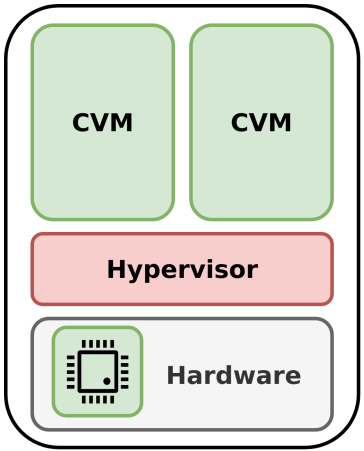
UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

TDXdown: Single-Stepping and Instruction Counting Attacks against Intel TDX

Luca Wilke*, Florian Sieck* and Thomas Eisenbarth
(*equal contribution)

ACM CCS'24, Salt Lake City, 15.10.2024

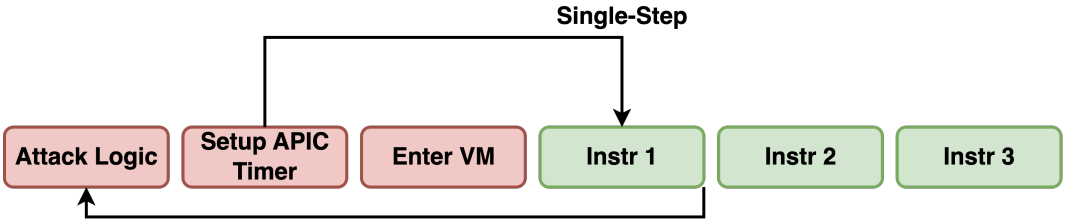
Goal: Remove cloud provider from TCB



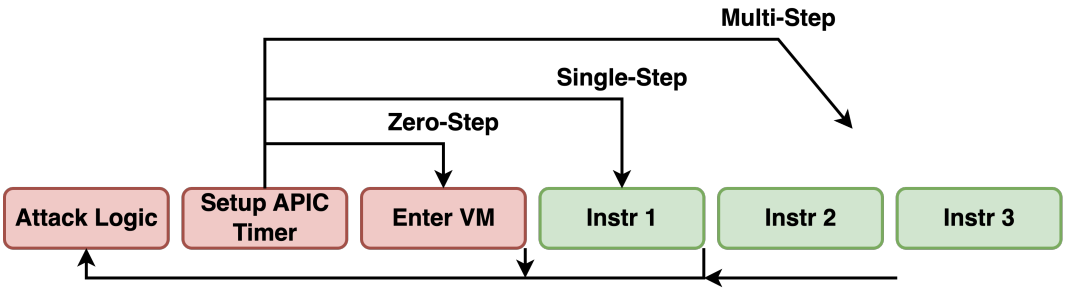
- AMD SEV-SNP
- Intel TDX
- (ARM CCA)

Available in the wild on

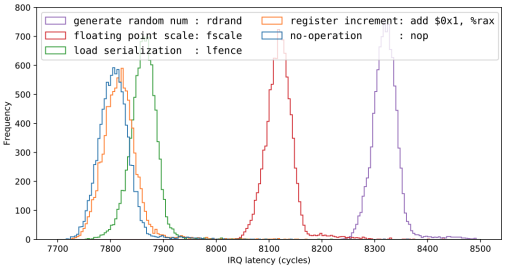
Single-Stepping: The bane of TEEs



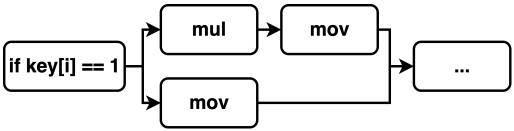
Single-Stepping: The bane of TEEs



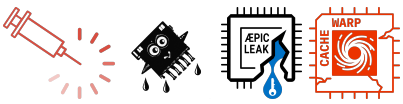
Single-Stepping: The bane of TEEs



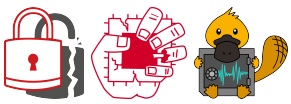
Interrupt Latency Attacks



Instruction Counting Attacks



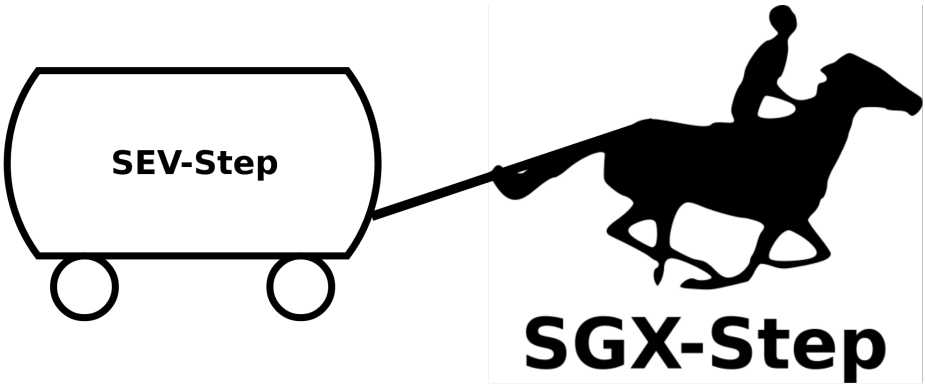
Amplifier



Zero-Stepping Attacks

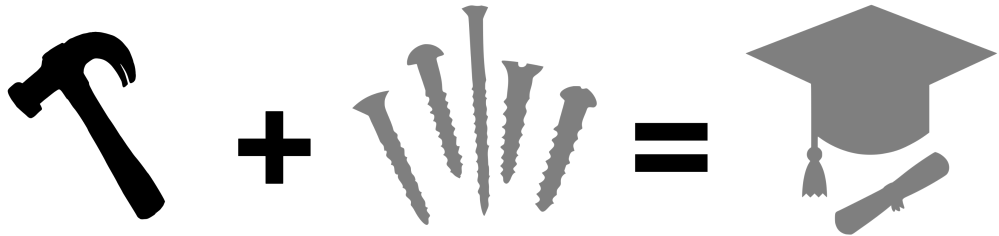
History of Single-Stepping

History of Single-Stepping

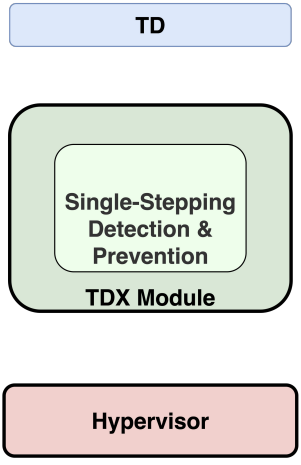


History of Single-Stepping

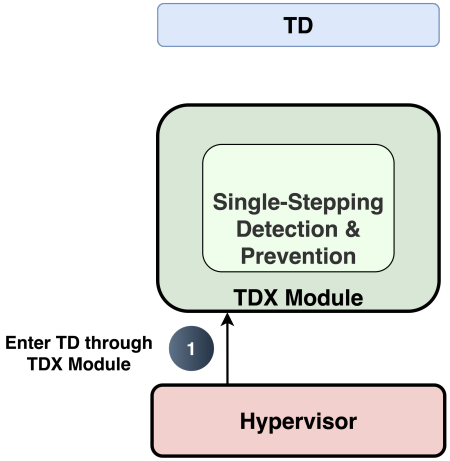
TDX Attack Primitives



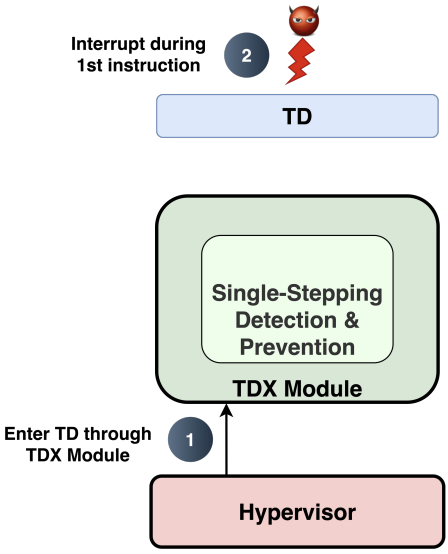
Single-Stepping Countermeasure



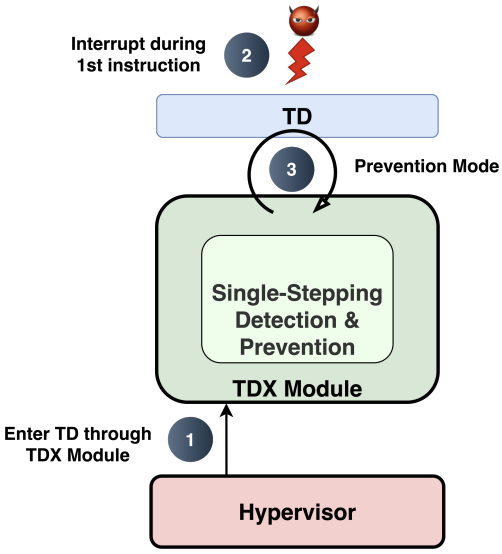
Single-Stepping Countermeasure



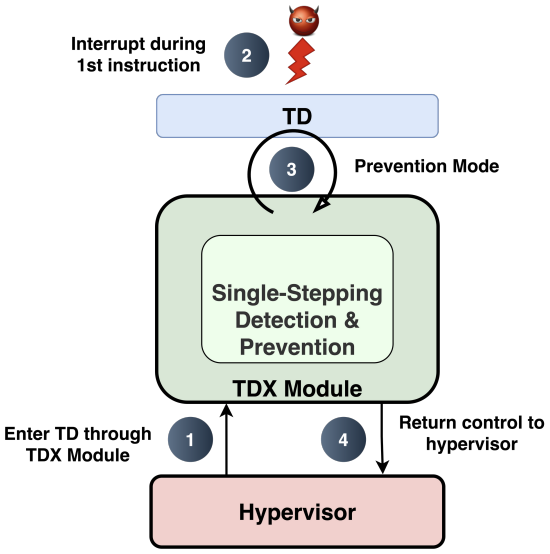
Single-Stepping Countermeasure



Single-Stepping Countermeasure



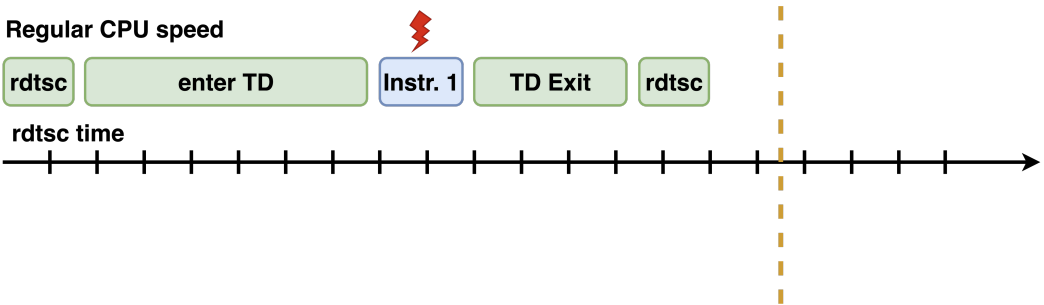
Single-Stepping Countermeasure



Single-Stepping Attack

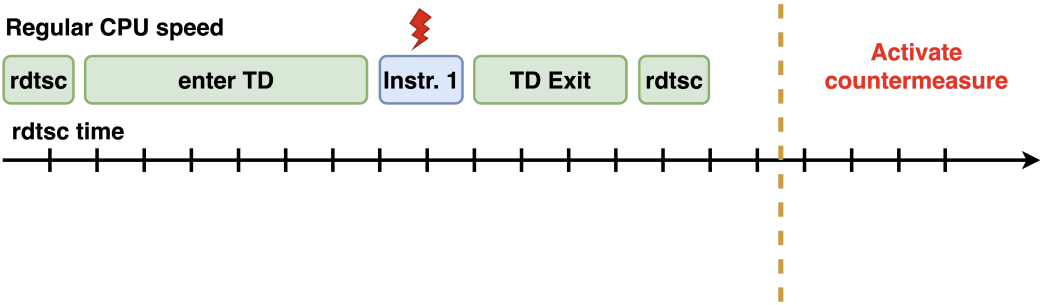
Re-enable Single-Stepping

Classified as benign if : "*> 2 Instructions*" OR "*> THRESH cycles*"



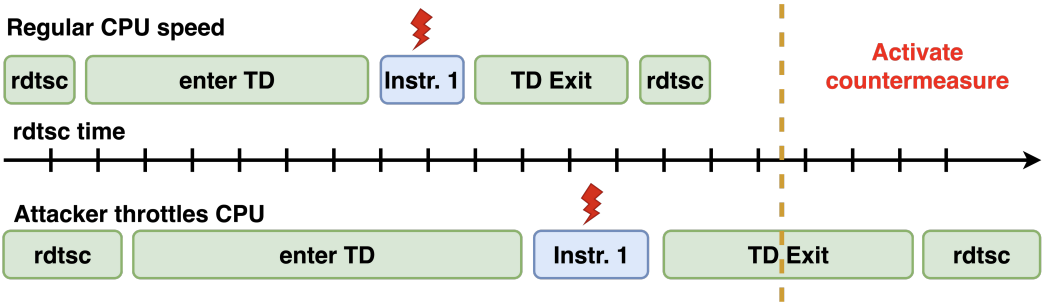
Re-enable Single-Stepping

Classified as benign if : "*> 2 Instructions*" OR "*> THRESH cycles*"



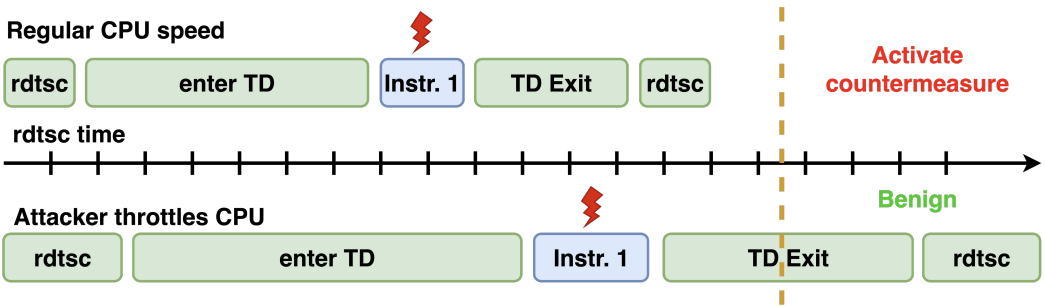
Re-enable Single-Stepping

Classified as benign if : "*> 2 Instructions*" OR "*> THRESH cycles*"



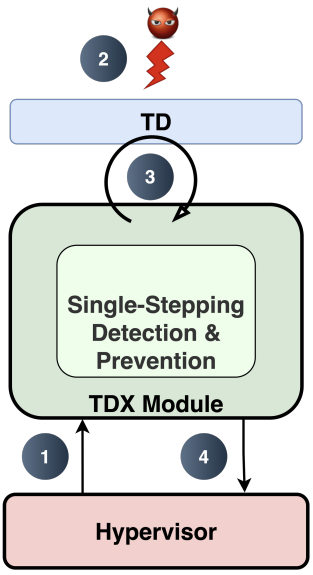
Re-enable Single-Stepping

Classified as benign if : "*> 2 Instructions*" OR "*> THRESH cycles*"

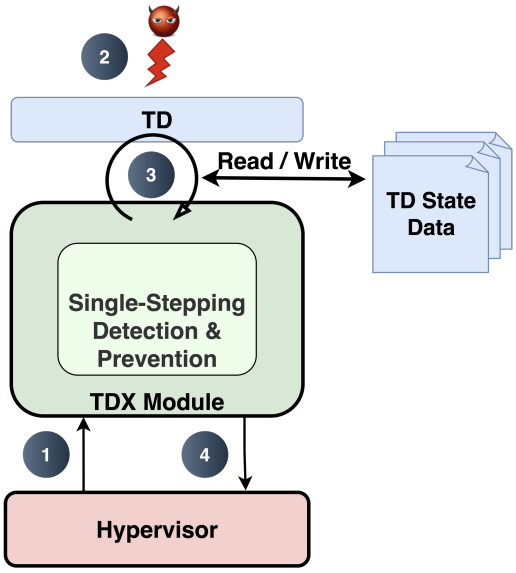


StumbleStepping Attack

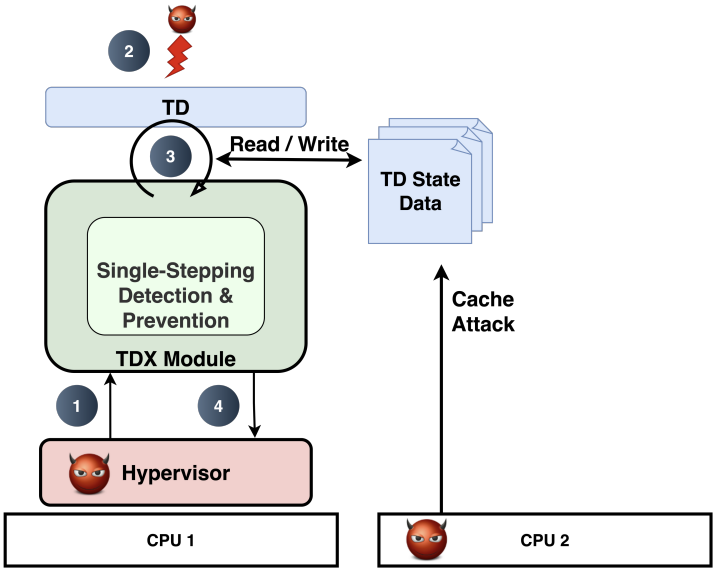
StumbleStepping



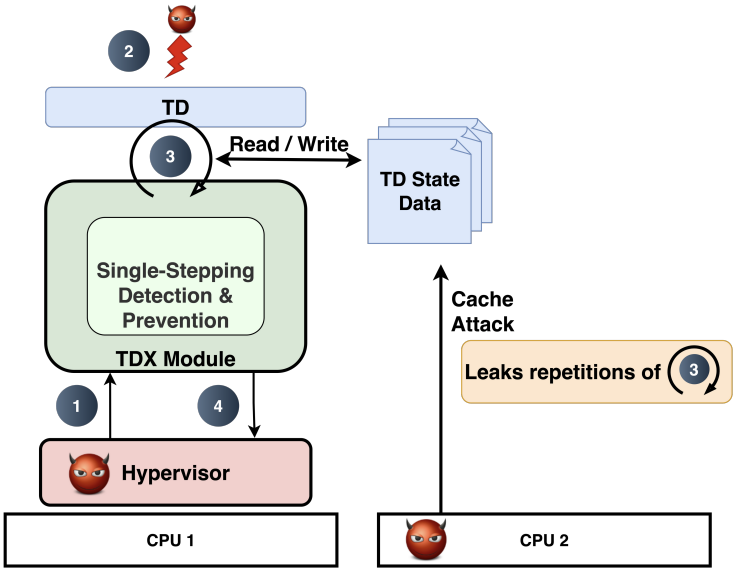
StumbleStepping

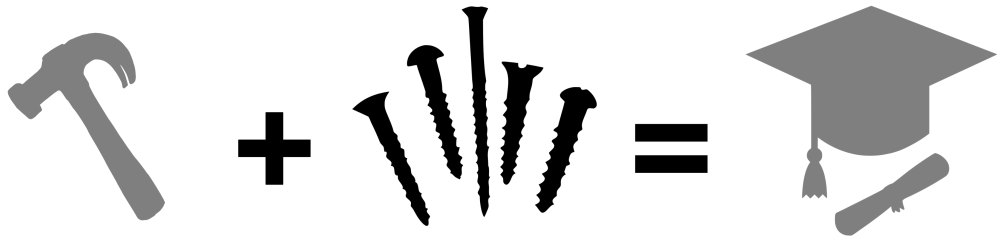


StumbleStepping



StumbleStepping




Attack Primitive
Cryptanalysis
Publication

Modular Reduction in ECDSA

ECDSA is a signature scheme, it requires a nonce k that must remain secret

1. Goal: Get random nonce $k < n$

Modular Reduction in ECDSA

ECDSA is a signature scheme, it requires a nonce k that must remain secret

1. Goal: Get random nonce $k < n$
2. Also: Get it fast

Modular Reduction in ECDSA

ECDSA is a signature scheme, it requires a nonce k that must remain secret

1. Goal: Get random nonce $k < n$
2. Also: Get it fast
3. Modular reduction approach:

Modular Reduction in ECDSA

ECDSA is a signature scheme, it requires a nonce k that must remain secret

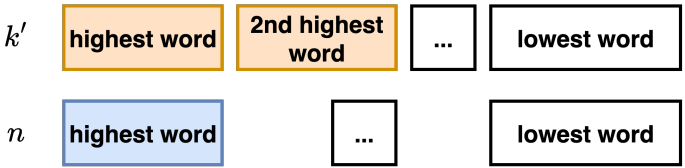
1. Goal: Get random nonce $k < n$
2. Also: Get it fast
3. Modular reduction approach:
   3.1 Sample candidate nonce k'

Modular Reduction in ECDSA

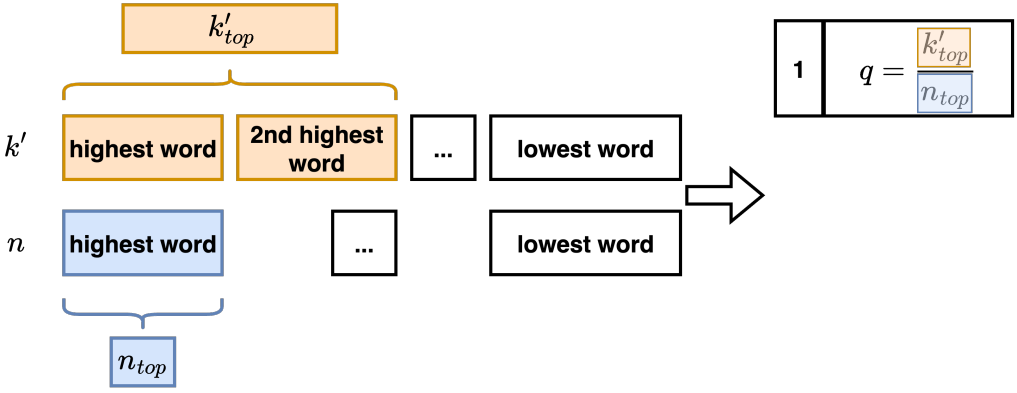
ECDSA is a signature scheme, it requires a nonce k that must remain secret

1. Goal: Get random nonce $k < n$
2. Also: Get it fast
3. Modular reduction approach:
   - 3.1 Sample candidate nonce k'
   - 3.2 Compute k as $k' \mod n$

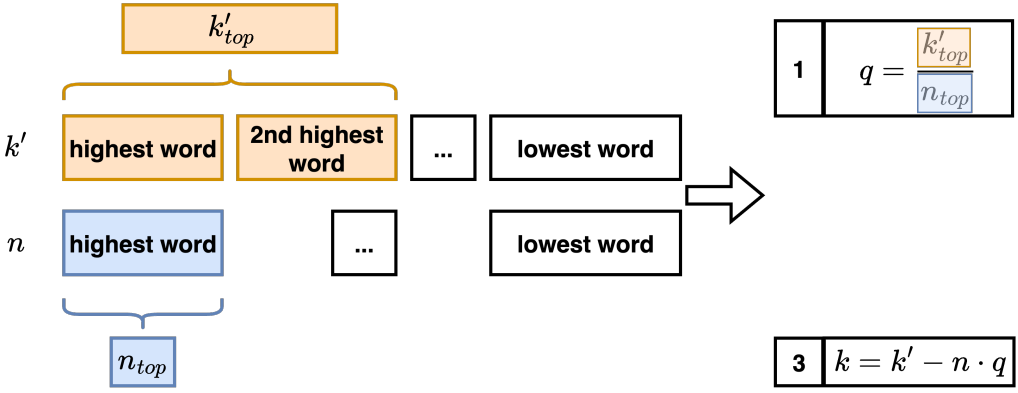
Compute k' mod n



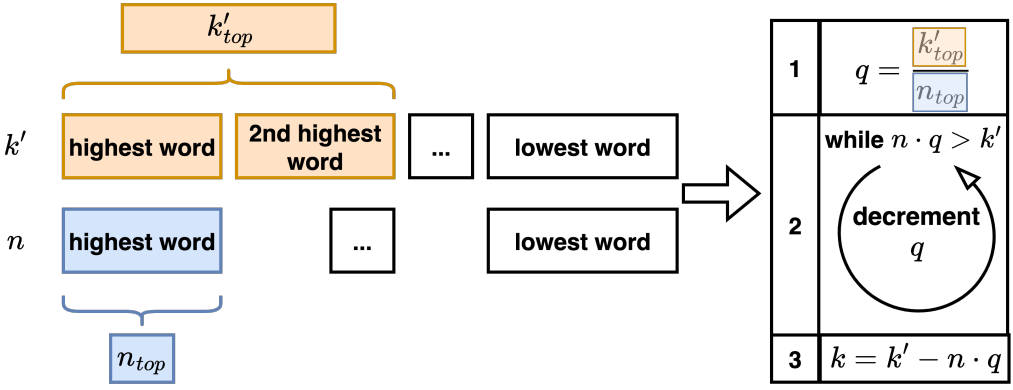
Compute k' mod n



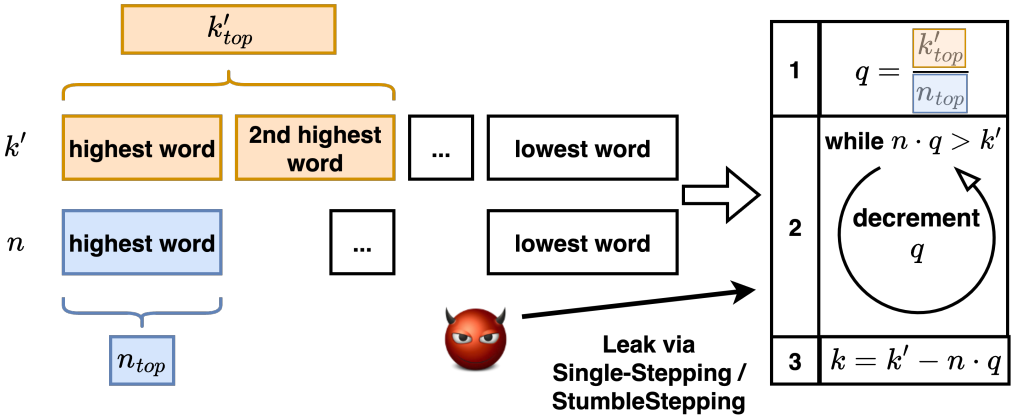
Compute k' mod n



Compute k' mod n

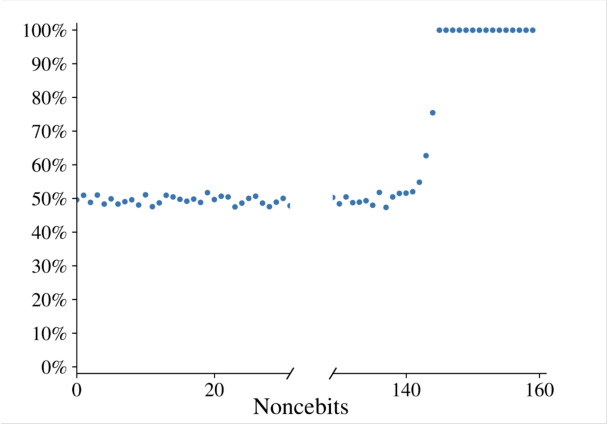


Compute k' mod n

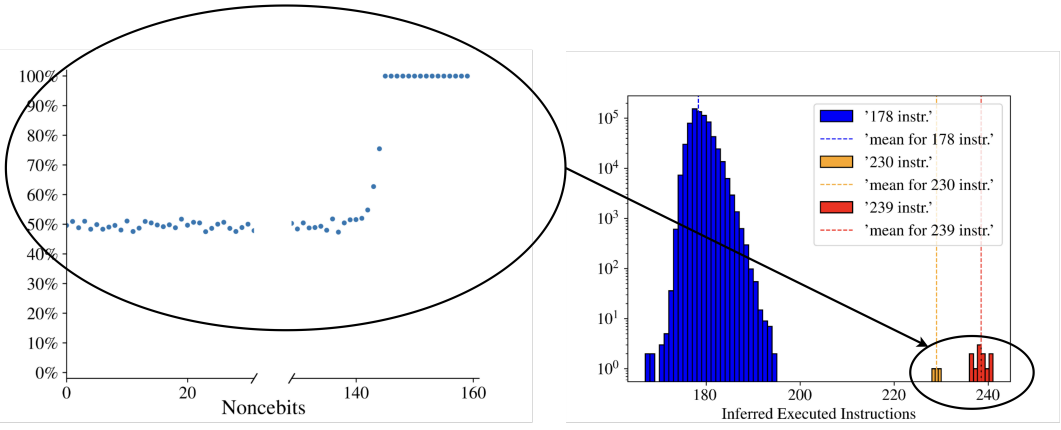


Nonce Bias

Noncebit distribution given leaked loop iterations for *secp160r1*



StumbleStep Nonce Bias



Summary

- Primitive 1: full single-stepping
- Primitive 2: *StumbleStepping*; instruction counting
- Nonce truncation in wolfSSL and OpenSSL leaks for certain curves
- Responsible Disclosure:
  - Intel fixed primitive 1 with TDX module 1.5.06 but won't fix primitive 2
  - wolfSSL and OpenSSL switched to rejection sampling

Artifact&Website

UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY