Afterword

We have been researching reconfigurable computing processors since 2006. At the beginning, our attention only focused on its hardware architecture, mapping mechanism, and programming paradigms, and no additional work was done on cryptographic application. With the constant progress of the research, we found that reconfigurable computing technology could possibly be used to solve many difficult problems that could not be solved by other traditional technologies if the reconfigurable computing technology was applied to cryptographic processors. Reconfigurable computing technology was probably the brand-new technology very much needed by cryptographic processors, which surprised us and made us feel excited! Then we began to establish our team from scratch, established a platform, and we mainly concentrated on this research direction. Supported by the Key Project of the National 863 Program and the National Natural Science Foundation of China (NSFC), with the continuous efforts of several-year postgraduates and postdoctoral researchers such as Min Zhu, Bo Wang, Hai Huang, Chenchen Deng, Yansong Guo, Xing Wang, Le Chang, Kai Luo, Shengyang Mao, Qihuan Huang, Neng Zhang, Zhuoquan Zhou, Dongxing Wang, and Ao Li, our team has successively published over ten high-quality academic papers on the cryptographic chip field and the hardware security field, authorized dozens of invention patents, implemented a series of practical technologies and solved some practical difficult problems of industrial production. Looking back at the past, we just happened to pay our attention to the application of the reconfigurable computing technology to cryptographic chips. However, it was deliberate that we then concentrated on the research direction and our team did the research with great efforts!

In 2014, we summarized the technological breakthroughs in the reconfigurable computing field we had achieved in the past ten years, wrote the book of *Reconfigurable Computing* and had it published by Science Press. On this basis, we have summarized the accumulated research results that we have achieved on reconfigurable cryptographic processors in recent seven to eight years in the same way and have written this book about the results to share with readers. We have had

our book published by the same press. If you find any improper description or anything not precise enough in the book, please let us know and we will appreciate it very much.

Tsinghua University, Beijing, P. R. China   Leibo Liu