

A Memory Unit for Priority Management in IPSec Accelerators

Luigi Dadda
ALaRI,
University of Lugano
DEI,
Politecnico di Milano,
dadda@alari.ch

Alberto Ferrante
ALaRI,
University of Lugano
ferrante@alari.ch

Marco Macchetti
C.E.C.,
Altran Group
mmacchetti@ceconsulting.it

Outline

IPSec and QoS

The Memory Architecture

Simulations

Conclusions and Future Work

- IPSec and QoS
- The Memory Architecture
- Simulations
- Conclusions and Future Work

IPSec

IPSec and QoS

IPSec

Quality of Service

The Memory Architecture

Simulations

Conclusions and Future Work

- ✓ Is a suite of protocols
 - ✗ adding security at IP (network) level;
- ✓ makes extensive use of cryptographic functions;
- ✓ requires at least 1 database query for each IP packet.

- ✓ Is a suite of protocols
 - ✗ adding security at IP (network) level;
- ✓ makes extensive use of cryptographic functions;
- ✓ requires at least 1 database query for each IP packet.

It is resource consuming.

Quality of Service

IPSec and QoS

IPSec

Quality of Service

The Memory
Architecture

Simulations

Conclusions and
Future Work

- ✓ Provide different levels of service to different fluxes of data;
- ✓ Managed in different ways:
 - ✗ FIFO on incoming packets;
 - ✗ Priority Queuing;
 - ✗ Custom Queuing;
 - ✗ Flow-based Weighted Fair Queuing.

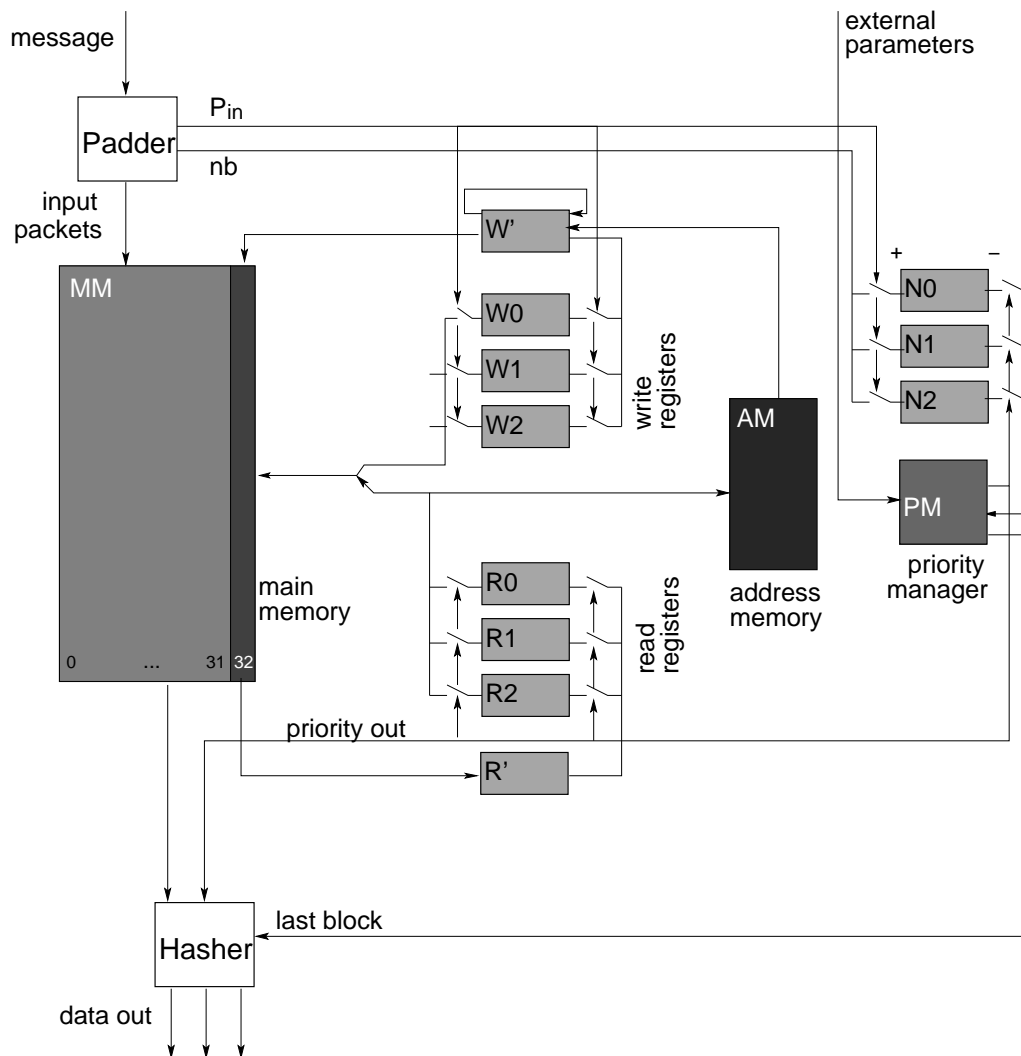
Architecture of the Memory

IPSec and QoS

The Memory Architecture
 Architecture of the Memory

Simulations

Conclusions and Future Work



MM: blocks of 16 32-bit words.

Description of the Simulations (1/2)

IPSec and QoS

The Memory
Architecture

Simulations

**Description of the
Simulations (1/2)**

Description of the
Simulations (2/2)

Simulation Results

Conclusions and
Future Work

- ✓ Functional evaluation of the architecture;
- ✓ SystemC model:
 - ✗ simulates the blocks of the architecture;
 - ✗ HMAC-SHA2 was only simulated;
 - ✗ rough estimation of performance figures.

Description of the Simulations (2/2)

IPSec and QoS

The Memory
Architecture

Simulations

Description of the
Simulations (1/2)

**Description of the
Simulations (2/2)**

Simulation Results

Conclusions and
Future Work

- ✓ Real and artificial traces as input; with both:
 - ✗ packets distributed in a cyclic way;
 - ✗ packets distributed depending on source IP address;
- ✓ discard policies:
 - ✗ unconditional discarding;
 - ✗ proportional discarding;
 - ✗ uniform discarding.

Simulation Results (1/2)

IPSec and QoS

The Memory Architecture

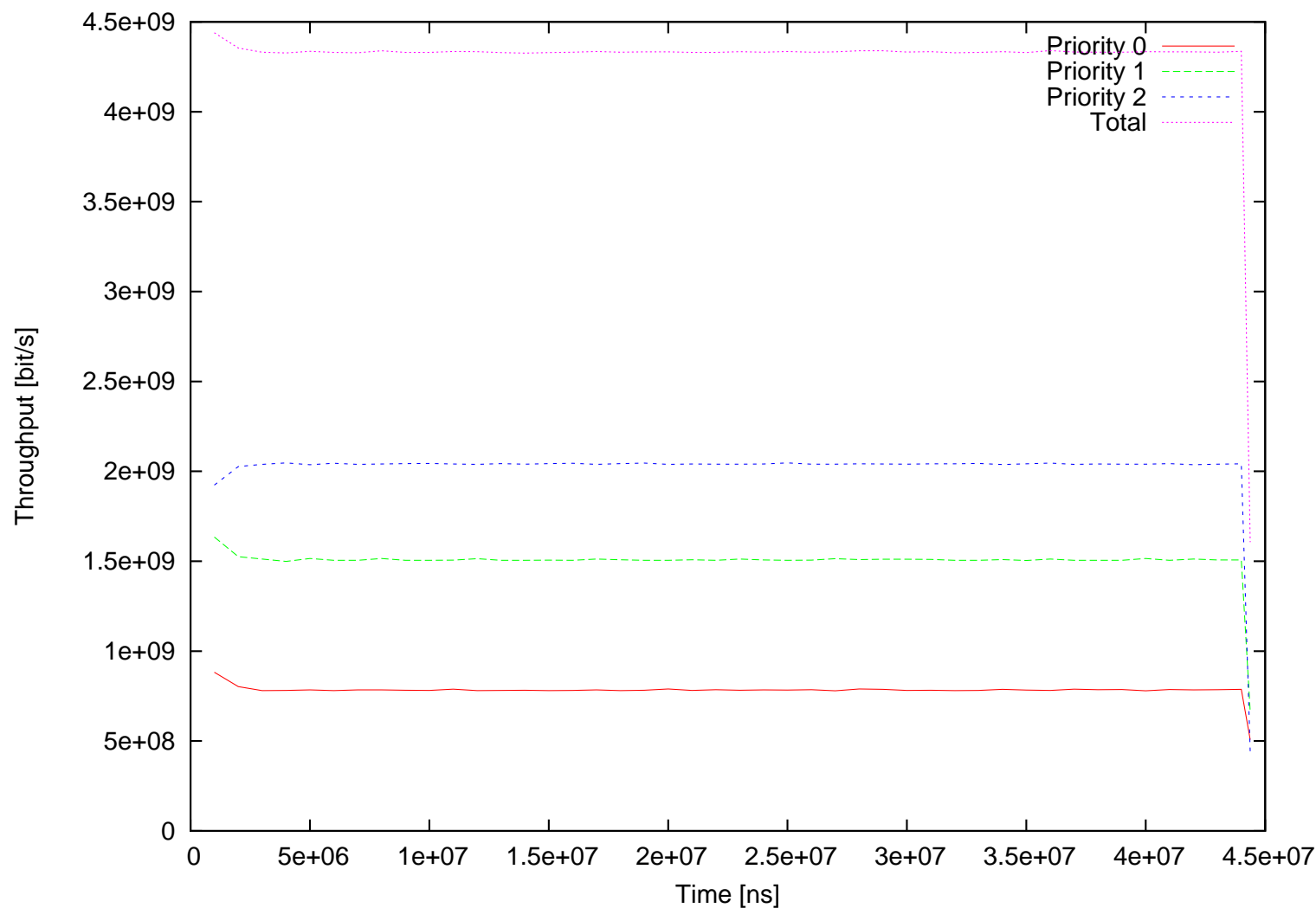
Simulations

Description of the Simulations (1/2)

Description of the Simulations (2/2)

Simulation Results

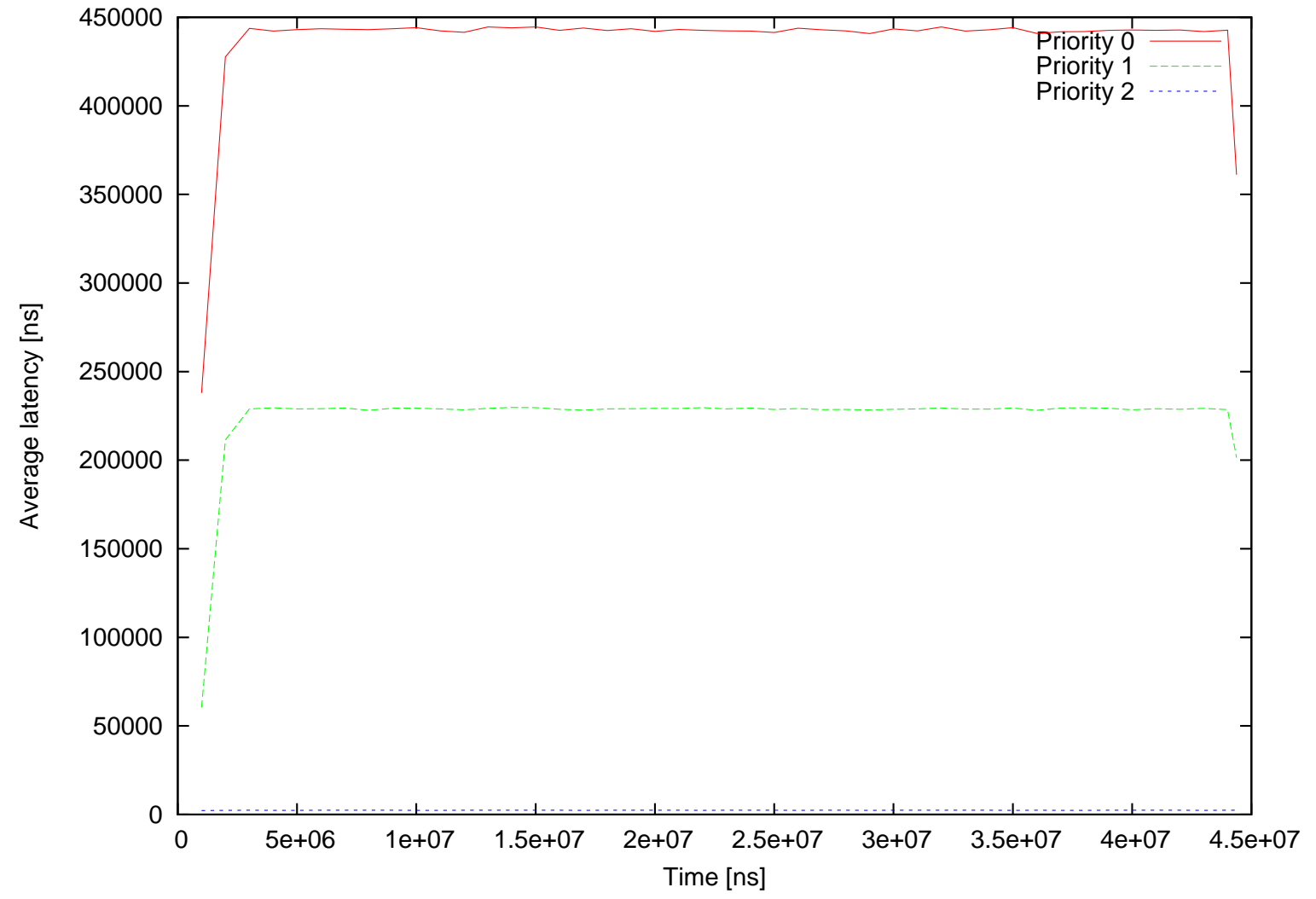
Conclusions and Future Work



Artificial trace; uniform discarding.

Simulation Results (2/2)

- IPSec and QoS
- The Memory Architecture
- Simulations
 - Description of the Simulations (1/2)
 - Description of the Simulations (2/2)
 - Simulation Results**
- Conclusions and Future Work



Artificial trace; uniform discarding.

Conclusions

IPSec and QoS

The Memory
Architecture

Simulations

Conclusions and
Future Work

Conclusions

Future Work

- ✓ We designed a memory architecture:
 - ✗ that supports QoS
 - without affecting performance;
 - ✗ needs a limited amount of additional hardware (7%);
- ✓ we performed functional simulations.

Future Work

IPSec and QoS

The Memory
Architecture

Simulations

Conclusions and
Future Work

Conclusions

Future Work

- ✓ Perform accurate simulations:
 - ✗ different cryptographic algorithms;
 - ✗ lower level simulations;
- ✓ derive performance figures for different QoS policies.