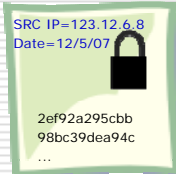


Why Functional Encryption?

Late Binding Access Control:

e.g. Network Logs



Src: 123.3.4.77 AND
Date: 12/5/07

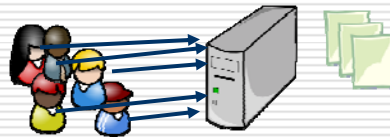


- Encrypt packet payload, tag with metadata
- Distribute capabilities later

Why Functional Encryption?

Scalability and Robustness:

Availability vs. Security



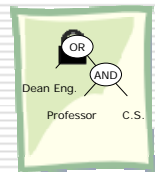
Personal Storage Devices



Why Functional Encryption?

Efficiency:

Scales with policy complexity



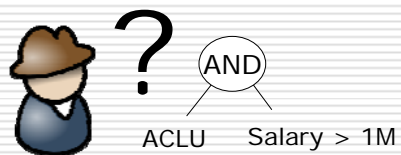
VS.



13

Why Functional Encryption?

Receiver Privacy:



14

A New Vision for Encryption Systems

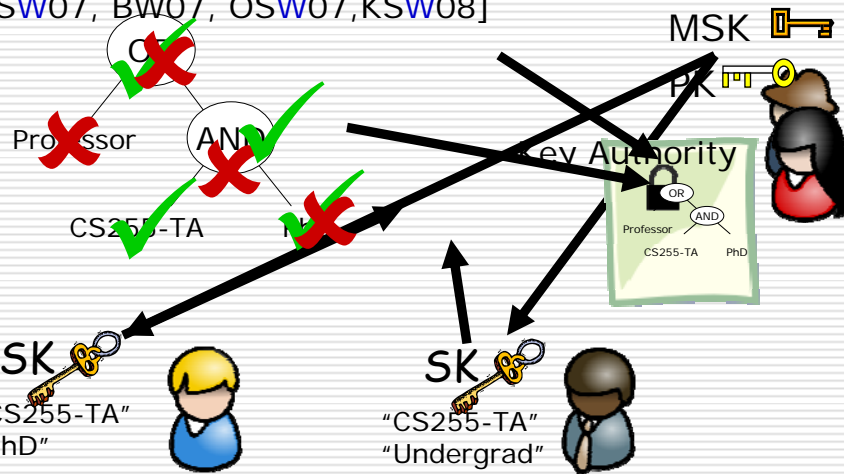
- Retrospect: Public vs. Secret Key Cryptography
- Secure Internet Connections (Public Key Exchange)
- Online Software Updates (Digital Signatures)

- The next step forward

15

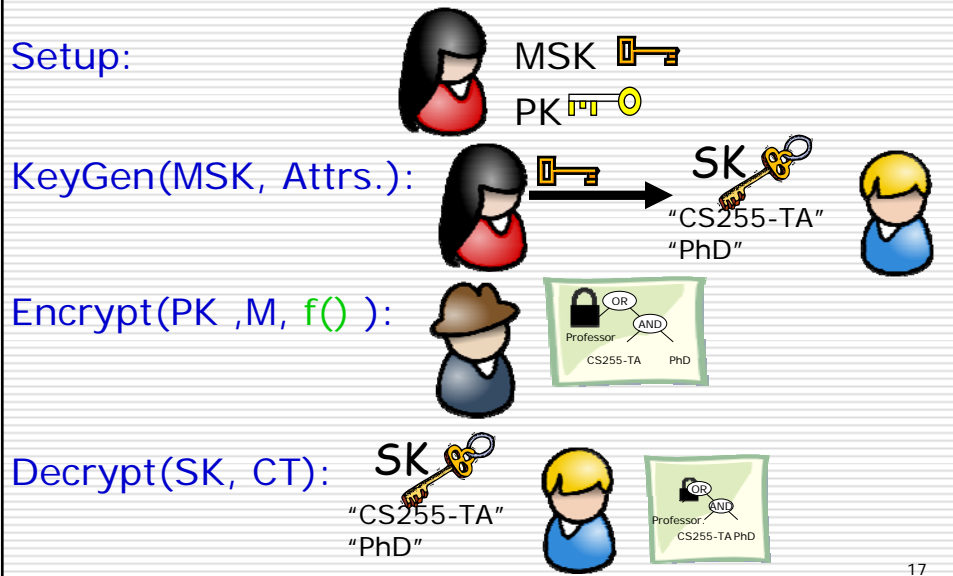
Functional Encryption for Formulas [SW05]

Line of Research: [SW05, GPSW06, PTMW06, BSW07, BW07, OSW07, KSW08]



16

Functional Encryption for Formulas

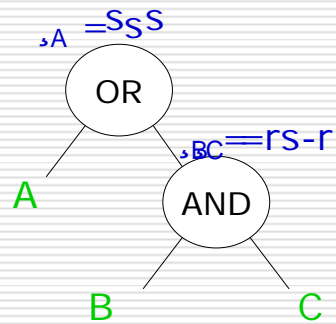


A First Approach

Question: Can we build functional encryption from standard techniques?

Attempt: Public Key Encryption + Secret Sharing

Secret Sharing [S78,B78,BL86]



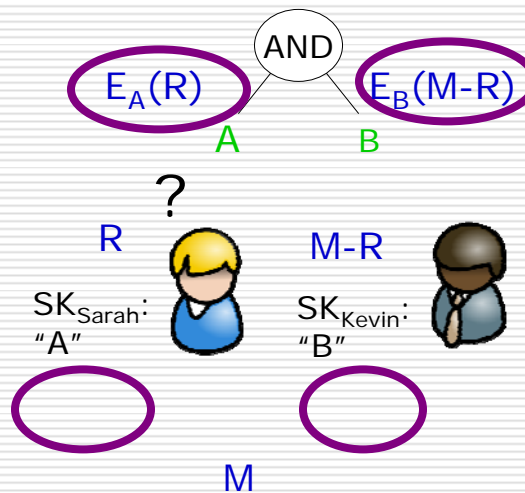
• Use finite field e.g. Z_p

• Ideas extend to more complex sharing

A First Approach

Combine S.S. and PKE

PK_A PK_B
 SK_A SK_B

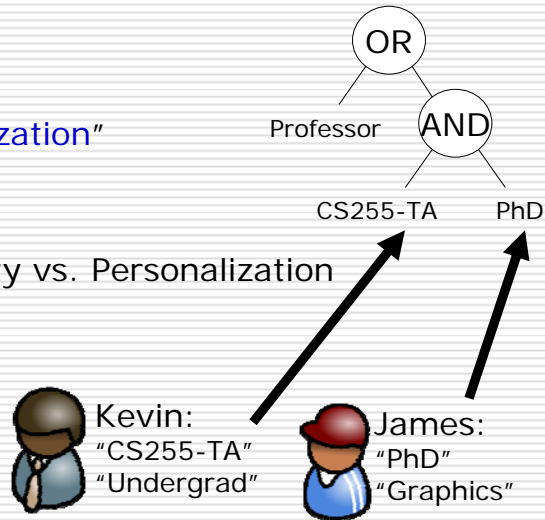


Collusion Attack!

Collusion Attacks: The Key Threat

Need: Key "Personalization"

Tension: Functionality vs. Personalization



21

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

22

System Setup



a, b chosen randomly $\in \mathbb{Z}_p$

 $PK = g, g^b, e(g, g)^a, \quad H : \{0, 1\}^* \rightarrow G$

 $MSK = a$

23

Key Generation





 $MSK = g^a, g^b$

Attributes:

x_1, \dots, x_ℓ



t random $\in \mathbb{Z}_p$  Personalization!

 $SK = g^{a+bt}, g^b, H(x_1)^t, \dots, H(x_\ell)^t$

't' ties components together

24

Key Personalization (Intuition)



Kevin:
"CS255-TA"



Random t

$$g^{a+bt}, g^t, H(\text{CS255-TA})^t$$



James:
"PhD"



Random t'

$$g^{a+bt'}, g^{t'}, H(\text{PhD})^{t'}$$

Components are incompatible

(Formal security proofs in papers)

25

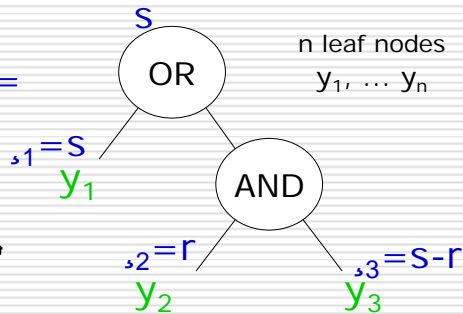
Encryption



$$\text{PK} = g, g^b, e(g, g)^a, H : \{0, 1\}^* \rightarrow G$$



$$f() =$$



$$s, r_1, \dots, r_n \text{ random } \in \mathbb{Z}_p$$

$$\text{CT: } Me(g, g)^{as}, g^s$$

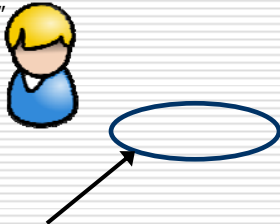
$$(g^{b\lambda_1} H(y_1)^{r_1}, g^{r_1}), \dots, (g^{b\lambda_n} H(y_n)^{r_n}, g^{r_n})$$

26

Making it work

CT: $Me(g, g)^{as}, g^s, (g^{b\lambda_1} H(y_1)^{r_1}, g^{r_1}), \dots$

"CS255-TA"
"PhD"



Message Randomization

Goal: Compute and cancel to get M

27

Making it work

CT: $Me(g, g)^{as}, g^s, (g^{b\lambda_1} H(y_1)^{r_1}, g^{r_1}), \dots$

SK: $g^{a+bt}, g^t, H(\text{CS255-TA})^t, H(\text{PhD})^t$

"CS255-TA"
"PhD"



$$e(g^s, g^{a+bt}) = e(g, g)^{s(a+bt)} =$$

$$e(g, g)^{sa} e(g, g)^{sbt}$$

Message Randomization

Personalized Randomization

Use Bilinear Map for Decryption
New goal: Personalized to user

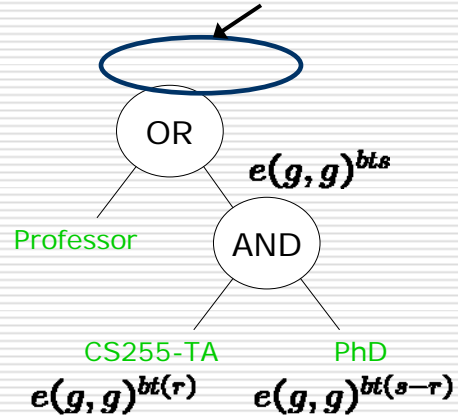
28

Making it work

"CS255-TA"
"PhD"



Personalized Randomization



- Shares are personalized (Use Bilinear-Map)
- Linearly Combine

29

Security

Theorem: System is (semantically) secure under chosen key attack

Number Theoretic Assumption:

Bilinear Diffie-Hellman Exponent [BBG05]

30

Impact

Line of Research: [SW05, GPSW06,PTMW06, BSW07, BW07, OSW07, KSW08]

Other Functional Encryption Work: [ACDMS06, C07, CCKN07, CN07, SBCDP07, TBEM08]

IBE: [S84, BF01, C01]

31

Impact

- Advanced Crypto Software Collection

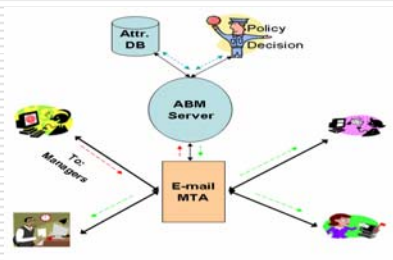
- Attribute-Based Messaging (UIUC)

- Group Key Management [CCKN07]

- Large Scale Content Distribution [TBEM08]

- Future NIST Standardization

```
$ cpabe-setup
$ cpabe-keygen -o sarah_priv_key pub_key master_key \
  sysadmin it_dept 'office = 1431' 'hire_date = 2002'
```

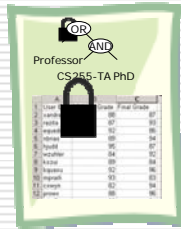



32


Beyond Access Control

Access Control Functions over encrypted data

- Only learn function's output



 Compute Average

 15th highest score

Challenge: Oblivious Evaluation


Only single keyword predicates [SWP00, BDOP04, BW06]

33


Beyond Access Control

Complex Predicates over data [KSW08] :

From = bob@yahoo.com **OR** From = alice@yahoo.com

 Can't tell why matched!

Idea: Inner Product Functionality
(Multiplication of Bilinear Map)

CT: $\vec{a} = \langle a_1, \dots, a_n \rangle$  SK $\vec{b} = \langle b_1, \dots, b_n \rangle$

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

Functionality: Polynomial Equations

$(x - y_1)(x - y_2) \stackrel{?}{=} 0$

34

Medical Studies

Collect DNA + medical information

Future: Database of sequenced genome



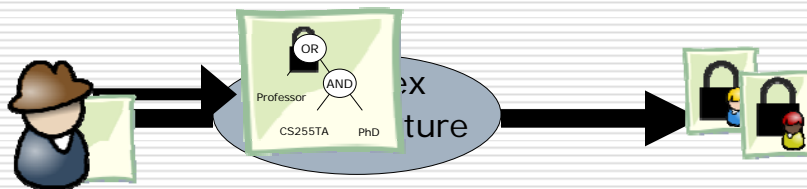
Limit Privacy Loss



Gene: TCF2 = AT **AND** Prostate Cancer

35

Functional Encryption Summary



- Tension: Functionality vs. Personalization

[SW05, GPSW06, PTMW06, BSW07, OSW07]

- Going Beyond Access Control [BW06, BW07, KSW08]

- Fundamental Change: Public Key Cryptography

36

Thank you
