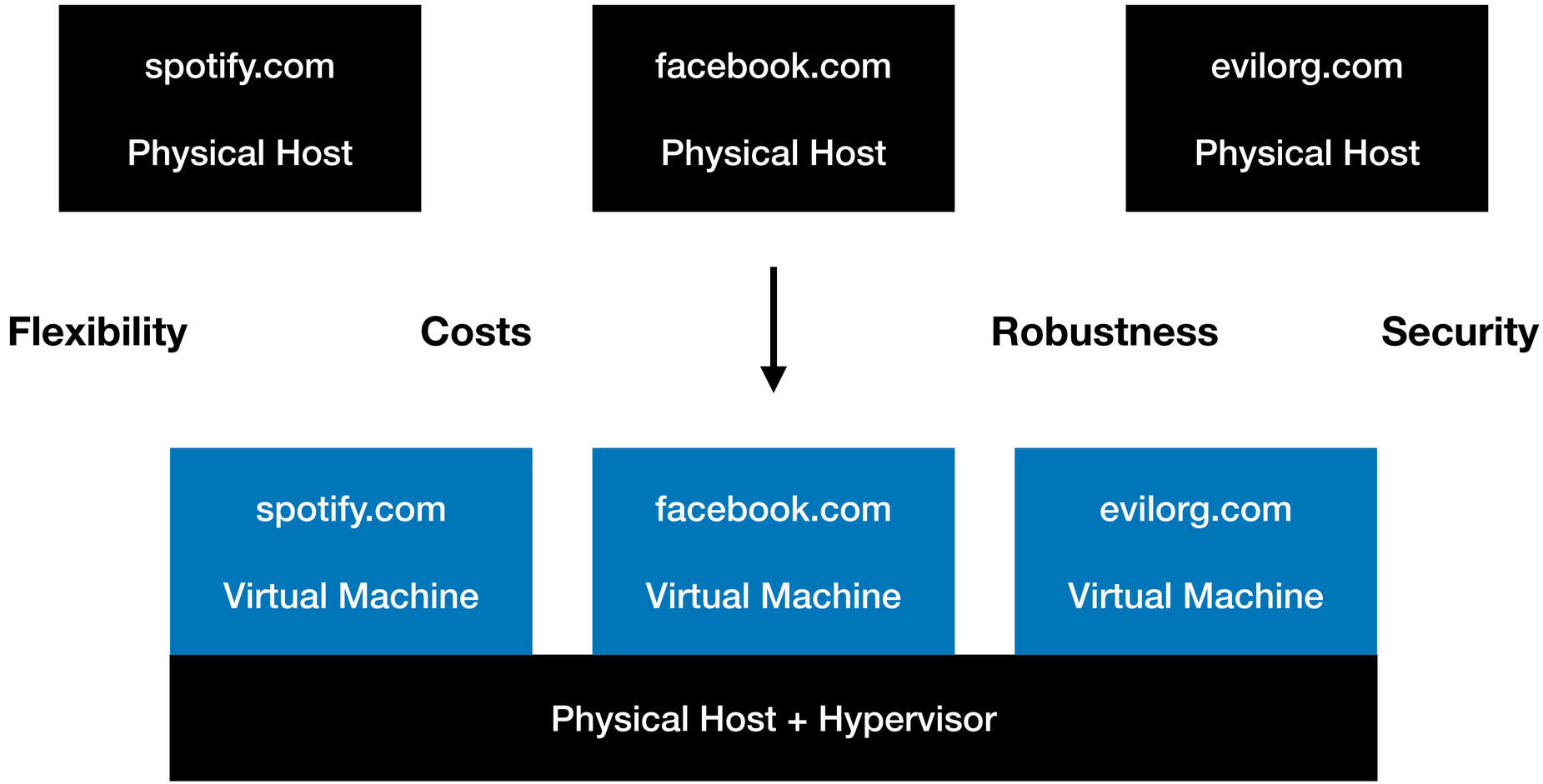
# High-Performance TLB Covert Channels

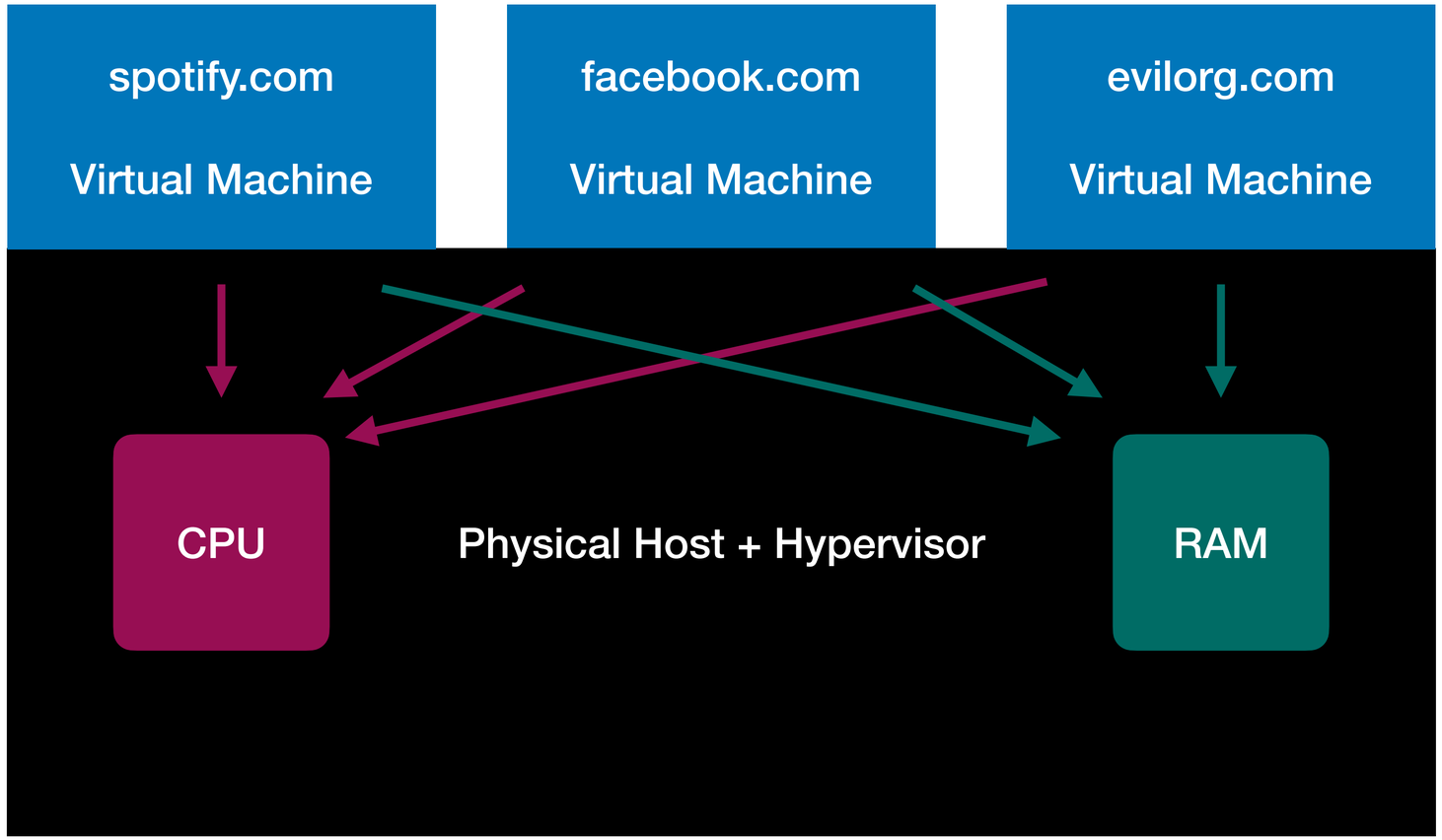
**Micha Hanselmann**

**ITEC Operating Systems Group, KIT Karlsruhe**

# Cloud Virtualization



# Security




**Shared Resources**
**Does it matter? Yes!**

**Side-Channel Attacks**

**Covert Channels**

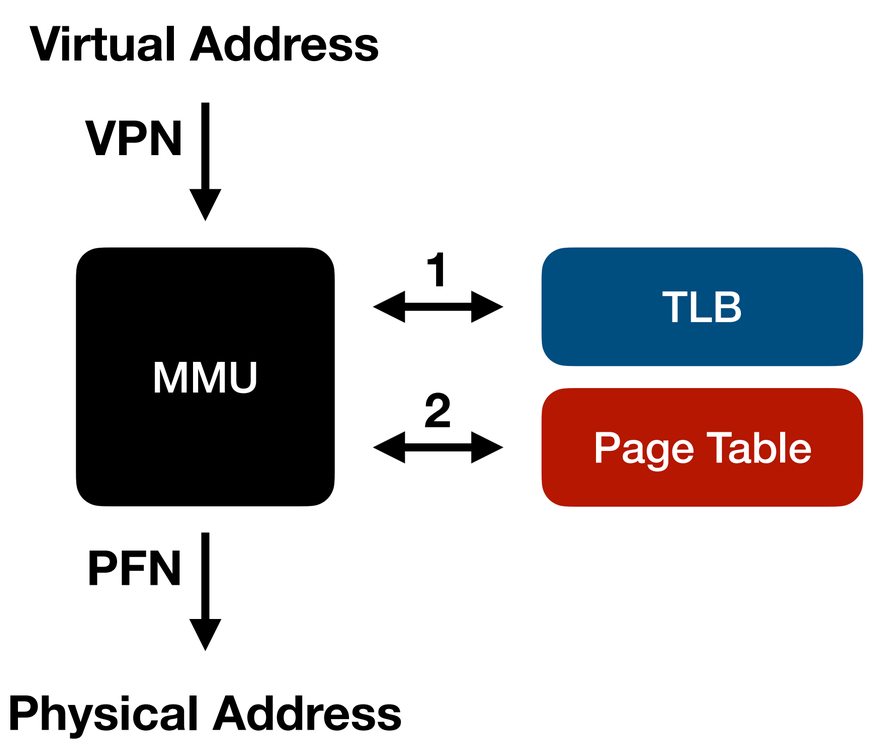
# Covert Channels

| Publication | Via | Setup | Bit Rate | Error Rate |
|---|---|---|---|---|
| Kalmbach [26] | CPU Frequency | VMs, cross-core | 0.135 B/s | 0 % |
| Percival [45] | CPU L1 Cache | Native, same core | 400 kB/s | — |
| Gruss et al. [19] | CPU L3 Cache | Native, cross-core | 496 kB/s | 0.84 % |
| Maurice et al. [41] | CPU L3 Cache | EC2, cross-core | 45.09 kB/s | 0 % |
| Pessl et al. [46] | DRAM Row Buffer | VMs, cross-CPU | 74.5 kB/s | 0.4 % |
| Gras et al. [18] | CPU TLB | Native, same core | 0.875 B/s | 0.002 % |

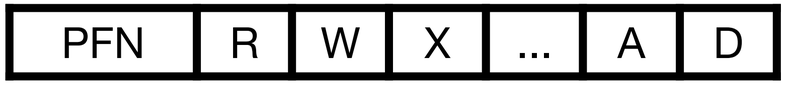
🏎️ **CPU caches allow channels with high bit rates**

⛔ **But can be prevented by cache isolation techniques (e.g., Intel CAT)**

# Translation Lookaside Buffer (TLB)



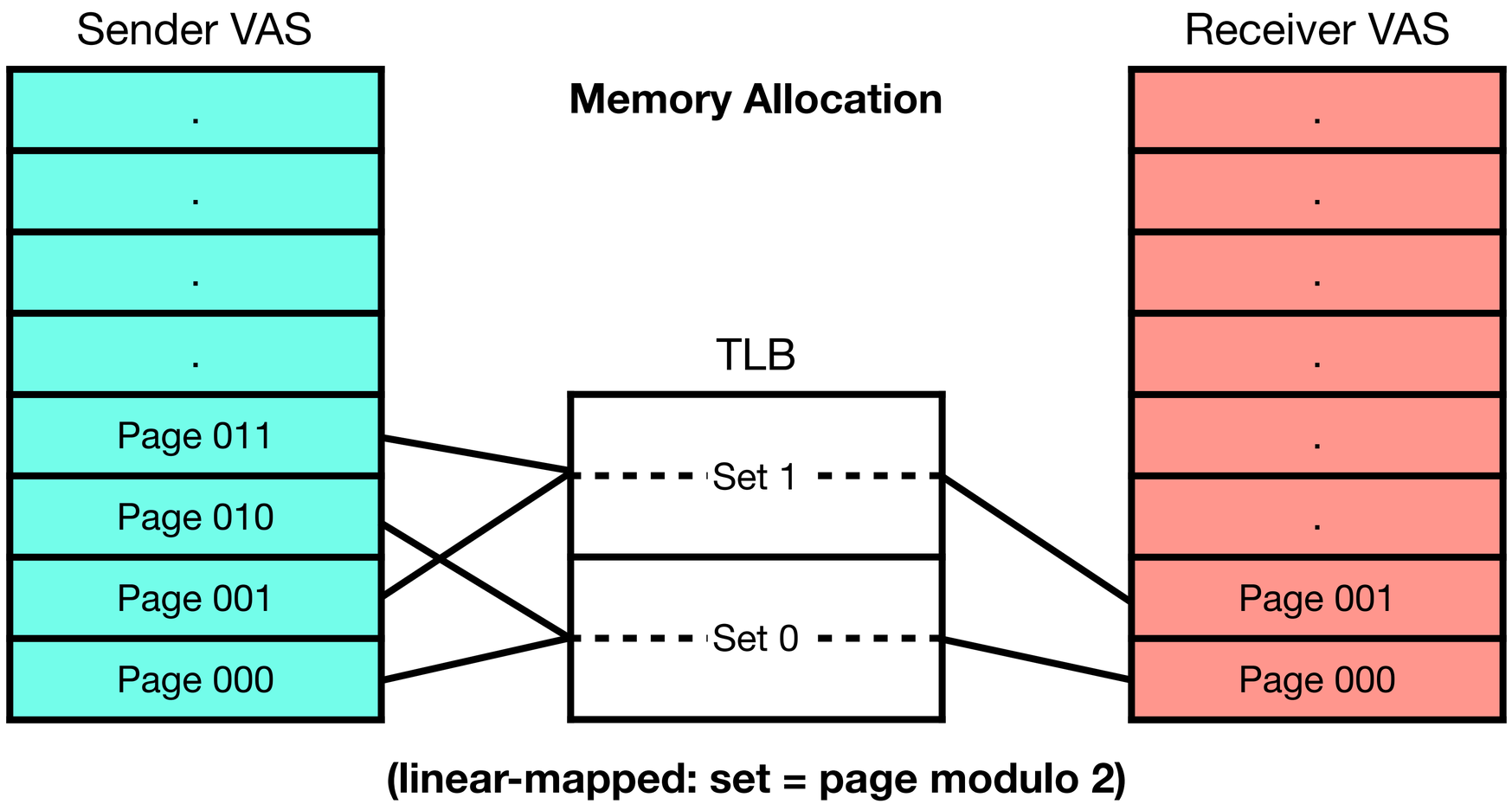

Page Table Entry




TLB Entry

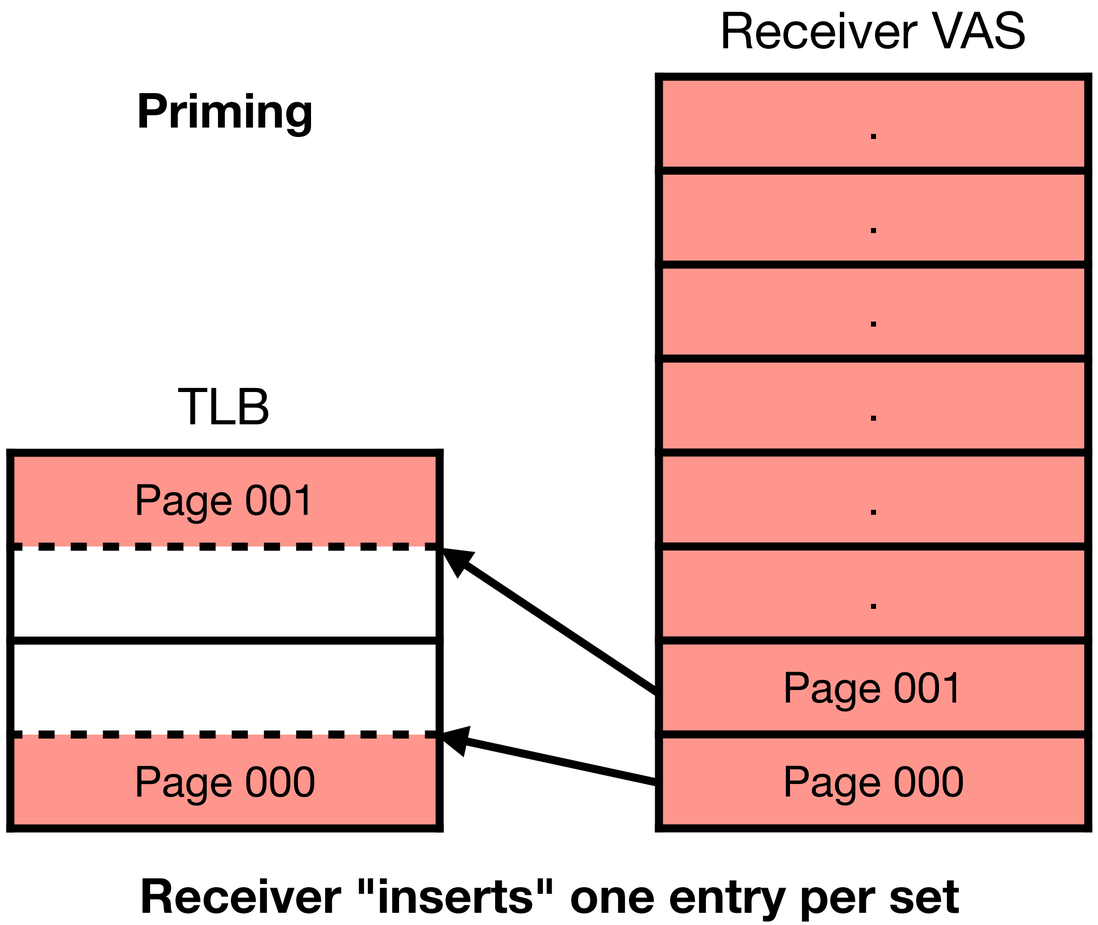

- **Not covered by Intel CAT / TSX**
- **Fast, unrestricted access**
- **128+ sets → decent resolution**
- **Bit rate? Reliability?**

# TLB Covert Channel



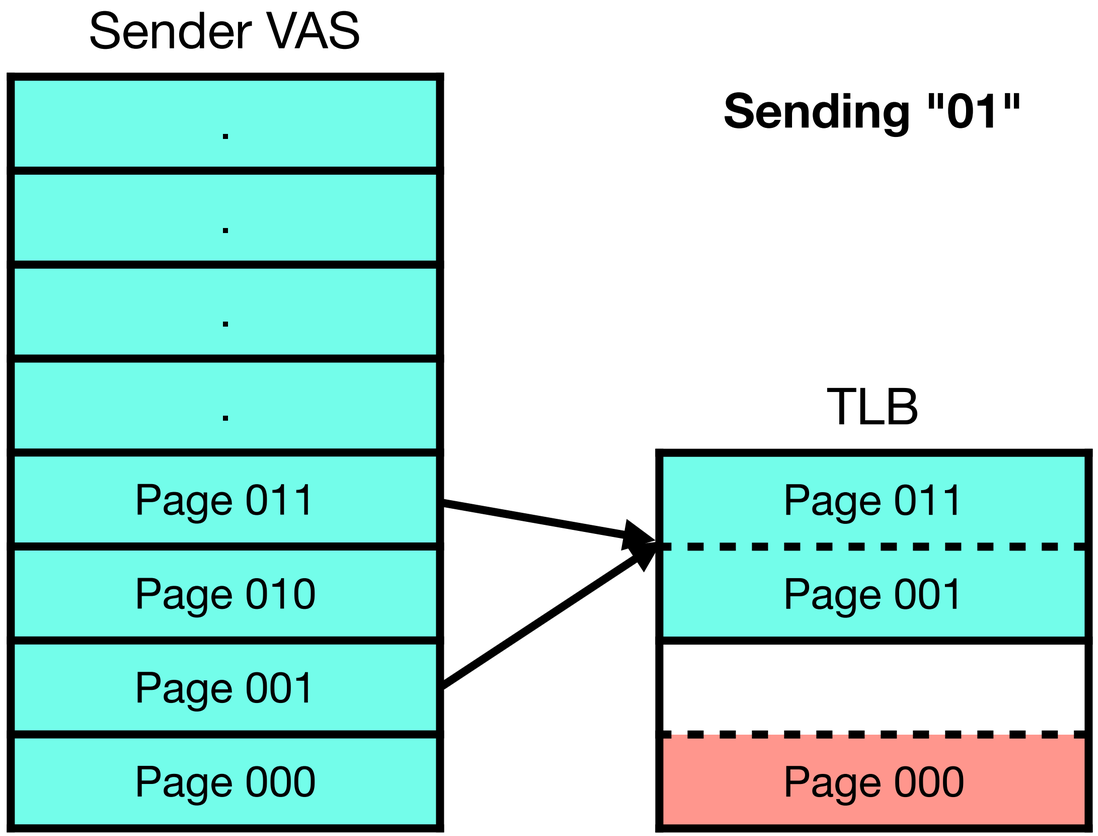

**(linear-mapped: set = page modulo 2)**

# TLB Covert Channel




**Receiver "inserts" one entry per set**

# TLB Covert Channel




**Sender evicts corresponding sets**

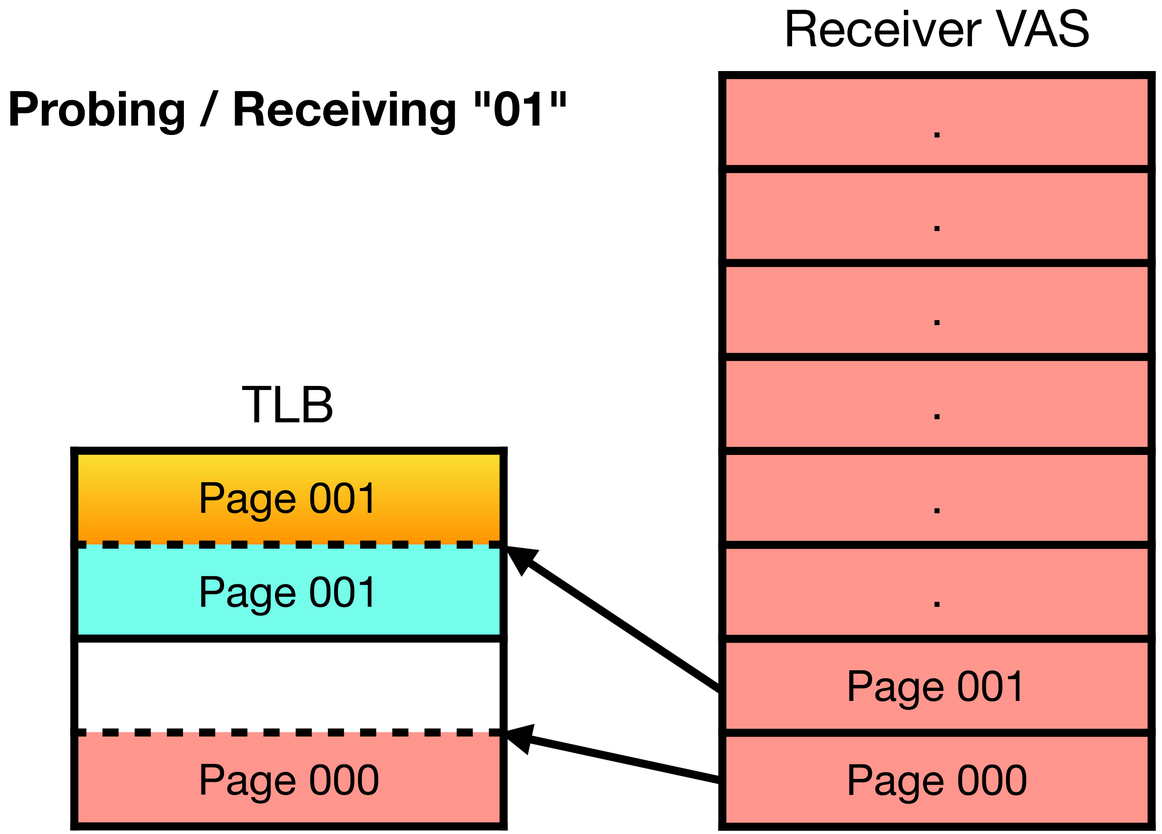
# TLB Covert Channel

**Via Timestamps**

- **Measures access latencies**
- **Time fluctuations → error-prone**

**Via Accessed Bits (ABs)**

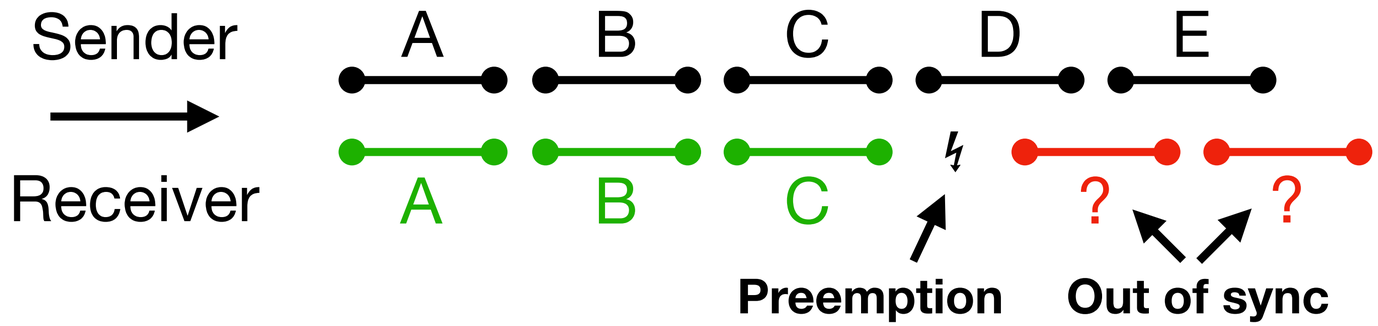
- **Resets ABs between accesses**
- **TLB miss → page walk → AB set**
- **Requires elevated permissions → unidirectional channel**



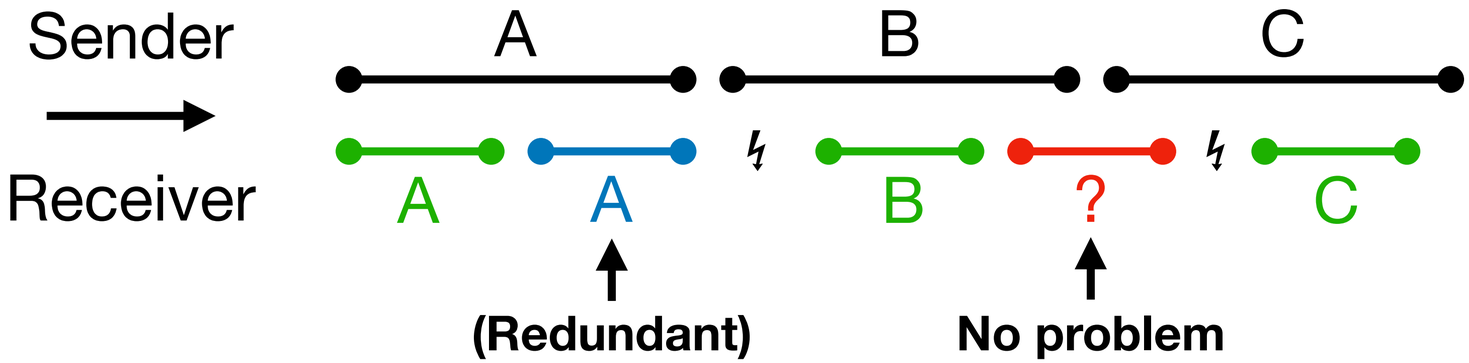

**Receiver interprets TLB hits (0) and misses (1)**

# Challenges

**Transmission successful ↔ receiver window falls completely in sender window**

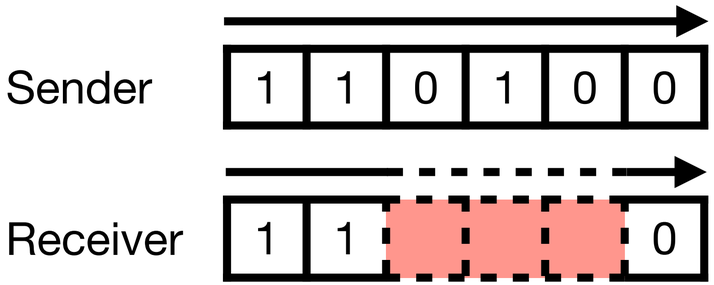



**Synchronization without direct communication / a common clock → sampling**

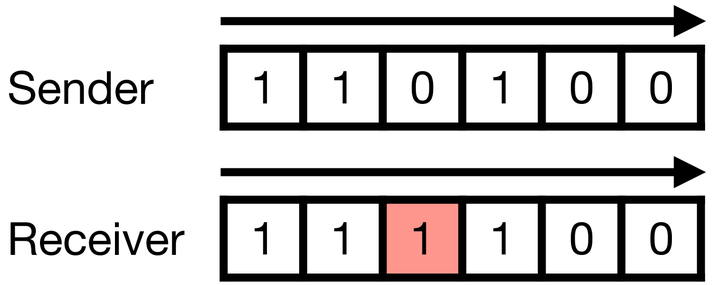


# Challenges

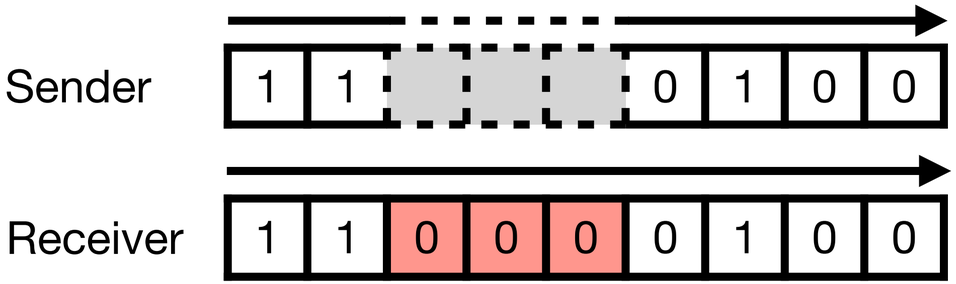
**Receiver not scheduled → deletion errors**




**Noise → substitution errors**




**Sender not scheduled → insertion errors**

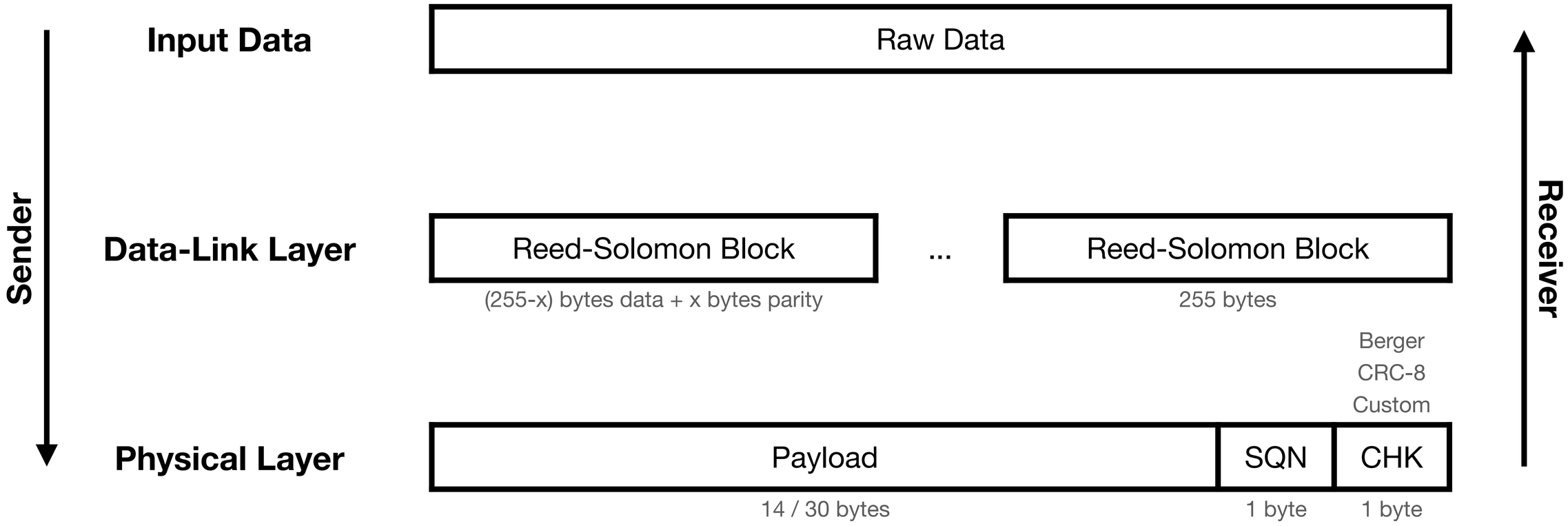



**Issues of synchronization and noise**

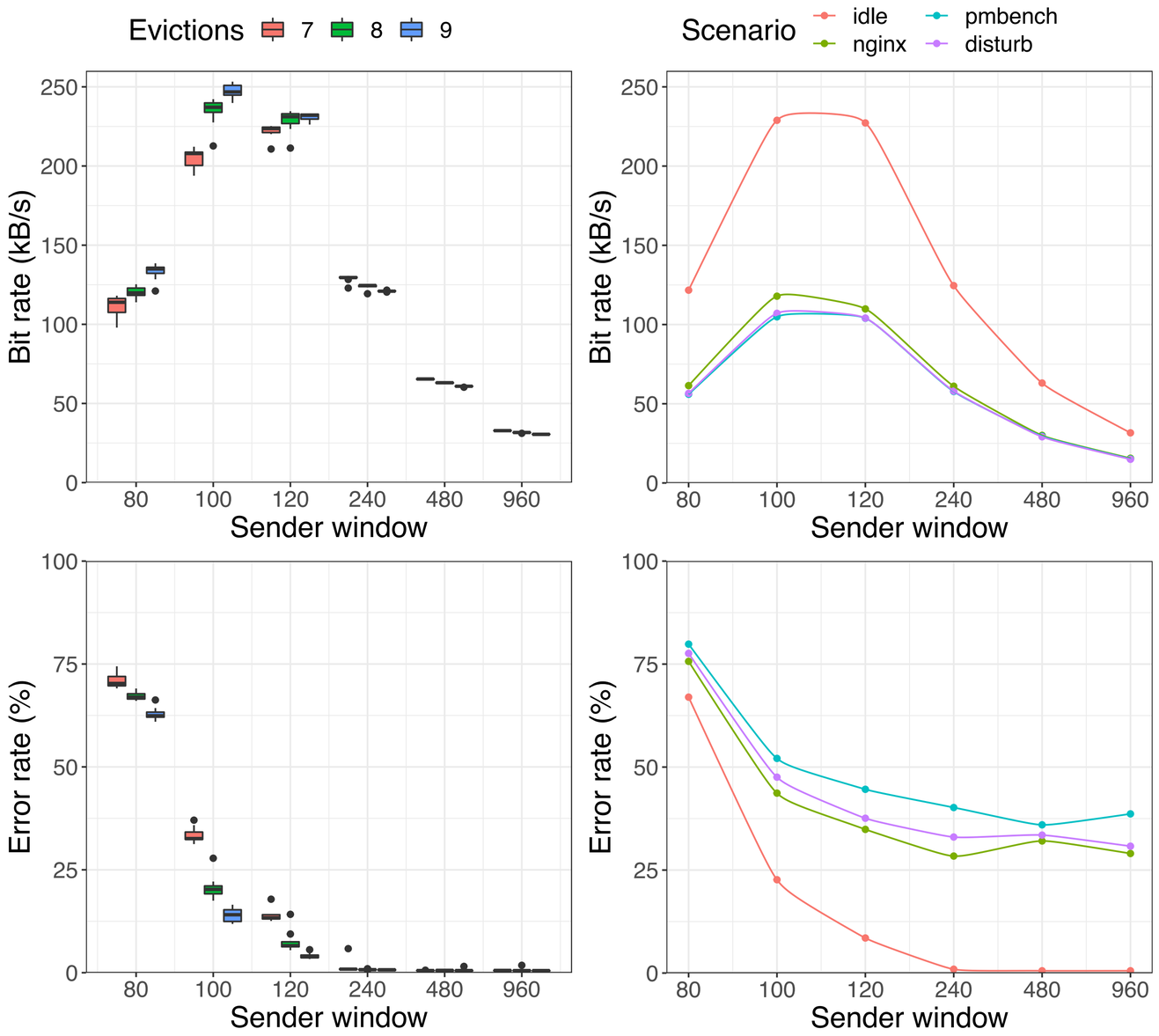
**→ detect / correct errors**

**→ an appropriate protocol is required**

# Protocol


Sender
Input Data
Raw Data
Data-Link Layer
Reed-Solomon Block
...
Reed-Solomon Block
(255-x) bytes data + x bytes parity
255 bytes
Berger
CRC-8
Custom
Physical Layer
Payload
SQN
CHK
14 / 30 bytes
1 byte
1 byte
Receiver

# Physical Layer only




Accessed Bits, 256 TLB Sets, CRC-8 Checksum

**Longer sender windows**

- **More redundancy**
- **Channel reliability ↑**
- **Maximum bit rate ↓**

**Enough redundancy**

- **Channel is saturated**
- **No further improvement**

**Concurrent processes**

- **Only half the performance**
- **Minimum error rate ↑**

# Limitations

**lost packet**

```
[snd] 1. Und es begab sich darnach, daß sich der Schenke des Königs in
Ägypten und der Bäcker versündigten an ihrem Herrn, dem König von
Ägypten.

[rcv] 1. Und es begab sich darnach, daß sich der Schenke des Königs in
Ägypten und der Bäcker versündigtvon Ägypten.
```

**corrupt packet**

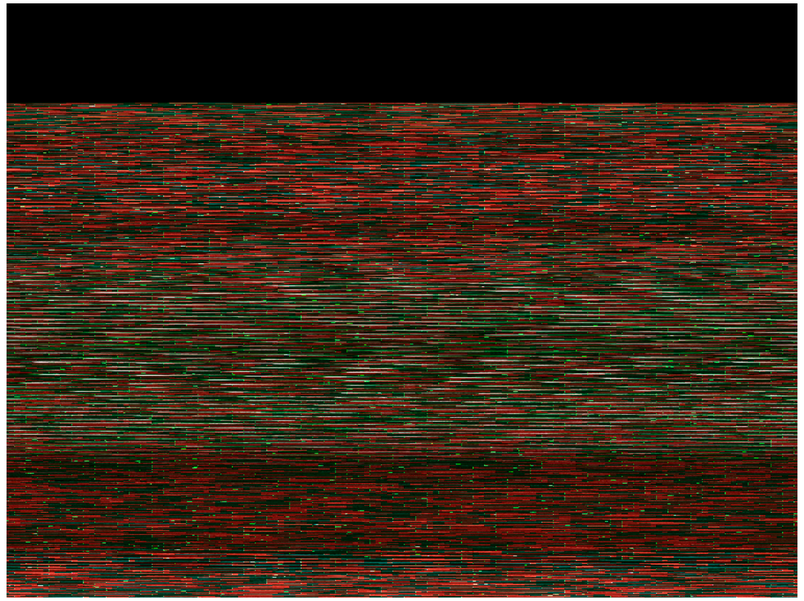
```
[snd] 2. Und Pharao ward zornig über seine beiden Kämmerer, über den
Amtmann über die Schenken und über den Amtmann über die Bäcker,

[rcv] 2. Und Pharao ward zornig über seine beiden a?d,oro{o über
weonemvminon?Kämmerer, über den Amtmann über die Schenken und über den
Amtmann über die Bäcker,
```

**Physical layer cannot correct errors**

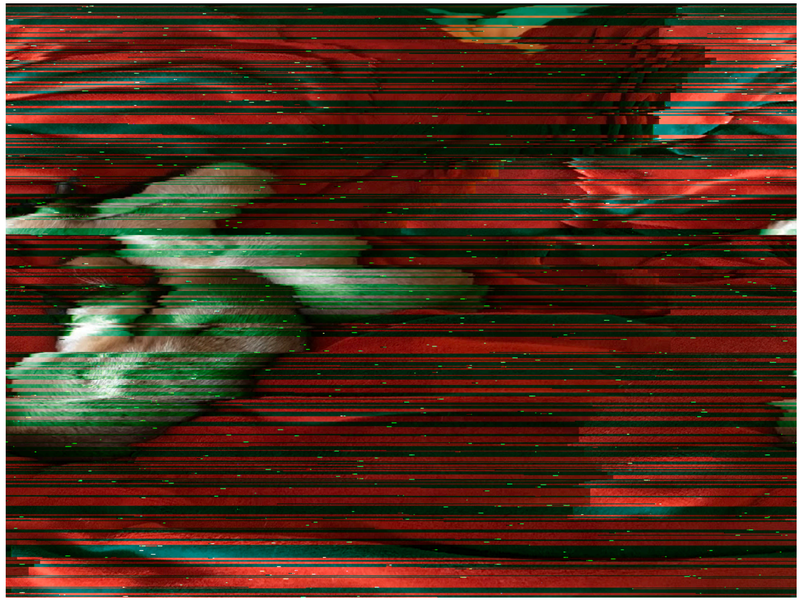
- **Sufficient for data with natural redundancy ✅**

# Limitations

Original



Error Rate 17.4 %

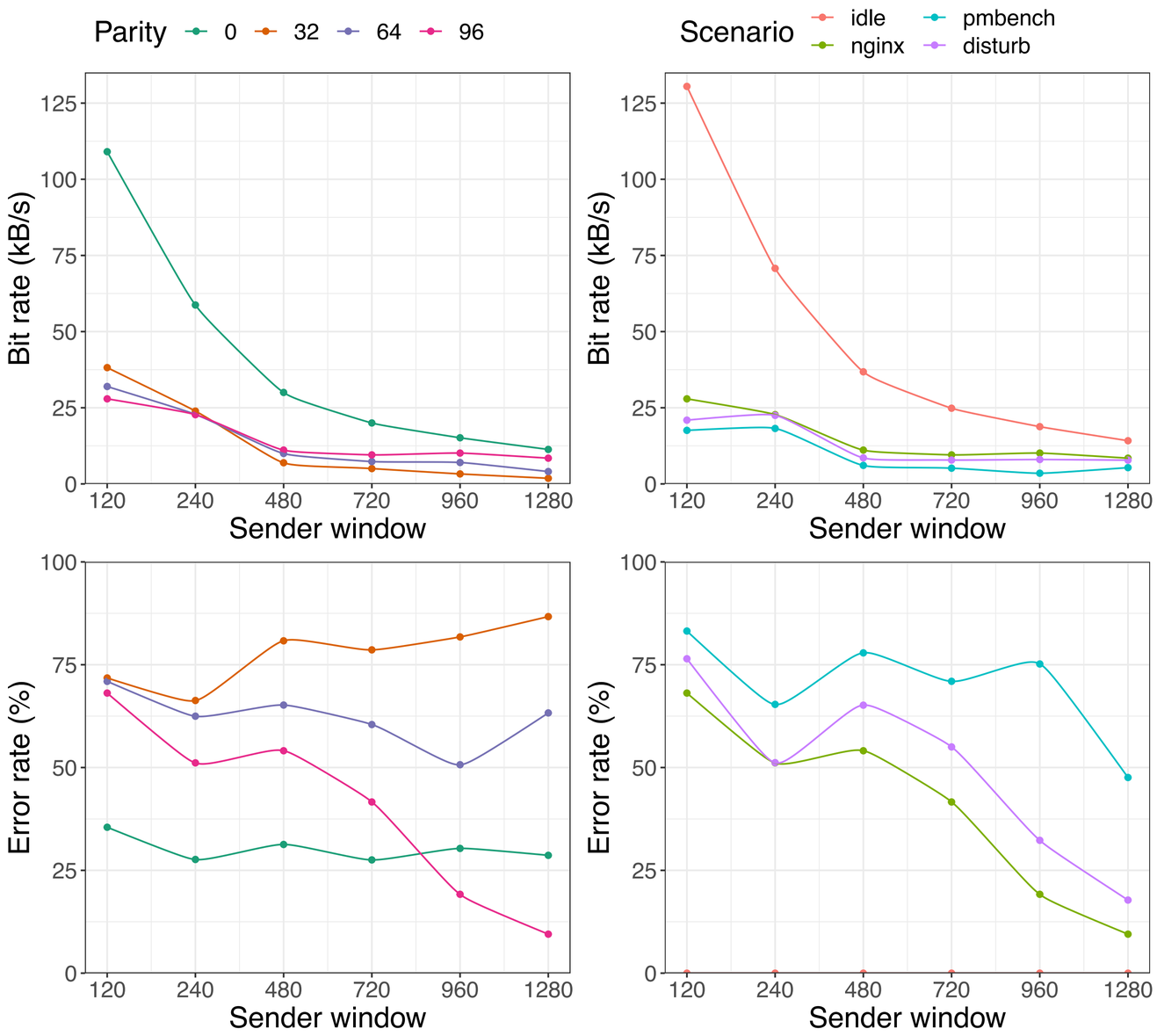


Error Rate 0.8 %

**Physical layer cannot correct errors**

- **Sufficient for data with natural redundancy ✅**
- **Unsuited for multimedia and passwords 😐**

# Both Layers




Accessed Bits, 256 TLB Sets, CRC-8 Checksum, Nginx (left), Parity: 96 (right)

**How much parity?**

- **Low amount sufficient for error-free transmissions in idle state**
- **Correction capabilities vs. overhead**

**Higher error rate when noise is present?**

- **Short sender windows → packet loss**
- **Long sender windows → corrupt packets**

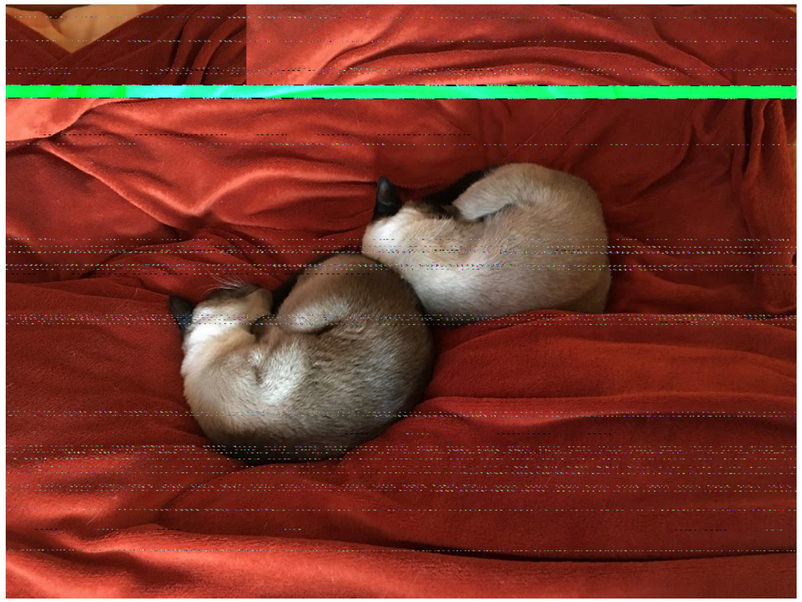
**→ RS-Blocks cannot be recovered**

**→ Higher parity amount is required**

# Both Layers

Original

Error Rate 68.4 %

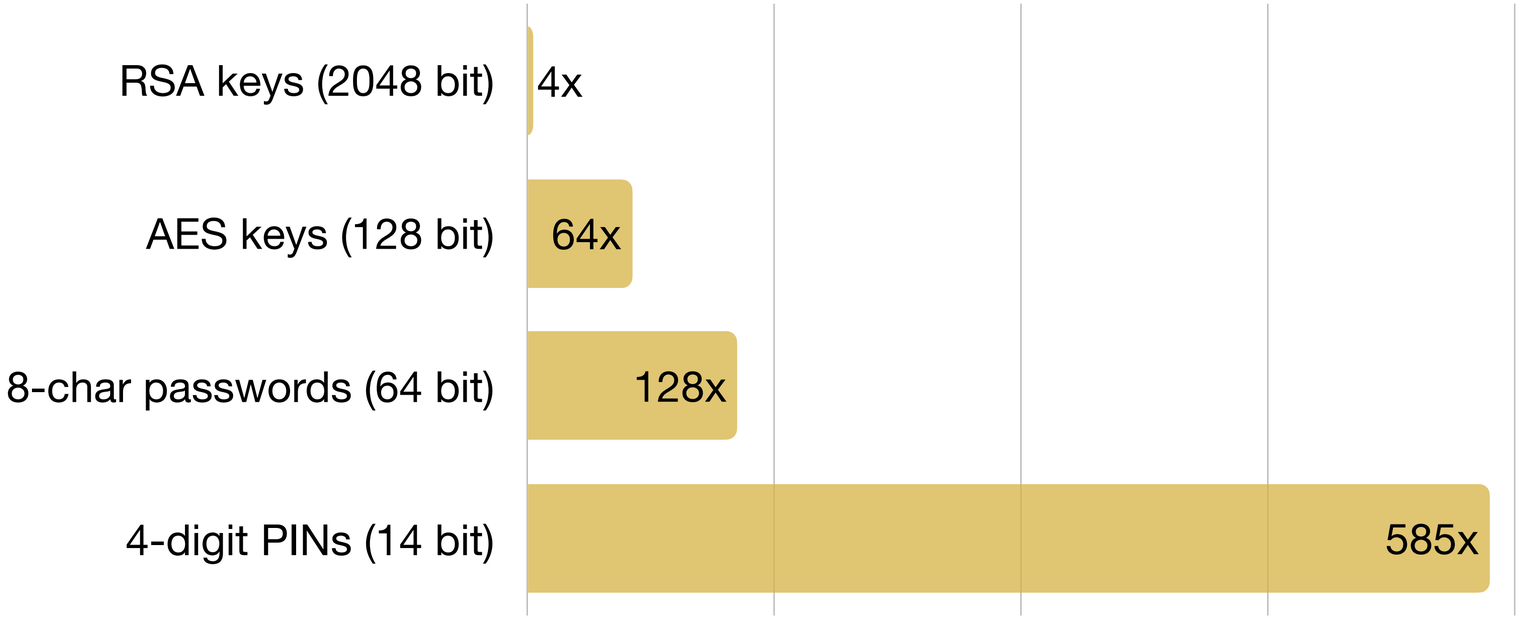


Error Rate 4.3 %

**Data-link layer worth it?**

- **Preserves file structure, even under interference ✅**
- **Unable to achieve high-performance channels ⚠️**

# Conclusion




🚨 **1 kB/s is still too much**

→ **Holistic isolation techniques are required**

# Demo

**https://github.com/deermichel/tlbchannels**

# Summary

- Shared resources pose a security risk to cloud virtualization
  → side-channel attacks & covert channels

- Cache-based covert channels allow high bit rates, but can be prevented by state-of-the-art isolation techniques

- TLB presents an alternative; transmitting bits via Prime+Probe
  → challenges: synchronization & noise → two-layer protocol

- We achieve high-performance covert channels in idle state, but under interference, the weaknesses of our unidirectional approach become visible
  → still, (implicitly) shared resources should be considered carefully