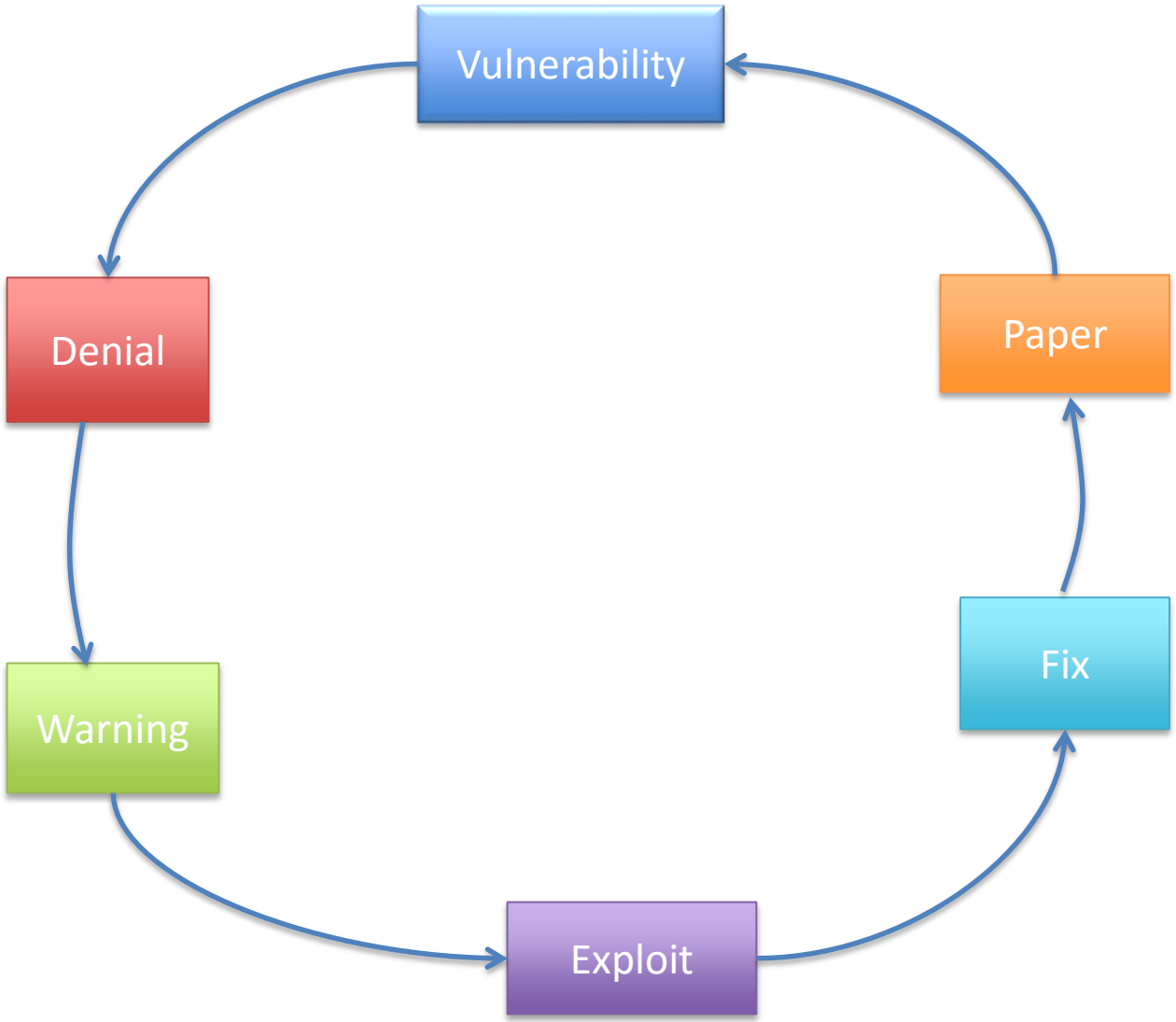
CacheBleed: A Timing Attack on OpenSSL Constant Time RSA

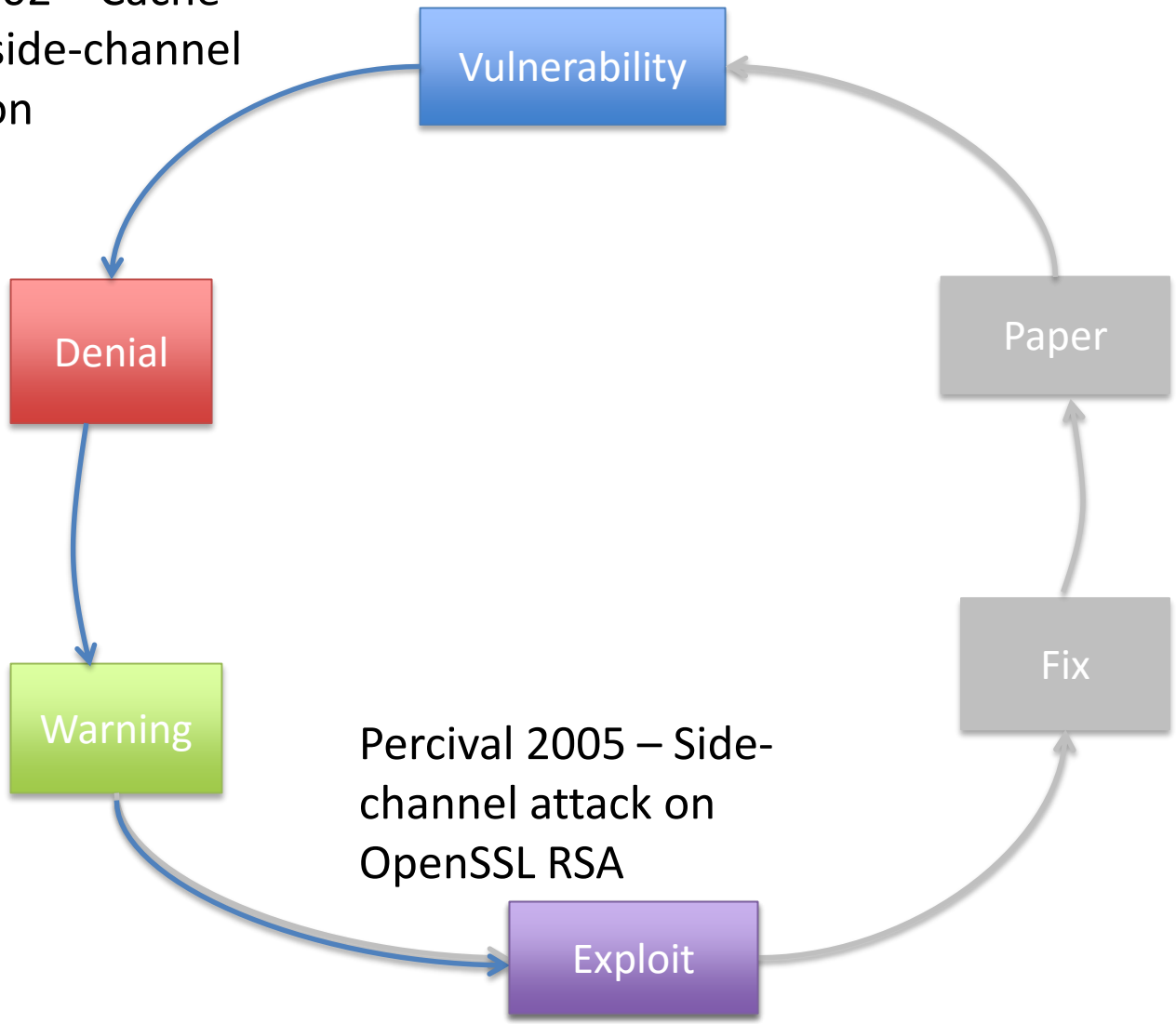
Yuval Yarom	The University of Adelaide and Data61
Daniel Genkin	Technion and Tel-Aviv University
Nadia Heninger	University of Pennsylvania

Attack Life Cycle



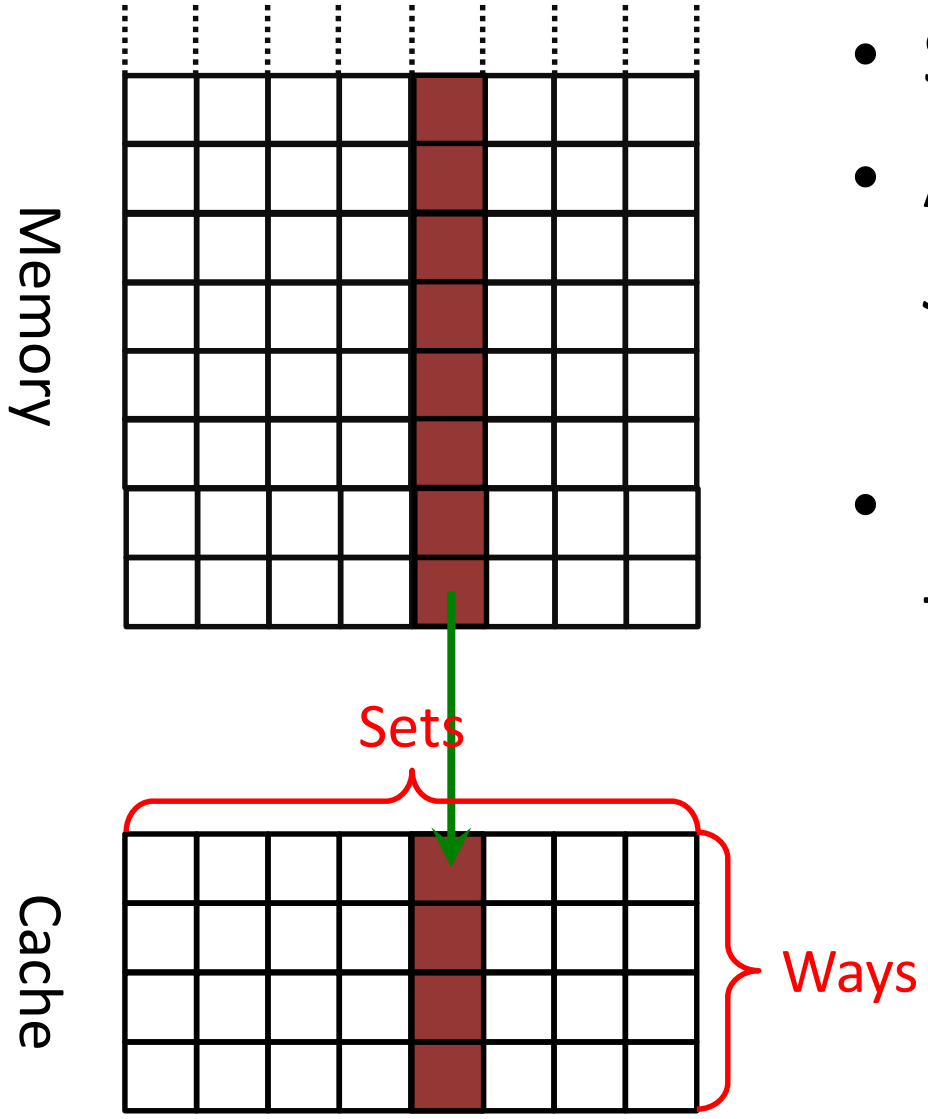
Round 1

Tsunoo 2002 – Cache may leak side-channel information



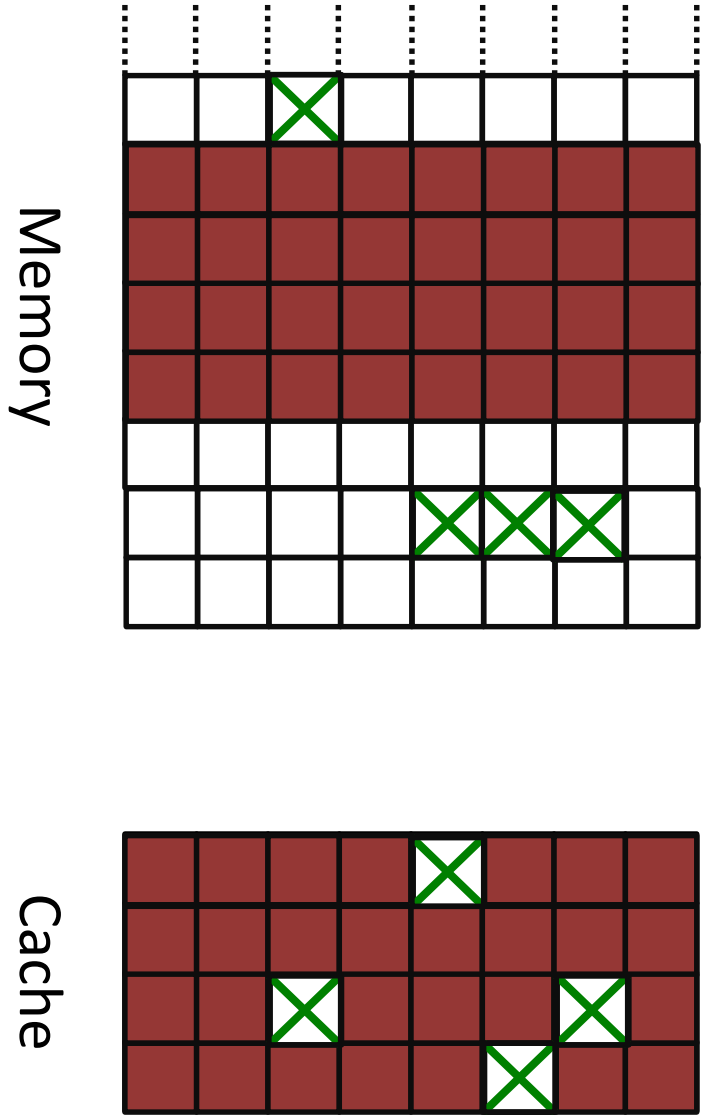
Percival 2005 – Side-channel attack on OpenSSL RSA

Cache Structure



- Stores fixed-size *lines*
- Arranged as multiple *sets*, each consisting of multiple *ways*.
- Each memory line maps to a single cache set
  - Can be cached in any of the ways in the set

The Prime+Probe attack [Per'05,OST'05]



- Choose a cache-sized memory buffer
- Access all the lines in the buffer, filling the cache
- Victim executes, evicting some of the buffer lines from the cache
- Measure the time to access the buffer
  - Accesses to cached lines is faster than to evicted lines

Fixed Window Exponentiation

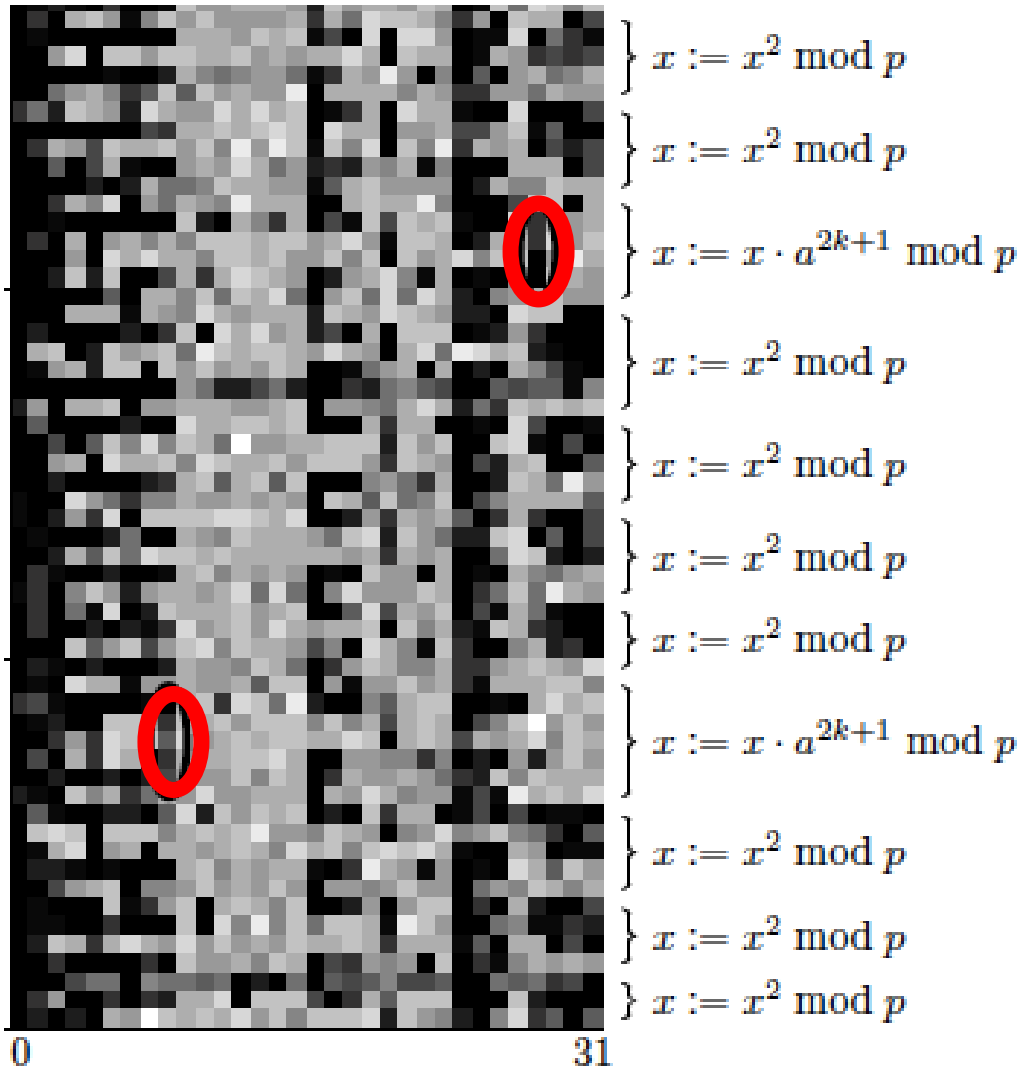
Algorithm 1: Fixed-window exponentiation

input : window size w, base a, modulus k, n-bit exponent $b = \sum_{i=0}^{\lceil n/w \rceil} b_i \cdot 2^{wi}$
output: $a^b \bmod k$

//Precomputation
$a_0 \leftarrow 1$
for $j = 1, \ldots, 2^w - 1$ **do**
  $a_j \leftarrow a_{j-1} \cdot a \bmod k$
end

//Exponentiation
$r \leftarrow 1$
for $i = \lceil n/w \rceil - 1, \ldots, 0$ **do**
  for $j = 1, \ldots, w$ **do**
    $r \leftarrow r^2 \bmod k$
  end
  $r \leftarrow r \cdot a_{b_i} \bmod k$
end
return r

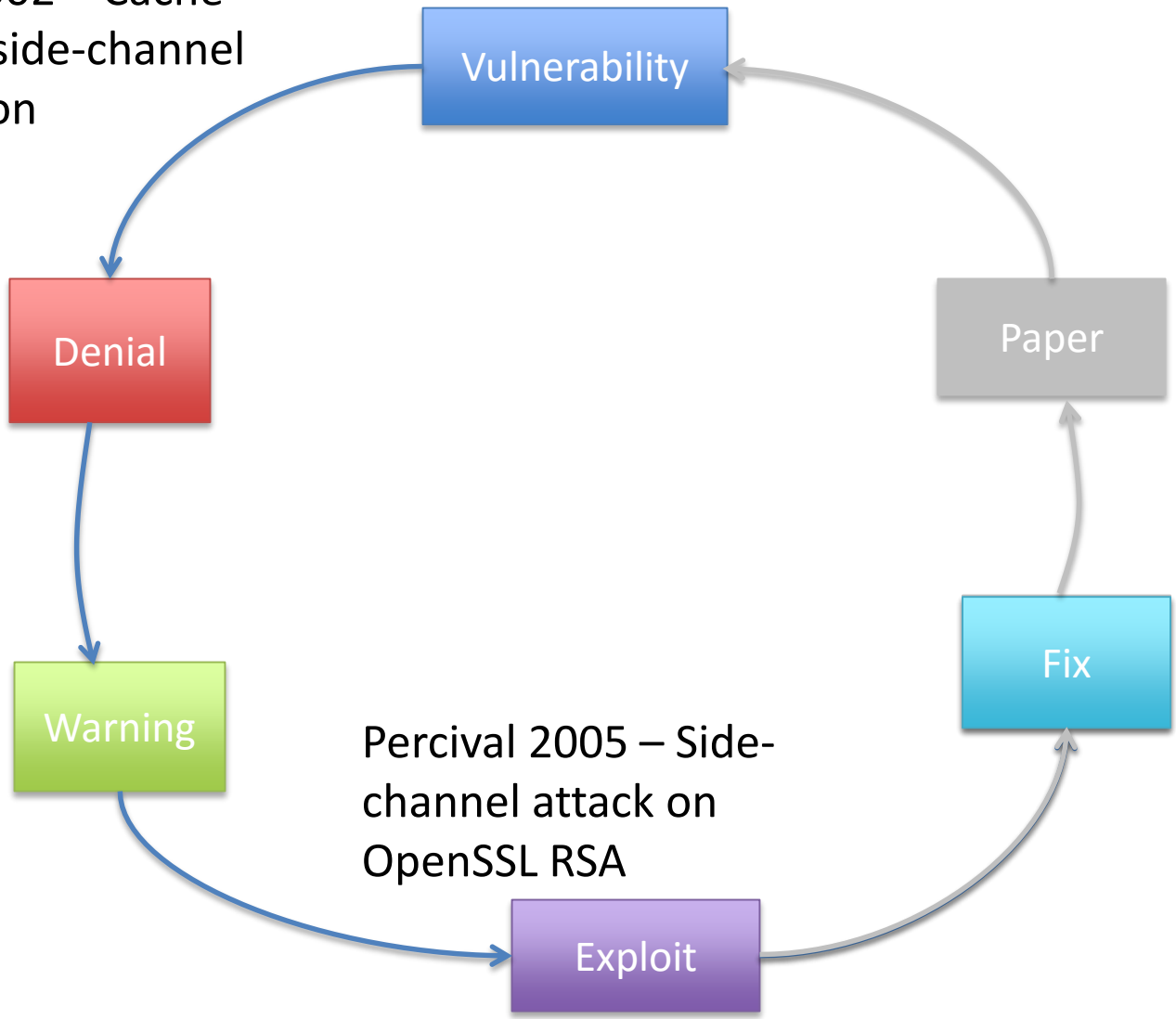
Prime+Probe and Windowed Exponentiation



([Per'05])

Round 1

Tsunoo 2002 – Cache may leak side-channel information

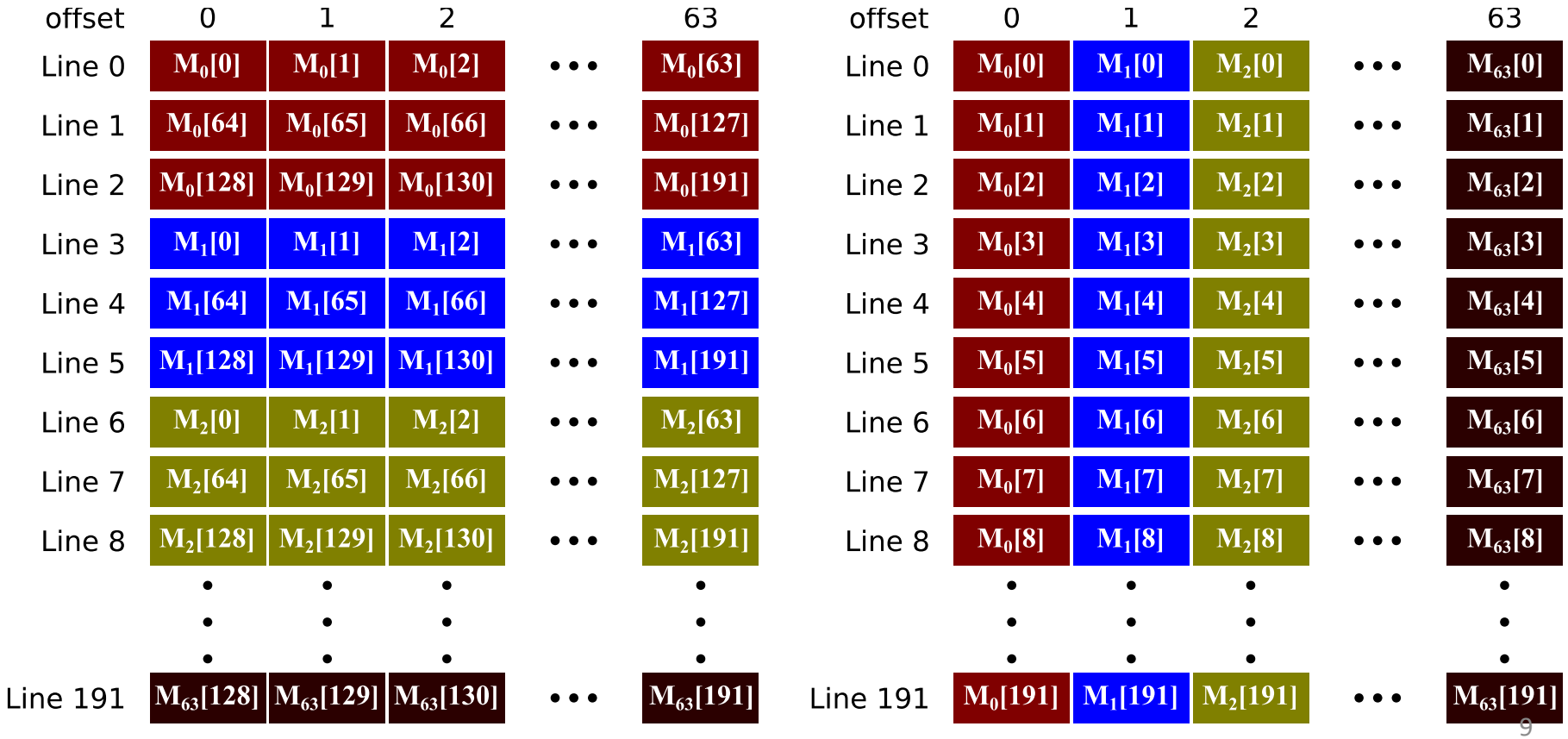


Intel 2005 – Use Scatter Gather

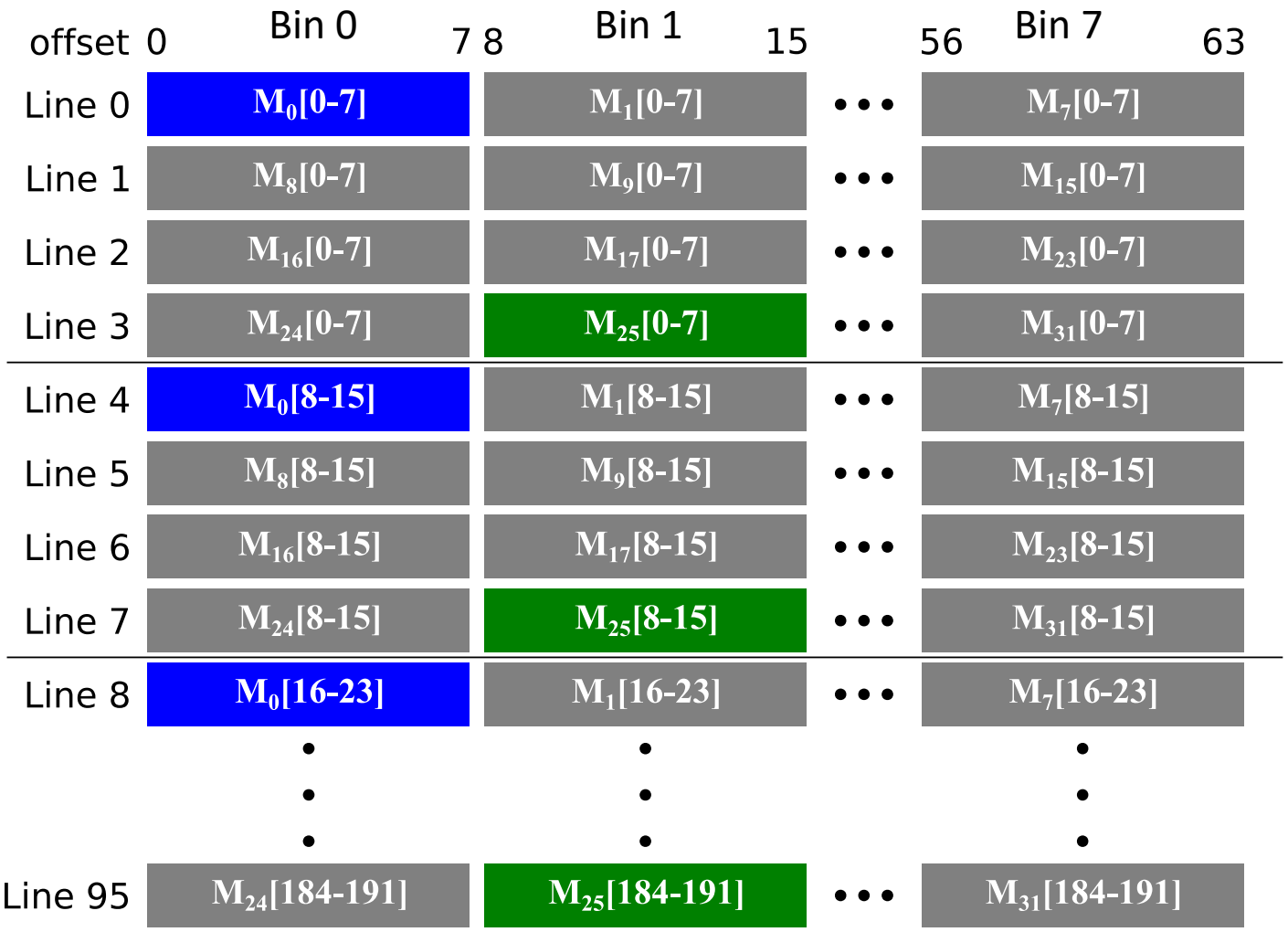
Percival 2005 – Side-channel attack on OpenSSL RSA

Scatter-Gather

- Mitigate Prime+Probe
  - Sequence of accesses to cache lines does not depend on secret data



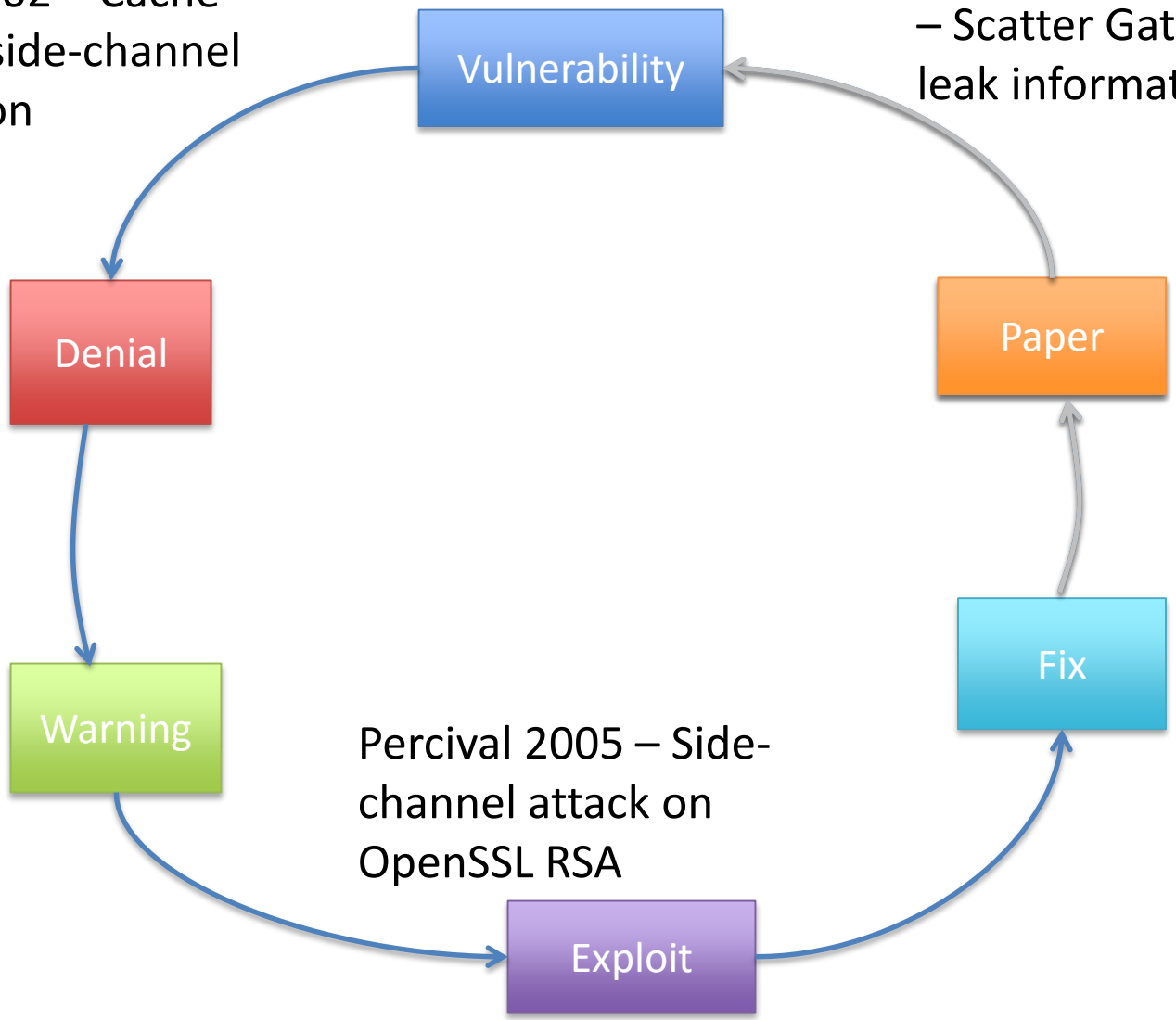
OpenSSL's Layout



Round 1

Tsunoo 2002 – Cache may leak side-channel information

Bernstein 2005, Osvik Shamir & Tromer 2006 – Scatter Gather may leak information

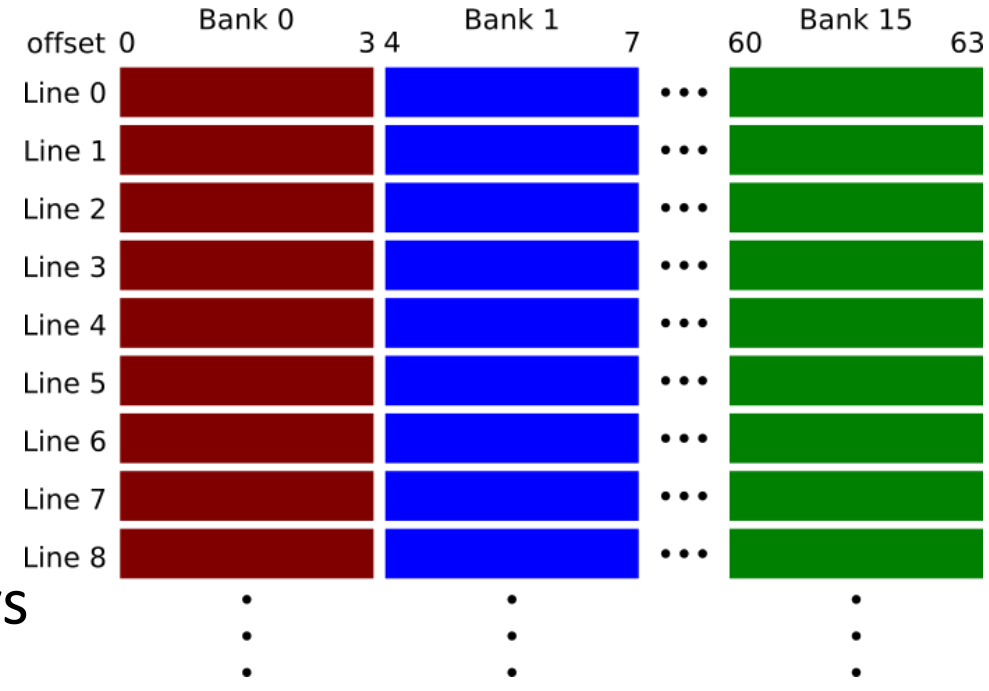


Intel 2005 – Use Scatter Gather

Percival 2005 – Side-channel attack on OpenSSL RSA

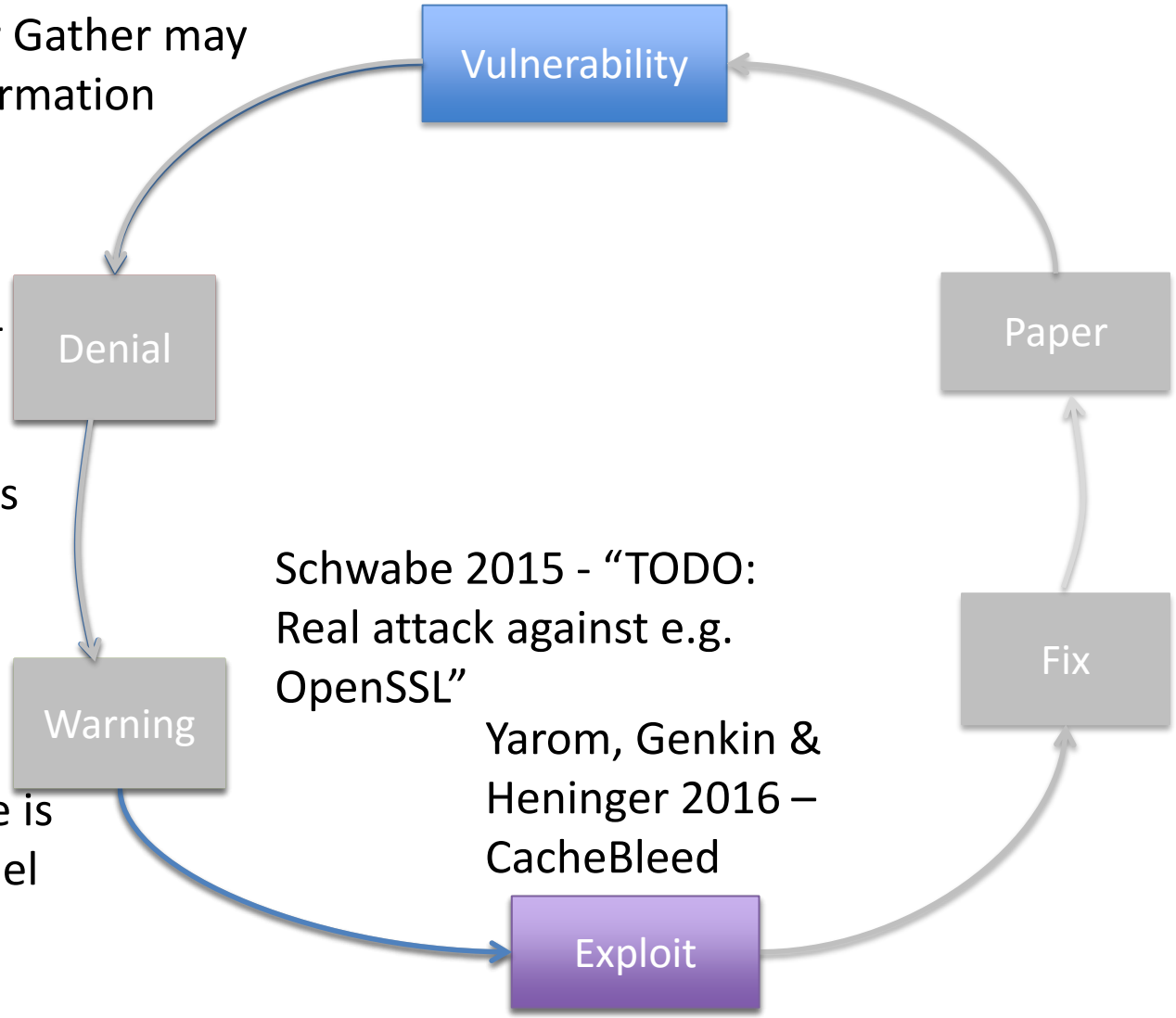
Cache banks

- To support superscalar processing the cache is divided into cache banks
  - Bits 2-5 of the address determine the bank
- In Sandy Bridge, each bank can serve only one request per cycle.
  - Concurrent access to the same bank causes delays
  - Concurrent access to different banks is always possible



Round 2

Bernstein 2005, Osvik Shamir & Tromer 2006 – Scatter Gather may leak information



Brickell 2011 – OpenSSL mitigates side channels

Schwabe 2015 - "TODO: Real attack against e.g. OpenSSL"

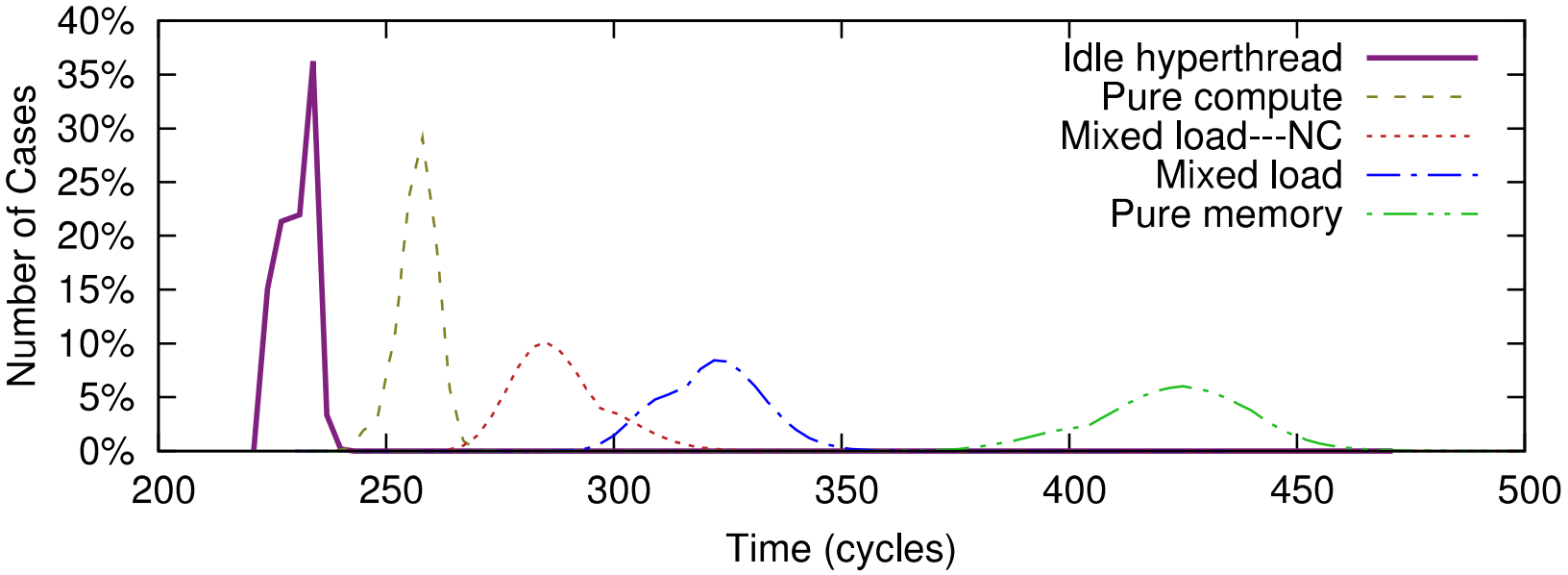
Yarom, Genkin & Heninger 2016 – CacheBleed

Bernstein & Schwabe 2013 – There is a side-channel

CacheBleed

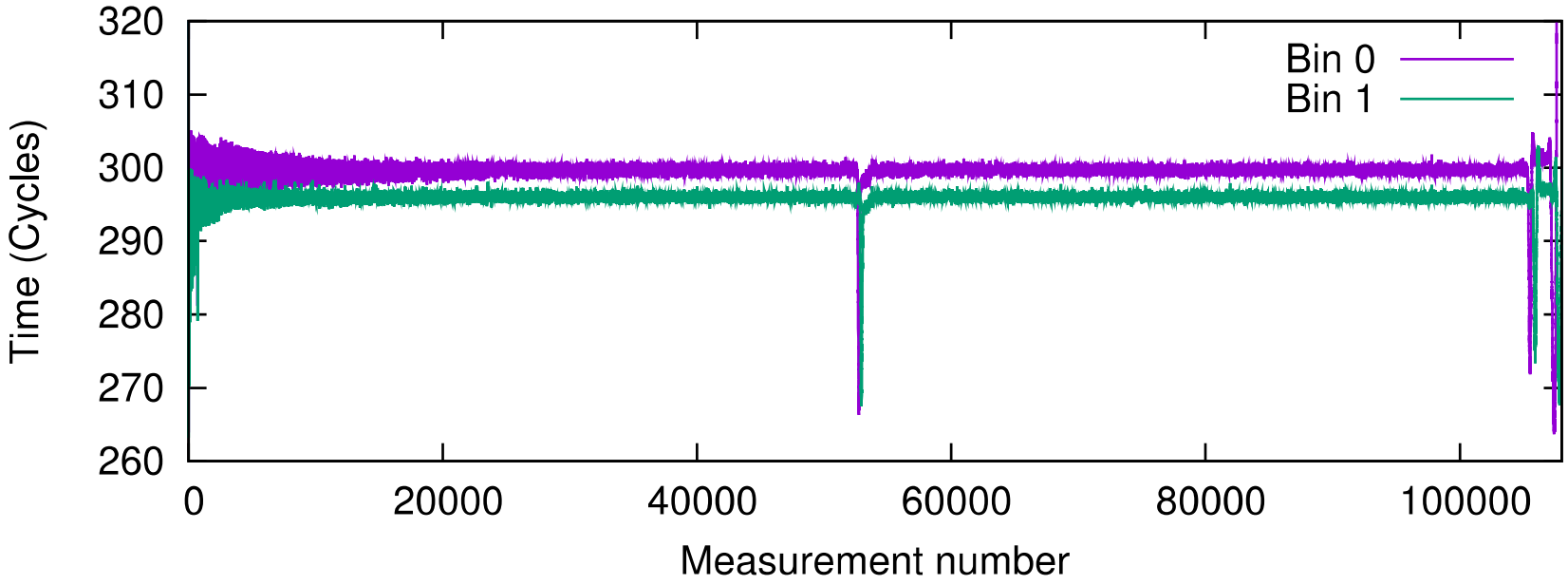
```
1    rdtscp
2    movq    %rax, %r10

4    addl    0x000(%r9), %eax
5    addl    0x040(%r9), %ecx
6    addl    0x080(%r9), %edx
7    addl    0x0c0(%r9), %edi
8    addl    0x100(%r9), %eax
9    addl    0x140(%r9), %ecx
10   addl    0x180(%r9), %edx
11   addl    0x1c0(%r9), %edi
.
.
.
256  addl    0xf00(%r9), %eax
257  addl    0xf40(%r9), %ecx
258  addl    0xf80(%r9), %edx
259  addl    0xfc0(%r9), %edi

261  rdtscp
262  subq    %r10, %rax
```

CacheBleed timing



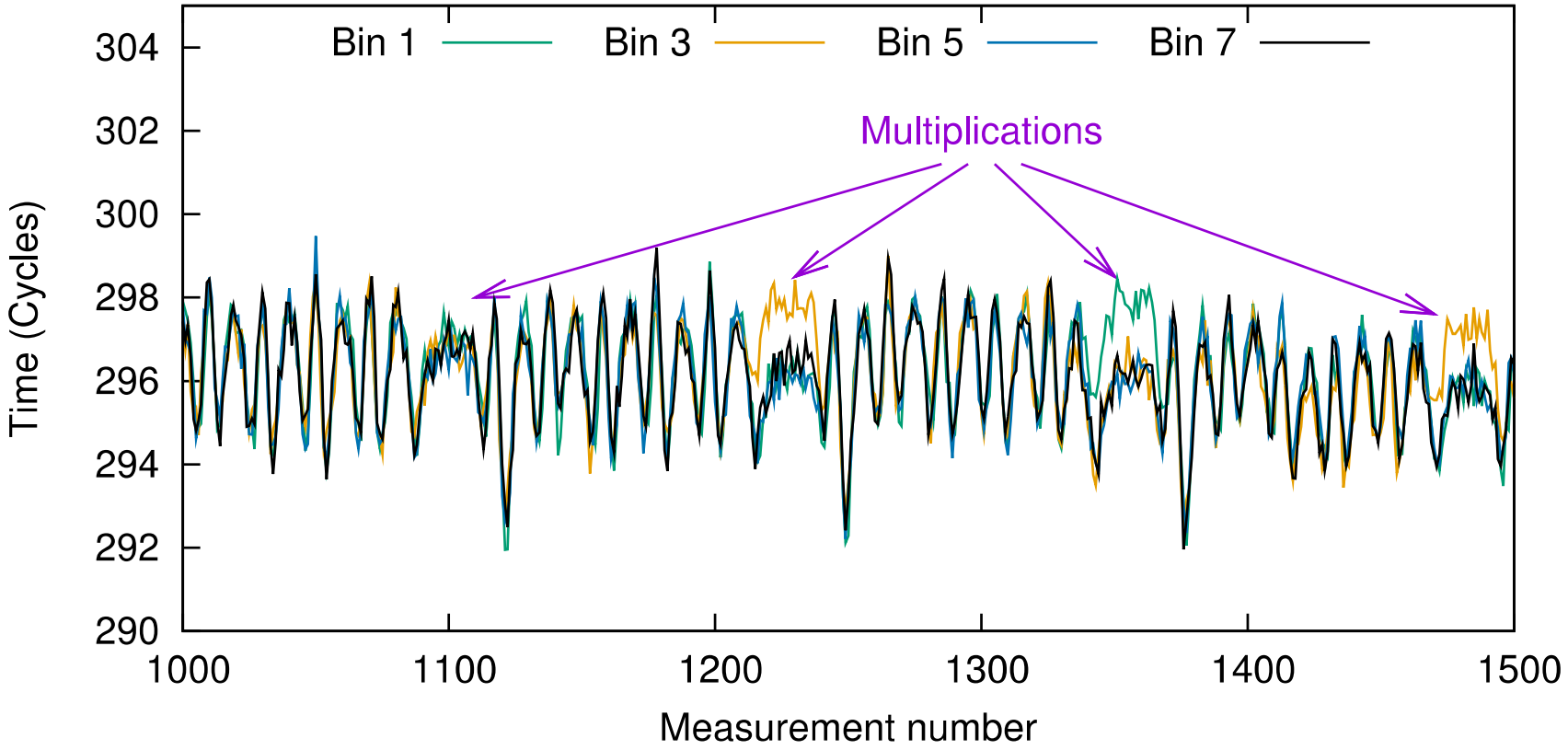
- Need multiple samples to determine cache-bank conflicts

CacheBleed on OpenSSL

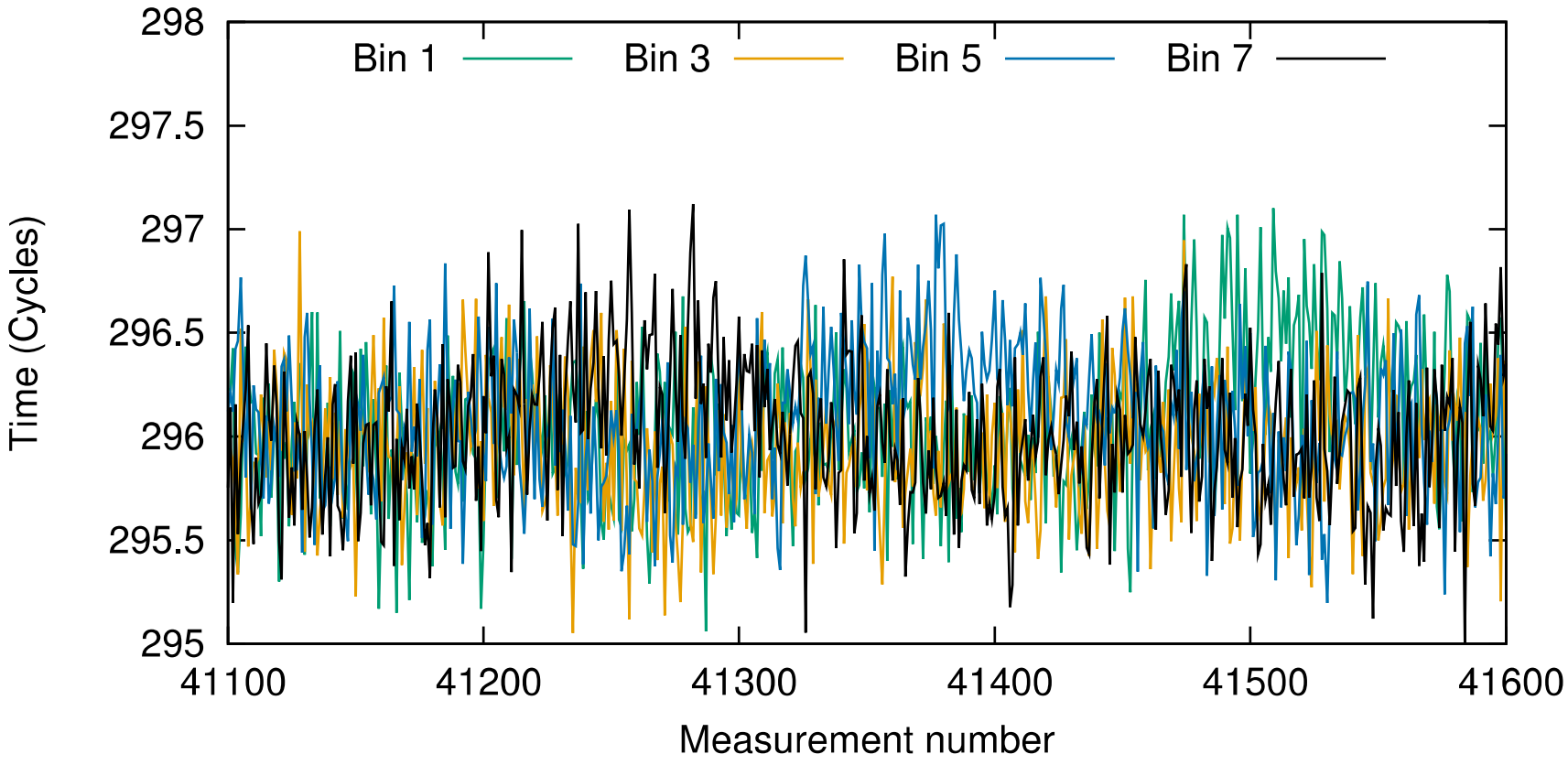


- Average of 1,000 sequences on each bin
- Odd and even bins have different timing characteristics

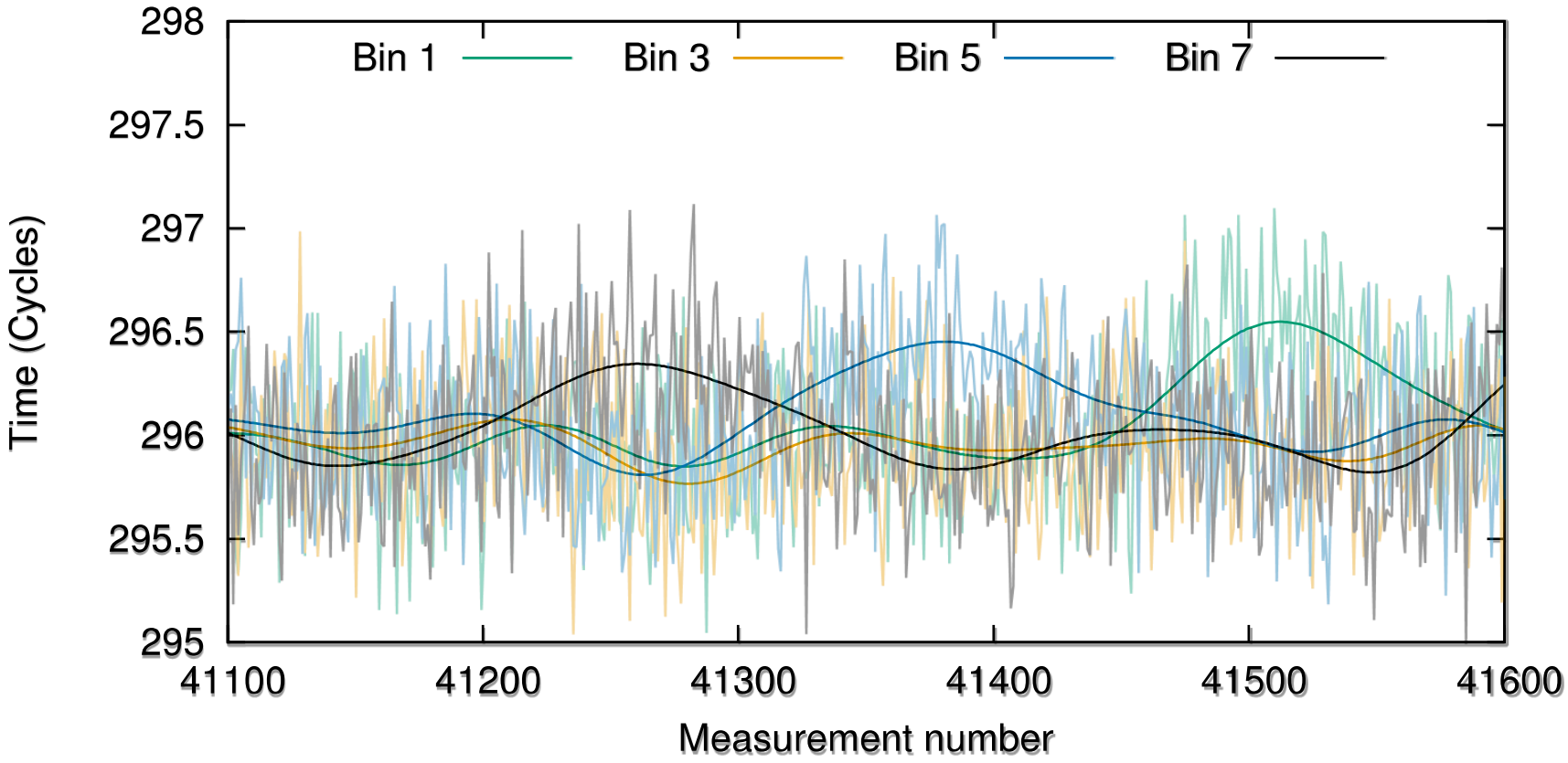
CacheBleed on OpenSSL - Details



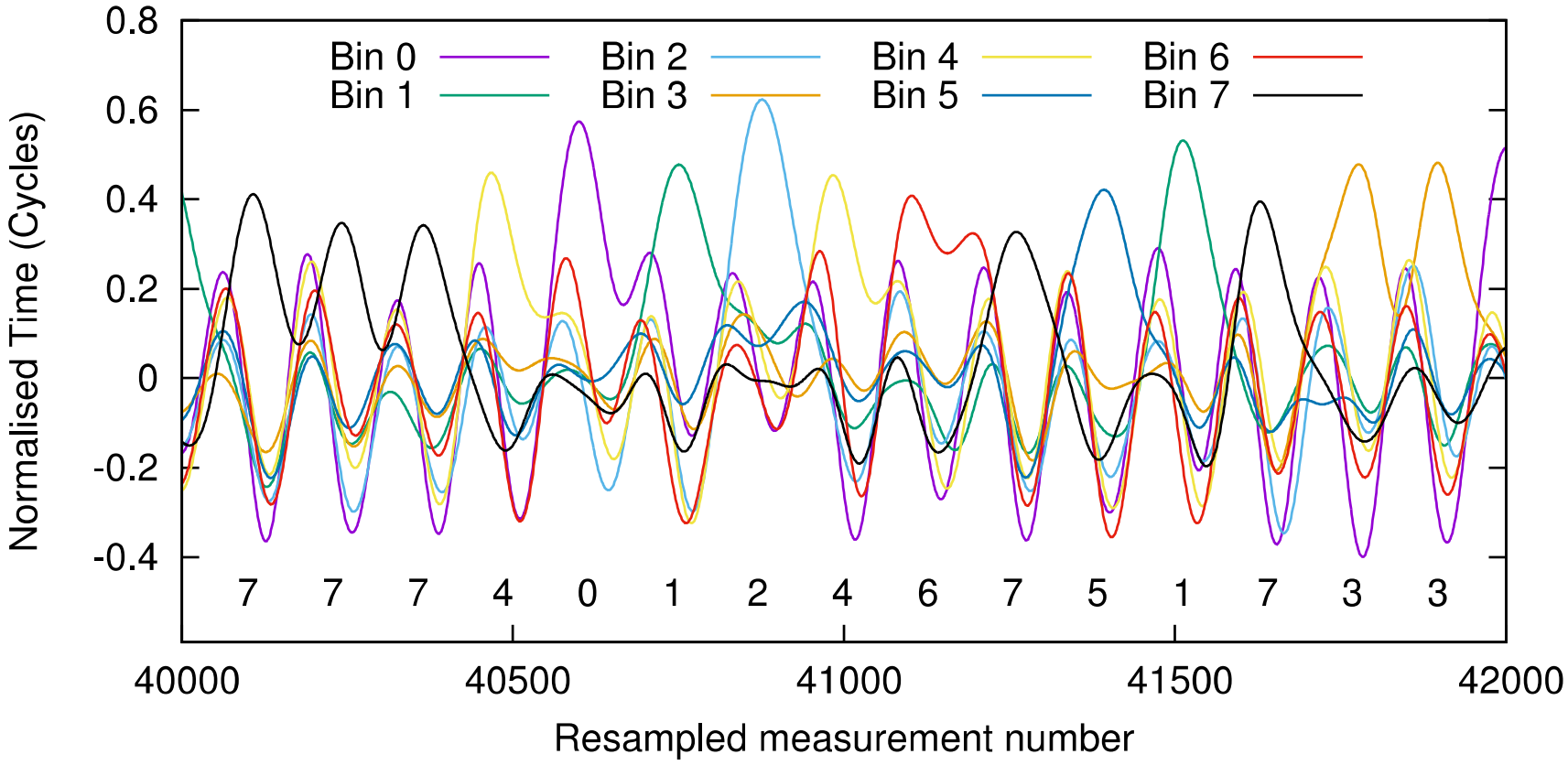
Clock Drift


Bin 1
Bin 3
Bin 5
Bin 7
298
297.5
297
296.5
296
295.5
295
Time (Cycles)
41100
41200
41300
41400
41500
41600
Measurement number

Low-pass filter



Normalised + resampled

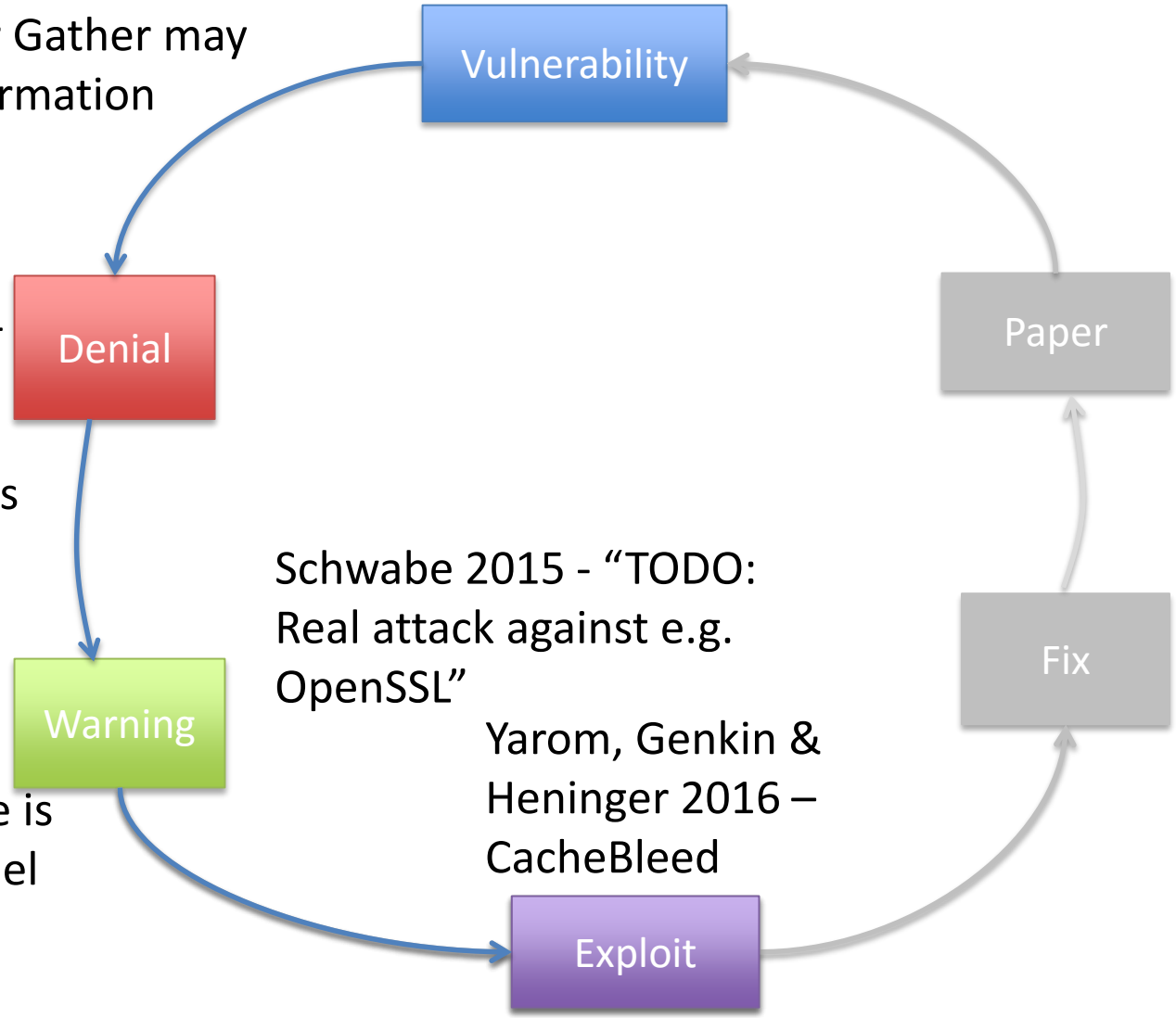


Results

- 16,000 decryptions (1,000 sequences per bin per exponentiation)
  - Less than 5 minutes online attack
- Recover three bits of each multiplier
  - Miss the first and last one or two multipliers
- Use the Heninger-Shacham algorithm to reconstruct the private key
  - Two CPU hours – less than 3 minutes on a high-end server.

Round 2

Bernstein 2005, Osvik Shamir & Tromer 2006 – Scatter Gather may leak information



Brickell 2011 – OpenSSL mitigates side channels

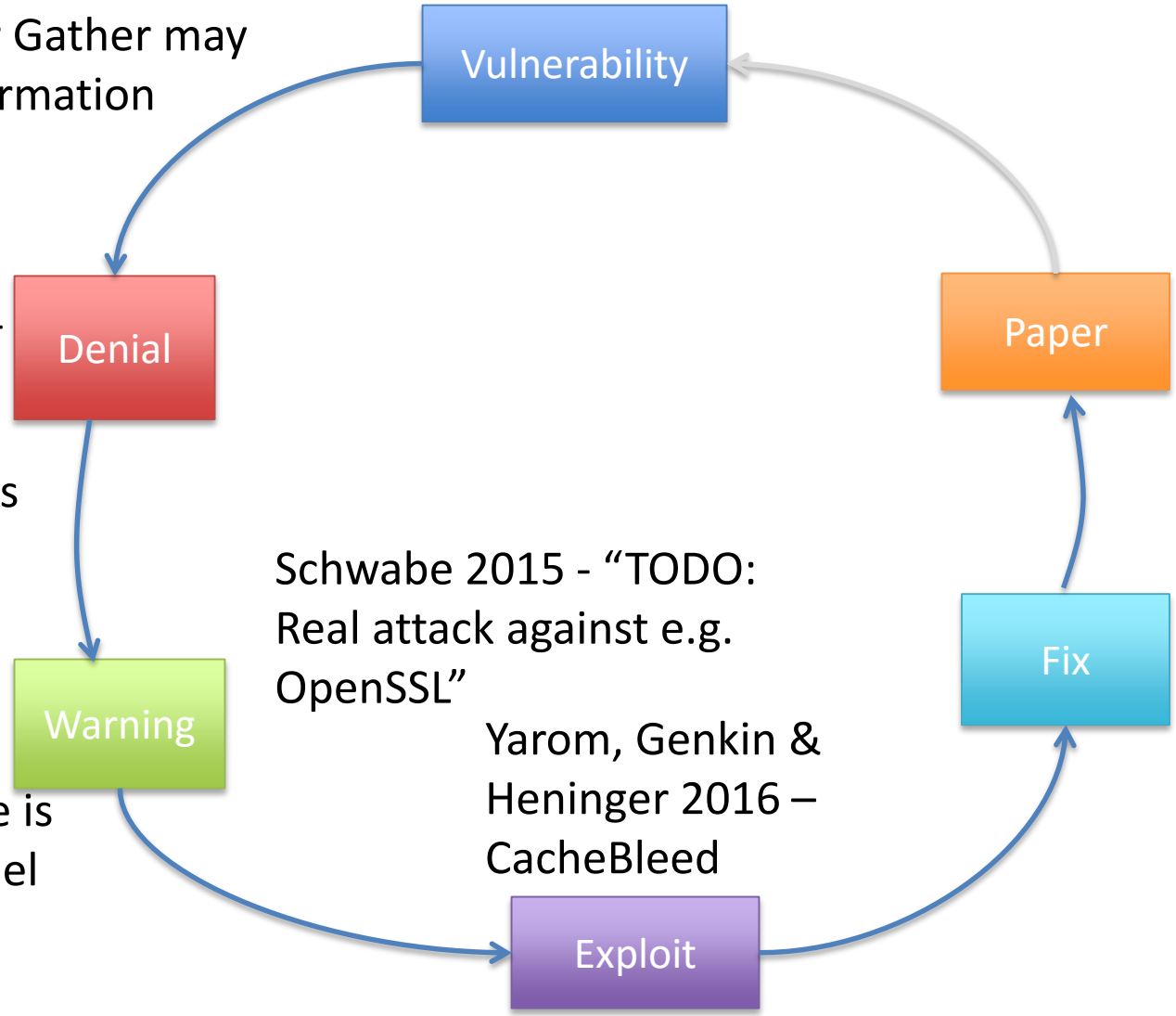
Schwabe 2015 - "TODO: Real attack against e.g. OpenSSL"

Yarom, Genkin & Heninger 2016 – CacheBleed

Bernstein & Schwabe 2013 – There is a side-channel

Round 2

Bernstein 2005, Osvik Shamir & Tromer 2006 – Scatter Gather may leak information



Brickell 2011 – OpenSSL mitigates side channels

Schwabe 2015 - "TODO: Real attack against e.g. OpenSSL"

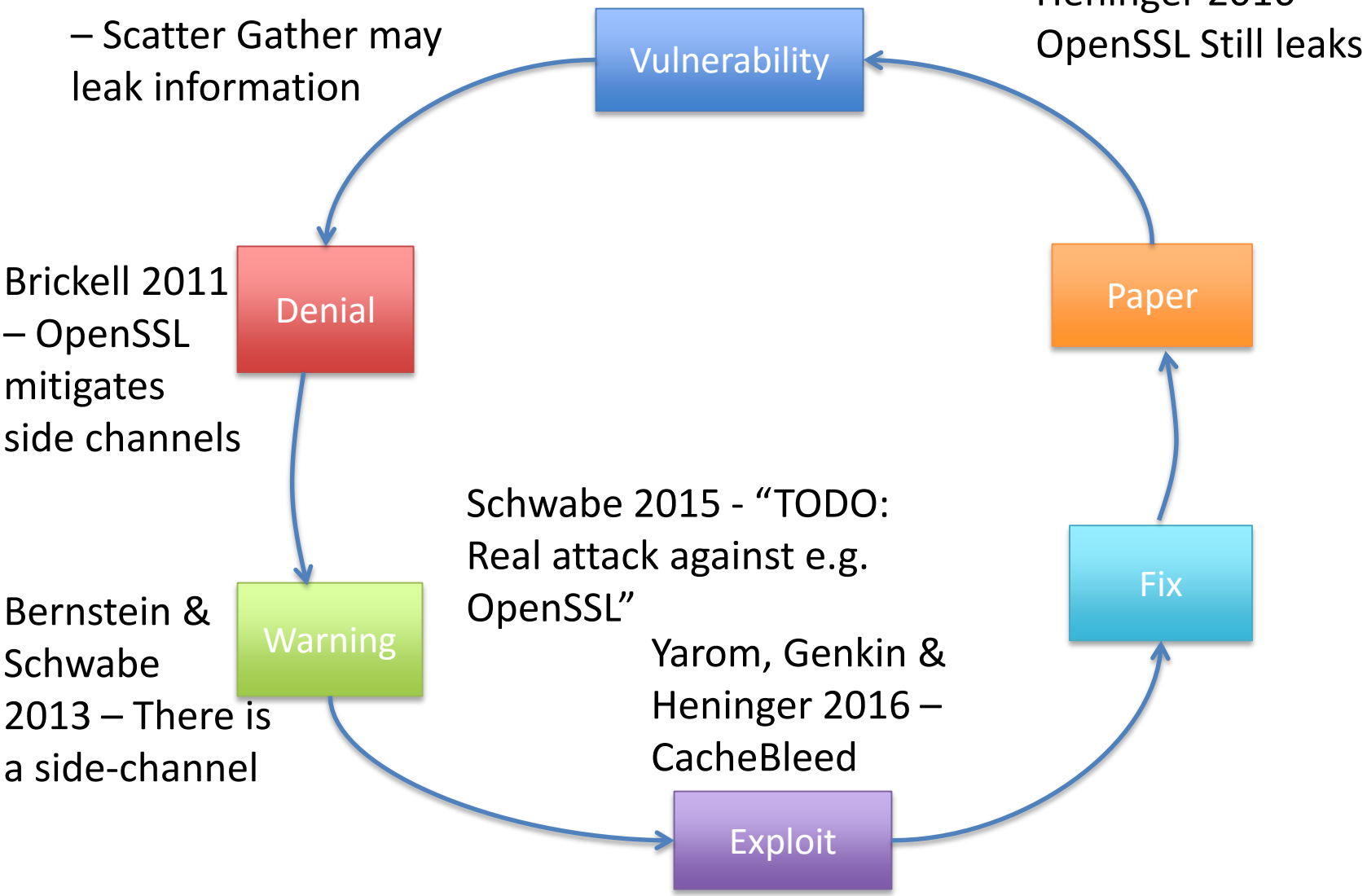
Yarom, Genkin & Heninger 2016 – CacheBleed

Bernstein & Schwabe 2013 – There is a side-channel

OpenSSL “Fix”

- Use 128-bit reads with masking
  - Only leaks 2 bits per multiplier
- Read at a different offset in each of the four cache lines
  - Order depends on the multiplier

Round 2


Bernstein 2005, Osvik Shamir & Tromer 2006 – Scatter Gather may leak information
Vulnerability
Yarom, Genkin & Heninger 2016 – OpenSSL Still leaks
Brickell 2011 – OpenSSL mitigates side channels
Denial
Paper
Schwabe 2015 - "TODO: Real attack against e.g. OpenSSL"
Yarom, Genkin & Heninger 2016 – CacheBleed
Fix
Bernstein & Schwabe 2013 – There is a side-channel
Warning
Exploit

Round 3

Yarom, Genkin & Heninger 2016 – OpenSSL Still leaks