

Functional Encryption: Beyond Public Key Cryptography

Brent Waters
SRI International

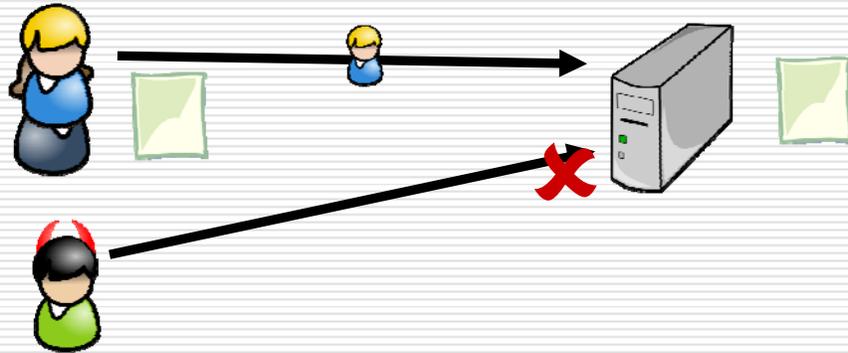
Protect Private Data



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



Access Control



3

Security Breaches

Intrusion:

- 45 Million Cards Stolen (Dec. 2006)



Physical Media Loss:

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



4

Access Control by Encryption

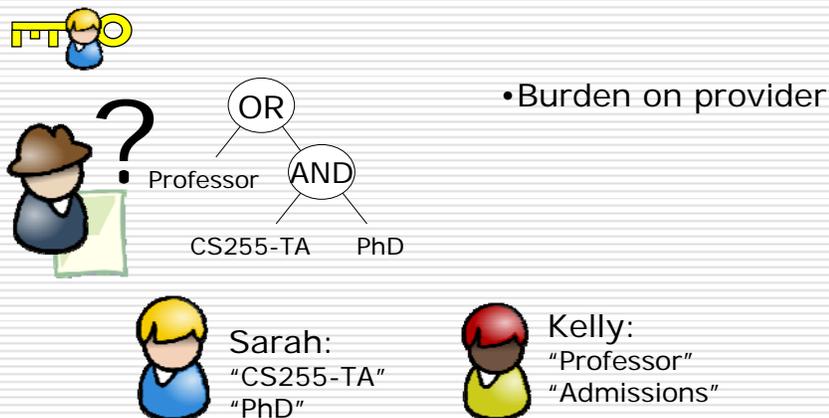
Idea: Need secret key to access data
e.g. PCI Standards



5

Realistic Data Sharing

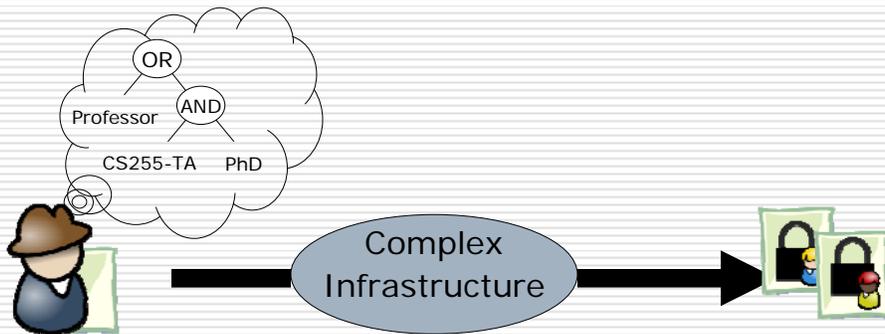
Problem: Disconnect between policy and mechanism



6

A Fundamental Gap

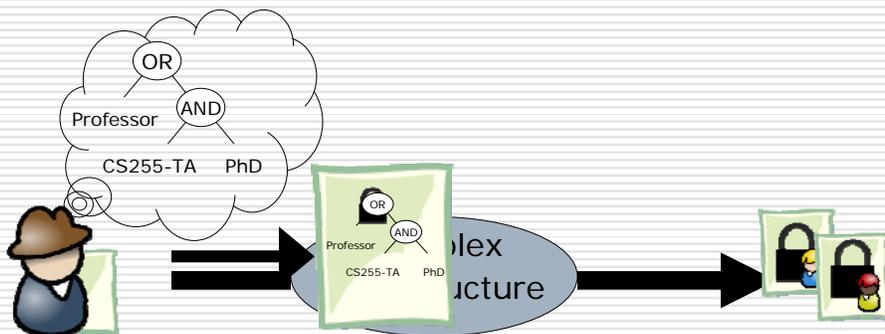
- Key Lookup
 - Group Key Management
-
- Online-Service
 - Complex
 - Several Keys



7

A New Vision

Functional Encryption



8

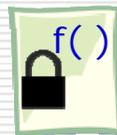
Functional Encryption: A New Perspective

 Public Parameters

SK  Cred. = X

Access Predicate: $f()$

If $f(X) = 1$

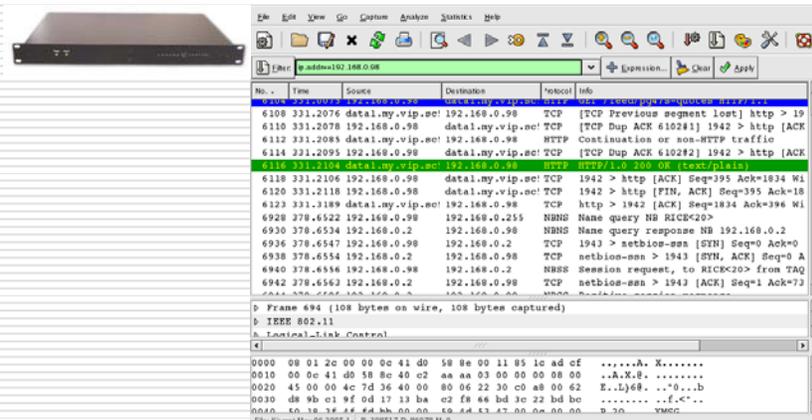


9

Why Functional Encryption?

Late Binding Access Control:

e.g. Network Logs



The screenshot shows a network traffic analysis tool interface. On the left, there is a small image of a network device. The main window displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The selected packet (No. 6116) is highlighted in green. Below the list, there is a detailed view of the selected packet, showing its structure and raw data. The raw data is displayed in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Info
6108	331.2076	data1.my.vip.net	192.168.0.98	TCP	[TCP Previous segment lost] http > 19
6110	331.2078	192.168.0.98	data1.my.vip.net	TCP	[TCP Dup ACK 610281] 1942 > http [ACK
6112	331.2085	data1.my.vip.net	192.168.0.98	HTTP	Continuation or non-HTTP traffic
6114	221.2095	192.168.0.98	data1.my.vip.net	TCP	[TCP Dup ACK 610282] 1942 > http [ACK
6116	331.2104	data1.my.vip.net	192.168.0.98	HTTP	HTTP/1.0 200 OK (text/plain)
6118	331.2106	192.168.0.98	data1.my.vip.net	TCP	1942 > http [ACK] Seq=395 Ack=1834 Wi
6120	331.2118	192.168.0.98	data1.my.vip.net	TCP	1942 > http [FIN, ACK] Seq=395 Ack=18
6122	331.3189	data1.my.vip.net	192.168.0.98	TCP	http > 1942 [ACK] Seq=1834 Ack=396 Wi
6928	378.6522	192.168.0.98	192.168.0.255	NBNS	Name query NB RICKC20>
6930	378.6534	192.168.0.2	192.168.0.98	NBNS	Name query response NB 192.168.0.2
6936	378.6547	192.168.0.98	192.168.0.2	TCP	1943 > netbios-ssn [SYN] Seq=0 Ack=0
6938	378.6554	192.168.0.2	192.168.0.98	TCP	netbios-ssn > 1943 [SYN, ACK] Seq=0 A
6940	378.6556	192.168.0.98	192.168.0.2	NBNS	Session request, to RICKC20> from TQq
6942	378.6563	192.168.0.2	192.168.0.98	TCP	netbios-ssn > 1943 [ACK] Seq=1 Ack=73

10

Why Functional Encryption?

Late Binding Access Control:

e.g. Network Logs



Src: 123.3.4.77 AND
Date: 12/5/07

SK



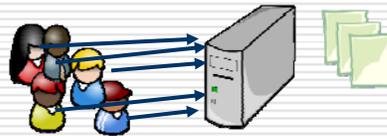
- Encrypt packet payload, tag with metadata
- Distribute capabilities later

11

Why Functional Encryption?

Scalability and Robustness:

Availability vs. Security



Personal Storage Devices

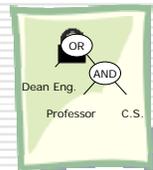


12

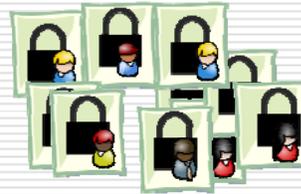
Why Functional Encryption?

Efficiency:

Scales with policy complexity

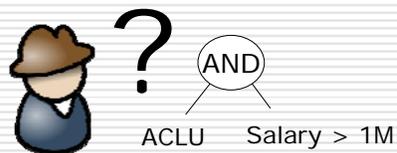


VS.



Why Functional Encryption?

Receiver Privacy:



A New Vision for Encryption Systems

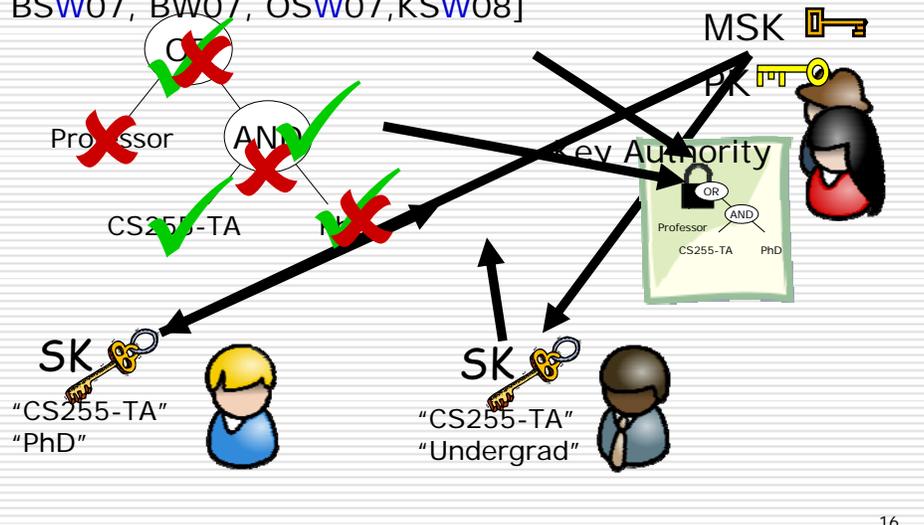
- Retrospect: Public vs. Secret Key Cryptography
- Secure Internet Connections (Public Key Exchange)
- Online Software Updates (Digital Signatures)

- The next step forward

15

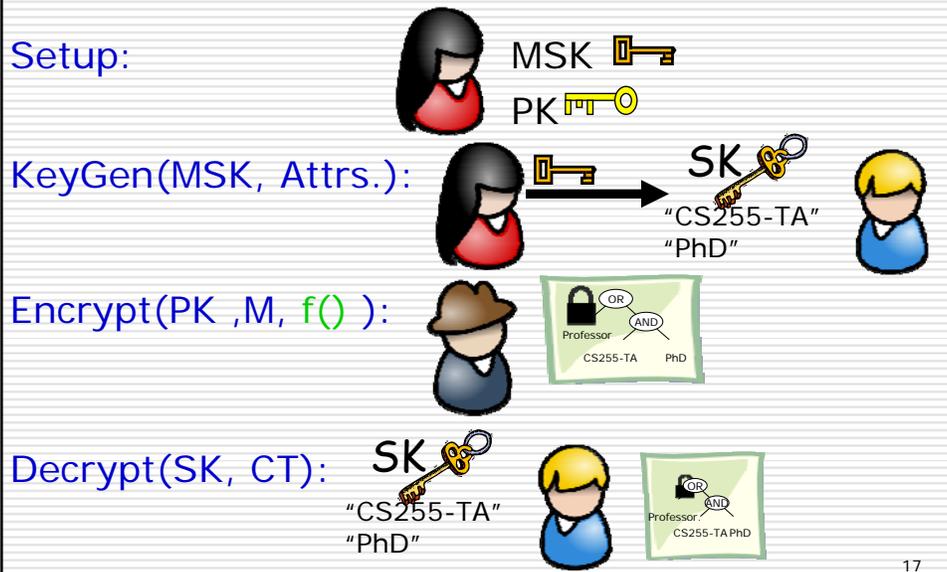
Functional Encryption for Formulas [SW05]

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



16

Functional Encryption for Formulas

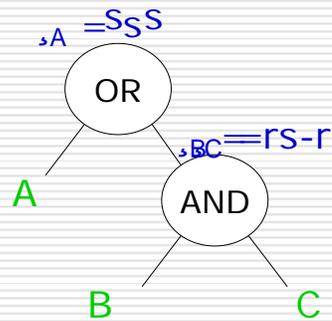


A First Approach

Question: Can we build functional encryption from standard techniques?

Attempt: Public Key Encryption + Secret Sharing

Secret Sharing [S78,B78,BL86]



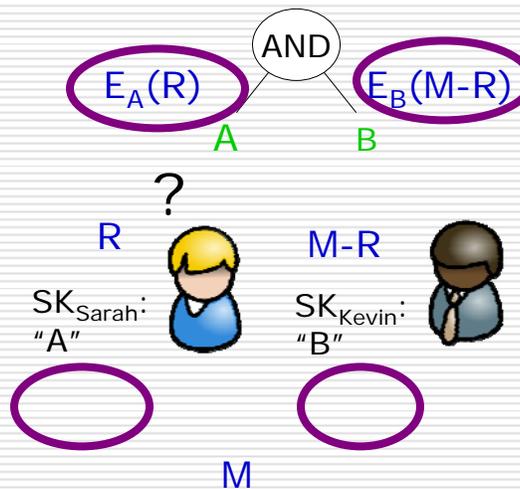
• Use finite field e.g. Z_p

• Ideas extend to more complex sharing

A First Approach

Combine S.S. and PKE

PK_A PK_B
 SK_A SK_B

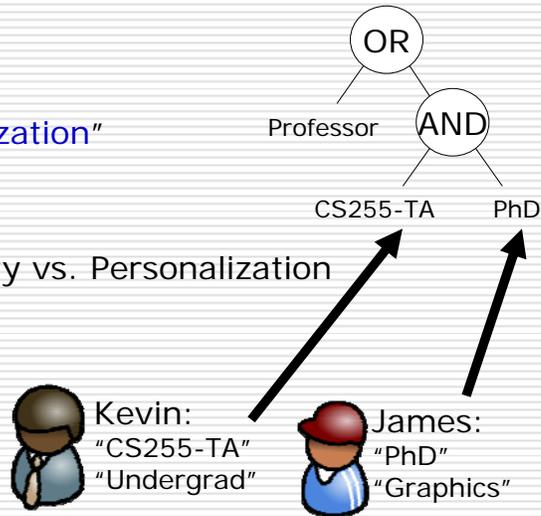


Collusion Attack!

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

 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^t , $H(x_1)^t, \dots, H(x_\ell)^t$

' 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

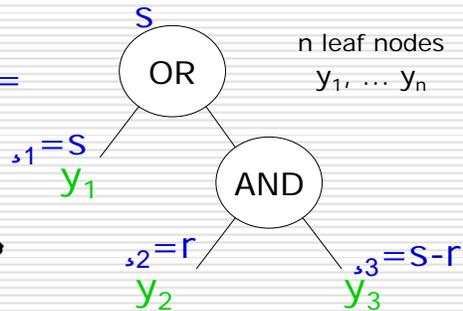
Encryption



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



$$f() =$$



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

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

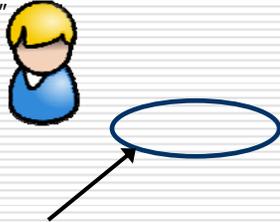
$$(g^{b\lambda_1} H(y_1)^{r_1}, g^{r_1}), \dots, (g^{b\lambda_n} H(y_n)^{r_n}, g^{r_n})$$

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

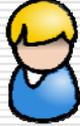
Personalized Randomization

Use Bilinear Map for Decryption
New goal: Personalized to user

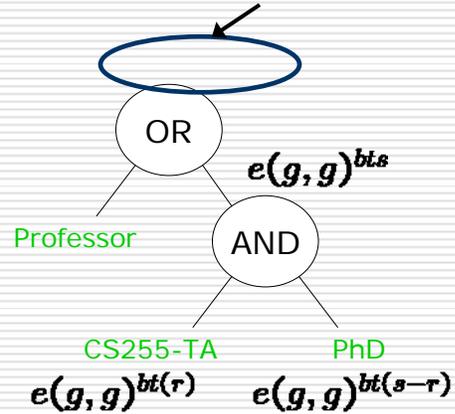
28

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

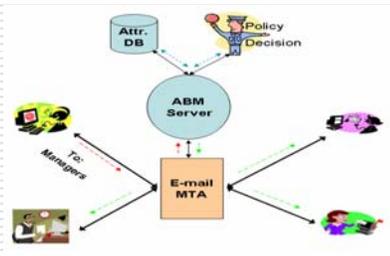
- Attribute-Based Messaging (UIUC)

- 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'
```

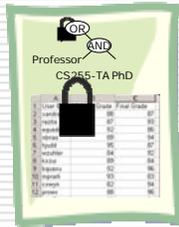


32

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

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



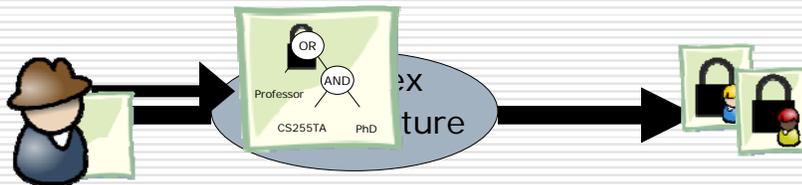
Limit Privacy Loss



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
