

# Functional Encryption

Amit Sahai, <http://www.cs.ucla.edu/~sahai>

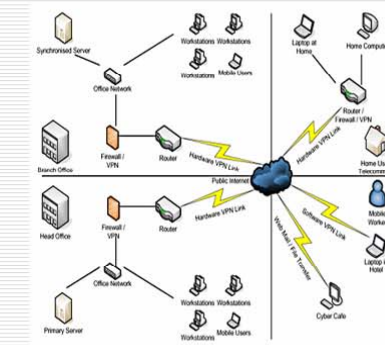
NSF Award CNS - 0627781



## Functional Encryption: Beyond Public Key Cryptography

A line of work initiated by  
Amit Sahai and Brent Waters  
[Sahai-Waters 2005]

The problem: How to Protect and Use Private Data



Ubiquitous:

- Enterprise
- Payment Card Industry (PCI)
- Web Services
- Health Care



## Security Breaches

Intrusion:

- 45 Million Cards Stolen (Dec. 2006)



Hard Drive Loss:

- 25 million U.K. citizens (Nov. 2007)



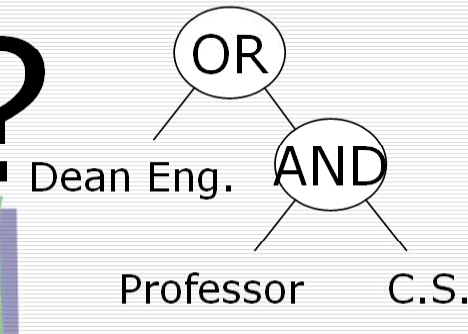
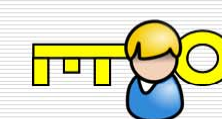
Perimeter Circumvention:

- Credit Union - USB tokens (June 2006)



## Realistic Data Sharing

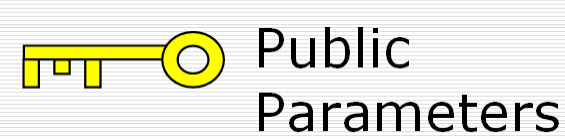
Problem: Disconnect between policy and mechanism



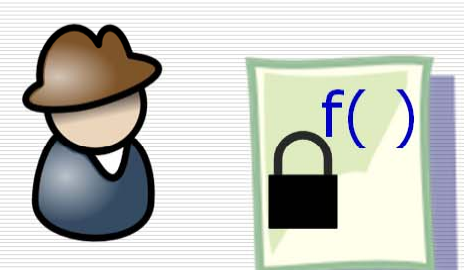
- Burden on provider
- Several Users
- Late Joins



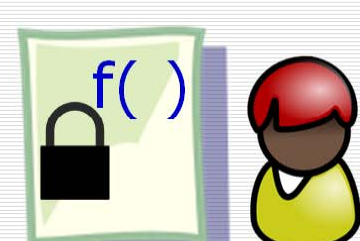
## Functional Encryption: A New Perspective



Access Predicate chosen at encrypt:  $f()$

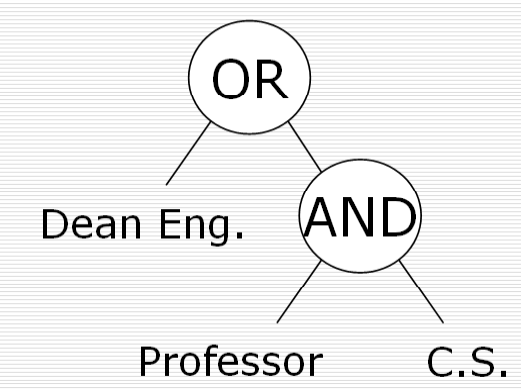


Learn output of  $f(X)$  (or decrypt 'payload' if  $f(X)=1$ )



## Collusion Attacks: The Key Threat

Need: Key "Personalization"



Tension: Functionality vs. Personalization



## Elliptic Curve Techniques

$G$  : multiplicative of prime order  $p$ . (Analogy:  $Z_q^*$ )

Intuitive Hardness Discrete Log:

Given:  $g, g^a$  Hard to get:  $a$

Bilinear map  $e: G \times G \rightarrow G_T$

$$e(g^a, g^b) = e(g, g)^{ab} \quad \forall a, b \in Z_p, g \in G$$

High Level: Single Multiplication

Key for satisfying functionality + personalization

## Beyond Access Control

Complex Predicates over data [KSW08] :

Idea: Inner Product Functionality (Multiplication of Bilinear Map)

$$SK: \vec{a} = \langle a_1, \dots, a_n \rangle$$

$$CT: \vec{b} = \langle b_1, \dots, b_n \rangle$$

Predicate:  $\vec{a} \cdot \vec{b} = 0?$

Functionality: Disjunctions, Conjunctions, Polynomial Equations

Papers by PI on functional encryption:  
[SW05, GPSW06, BSW07, OSW07, KSW08]