

# cDB: Strong Regulatory Compliant Databases



# NSAC

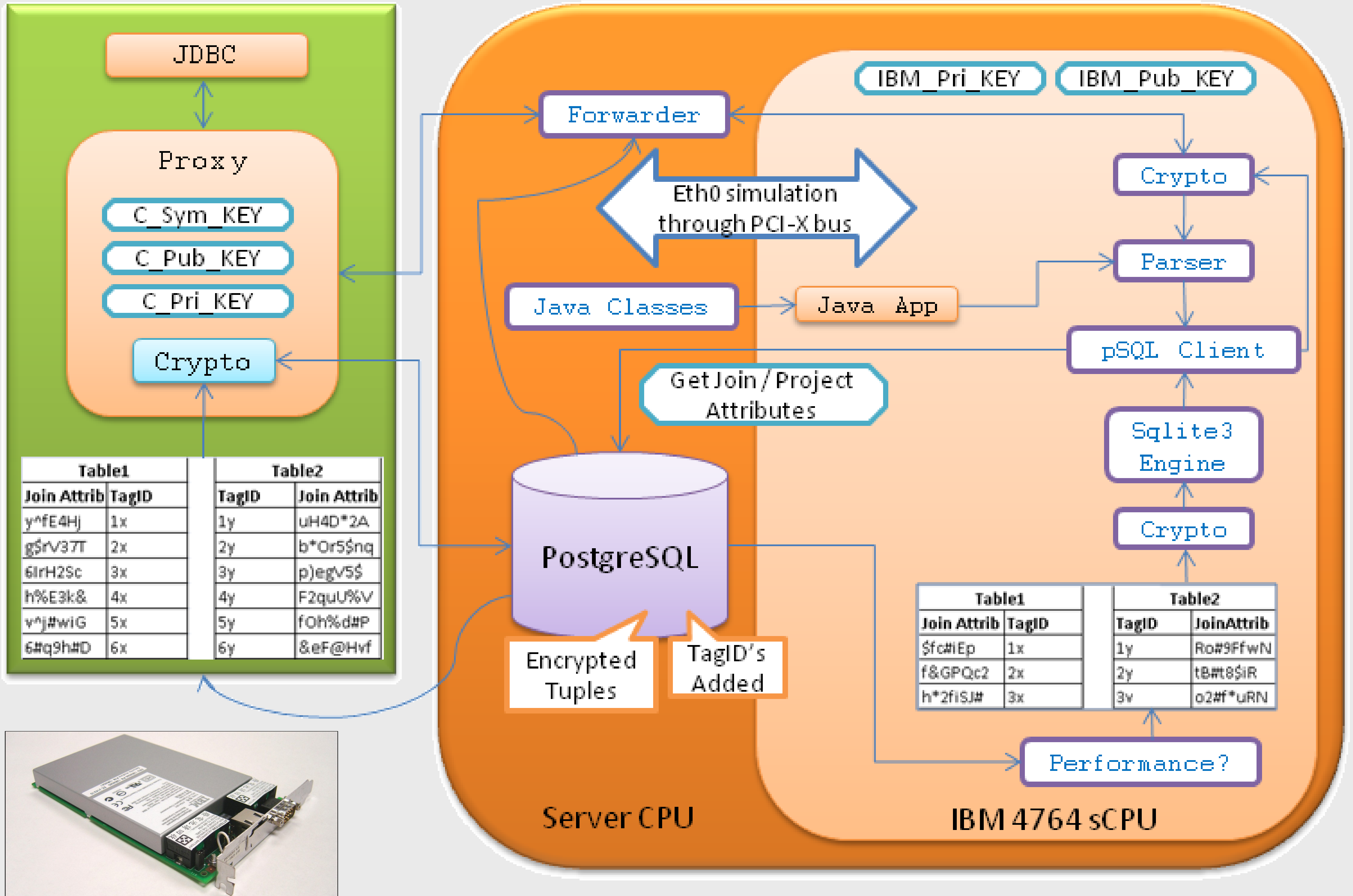
NSF IIS 0803197  
CRI CNS 0708025

Rajarshi Agnihotri, Ashish Anand, Radu Sion  
{rajarsi, aanand, sion}@cs.stonybrook.edu  
www.crypto.cs.stonybrook.edu

Network Security and Applied Cryptography Lab

## Problem: Untrusted Service Providers

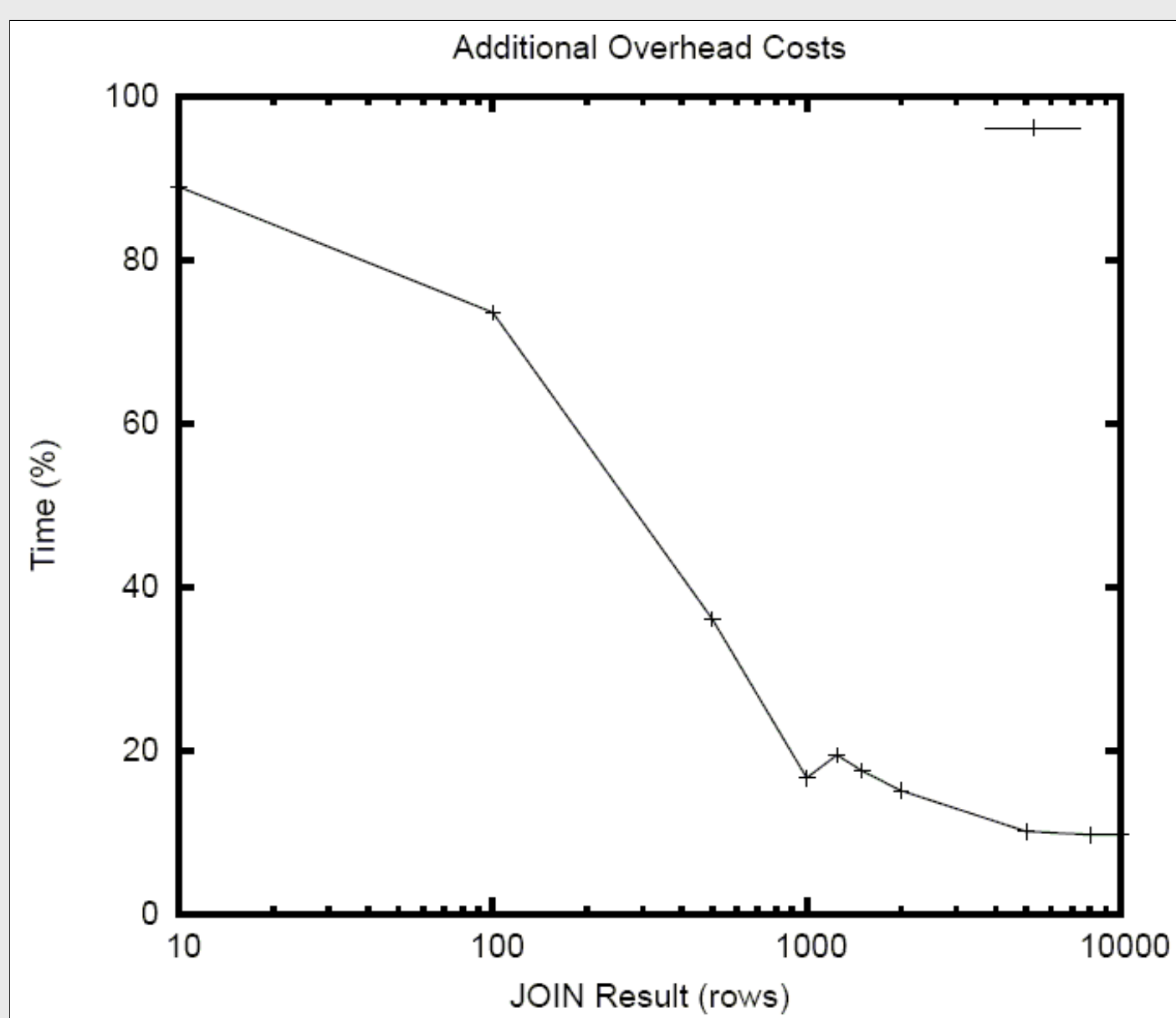
Server-side processing of encrypted databases assume hosting server is trusted  
Server may tamper with replies & database itself



IBM 4764 Secure Coprocessor

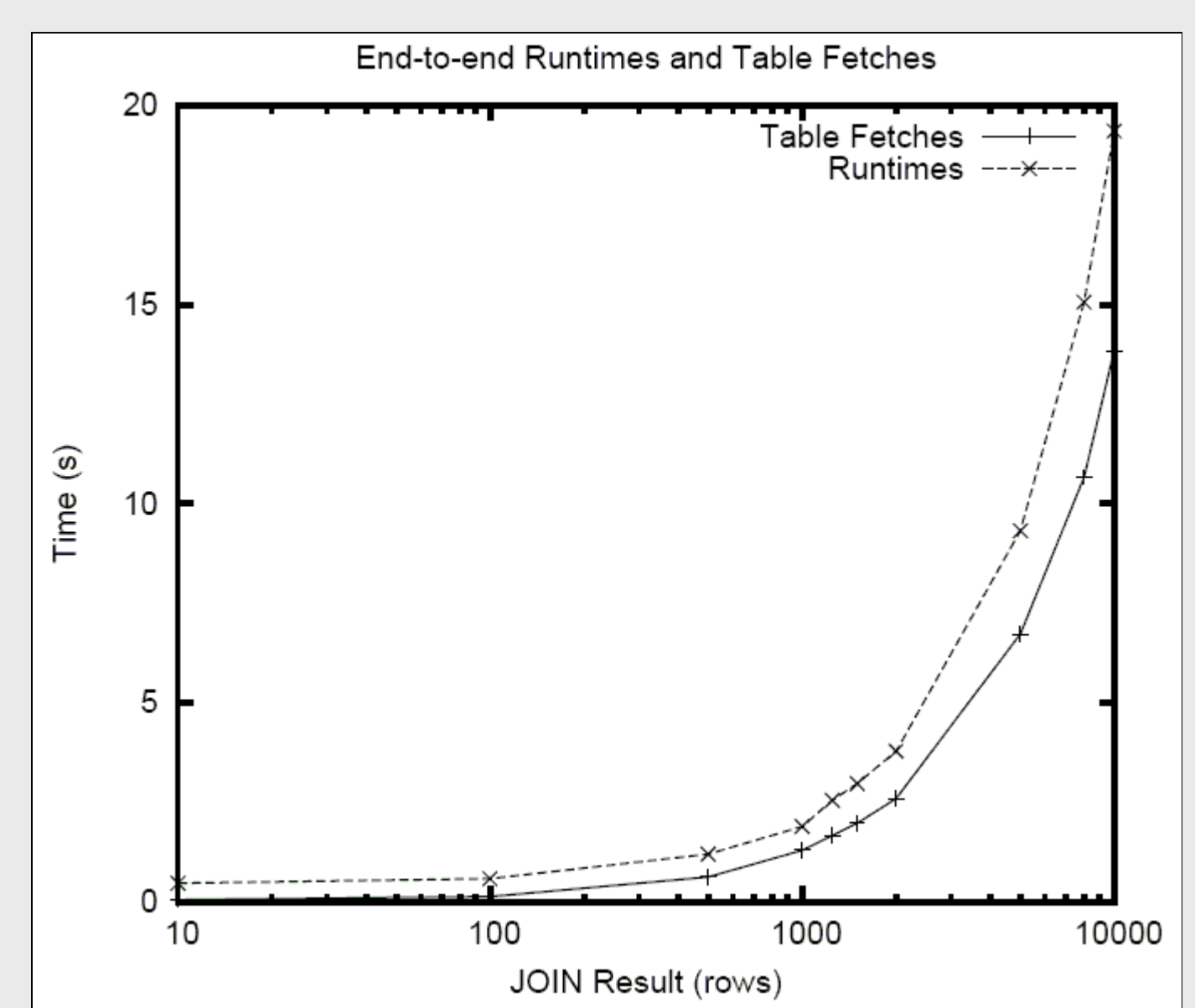
## Idea: Deploy Secure Hardware Efficiently (ICDCS '08)

The untrusted service provider is handled by deploying appropriate tamper-reactive hardware defenses. This is hard because secure hardware is significantly computation and storage constrained (by orders of magnitude)



Sqlite3 JOIN Times Inside sCPU

Rows	Time
10	0.005126
100	0.026445
500	0.142979
1000	0.285114
1250	0.390459
1500	0.477823
2000	0.617778
5000	1.651994
8000	2.947101
10000	3.647962



### Performance Optimizations

Overheads include encryption/decryption costs, I/O costs, network or card-host bus transfer costs

### Performance Bottlenecks

Fetching join attributes + TagIDs and performing JOINS inside sCPU