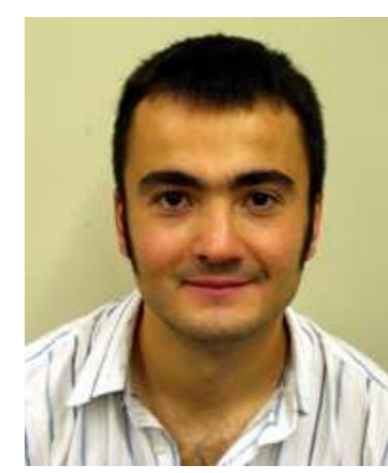


# NS<sup>3</sup>: Networked Secure Searchable Storage with Privacy and Correctness

Radu Sion, Erez Zadok, <http://crypto.cs.stonybrook.edu>



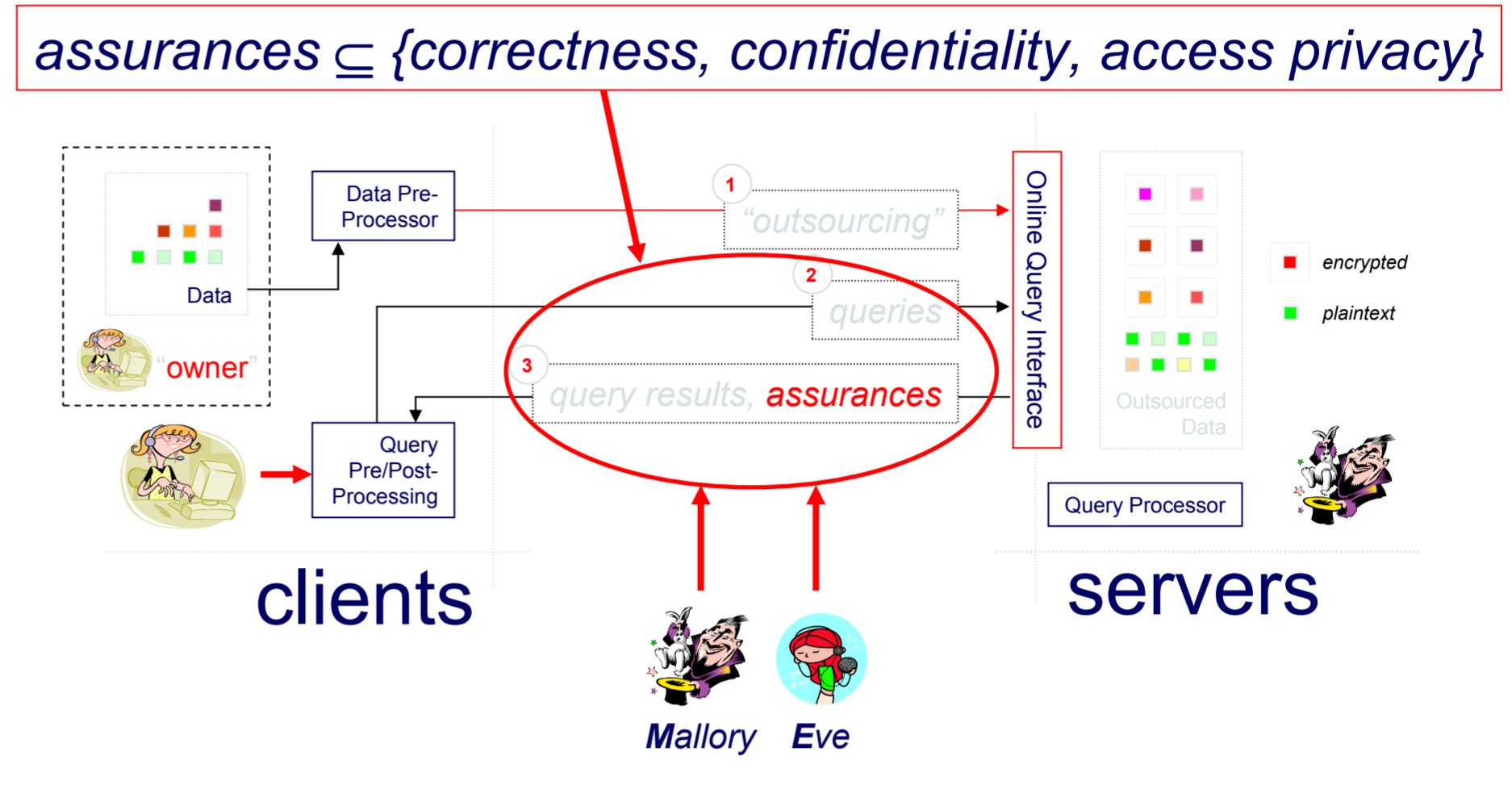
# NSAC

Network Security and Applied Cryptography Lab

## Overview

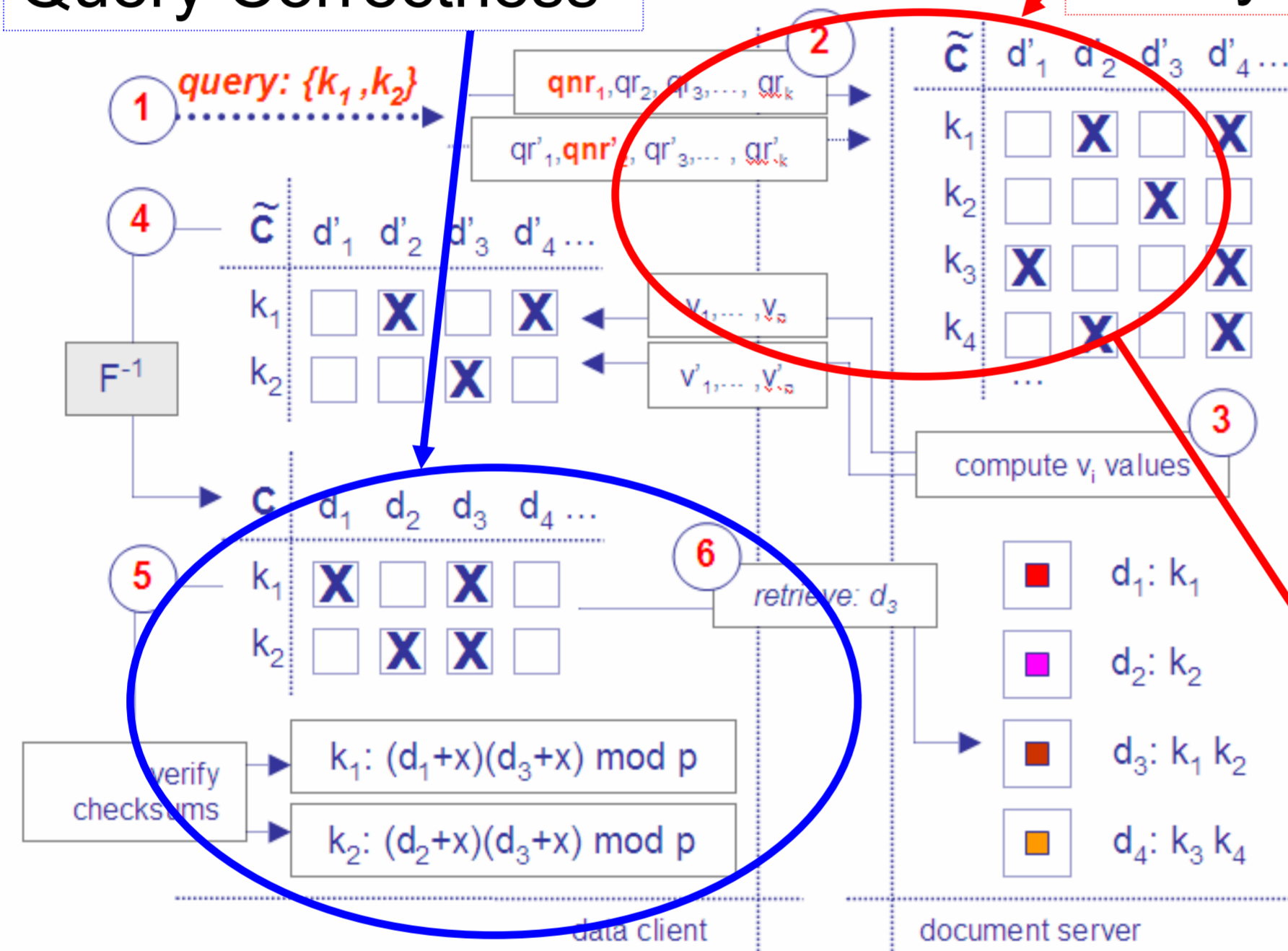
We are building robust, efficient, and scalable networked data storage offering three strong security assurances: (1) **data confidentiality**, (2) **search pattern privacy**, and (3) **query correctness**.

The total cost of ownership of storage is 5-10 times greater than the hardware costs, and more information is produced and lives digitally every day. In the coming years, secure, robust, and efficient storage management will be demanded by users, to detect and deter malicious attacks or faulty behavior.

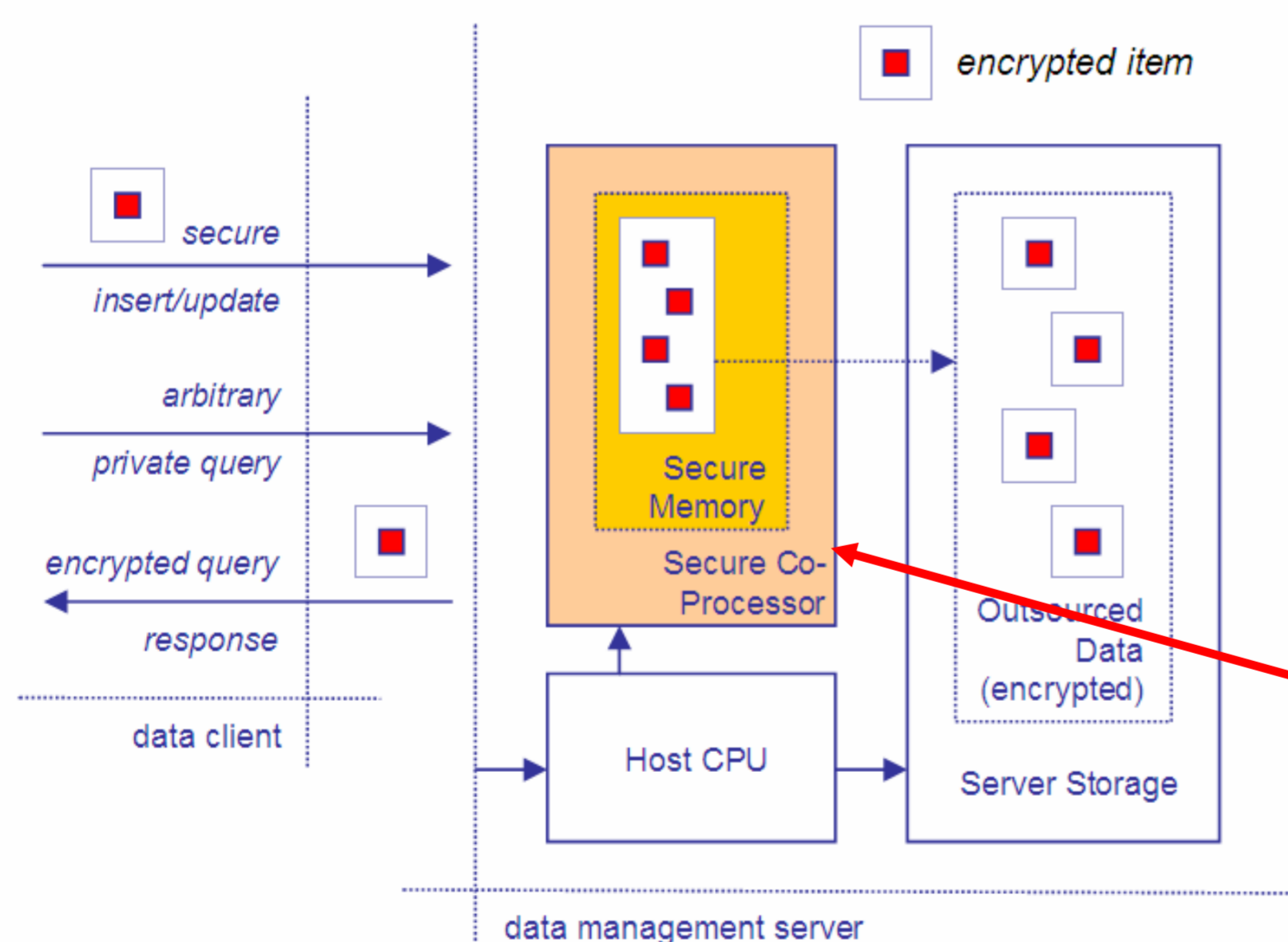


### Query Correctness

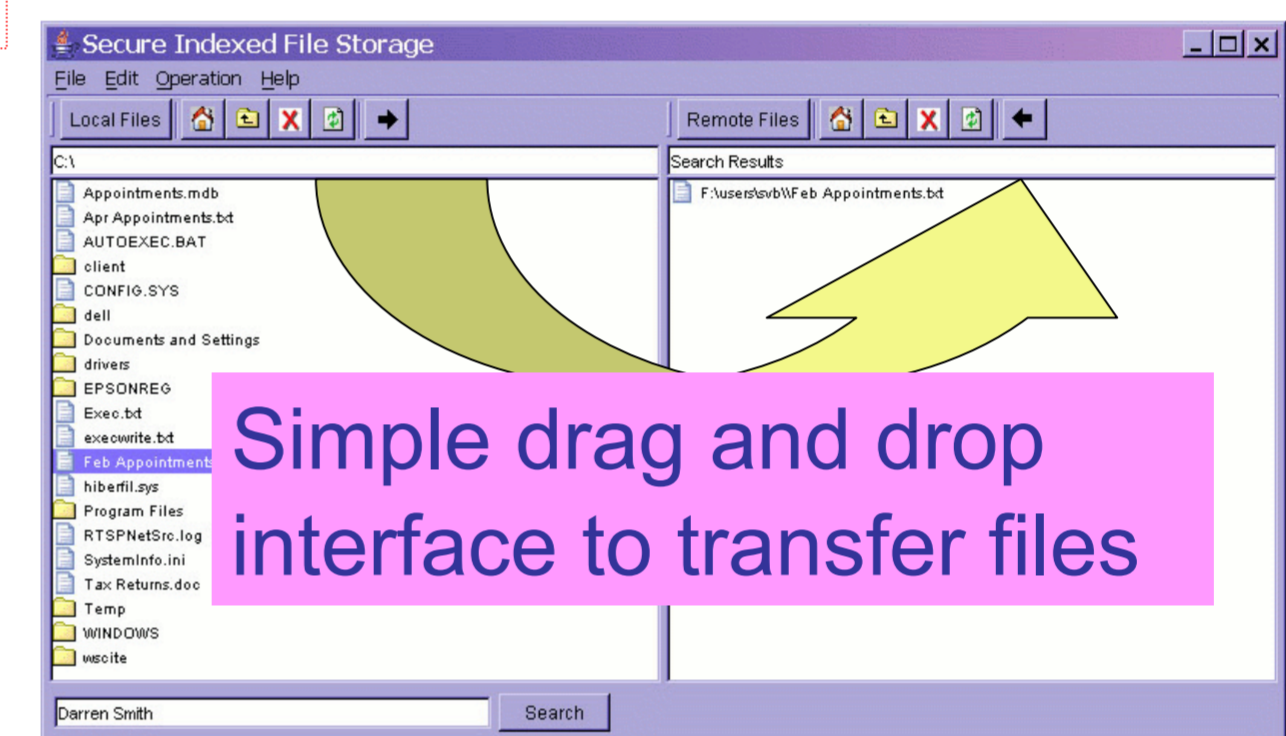
### Query Obliviousness



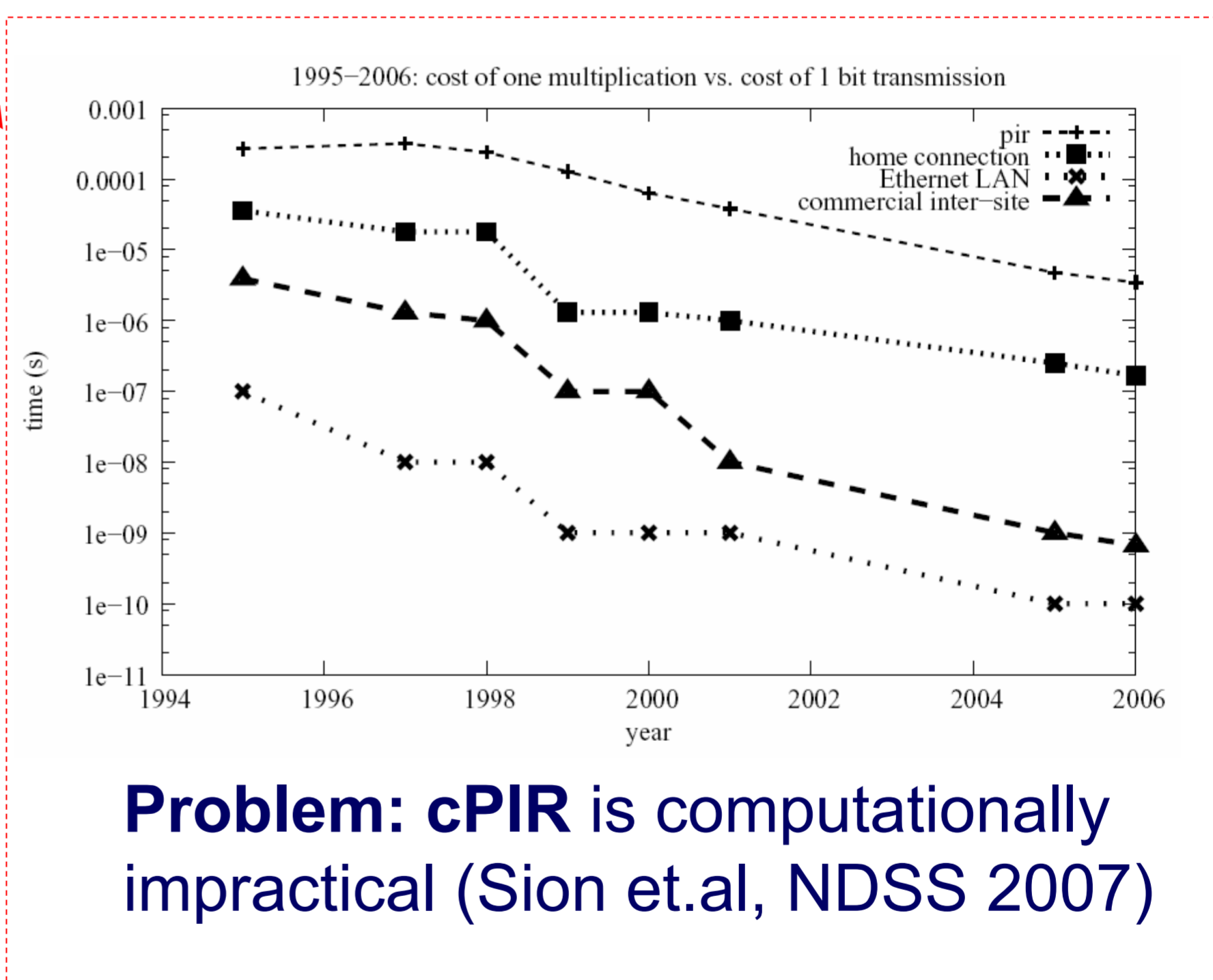
### Protocol Overview



### Deploying Trusted Hardware



### Prototype Client



**Problem: cPIR is computationally impractical (Sion et.al, NDSS 2007)**

RSA1024 Sign: **848/sec**  
 RSA1024 Verify: **1157/sec**  
 3DES: **1-8MB/sec**  
 DES: **1-8MB/sec**  
 SHA1: **1-21MB/sec**

IBM 4764-001: 266MHz PowerPC. 64KB battery-backed SRAM storage. Crypto hardware engines: AES256, DES, TDES, DSS, SHA-1, MD5, RSA. FIPS 140-2 Level 4 certified.

**Challenge: SCPU is very slow for general purpose logic.**