

Michael Rossberg · Michael Pfeiffer

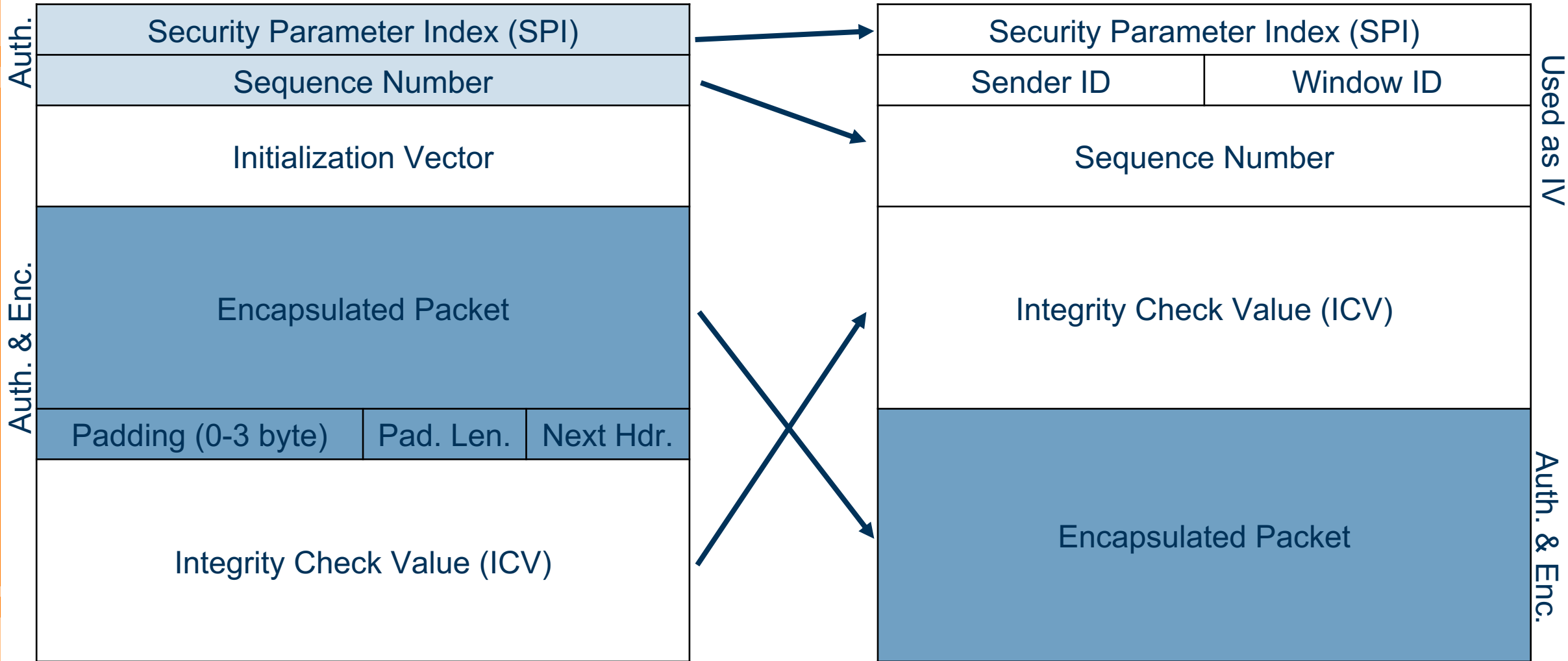
Technische Universität Ilmenau, Germany

PROPOSED IMPROVEMENTS TO ESP AIDING DATA CENTER DEPLOYMENTS

Motivation

- Scenario: ESP as is in data centers
 - Due to handling of sequence numbers:
 - Limited parallelism
 - No multicast replay protection
 - Issues with QoS
 - Due to trailer: complex protocol handling
 - Fragments
 - Segments
 - Alignment
- Approach: change ESP a “little” → New protocol/version/mode?

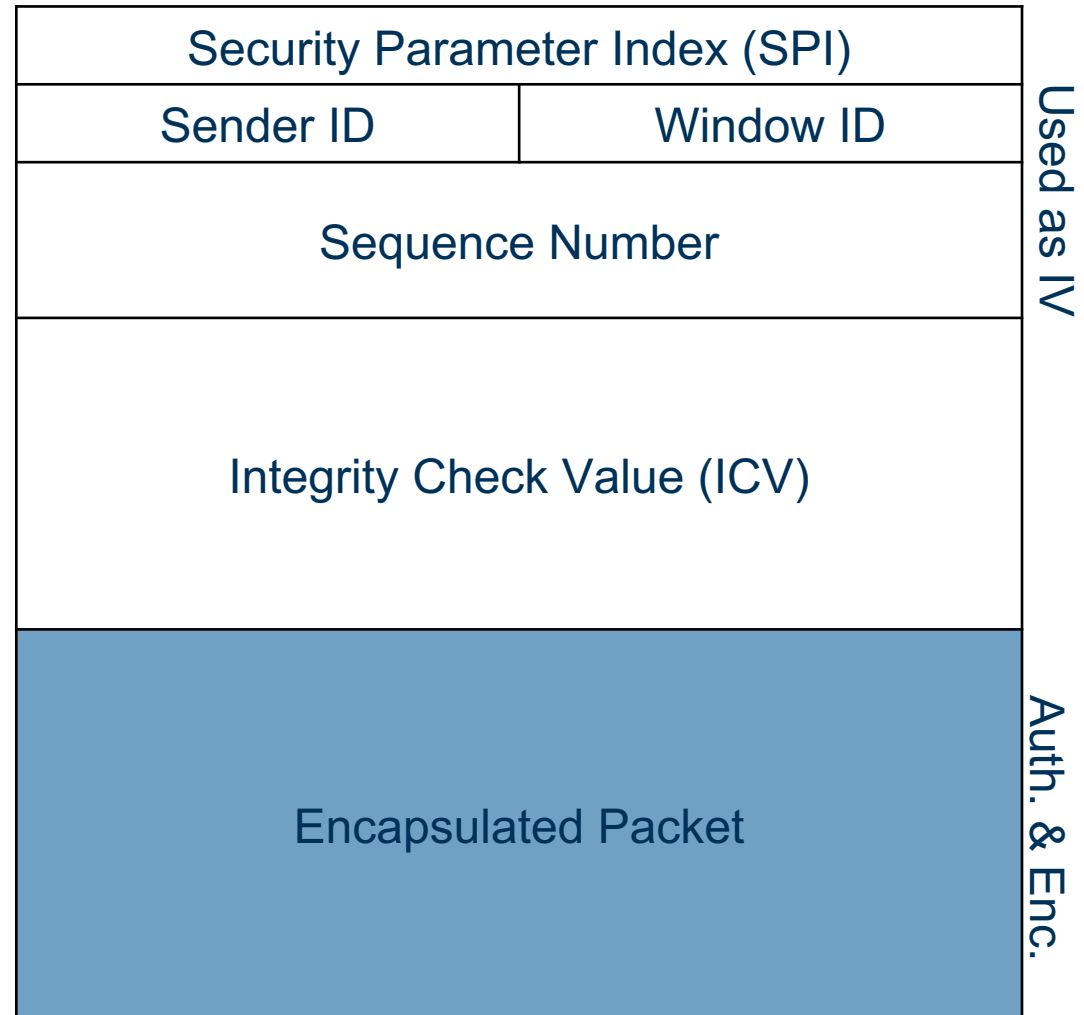
Packet Layout for Tunnel Mode



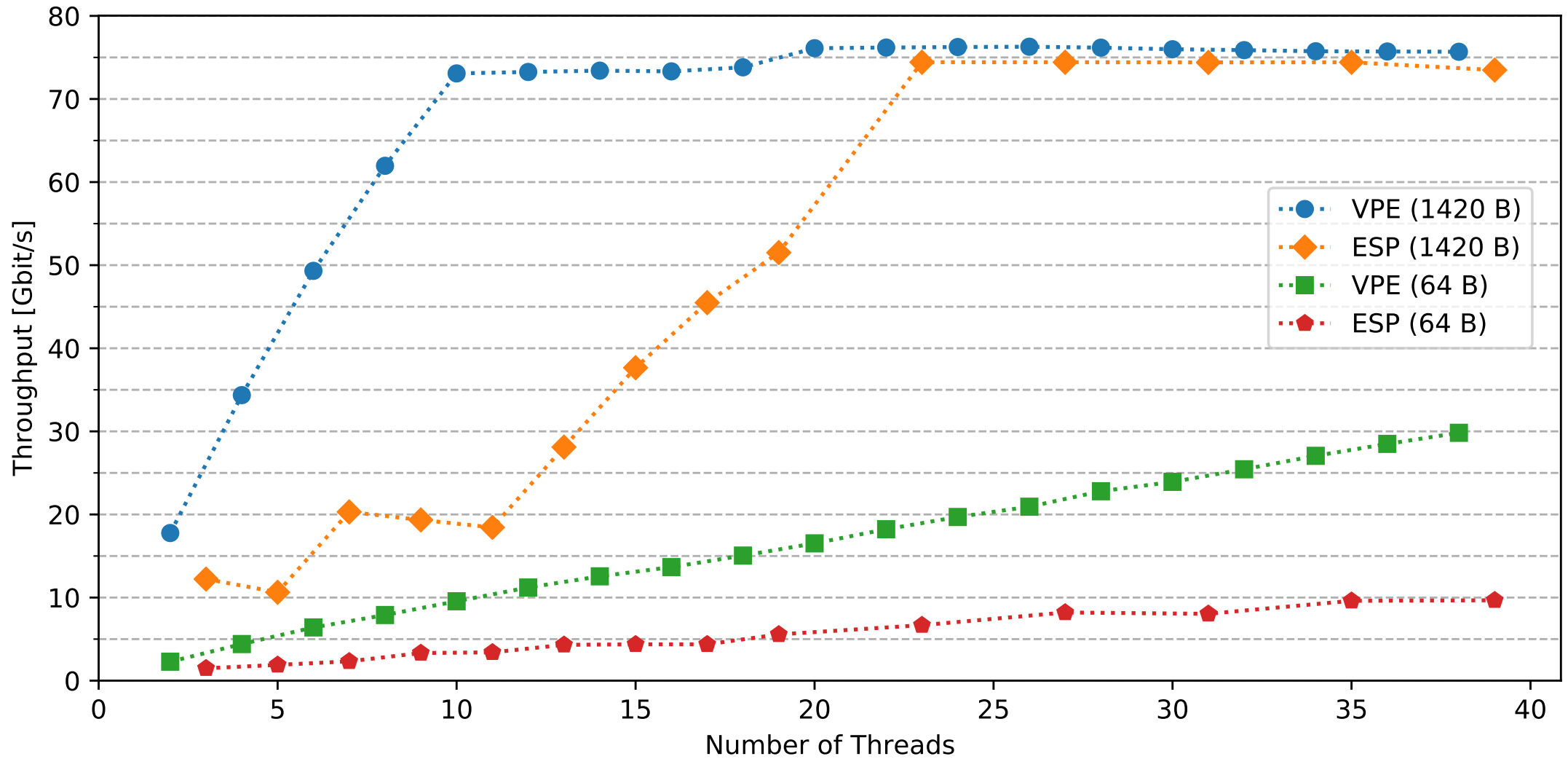
Resulting Packet Layout for Tunnel Mode

- Multiple replay windows per SA
 - Allows scaling over CPU cores,
 - Multicast replay protection &
 - Replay window per QoS class
- Full 64-bit sequence counter
- No trailer required
- Implicit padding if required
- No AAD required

Could be negotiated during IKE & coexist



Multi-Core Throughput



THANKS FOR LISTENING!

Contact:

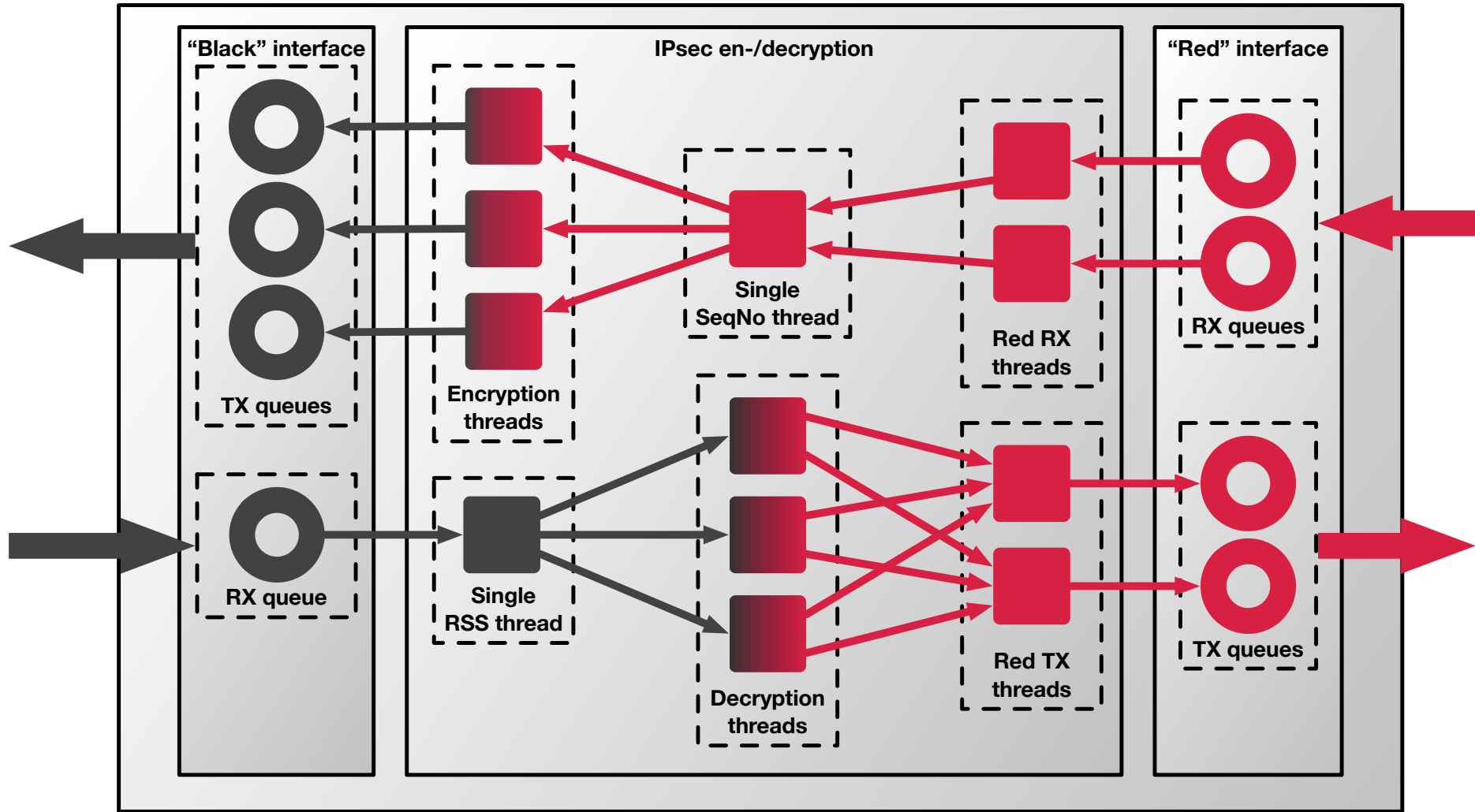
michael.rossberg@tu-ilmenau.de & michael.pfeiffer@tu-ilmenau.de

Further details:

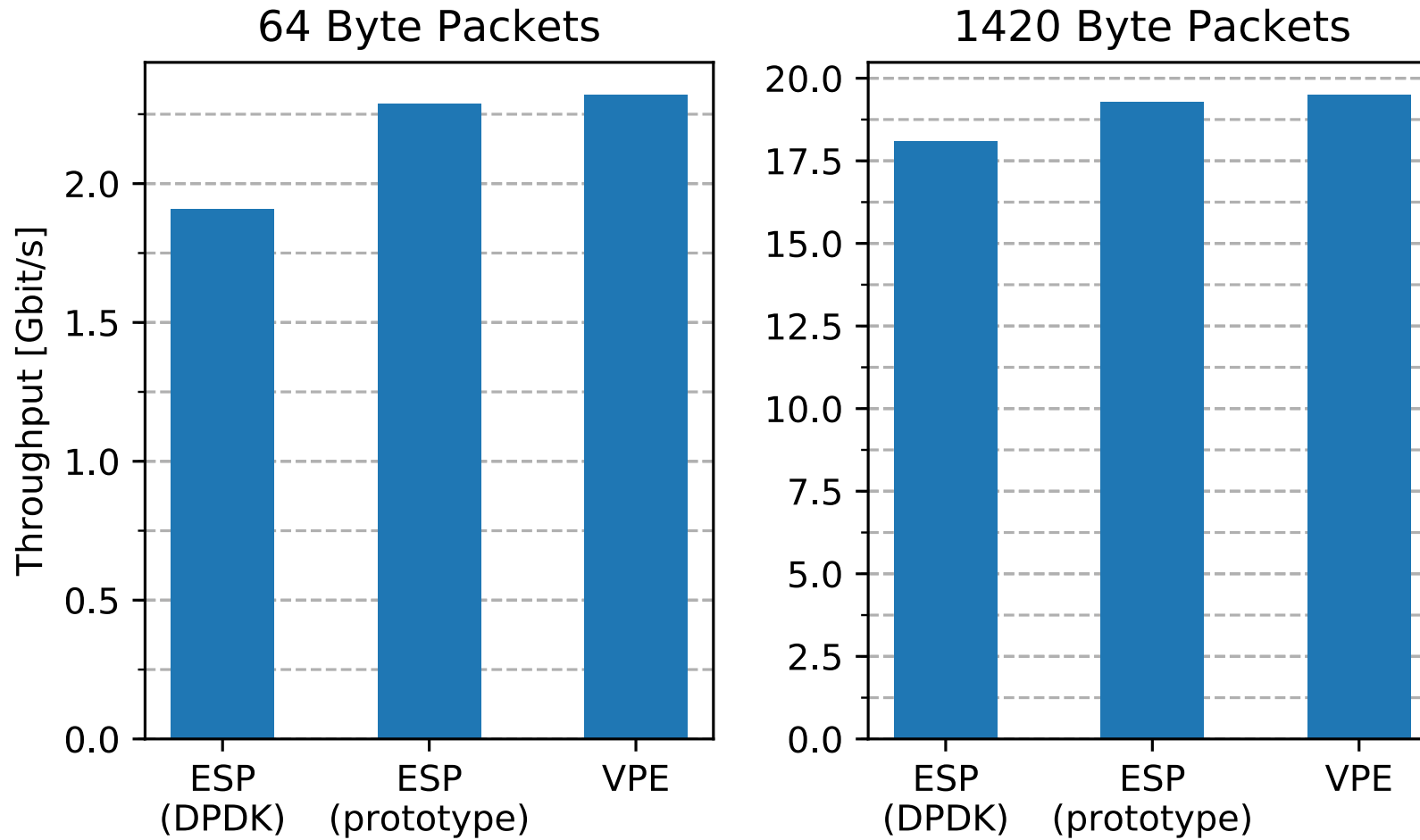
[1] <https://telematik.prakinf.tu-ilmenau.de/files/packetformat.pdf>

[2] <https://telematik.prakinf.tu-ilmenau.de/files/VPE.pdf>

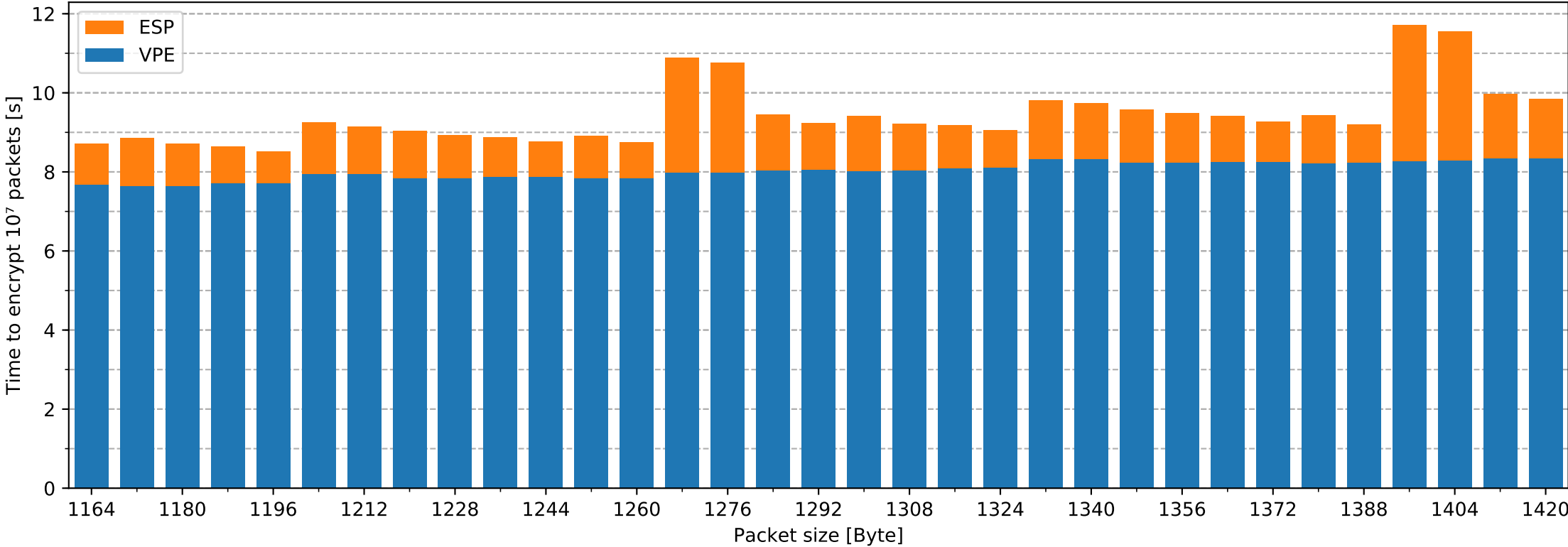
Parallel ESP processing: Threading model



Non-parallel "well-behaved" throughput



Processing Time vs. Packet Size



Processing Time vs. Additional Headroom

