SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Efficient flush-reload cache attack on scalar multiplication based signature algorithm

Ping ZHOU[1], Tao WANG[1], Xiaoxuan LOU[3], Xinjie ZHAO[2], Fan ZHANG[3,4*] & Shize GUO[1]

[1]*Department of Information Engineering, Ordnance Engineering College, Shijiazhuang* 050003*, P.R.China;*
[2]*Institute of North Electronic Equipment, Beijing* 100191*, P.R.China;*
[3]*College of Information Science and Electrical Engineering, Zhejiang University* 310027*, P.R.China;*
[4]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, P.R.China*

Appendix A Illustration for Figure 1(d)

Fig.1(d) illustrates the measured loading time of the monitored memory lines $addr_A$ and $addr_D$ during 100 round of monitoring. The horizontal axis is the round of monitoring and the loading time is shown on the vertical axis. The dashed line is the threshold h which is equal to the median value of L3 cache access delay and memory access delay. Loading time which is less than the threshold indicates a victim access to the monitored memory line. The operations executed by the victim during this period can be identified clearly as '$DDDADADADDAD$'. In binary method, the scalar bit 0 corresponds to a 'D' operation and the scalar bit 1 corresponds to an 'AD' operation, therefore the fragment of the scalar bits can be recovered as '00111010'.

Appendix B Apply to sliding window and wNAF

The presented method is not limited to the scalar multiplication using the binary method. We also apply this attack to ECDSA using wNAF method [1] and SM2-DSA using sliding window method [2] in OpenSSL. Both of these two methods reform the representation of the scalar and process multiple scalar bits during a single iteration. Thus, the scalar multiplication can be computed faster as the total number of additions is reduced. In OpenSSL, the window size is set as 3-bit for 256-bit scalars. In this situation, our method can recover the AD sequence with an error rate as low as 0.15%. In 73% of the signatures, the sequence of operations are fully recovered. The rest work to recover the private key need to use the lattice techniques [3] [4]. With lattice attack, $\lceil 256/l \rceil$ signature samples are required to recover a 256-bit private key when last l bits of the scalar is known. The sequence of operations which end with 'ADD' or 'DDD' can confirm a scalar ending with '100' or '000'. As the probability of this bit pattern is expected as 2^{-2}, the adversary need about $\lceil 256/3 \rceil/(2^{-2}) = 344$ signatures to recover the whole private key.

Appendix C Comparison with other monitored memory

In this letter, we select the monitored memory lines that contain four *call* instructions, resulting in 0.96 error bits in each 256-bit scalar. We also conduct the same experiment but select the monitored memory lines that contain no *call* instructions, resulting in more than 25 error bits in each 256-bit scalar. This result shows that the presented method effective.

References

1 Koyama K, Tsuruoka Y. Speeding up elliptic curve cryptosystems using a signed binary windows method. In: Porceedings of CRYPTO92, Santa Barbara, US, 1992. 345-357
2 State Administration of cryptography. Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves. http://www.oscca.gov.cn/UpFile /20101222214822692

* Corresponding author (email: fanzhang@zju.edu.cn)

3 Nguyen P Q, Shparlinski I E. The Insecurity of the Ellipitc Curve Digital Signature Algorithm with Partially Known Nonces. Designs Codes & Cryptography, 2003, 30(2):151-176
4 Liu M, Chen J. Partially Known Nonces and Fault Injection Attacks on SM2 Signature Algorithm. In: Proceedings of Information Security and Cryptology, Guangzhou, China, 2013. 343-358