Tesi di Dottorato di Ricerca

A Design Methodology for HW/SW Security Protocols

Alberto Ferrante
XVIII Ciclo

Relatore: **Prof. Vincenzo Piuri**

Correlatori: **Prof. Luigi Dadda**
ALaRI, Università della Svizzera italiana, Lugano

Dr. Jeff Owen
ST Microelectronics, San Jose, CA, USA

Sommario

1. IPSec;
2. valutazione delle risorse per IPSec;
3. tecnologie presenti e trend;
4. obiettivi della tesi;
5. modellizzazione e testing di IPSec;
6. ottimizzazione dei sistemi esistenti;
7. system on chip per IPSec;
8. conclusioni.

IPSec

IPSec

- È una suite di protocolli:
  - permette di aggiungere meccanismi di sicurezza a livello di IP;
- fa un uso pesante di funzioni crittografiche:
  - consuma molte risorse computazionali.

Importanza di IPSec

- È incluso come meccanismo per la sicurezza in IPv6;
- è il protocollo più utilizzato per la creazione di VPN.

AH e ESP

- È composto da 2 protocolli:
  - Authentication Header (AH);
  - Encapsulating Security Payload (ESP);
- entrambi i protocolli possono essere utilizzati in:
  - transport mode;
  - tunnel mode.

Database

- Vengono utilizzati 2 database:
  - il Security Policy Database (SPD);
  - il Security Association Database (SAD);
    - i record sono detti Security Association (SA).

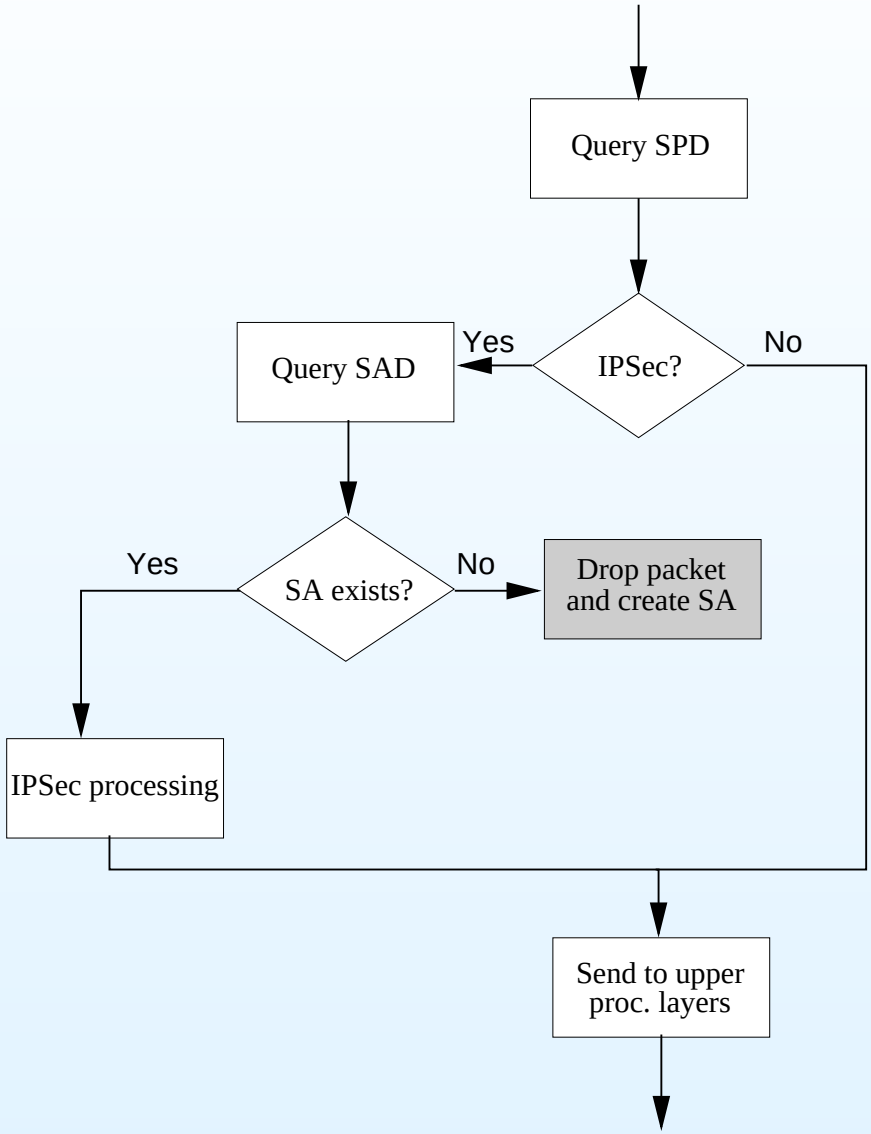
Security Association

- Ogni SA contiene:
  - impostazioni dei protocolli e degli algoritmi;
  - chiavi per gli algoritmi crittografici;
- le SA sono monodirezionali:
  - è necessario crearne 2 per le normali comunicazioni bidirezionali;
- le SA possono essere identificate con dei “canali sicuri”.

Internet Key Exchange (IKE)

- È stato pensato per l'utilizzo con IPSec allo scopo di:
  - negoziare i parametri di protocolli ed algoritmi;
  - scambiare le chiavi;
- crea le SA.

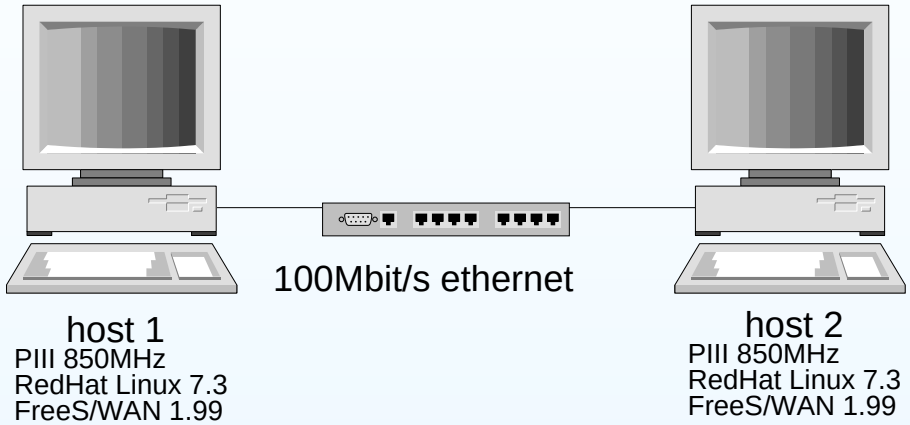
Processing di pacchetti IPSec



Valutazione delle risorse richieste da IPSec

Rete di test

- È stata installata una rete di test [1]:

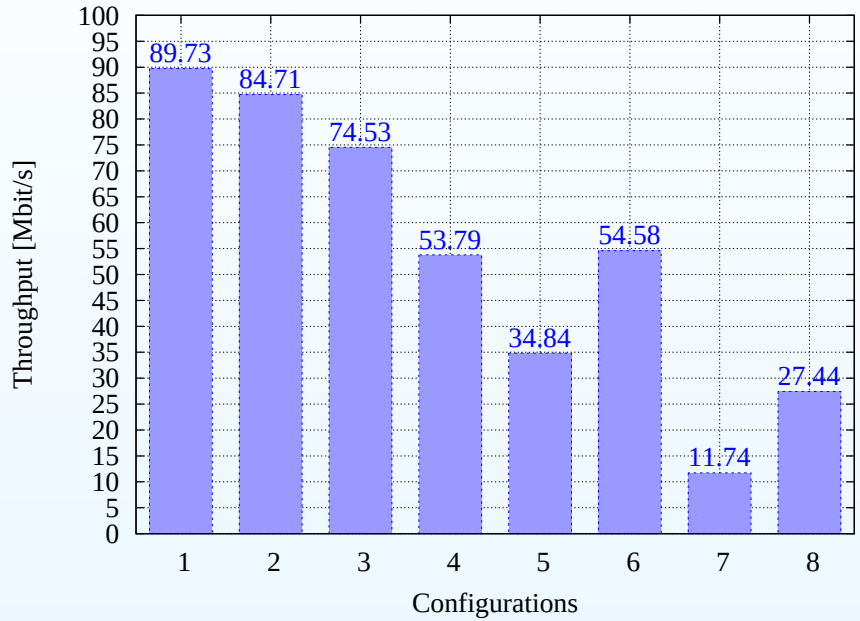


- ha permesso di misurare:
  - il throughput medio ed il traffico di rete istantaneo;
  - l'occupazione media ed istantanea della CPU;
  - l'effort.

[1] Alberto Ferrante, Vincenzo Piuri, and Jeff Owen, "IPSec Hardware Resource Requirements Evaluation," in *NGI 2005*. Rome, Italy: EuroNGI, 18 Apr. 2005

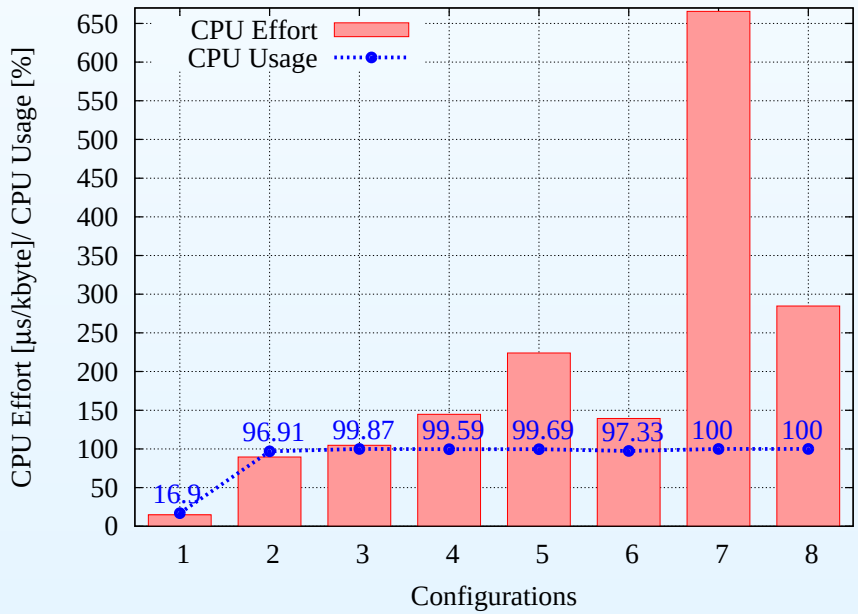
Risultati ottenuti

Throughput



1. No IPSec
2. ESP (NULL, HMAC-SHA-1)
3. ESP (AES 128)
4. ESP (AES 128, HMAC-SHA-1)
5. ESP (AES 128, HMAC-SHA-2 256)
6. ESP (AES 128), AH (HMAC-SHA-1)
7. ESP + IPComp utile
8. ESP + IPComp non utile

Effort ed uso della CPU



Tecnologie presenti e trend

Tecnologie presenti

- Vengono principalmente utilizzati acceleratori off-line:
  - non sono sul percorso principale seguito dai pacchetti:
    - i pacchetti vengono mandati all'acceleratore e rispediti indietro una volta processati;
  - accelerano solo parti di IPSec.

Trend

- Processori on-line *(flow-through)*:
  - processing trasparente dei pacchetti IPSec;
  - i pacchetti transitano solo una volta dall'acceleratore:
    - minor richiesta di banda nella comunicazione con il processore centrale;
  - devono implementare tutto IPSec;
  - esiste un'implementazione con throughput non molto elevato e senza supporto per la quality of service.

Obiettivi della tesi

Obiettivi

- Studiare
  come implementare in modo efficiente IPSec;
- passi seguiti:
  - sviluppo di un modello formale
    (non presente in letteratura);
  - sviluppo di ottimizzazioni innovative
    per le implementazioni attuali;
  - sviluppo dell'architettura ad alto livello
    di un SoC innovativo.

Modellizzazione e testing di IPSec

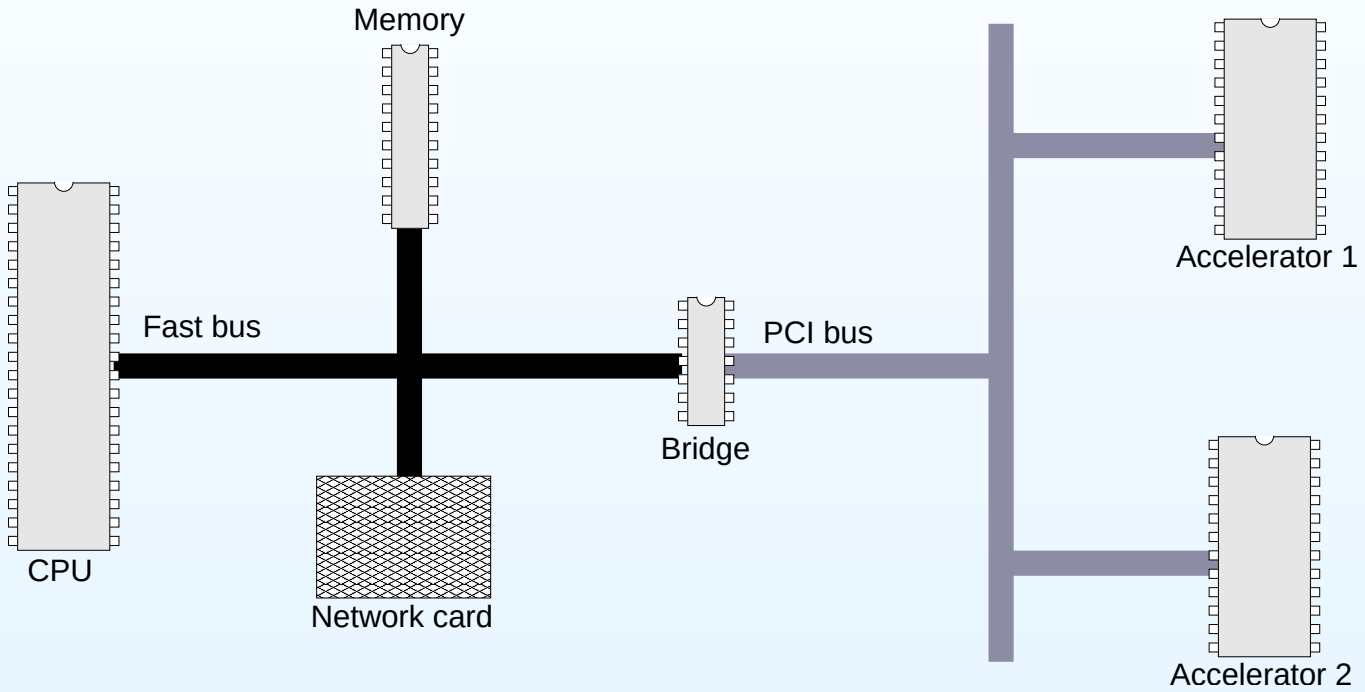
Modello di IPSec

- Modello UML che descrive:
  - la struttura generale (class diagram);
  - il funzionamento delle varie parti ed il modo in cui interagiscono (statecharts);
- fondamentale durante il design;
- può essere usato per il testing funzionale delle implementazioni [2]:
  - permette di generare test pattern tramite un criterio di copertura (*transition coverage*).

[2] Alberto Ferrante, Uljiana Boiko, Antonietta Lo Duca, and Vincenzo Piuri, “A Testing Methodology for IPSec-based Systems,” in *SoftCOM 2004*. Dubrovnik and Split, Croatia, Venice, Italy: University of Split, Oct. 2004, pp. 22–26, sponsored by the IEEE Communication Society and by the UNESCO Communication and Information Society

Ottimizzazione dei sistemi esistenti

Architettura di riferimento



Tutti i trasferimenti di dati avvengono in DMA.

Ottimizzazioni proposte (1/3)

- Algoritmi di scheduling
  per sistemi basati
  su acceleratori crittografici multipli:
  - scheduling di pacchetti
    tra diversi acceleratori e la CPU.

Ottimizzazioni proposte (2/3)

- Algoritmo base [3]:
  - pacchetto allocato al processore sul quale si registra il minor *finishing time*;
  - proposta di miglioramenti architetturali (prefetching e write buffer).

[3] Fabien Castanier, Alberto Ferrante, and Vincenzo Piuri, “A Packet Scheduling Algorithm for IPSec Multi-Accelerator Based Systems,” in *ASAP 2004*. Galveston, TX, USA: IEEE Computer Society Press, Sept. 2004, pp. 387–397

Ottimizzazioni proposte (3/3)

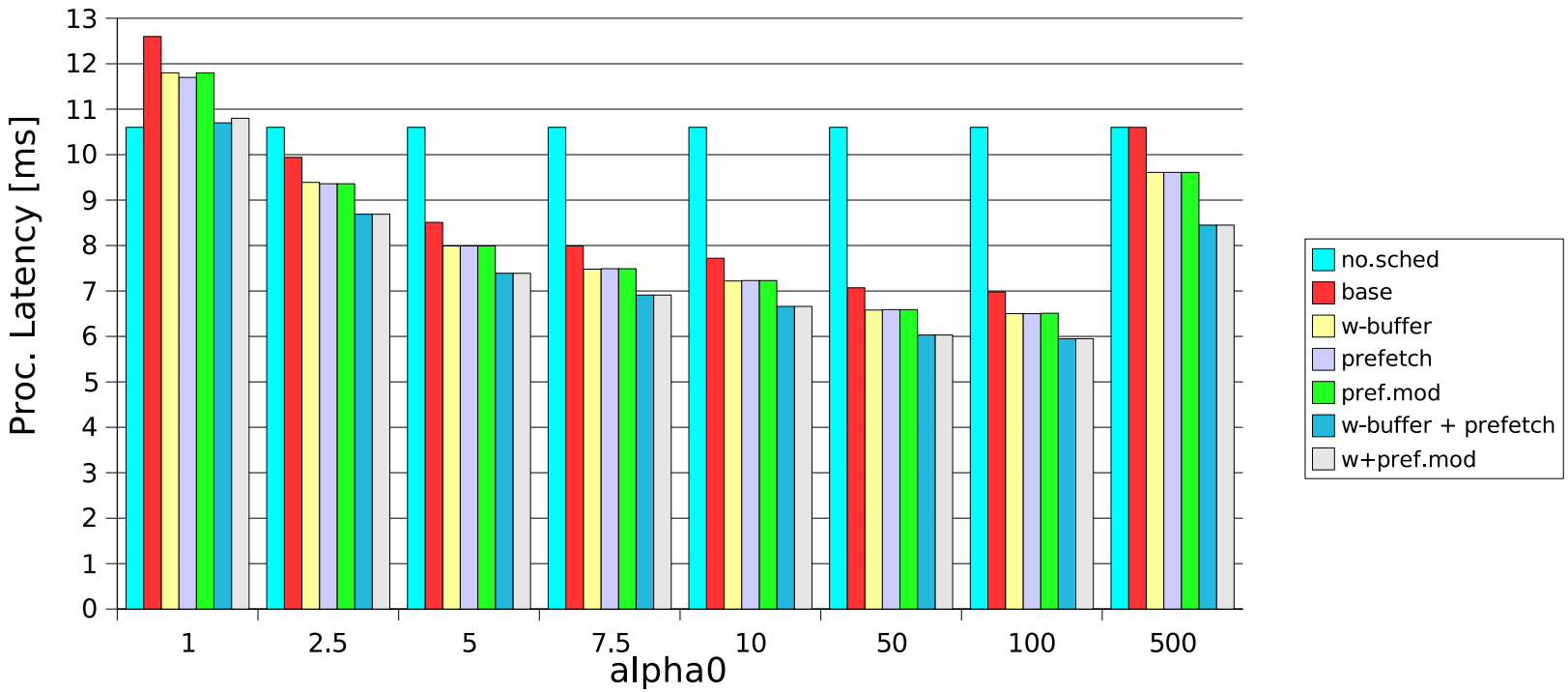
- Modifiche all'algoritmo base:
  - algoritmo per "pacchetti piccoli" [4]:
    - metodo di raggruppamento dei pacchetti piccoli per ridurre l'influenza degli overhead di trasferimento;
  - algoritmo con supporto per la QoS [5]:
    - supporto della soft QoS tramite code a priorità.

[4] Antonio Vincenzo Taddeo, Alberto Ferrante, and Vincenzo Piuri, "Scheduling Small Packets in IPSec-based Systems," in *CCNC 2006*. Las Vegas, NV, USA: IEEE, 8 Jan. 2006

[5] Alberto Ferrante, Vincenzo Piuri, and Fabien Castanier, "A QoS-enabled Packet Scheduling Algorithm for IPSec Multi-accelerator Based Systems." in *Computing Frontiers*. Ischia, Italy: ACM, May 2005, pp. 221–229

Risultati

Latenza media



Algoritmo base

Banda richiesta 1Gbit/s

System on chip per IPSec

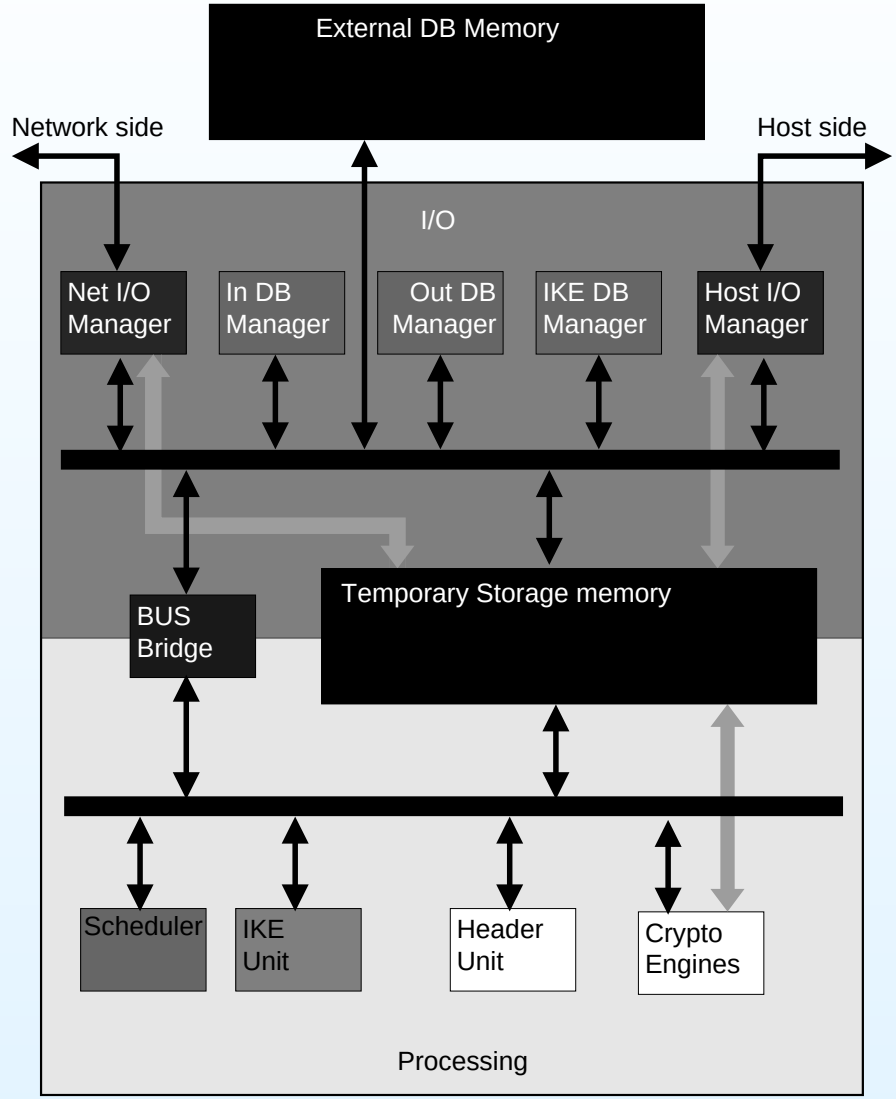
Descrizione

- Sviluppo dell'architettura ad alto livello:
  - architettura pass through [6];
  - possibilità di supporto della QoS [7];
- specifica del comportamento
  - dei blocchi funzionali (Class diagram e Statecharts);
  - delle loro interazioni (Statecharts).
- architettura di alcuni blocchi.

[6] Sottomesso a conferenza internazionale
[7] Pubblicazione in preparazione

Architettura

- Bus dedicati per i dati;
- comunicazione shared memory:
  - minor spostamento di dati;
- bus condiviso per il controllo.



Blocchi funzionali

- Studio delle dimensioni ottimali della memoria;
- metodi di query veloci dei database (caching + multithreading) [8];
- modello SystemC di IKE per il partizionamento HW/SW.

[8] Sottomesso a conferenza internazionale

Conclusioni

Conclusioni

- Tramite una rete di test
  si sono compresi i requisiti di IPSec;
- è stato realizzato
  un modello UML di IPSec;
- partendo dallo studio dei sistemi attuali
  è stato possibile:
  - ottimizzarli;
  - comprenderne le limitazioni;
- proposta di un'architettura efficiente.

Lavoro futuro

- Testing degli algoritmi di scheduling in un'implementazione reale;
- simulazione dell'architettura del SoC.

Grazie

per

l’attenzione...

... Domande?