Junwei WANG

41 Boulevard des Capucines
75002 Paris, France
junwei.wang@cryptoexperts.com
(+33) 7 69 39 52 85
https://junwei.co

EDUCATION

Ph.D. Candidate in Cryptography April 2017 - Now

CryptoExperts SAS, Paris, France
University of Luxembourg, Esch-sur-Alzette, Luxembourg
University Paris 8, Saint-Denis, France

My research interests is white-box cryptography. My thesis is under the supervisor of Prof. Jean-Sébastien Coron, Prof. Sihem Mesnager, Dr. Pascal Paillier, and Dr. Matthieu Rivain. I am an ECRYPT-NET fellow and receive funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 643161.

Master in Information and Computer Science September 2013 - September 2014

University of Luxembourg, Luxembourg City, Luxembourg

Thesis entitled *Efficient Implementation of High-Order DPA Countermeasures for the AES using the ARM NEON Instruction Set*, under the supervision of Prof. Jean-Sébastien Coron.

Master of Computer Science and Technology September 2012 - June 2015

Shandong University, Jinan, China

Bachelor of Software Engineer September 2008 - June 2012

Shandong University, Jinan, China

WORKING EXPERIENCE

Research Intern April 2018 - July 2018

Riscure B.V., Delft, the Netherlands

Senior Software Engineer July 2015 - April 2017

Baidu Inc., Beijing, China

I was at Knowledge Graph Department. My job was design and development of systems for efficient production of knowledge data.

R&D Engineer (Intern) December 2014 - May 2015

Eyespage, Beijing, China

- Designed and developed the API.
- Developed a spider to crawl data from Google Play Store by using the Scrapy framework.
- Operated and monitored with Elastic-Logstash-Kibana stack, Zabbix and so on.
- Co-designed the system architecture.

R&D Engineer (Intern) August 2011 - January 2012

Baidu Inc., Beijing, China

- Developed a “user friendly" monitoring and warning system for online services of Baidu, mainly focusing on obtaining, processing and displaying data.

PUBLICATIONS

[1] Junwei Wang, Praveen Kumar Vadnala, Johann Großschädl, and Qiuliang Xu. Higher-Order Masking in Practice: A Vector Implementation of Masked AES for ARM NEON. In Kaisa Nyberg, editor, *The Cryptographer's Track at the RSA Conference 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 181–198. Springer, 2015.

LANGUAGES

- *Chinese* (mother tongue) and *English* (work proficiency)