

Junwei WANG

2 Alle Joseph Lalande
94000 Créteil, France
junwei.wang@cryptoexperts.com
(+33) 7 69 39 52 85
<http://junwei.co>

EDUCATION

<i>Ph.D. Candidate in White-Box Cryptography</i> University of Paris 8	April 2017 - Now Saint-Denis, France
<i>Master in Information and Computer Science</i> University of Luxembourg Thesis: <i>Efficient Implementation of High-Order DPA Countermeasures for the AES using the ARM NEON Instruction Set</i> , under the supervision of Prof. Jean-Sébastien Coron	September 2013 - September 2014 Luxembourg City, Luxembourg
<i>Master of Computer Science and Technology</i> Shandong University , Jinan, China	September 2012 - June 2015
<i>Bachelor of Software Engineer</i> Shandong University , Jinan, China	September 2008 - June 2012

WORKING EXPERIENCE

<i>Ph.D. Candidate</i> CryptoExperts , Paris, 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 Unions Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 643161.	April 2017 - now
<i>Senior Software Engineer</i> Baidu Inc. , Beijing, China I was at Knowledge Graph Department. My job was design and development of systems for efficient production of knowledge data.	July 2015 - April 2017

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 Cryptographers Track at the RSA Conference 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 181198. Springer, 2015.

LANGUAGES

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