Ciphertext-Policy, Attribute-Based Encryption

John Bethencourt
CMU

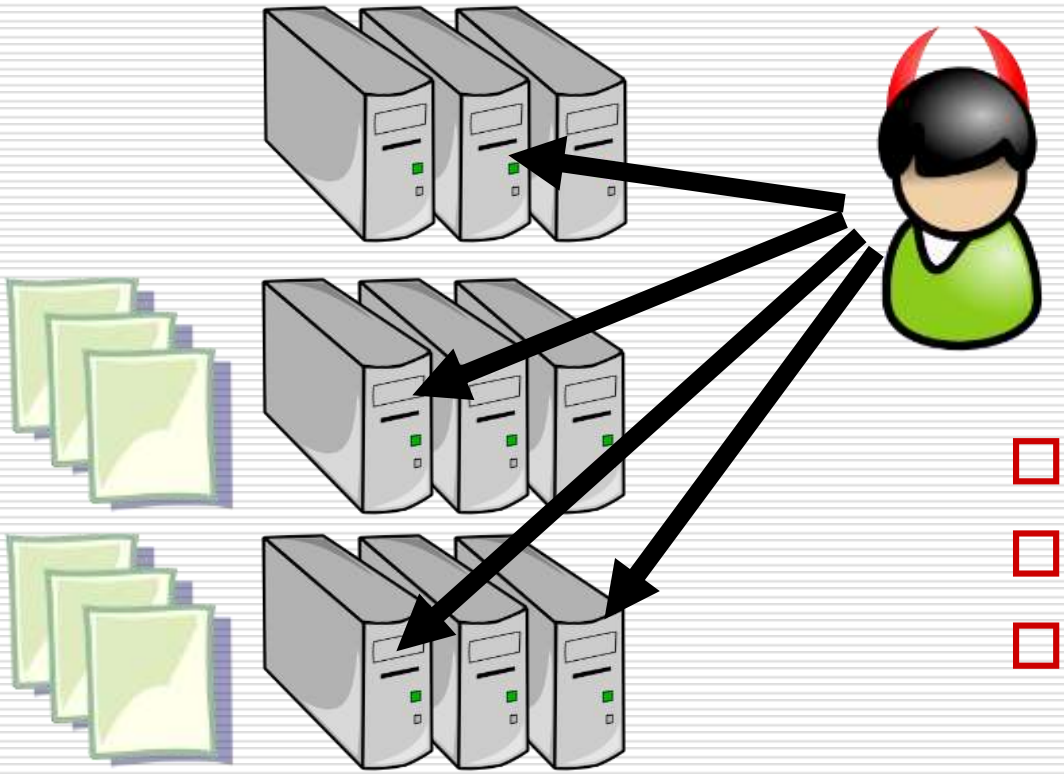
Amit Sahai
UCLA

Brent Waters
SRI International

What is Ciphertext-Policy Attribute-Based Encryption (CP-ABE)?

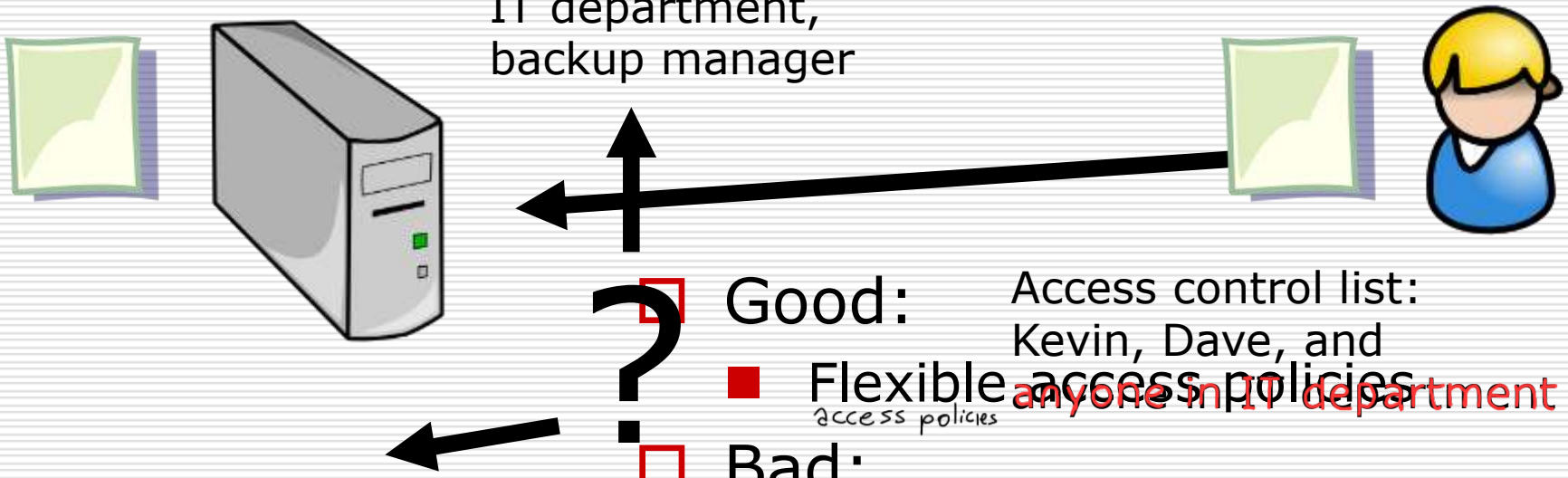
- Type of identity-based encryption
  - One public key
  - Master private key used to make more restricted private keys
- But very expressive rules for which private keys can decrypt which ciphertexts
  - Private keys have “attributes” or labels
  - Ciphertexts have decryption policies

Remote File Storage: Interesting Challenges



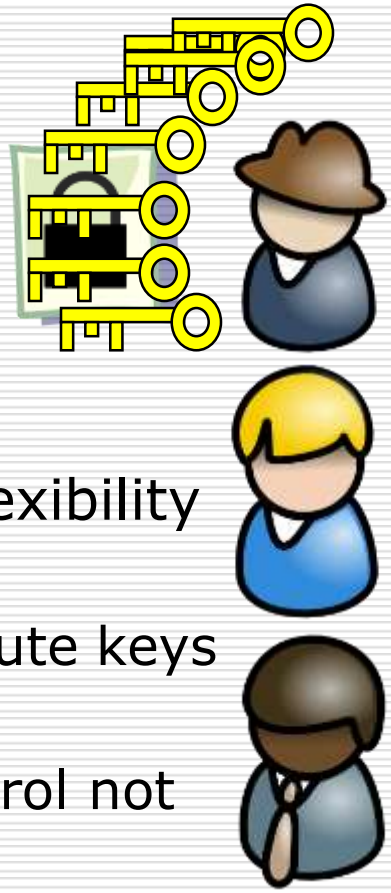
- Scalability
- Reliability (duplica risorse)
- … But we also want security

Remote File Storage: Server Mediated Access Control



- Good:
  - Flexible access policies
- Bad:
  - Data vulnerable to compromise
  - Must trust security of server

Remote File Storage: Encrypting the Files

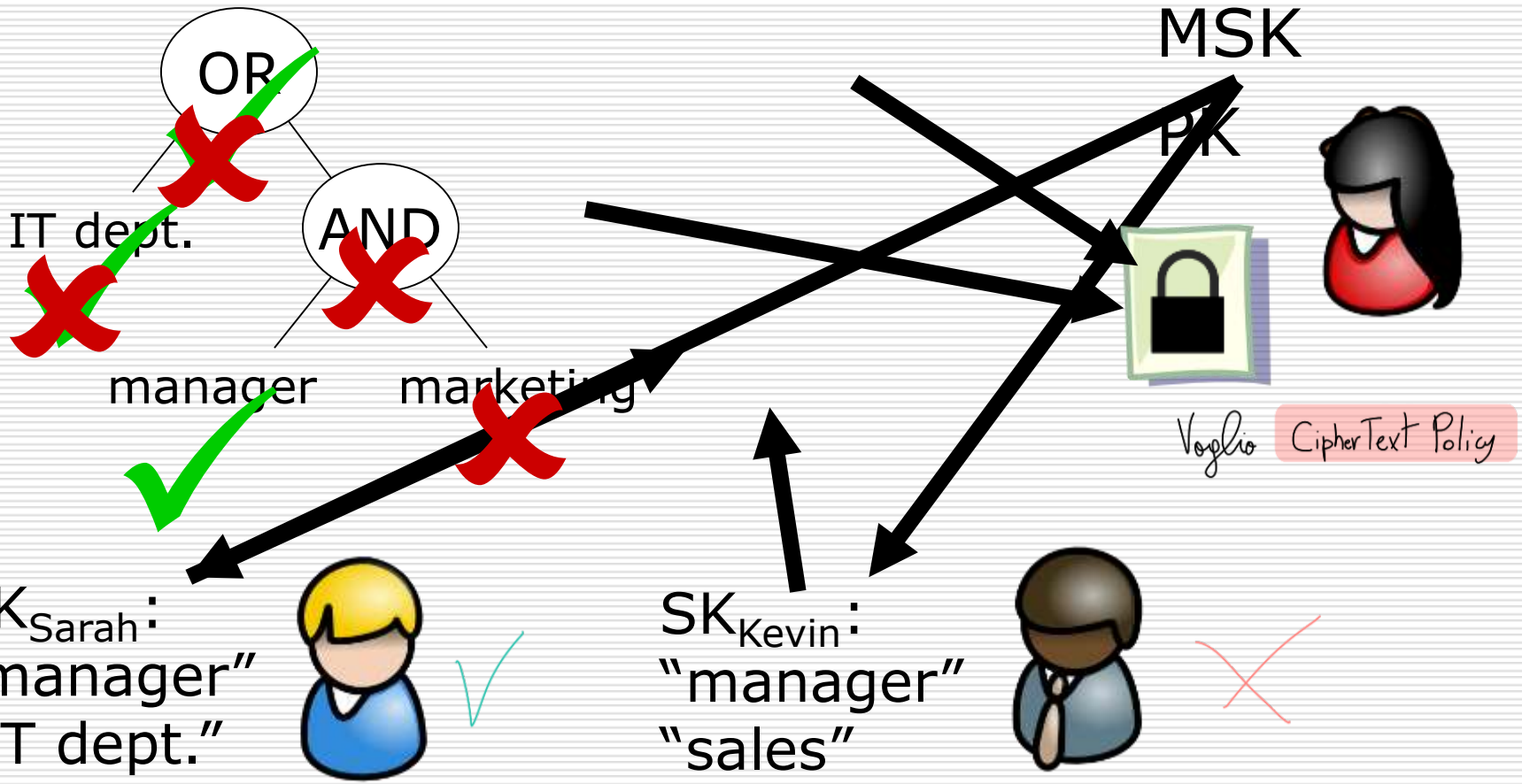


- More secure, but loss of flexibility
- New key for each file:
  - Must be online to distribute keys
- Many files with same key:
  - Fine grained access control not possible

Remote File Storage: We Want It All (Access Control + Encryption)

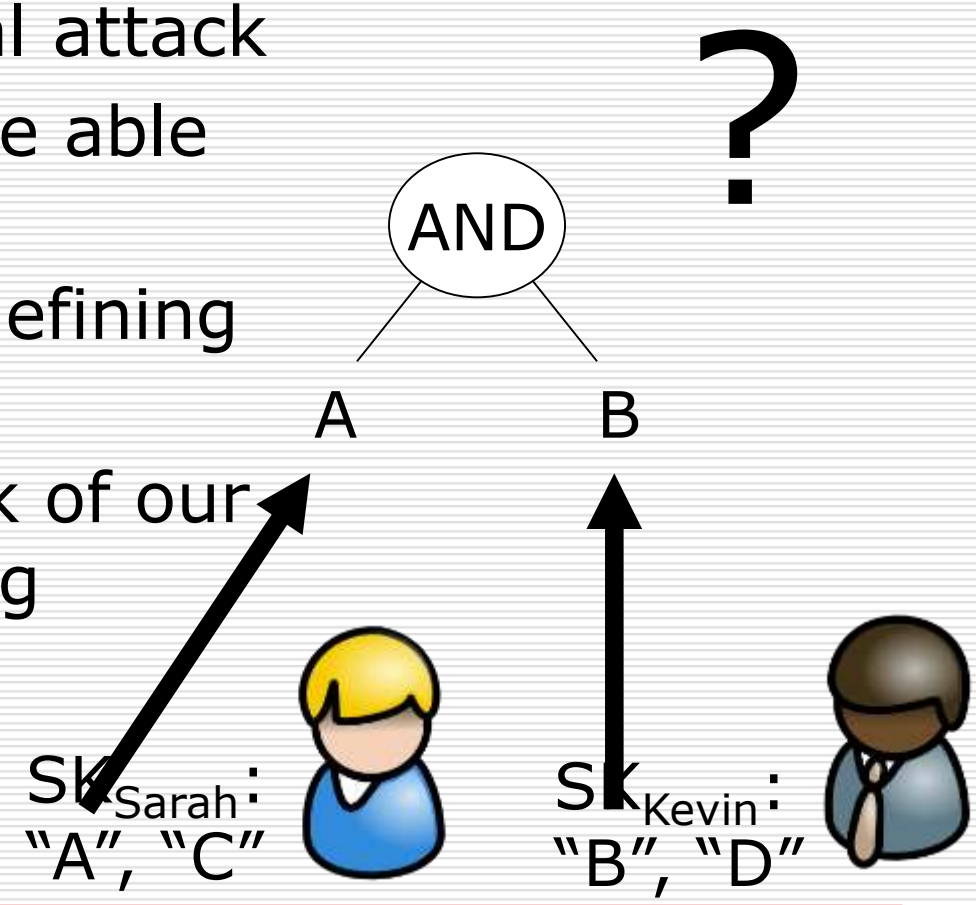
- Wishlist:
  - Encrypted files for untrusted storage
  - Setting up keys is offline
  - No online, trusted party mediating access to files or keys
  - Highly expressive, fine grained access policies
- Ciphertext-policy attribute-based encryption does this!
  - User private keys given list of "attributes"
  - Files can encrypted under "policy" over those attributes
  - Can only decrypt if attributes satisfy policy

Remove File Storage: Access Control via CP-ABE



Collusion Attacks: The Key Threat

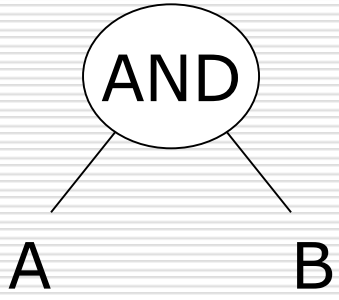
- Important potential attack
- Users should not be able to combine keys
- Essential, almost defining property of ABE
- Main technical trick of our scheme: preventing collusion



Voglio accedere a film, devo pagare e avere +18 anni. Posso farlo fare ad amico che rispetta l'età!

Collusion Attacks: A Misguided Approach to CP-ABE

- Collusion attacks rule out some trivial schemes …



PK_A PK_B PK_C PK_D

SK_A SK_B SK_C SK_D

$M = M_1 + M_2$

$C = (E_A(M_1), E_B(M_2))$

Combino per rispettare la policy

SK_{Sarah}: "A", "C"

SK_A SK_C

SK_{Kevin}: "B", "D"

SK_B SK_D

Highlights From Our Scheme: Background (PAIRING)

$$|G| = |G_T| = p \qquad g \in G, < g >= G$$

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

$$\forall a, b \in \mathbb{Z}^p, \quad e(g^a, g^b) = e(g, g)^{ab}$$

Highlights From Our Scheme: Public Key and Master Private Key

$$\alpha, \beta \xleftarrow{R} \mathbb{Z}p$$

prima era g^s

$$\mathsf{PK} = (g, g^{\beta}, e(g,g)^{\alpha}) \rightarrow \in \text{Authority}$$

generator — EC punti — transformation

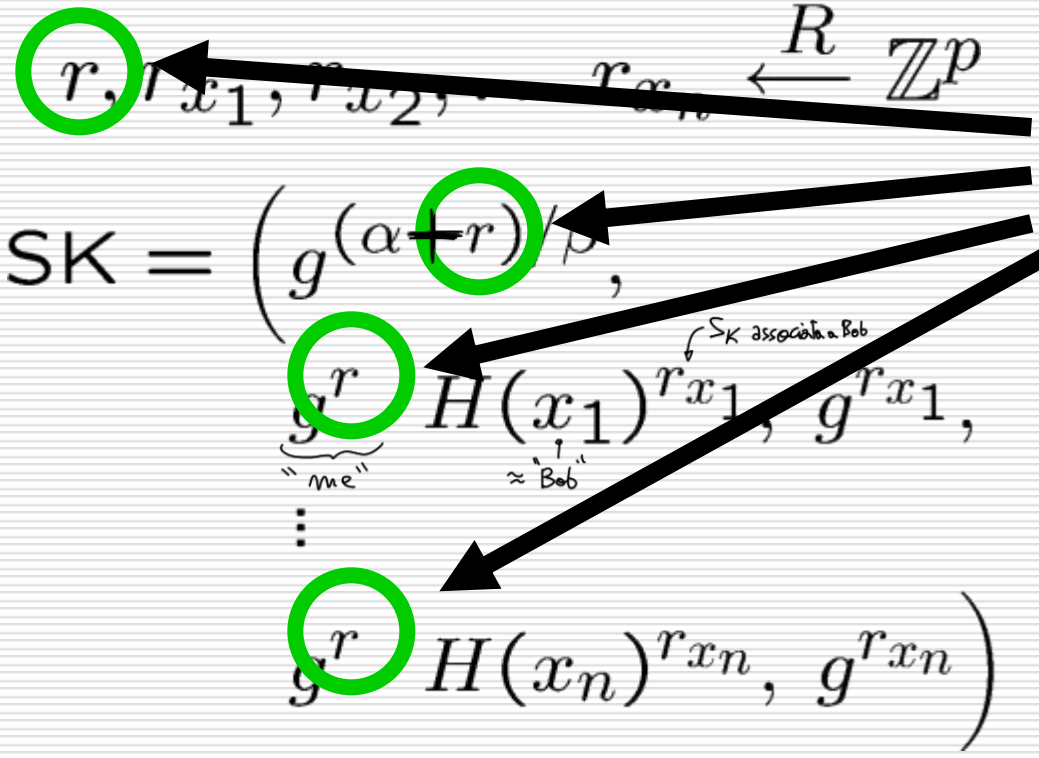
prima era 's'

$$\mathsf{MSK} = (\beta, g^{\alpha})$$

più complesse per via del Collusion Attack

Highlights From Our Scheme: Private Key Generation

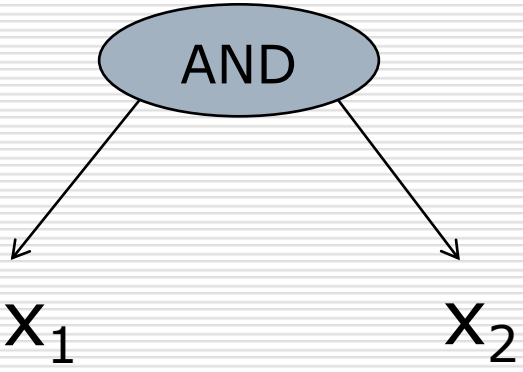
desired attributes: $x_1, x_2, \ldots x_n \in \{0,1\}^*$



- "Binds" key components to each other
- Makes components from different keys incompatible
- Key to preventing collusion attacks

(GB addition): Encrypt Simpler case of AND policy

- AND policy



- s ← random
- Shares (AND example)
  - s1 = s-d
  - s2 = d (rand)
- For each attr:

$$C_j = g^{s_j}, H(x_j)^{s_j}$$

- For the whole message:

$$C = g^{\beta \cdot s}, \tilde{C} = Me(g,g)^{\alpha \cdot s}$$

NB $u = g^x$, $v = g^y$

$e(u \cdot v, g^s) = e(g^x \cdot g^y, g^s) = e(g^{x+y}, g^s) = e(g,g)^{(x+y)\cdot s} = e(g,g)^{xs+ys} = e(g,g)^{xs} \cdot e(g,g)^{ys} = e(g^x, g^s) \cdot e(g^y, g^s) = e(u, g^s) \cdot e(v, g^s)$

(GB addition): Decrypt (1)

- Receive ciphertext, parse policy & attr
- For each attr user has
  - Ciphertext $C_j = g^{s_j}, H(x_j)^{s_j}$
  - Secret key $D_j = g^{r_{x_j}}, g^r \cdot H(x_j)^{r_{x_j}}$
- Hence:

$$\frac{e(g^r \cdot H(x_j)^{r_{x_j}}, g^{s_j})}{e(g^{r_{x_j}}, H(x_j)^{s_j})} = \frac{e(g^r, g^{s_j}) \cdot e(H(x_j)^{r_{x_j}}, g^{s_j})}{e(g^{r_{x_j}}, H(x_j)^{s_j})} = e(g,g)^{r \cdot s_j}$$

(GB addition): Decrypt (2)

- For the simpler AND policy example (generalization very easy, now..)
  - Multiply terms

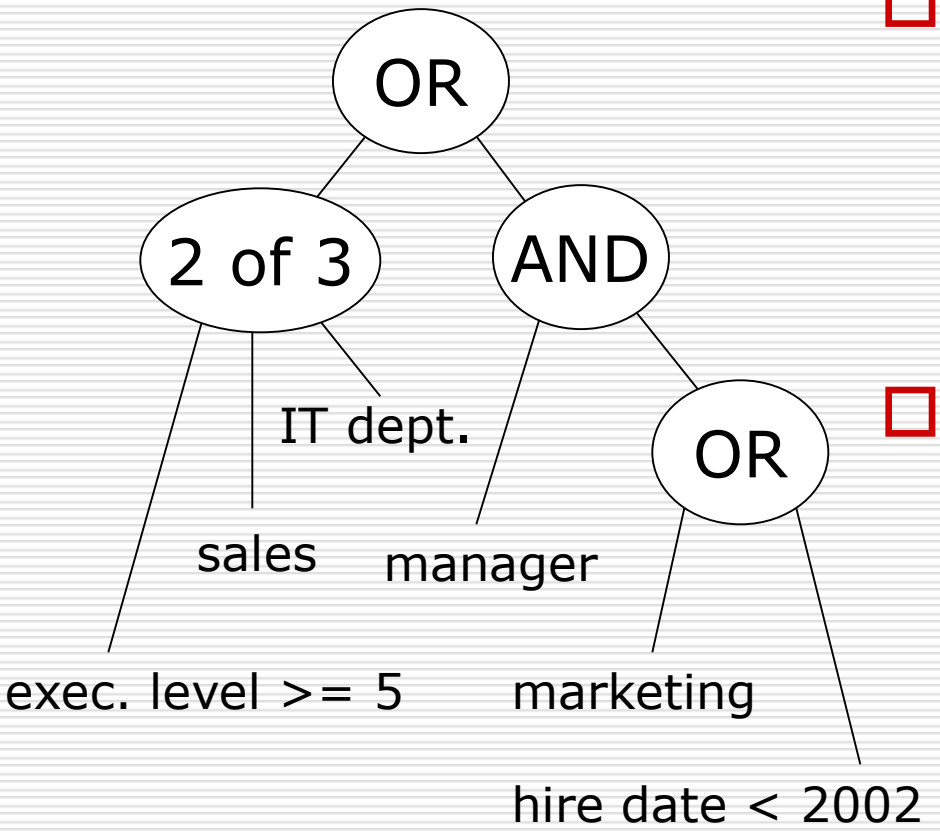
$$A = \prod e(g,g)^{r \cdot s_j} = e(g,g)^{r \cdot (s-d)} \cdot e(g,g)^{r \cdot d} = e(g,g)^{r \cdot s}$$

  - Remember that $C = g^{\beta \cdot s}, \tilde{C} = Me(g,g)^{\alpha \cdot s}$
  - And private key: $D = g^{(\alpha+r)/\beta}$
  - Hence:

$$\frac{\tilde{C}}{e(C,D)/A} = \frac{Me(g,g)^{\alpha \cdot s}}{e(g^{\beta s}, g^{(\alpha+r)/\beta})/e(g,g)^{r \cdot s}} =$$

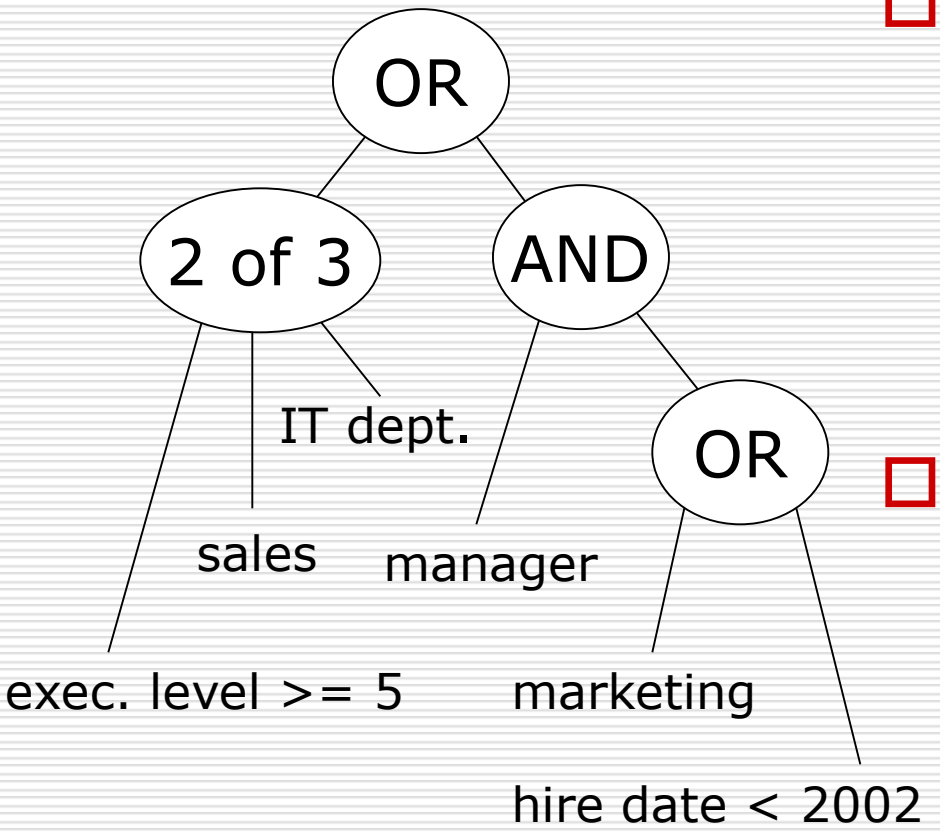
$$= M \frac{e(g,g)^{\alpha \cdot s}}{e(g,g)^{\beta s(\alpha+r)/\beta}/e(g,g)^{r \cdot s}} = M \frac{e(g,g)^{\alpha \cdot s}}{e(g,g)^{s\alpha} e(g,g)^{sr}/e(g,g)^{r \cdot s}} = M$$

Highlights From Our Scheme: Policy Features



- Leaf nodes:
  - Test for presence of string attribute in key
  - Also numerical attributes and comparisons
- Internal nodes:
  - AND gates
  - OR gates
  - Also k of n threshold gates

Highlights From Our Scheme: Encryption and Decryption



- Encryption:
  - Use general secret sharing techniques to model policy
  - One ciphertext component per leaf node
- Decryption:
  - Uses LaGrange interpolation "in the exponents"

Highlights From Our Scheme: Security

- Proven secure, including collusion resistance
  - Assumes random oracle model
  - Assumes generic group model
- Generic group model
  - "Black box" heuristic similar to random oracle model
  - Good future work: scheme without this assumption

Implementation: The cp-abe Toolkit

```
$ cpabe-setup

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

$ cpabe-enc pub_key security_report.pdf
(sysadmin and (hire_date < 2005 or security_team)) or
2 of (executive_level >= 5, audit_group, strategy_team))
```

Implementation: Performance

- Benchmarked on 64-bit AMD 3.7 GHz workstation
- Essentially no overhead beyond group operations in PBC library

Operation	**Approximate Time**
Private key gen.	35 ms per attribute
Encryption	27 ms per leaf node
Decryption	0.5–0.8 ms per leaf node

Implementation: Availability

- Available as GPL source at Advanced Crypto Software Collection (ACSC)
  - New project to bring very recent crypto to systems researchers
  - Bridge the gap between theory and practice
  - Total of 8 advanced crypto projects currently available
  - http://acsc.csl.sri.com

Attribute Based Encryption: Related Work

	Collusion resistant	Policies w/ infinite attr. space	Policies w/ fixed attr. space	Attributes	Policy
[1,2]	**Yes**	**Single thresh. gate**	**Single thresh. gate**	In ciphertext	In key
[3]	**Yes**	**Monotone formulas**	**All boolean formulas**	In ciphertext	In key
This	**Yes**	**Monotone formulas**	**All boolean formulas**	In key	In ciphertext
[4]*	**No**	**None**	**All boolean formulas**	In key	In ciphertext

* Has additional policy hiding property, but needs online, semi-trusted server to perform encryption

Attribute Based Encryption: Related Work

[1] Sahai, Waters. Eurocrypt 2005.

[2] Pirretti, Traynor, McDaniel, Waters. CCS 06.

[3] Goyal, Pandey, Sahai, Waters. CCS 06.

[4] Kapadia, Tsang, Smith. NDSS 07.

Thanks for Listening!

- bethenco@cs.cmu.edu
- http://acsc.csl.sri.com