Attacking SHARP with Cache Side-Channel Attacks Using Multiple Spies

Joseph Reeves, Nuno Sabino

November 22, 2021

1 Introduction

wait time for spy [5]
square and multiple algorithm [2]
need only partial key to determine entire key [1]

2 SHARP

SHARP [4]
paper pointing out holes in SHARP [3]

3 Multiple Spy Attack

4 Shared Core Attack

5 Implementation

6 Conclusion and Future Work

References

[1] Matthew Campagna and Amit Sethi. Key recovery method for crt implementation of rsa. *IACR Cryptology ePrint Archive*, 2004:147, 01 2004.

[2] Daniel M. Gordon. A survey of fast exponentiation methods. *Journal of Algorithms*, 27(1):129–146, 1998.

[3] Dixit Kumar, Chavhan Sujeet Yashavant, Biswabandan Panda, and Vishal Gupta. How sharp is SHARP ? In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, August 2019. USENIX Association.

[4] Mengjia Yan, Bhargava Gopireddy, Thomas Shull, and Josep Torrellas. Secure hierarchy-aware cache replacement policy (sharp): Defending against cache-based side channel attacks. In *2017 ACM/IEEE 44th Annual International Symposium on Computer Architecture (ISCA)*, pages 347–360, 2017.

[5] Yuval Yarom and Katrina Falkner. Flush+reload: A high resolution, low noise, l3 cache side-channel attack. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 719–732, San Diego, CA, August 2014. USENIX Association.