# 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 Computer Science* April 2017 - Now

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

My thesis is supervised by Prof. Jean-Sébastien Coron, Prof. Sihem Mesnager, Dr. Pascal Paillier, and Dr. Matthieu Rivain. I was an ECRYPT-NET fellow and received funding from the European Unions Horizon 2020 research and innovation programme under the Marie Skodowska-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] Andrey Bogdanov, Matthieu Rivain, Philip S. Vejre, and Junwei Wang. Higher-order DCA against standard side-channel countermeasures. In Polian and Stöttinger, editors. *Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings*, volume 11421 of *Lecture Notes in Computer Science*. pages 118–141. Springer, 2019.

[2] Matthieu Rivain and Junwei Wang. Analysis and improvement of differential computation attacks against internally-encoded white-box implementations. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(2):225–255, 2019.

[3] Louis Goubin, Pascal Paillier, Matthieu Rivain, and Junwei Wang. How to reveal the secrets of an obscure white-box implementation. *IACR Cryptology ePrint Archive*, 2018:098, 2018.

[4] 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, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 181–198. Springer, 2015.


## LANGUAGES

- *Chinese* (mother tongue)
- *English* (work proficiency)
- *French* (beginner)