **学科**: 数学
- **毕业荣誉**：cum Laude （高等荣誉, 前 10%）

公园中学，法国，Lycée du Parc，科学预科-等同于本科一二年级 2011.09 - 2013.09

- **学科**: MPSI-MP* 数学物理实验班
- **项目**: 中法教育部联合项目-50 名中国学生就读法国理科预科班
- **毕业荣誉**：Summa cum Laude （最高等荣誉, 前 2%）

论文发表

公钥密码学领域，论文作者默认以姓氏首字母排序。

- 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**.

基金项目

- 作为博士生参与法国国家科研署资助 ALAMBIC 项目（ANR project：ALAMBIC）。
- 作为博士生参与欧洲地平线 2020 科研项目 Prometheus（European H2020 Project：Prometheus）。
- 有意向申请 2022 年度国家自然科学基金优秀青年科学基金项目（海外）。

审稿经历

- IACR 密码学国际会议：Crypto (2021,2019), Eurocrypt (2021), Asiacrypt (2021,2020,2019), PKC (2022, 2020,2019,2018), TCC (2021,2020)。
- 密码学期刊：IET Information Security, SCN (2018), TCS (2021)。
- 其他密码学会议：包括 CT-RSA, ProvSec 等。

学术报告

- **会议报告：** PKC'19, ESORICS'18, PKC'17, AsiaCCS'16。
- **邀请报告：**里昂高等师范月度格密码交流-2018，法国年度编码和密码学日-2017，2018。
- **学生报告：** LatinCrypt'15。

教学经历

密码学可证明安全 2020 - 2021

- 共同主讲，面向硕士/博士，挪威科技大学，NTNU, 挪威
- 介绍密码学的可证明性安全，以及密码学协议构造的常用技巧，包括公钥密码，数字签名等。

密码学可证明安全 2019 - 2020

- 主讲，面向硕士/博士，挪威科技大学，NTNU, 挪威
- 介绍密码学的可证明性安全，以及密码学协议构造的常用技巧，包括公钥密码，数字签名等。

计算机基础算法 2018 - 2019

- 助教，面向本科一年级，雷恩一大，Univ Rennes 1，法国
- 计算机算法的基础课程，覆盖基础的算法，面向对象编程以及 Java 实现。

函数式编程原理 2018 - 2019

- 助教，面向本科三年级，国立雷恩应用科学学院，INSA Rennes，法国
- 包含函数式编程，λ 计算的基本原理，包含利用 OCaml 对函数式编程原理的实现。

计算机基础算法 2017 - 2018

- 助教，面向本科一年级，雷恩一大, Univ Rennes 1，法国
- 计算机算法的基础课程，覆盖基础的算法，面向对象编程以及 Java 实现。

计算机系统 2016 - 2017

- 主讲，面向本科三年级，雷恩一大，Univ Rennes 1，法国
- 计算机系统的基础课程，涵盖计算机的不同文件系统结构，读取以及存贮方式等。

语言

- 中文（母语）
- 英文（接近母语）
- 法语（接近母语），从初中开始学习（南京外国语学校）