Sunghyun Jin

Ph.D. student
School of Cyber Security
Center for Information Security Technologies
Institute of Cyber Security and Privacy
Korea University
145 Anam-ro, Seongbuk-gu, Seoul, 02841, Republic of Korea

sunghyunjin@korea.ac.kr
ORCID(0000-0002-9521-0937)
https://mcsmonk.github.io

last modified : 25 Nov 2021

Research Interests

- Cryptographic Engineering
  - Side-Channel Analysis and its Countermeasures
  - Cryptosystem Implementation Optimization

Education

- **Korea University** — Seoul, Republic of Korea
  Ph.D. in Information Security — Mar 2017 - **Present**
  Thesis: Side-Channel Key Recovery Attack on Secure ECDSA Implementations (working title)
  Supervised by Seokhie Hong and HeeSeok Kim
  Research on side-channel analysis and its countermeasures

- **Korea University** — Seoul, Republic of Korea
  M.S. in Information Security — Mar 2015 - Feb 2017
  Thesis: 프로파일링 단계에서 파형 선별을 통한 템플릿 공격의 성능 향상
  Supervised by Seokhie Hong
  Research on side-channel analysis and its countermeasures

- **University of Seoul** — Seoul, Republic of Korea
  B.S. in Mathematics and Computer Science — Mar 2009 - Feb 2015
  mandatory serve in the army from Jan 2010 to Nov 2011

Experience

- **Graduate student researcher**, Center for Information Security Technologies (CIST), Institute of Cyber Security and Privacy (ICSP), Korea University, Seoul, Republic of Korea, Mar 2015 - **Present**

Publication

- International Journal
  1. **Sunghyun Jin**, Sangyub Lee, Sung Min Cho, HeeSeok Kim, Seokhie Hong. Novel Key Recovery Attack on Secure ECDSA Implementation by Exploiting Collisions between Unknown Entries, IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(4): 1-26, 2021
     - Presented in the annual Conference on Cryptographic Hardware and Embedded Systems, CHES 2021
  2. **Sunghyun Jin**, Suhri Kim, HeeSeok Kim, Seokhie Hong. Recent advances in deep learning-based sde-channel analysis. ETRI Journal 42.2: 292-304, 2020
  3. Soojung An, Suhri Kim, **Sunghyun Jin**, HanBit Kim, HeeSeok Kim. Single Trace Side Channel Analysis on NTRU Implementation. Applied Sciences 8.11, 2018
  4. Sung Min Cho, **Sunghyun Jin**, HeeSeok Kim. Side-Channel Vulnerabilities of Unified Point Addition on Binary Huff Curve and Its Countermeasure. Applied Sciences 8.10, 2018

- International Conference
  1. Suhri kim, **Sunghyun Jin**, Yechan Lee, Byeonggyu Park, Hanbit Kim, Seokhie Hong. Single Trace Side Channel Analysis on Quantum Key Distribution. International Conference on Information and Communication Technology Convergence (ICTC), 2018

- Domestic Journal (Republic of Korea)
  1. Yechan Lee, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. New Higher-Order Differential Computation Analysis on Masked White-Box AES. Journal of the Korea Institute of Information Security and Cryptology, Vol. 30, No. 1, 2020
  2. Donggeun Kwon, **Sunghyun Jin**, HeeSeok Kim, Seokhie Hong. Improving Non-Profiled Side-Channel Analysis Using Auto-Encoder Based Noise Reduction Preprocessing. Journal of the Korea Institute of Information Security and Cryptology, Vol. 29, No. 3, 2019
  3. Byeonggyu Park, Suhri kim, Hanbit Kim, **Sunghyun Jin**, HeeSeok Kim, Seokhie Hong. Single Trace Analysis against HyMES by Exploitation of Joint Distributions of Leakages. Journal of the Korea Institute of Information Security and Cryptology, Vol. 28, No. 5, 2018

4. Soojung An, Suhri kim, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. Single Trace Side Channel Analysis on NTRUEncrypt Implementation. Journal of the Korea Institute of Information Security and Cryptology, Vol. 28, No. 5, 2018
5. Gayeong Ko, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. Improved Side Channel Analysis Using Power Consumption Table. Journal of the Korea Institute of Information Security and Cryptology, Vol. 27. No. 4, 2017
6. **Sunghyun Jin**, Taewon Kim, HeeSeok Kim, Seokhie Hong. Power Trace Selection Method in Template Profiling Phase for Improvements of Template Attack. Journal of the Korea Institute of Information Security and Cryptology, Vol. 27, No. 1, 2017

- Domestic Conference (Republic of Korea)
  1. **Sunghyun Jin**, HeeSeok Kim, Seokhie Hong. 다중 작업 학습을 이용한 딥러닝 기반 부채널 분석 연구. Conference on Information Security and Cryptography Summer (CISC-S), Korea Institute of Information Security and Cryptology, 2020.07.15.
  2. Donggeun Kwon, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. 차분 딥러닝 분석 성능 향상을 위한 새로운 구조 제안. Conference on Information Security and Cryptography Winter (CISC-W), Korea Institute of Information Security and Cryptology, 2019.11.30.
  3. Yechan Lee, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. 동적 분석 기반 공개키 암호알고리즘의 부채널 취약 구현 평가 연구. Conference on Information Security and Cryptography Winter (CISC-W), Korea Institute of Information Security and Cryptology, 2019.11.30.
  4. **Sunghyun Jin**, Donggeun Kwon, HeeSeok Kim, Seokhie Hong. 논프로파일링 환경에서 CPA 성능향상을 위한 딥러닝 기반 Correlation Optimization 기술 연구. Conference on Information Security and Cryptography Summer (CISC-S), Korea Institute of Information Security and Cryptology, 2019.06.20.
  5. Donggeun Kwon, **Sunghyun Jin**, HeeSeok Kim, Seokhie Hong. Study of Generative Adversarial Networks for Improving Side-Channel Attack. Conference on Information Security and Cryptography Summer (CISC-S), Korea Institute of Information Security and Cryptology, 2019.06.20.
  6. Yechan Lee, **Sunghyun Jin**, Hanbit Kim, HeeSeok Kim, Seokhie Hong. 마스킹 화이트 박스 암호에 대한 새로운 2차 차분 계산 분석 기술 연구. Conference on Information Security and Cryptography Summer (CISC-S), Korea Institute of Information Security and Cryptology, 2019.06.20.
  7. Donggeun Kwon, **Sunghyun Jin**, HeeSeok Kim, Seokhie Hong. 오토인코더 기반 딥러닝을 활용한 부채널 분석 노이즈 제거 기술 연구. Conference on Information Security and Cryptography Winter (CISC-W), Korea Institute of Information Security and Cryptology, 2018.12.08.

- ETC
  1. **Sunghyun Jin**, HeeSeok Kim. 딥러닝을 이용한 부채널 분석 기술 연구 동향. Korea Institute of Information Security and Cryptology, Review of Korea Institute of Information Security and Cryptology, page 43-53, Vol. 30(1), Feb 2020 (Korean)

- Work in Progress
  1. **Sunghyun Jin**, Sung Min Cho, HeeSeok Kim, Seokhie Hong. Enhanced Side-Channel Analysis on ECDSA Employing Fixed-Base Comb Method, under review
  2. **Sunghyun Jin**, Philip Johansson, HeeSeok Kim, Seokhie Hong. Enhancing Time-Frequency Analysis with Zero-mean Preprocessing, under review

Patent

- Seokhie Hong, Soojung An, **Sunghyun Jin**, DongWon Park. Method for Restorating Prime Number using Thread Information, Device and Computer Readable Medium for Performing the Method. KR1021995070000, 2021-01-06

Community Service

- Peer Reviewing
  - Reviewer
    1. 2019, Hindawi Security and Communication Networks, https://www.hindawi.com/journals/scn/
  - Subreviewer
    1. 2021, MDPI Sensors, https://www.mdpi.com/journal/sensors
    2. 2020, TCHES 2021 issue1, https://ches.iacr.org/2021/
    3. 2019, Asiacrypt 2019, https://asiacrypt.iacr.org/2019/

Honor and Award

- Excellence Award in the Theory Category of the National Cryptography Contest, Korea Cryptography Forum, 2021
- President's Award, Korea University, 2017
- Grand Prize in the National Cryptography Technology Professional Training Course, National Security Research institute, 2016
- Participation Award in the 1st Category of the National Cryptography Contest, Korea Cryptography Forum, 2014

Reference

- Seokhie Hong (shhong@korea.ac.kr, orcid: 0000-0001-7506-4023) : Superevisor
- HeeSeok Kim (80khs@korea.ac.kr, orcid: 0000-0001-8137-4810) : Co-supervisor