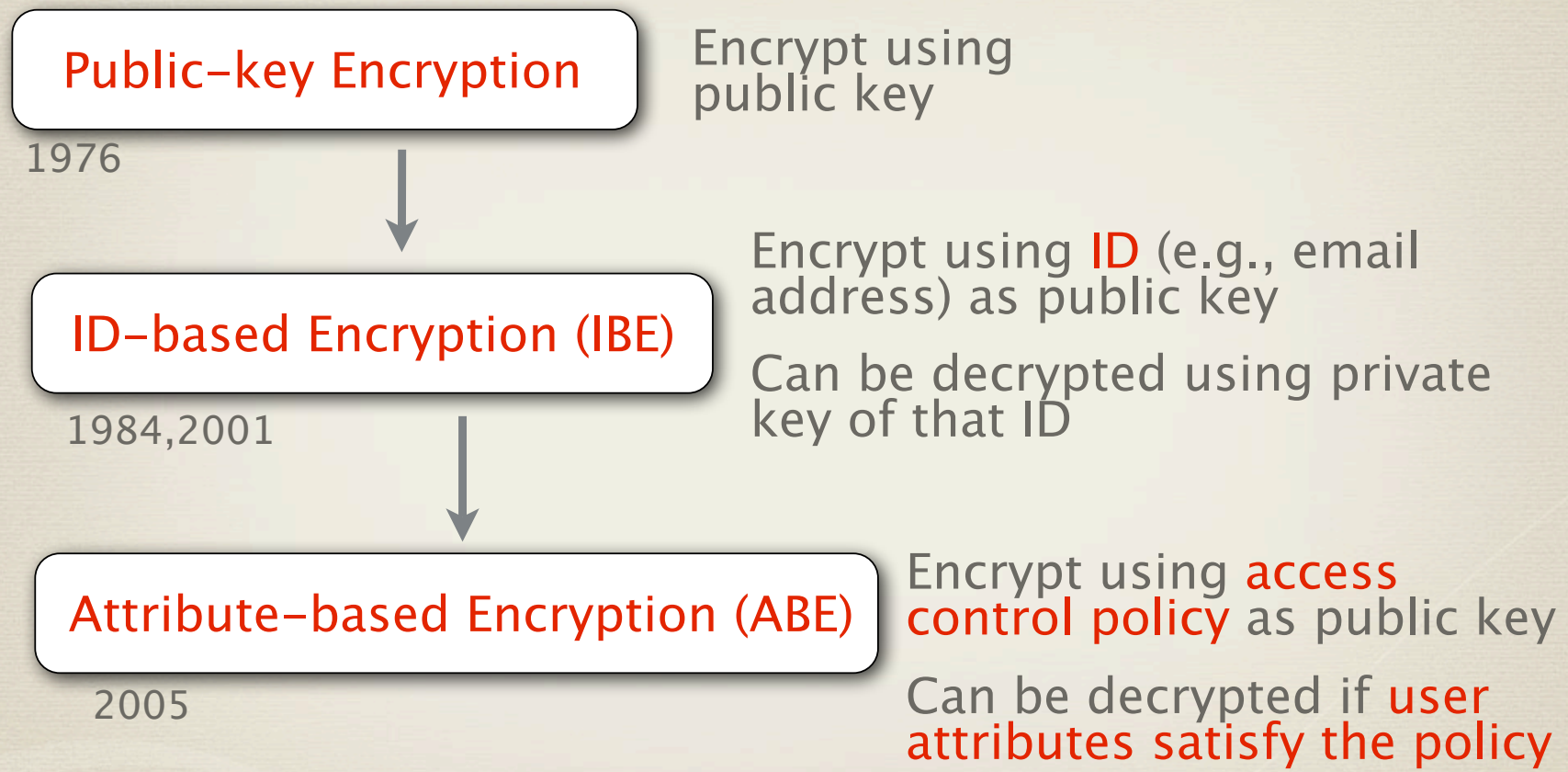
REVOCATION SCHEME FOR ATTRIBUTE-BASED ENCRYPTION

Nuttapong Attrapadung (Nuts)
Security Fundamental Team, RCIS, AIST

For RCIS Workshop Talk 2008.05.16

What is Attribute-based Encryption?



Hot topic in crypto research community

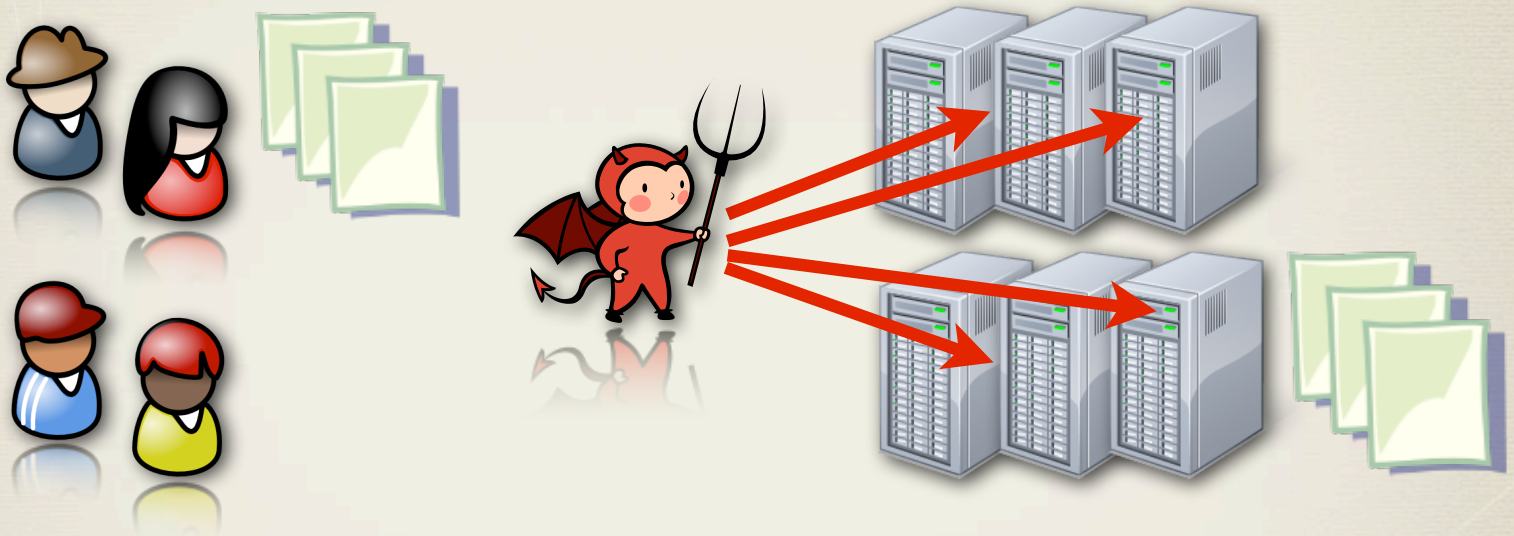
In this talk, we will

- Give a short survey on ABE
- Present our revocation scheme for ABE

Outline of Talk

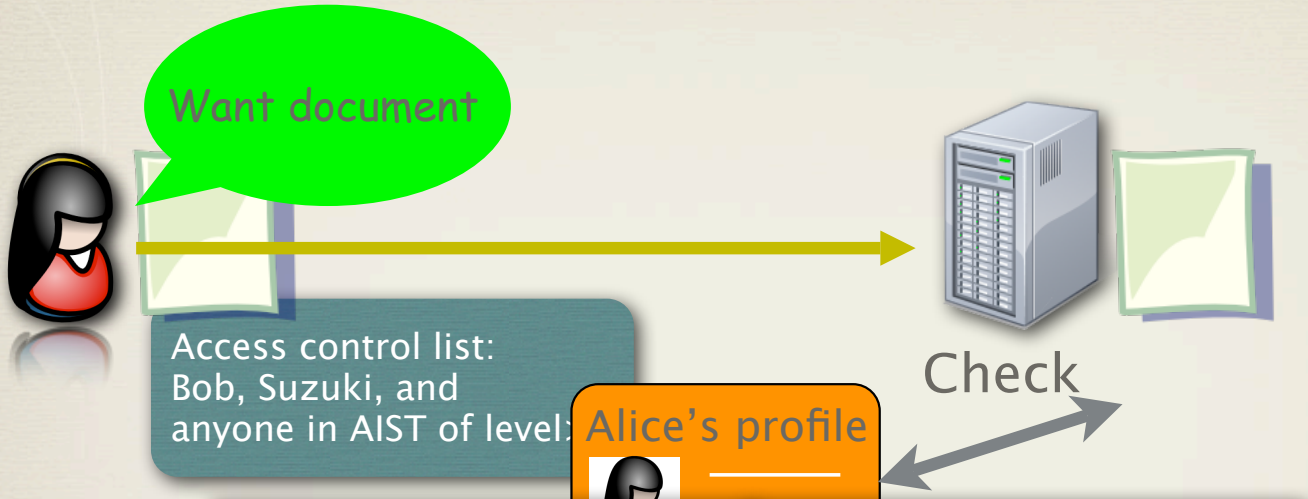
- Motivating problem: Secure Remote File Storage
- Introducing Attribute-based Encryption (ABE)
- Motivation for revocable ABE
- Our solution: Broadcast-conjunctive ABE
- Constructions

A Challenge for Ubiquitous Society: Remote File Storage



- Scalability
- Reliability
- Security

Security Solution 1 (not so nice): Access Control via Trust Server



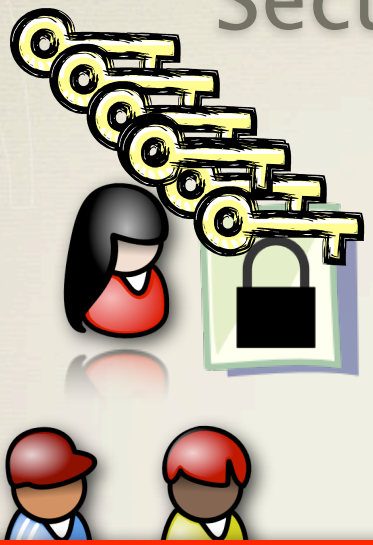
Good:

- ★ Fine-grained access control

Bad:

- ✳ Must trust server
- ✳ Data vulnerable to compromise

Security Solution 2 (not so nice): Security via Encryption



Good:

- No need of trust server
- Encryption ensures security

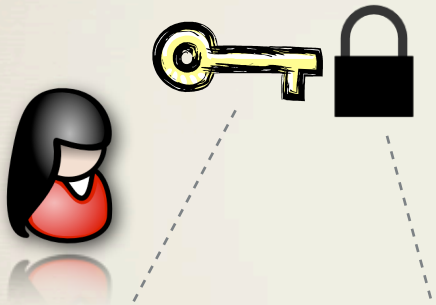
Bad:

- Must be online to distribute keys (1key/1file) or
- Fine-grained access control not possible (1key/many files)

List of Wanted Properties

☑ Possible offline trusted party

☑ Files are encrypted



☑ No online key distribution

☑ Universal public key

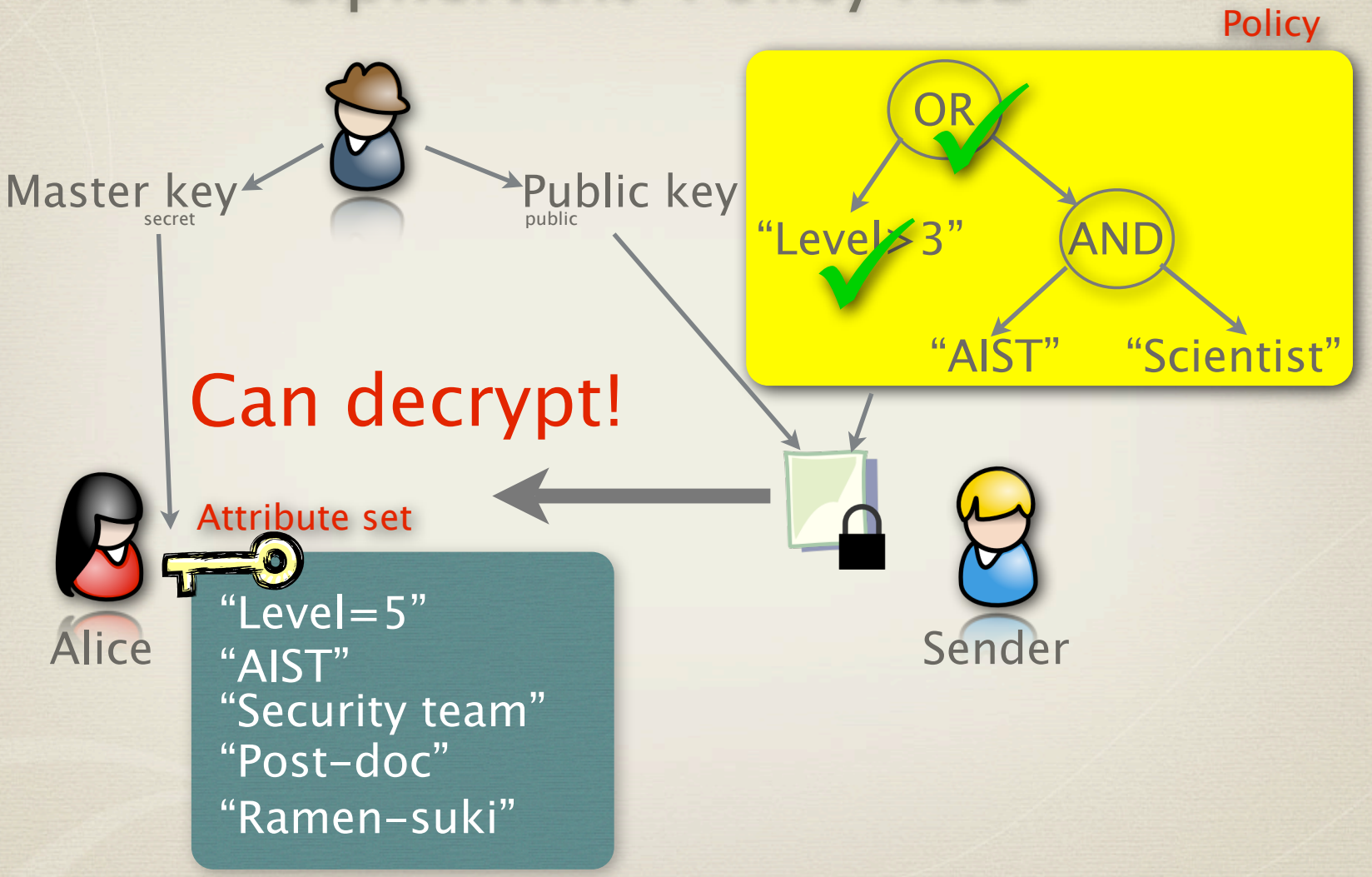
☑ Untrusted storage

☑ Flexible fine-grained access control

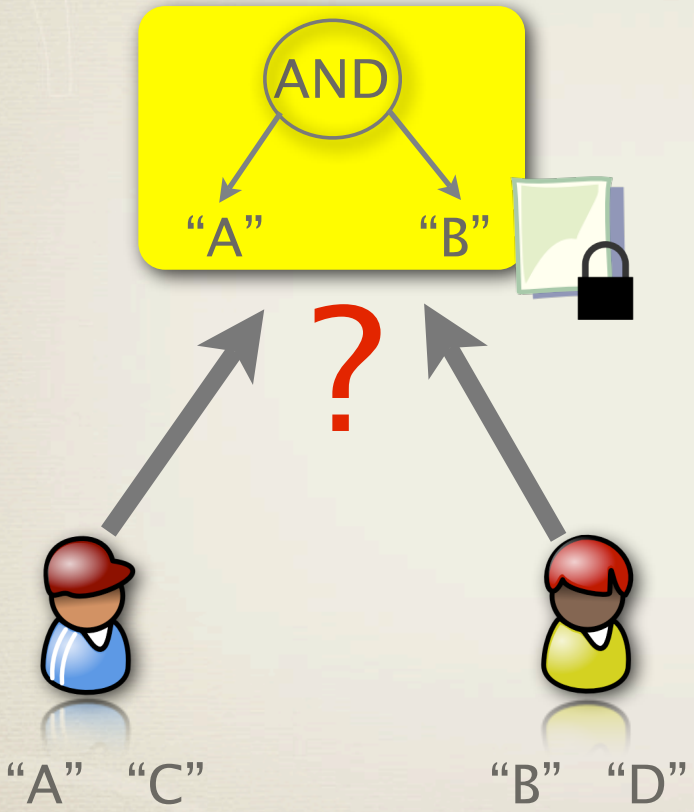
Ciphertext-Policy ABE: Concept

- Private key assigned to "attributes"
- Ciphertext associated with "access policy"
- Can decrypt only when attributes satisfy policy

Ciphertext-Policy ABE



Security Against Collusion Attack



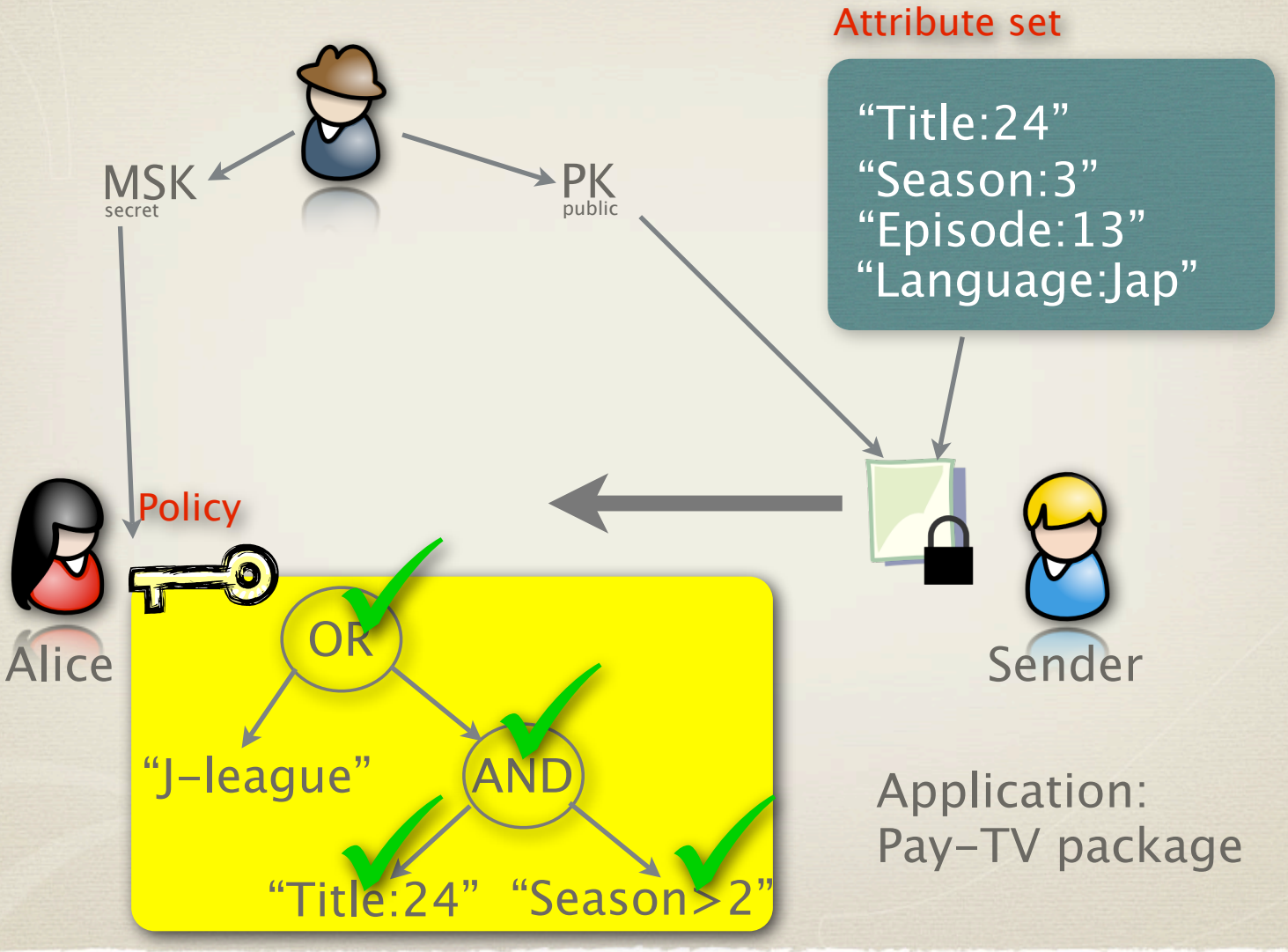
- Users should not be able to combine their keys
- Main security point for ABE
- Multiple encryption does not give secure ABE.

Another type of ABE
Key-Policy ABE

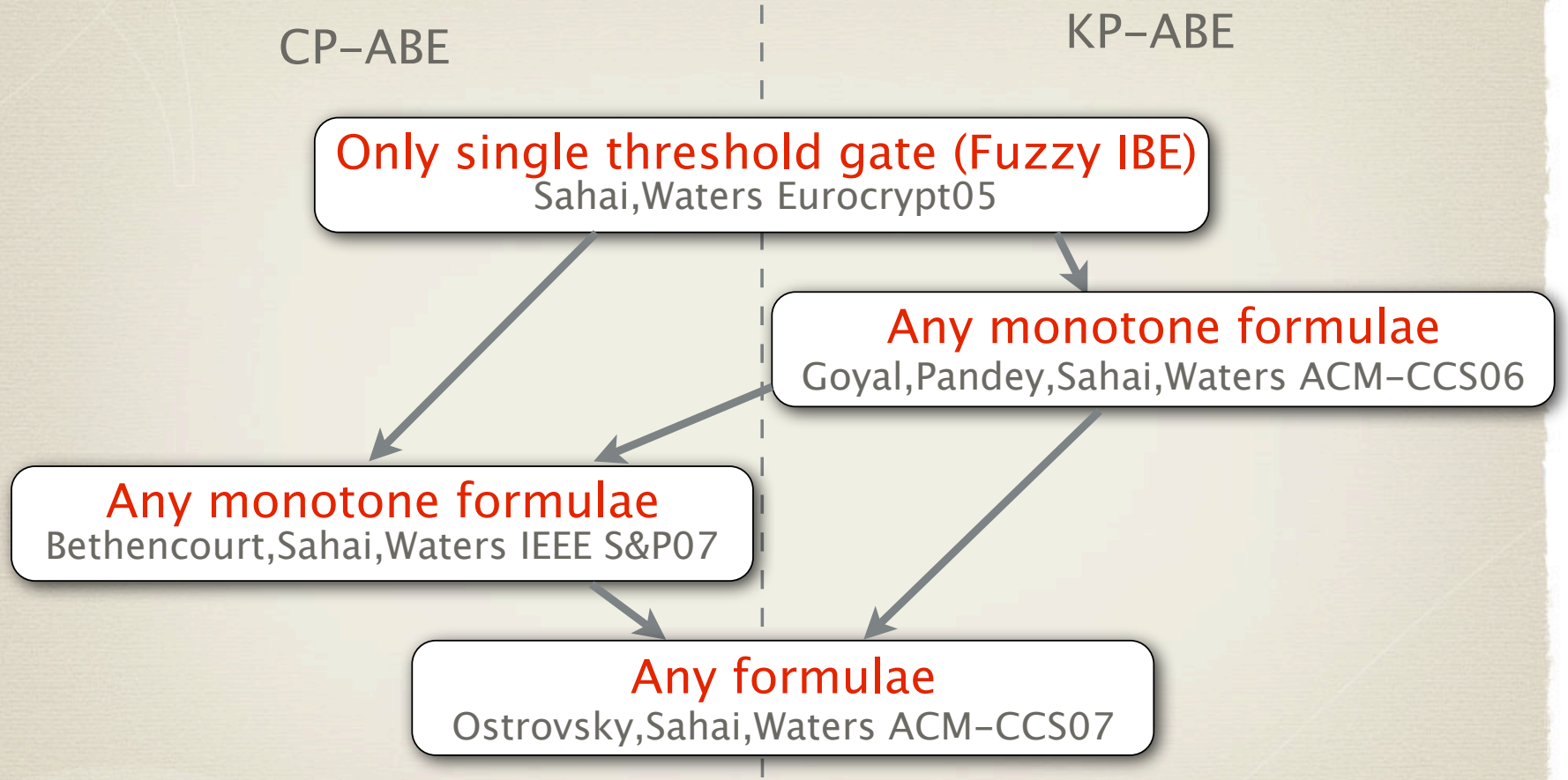
Role of attributes and policy swapped

- Private key assigned to "access policy"
- Ciphertext associated with "attributes"
- Can decrypt only when attributes satisfy policy

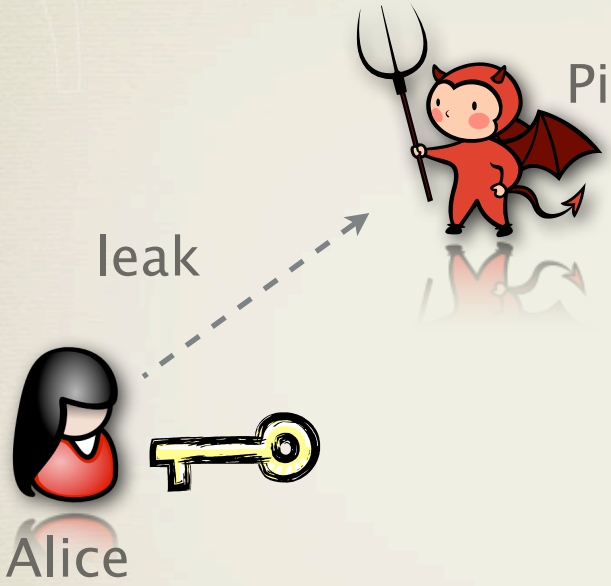
Key-Policy ABE



Previous Works



Next Challenge (Our Focus Here): To Revoke Leaked Keys



Want to exclude Alice without affecting other users

Importance of Revocation Scheme

- Without it, no security control ensured
  - Failure of copy protection for copyrighted DVD distribution

- With revocation scheme, we have a countermeasure against piracy
  - In next-generation disc (Blu-ray), revocation scheme is enabled by Broadcast Encryption (BE)

Previous Revocation Solution for ABE

- For Ciphertext-policy ABE, [Ostrovsky et al. 2007] scheme can be applied.
  - Using the idea of negative attributes
  - But not so efficient
- For Key-Policy ABE, no solution yet so far.

We propose efficient revocation mechanism for ABE

Use new primitive:
Broadcast-conjunctive ABE

Our Contributions

	Revocable CP-ABE	Revocable KP-ABE
Previous	[OSW07] |Cipher|= (2t+2) +r |Key|= (2m+2) · (log m)	None
This work	|Cipher|= (2t+2) +1 |Key|= (2m+2) +1	|Cipher|= (m+2) +1 |Key|= 2t

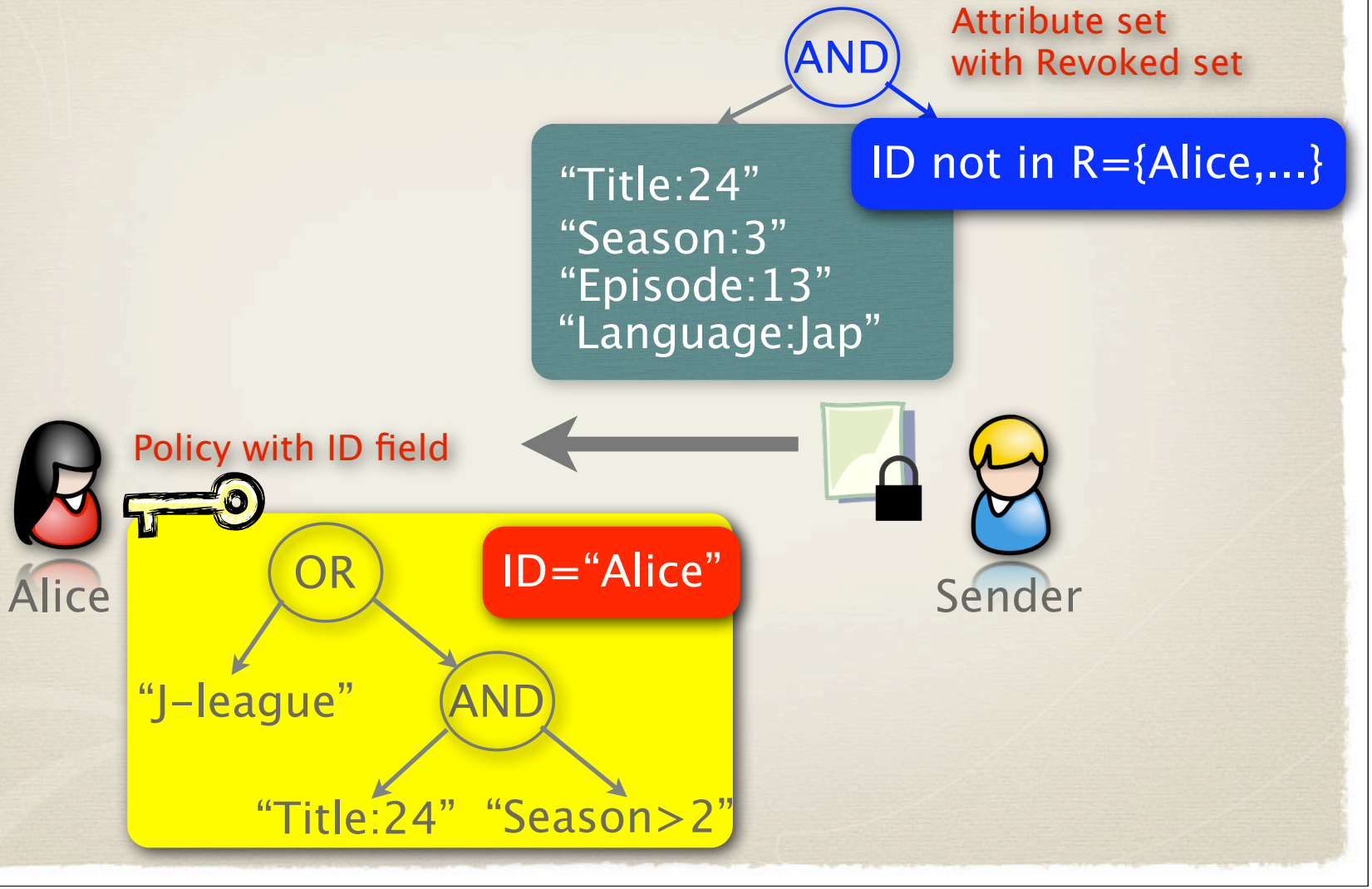
r=|revoked users|, m=max |attribute set|, t=|leaves in tree|

Our Contributions

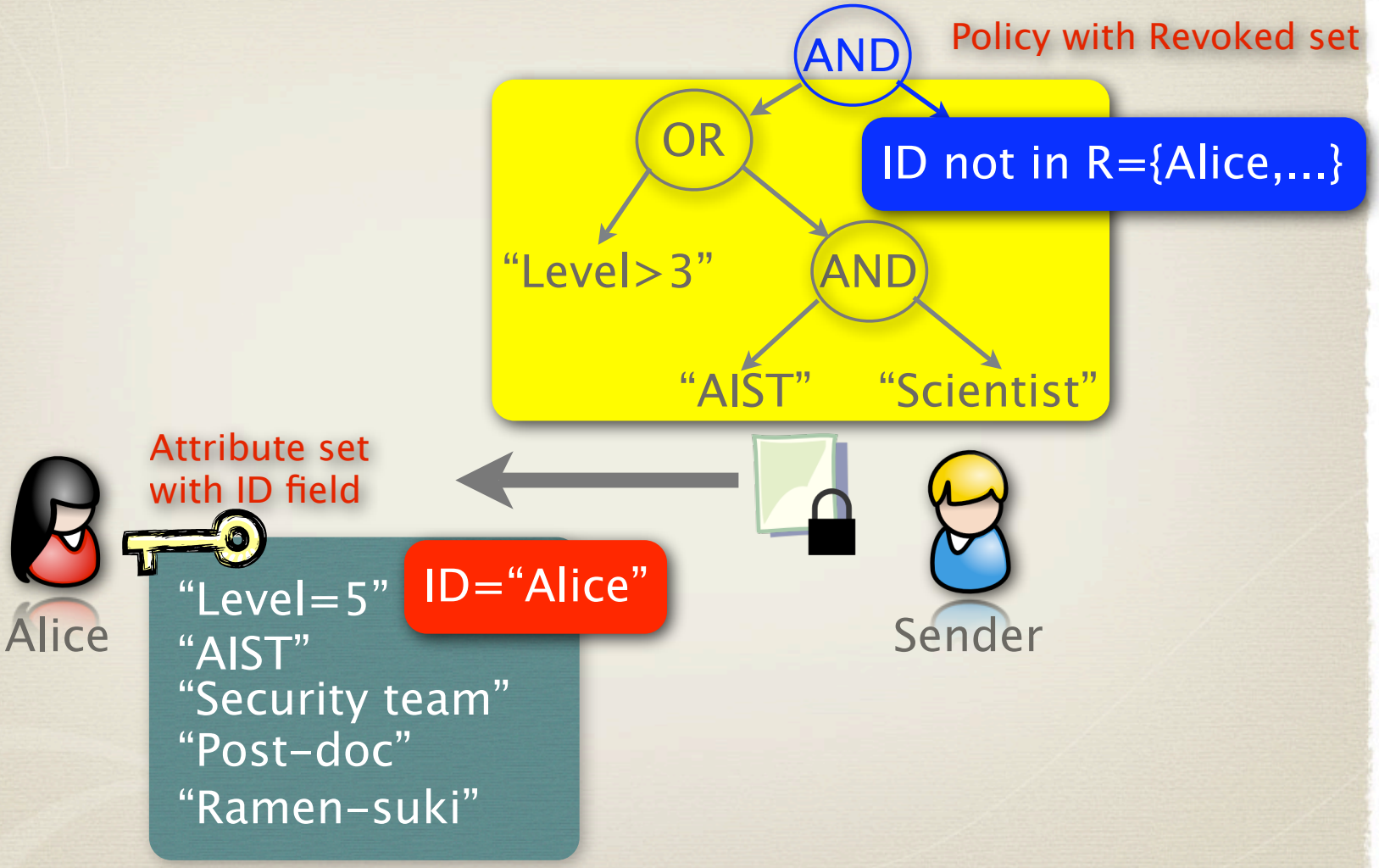
	Revocable CP-ABE	Revocable KP-ABE
Previous	[OSW07] |Cipher|= [BSW07] +r |Key|= [BSW07] · (log m)	None
This work	|Cipher|= [BSW07] +1 |Key|= [BSW07] +1	|Cipher|=[GPSW07]+1 |Key|=[GPSW07]

r=|revoked users|, m=max |attribute set|

Broadcast-Conjunctive KP-ABE

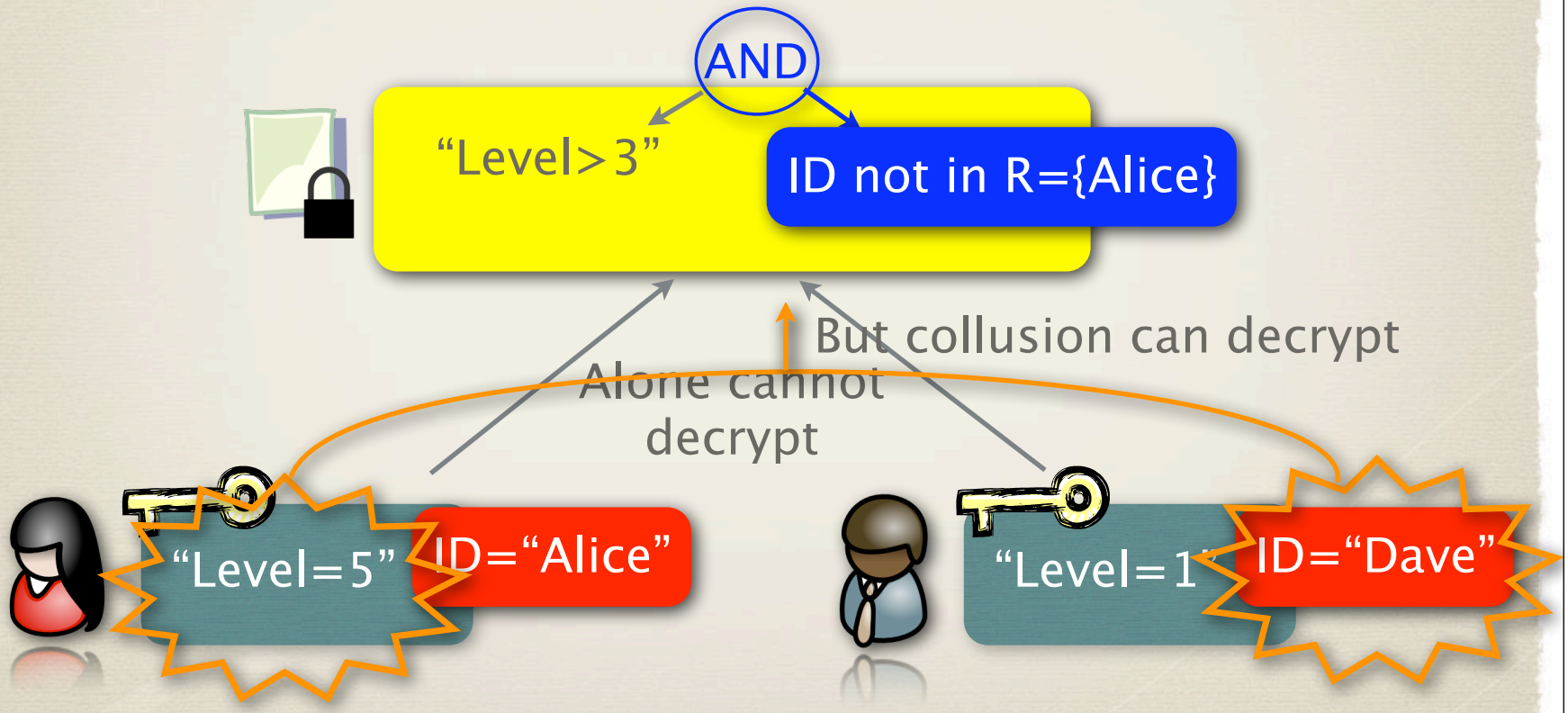


Broadcast-Conjunctive CP-ABE

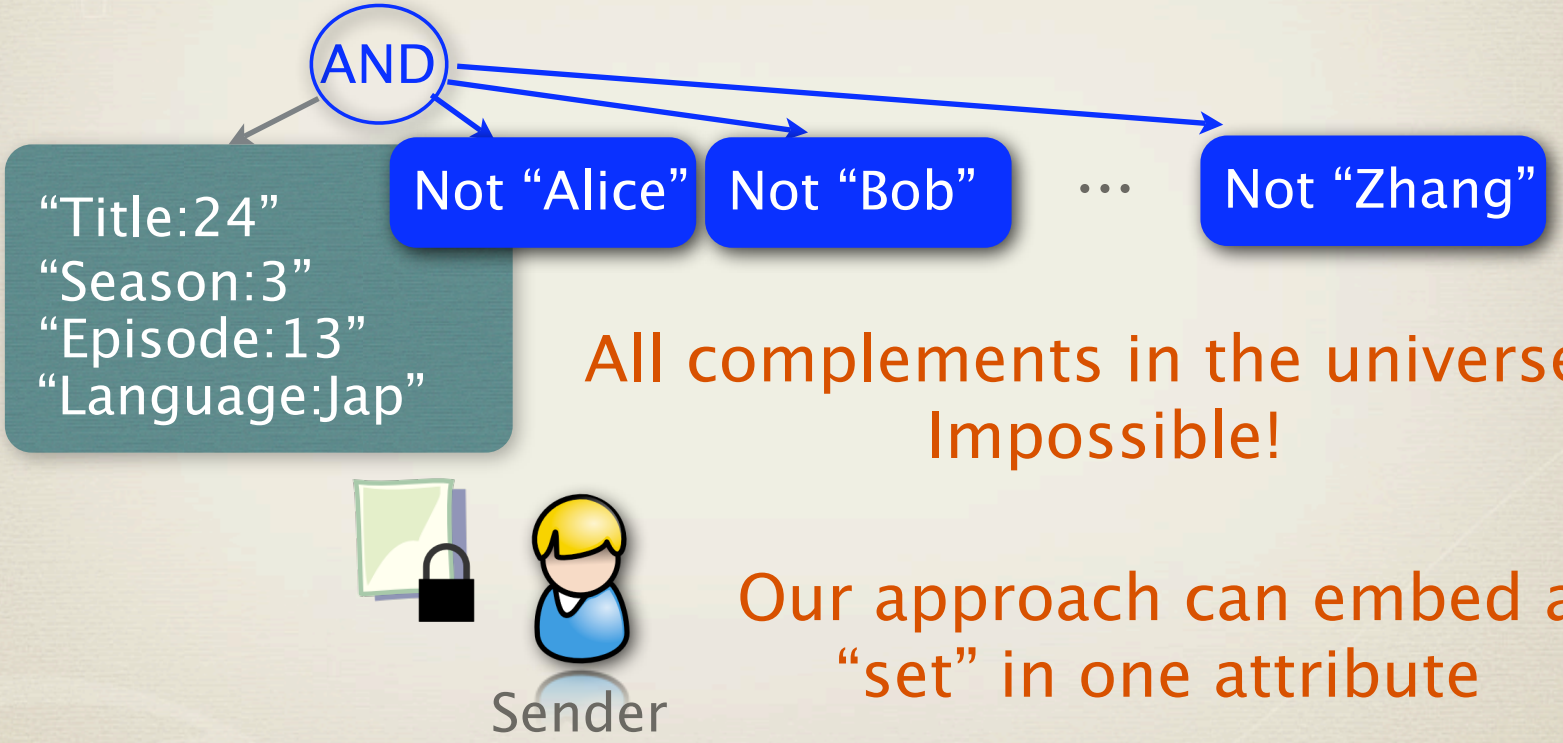


Misguided Approach 1: Double Encryption of BE&ABE

Vulnerable to "Collusion attack"



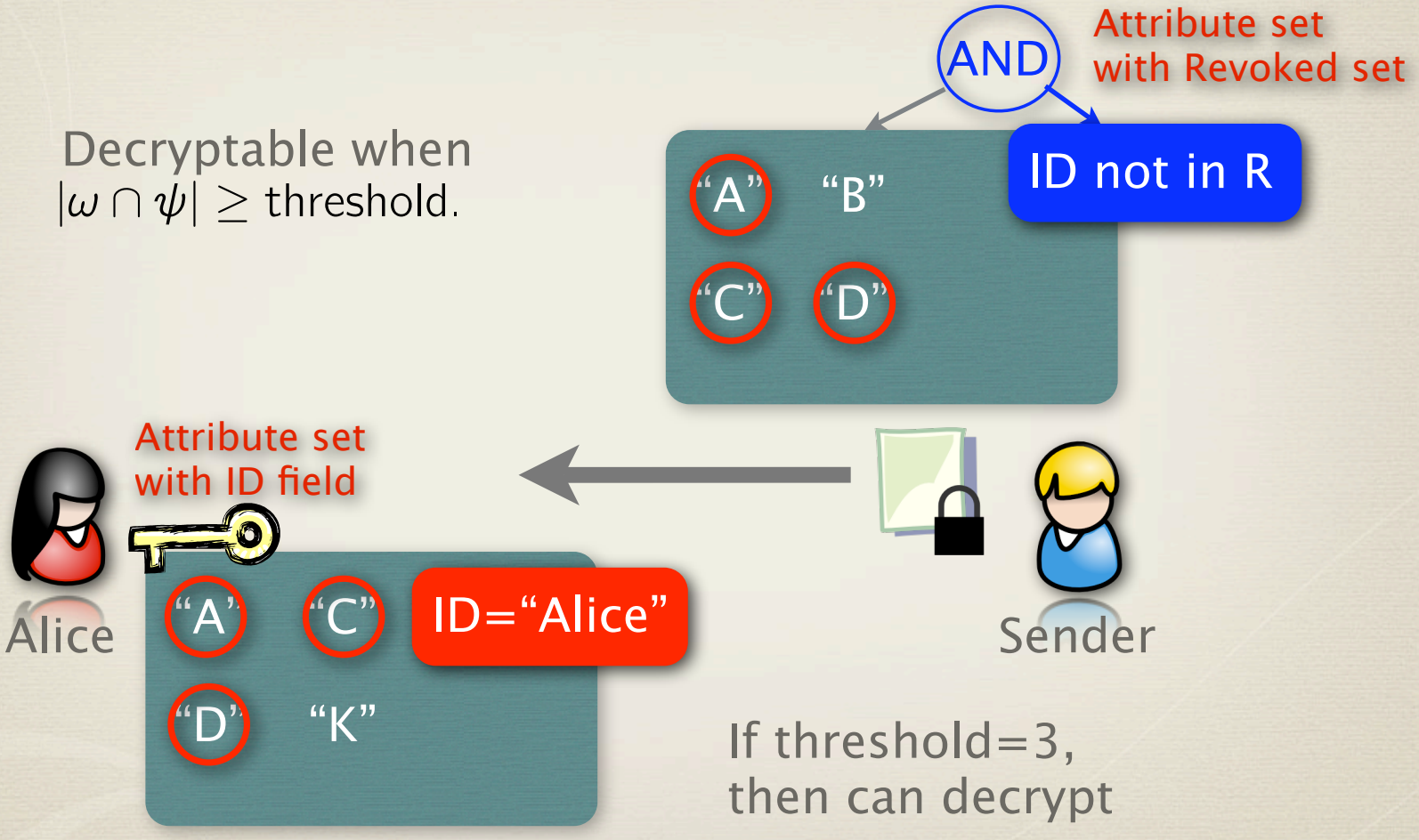
Misguided Approach 2: Include All Negative Attributes



All complements in the universe!!
Impossible!

Our approach can embed a "set" in one attribute

Special Case: Broadcast Fuzzy IBE



Construction (1/2)

Setup(n, d): Let $\mathbb{G}$ be a bilinear group of prime order p with bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. $n = |\text{users}|$, $d + 1 = \text{thres}$.
Let $g \leftarrow \mathbb{G}$ and $\alpha, \gamma, p_1, \ldots, p_d, f_1, \ldots, f_d \leftarrow \mathbb{Z}_p$.
Let $g_i = g^{(\alpha^i)}$, $v = g^{\gamma}$, $h_j = g_n{}^{p_j} g^{f_j}$.

$$\text{pk} = \Big(g, \underbrace{g_1, \ldots, g_n, g_{n+2}, \ldots, g_{2n}, v}_{BE}, \underbrace{h_1, \ldots, h_d}_{ABE} \Big) \in \mathbb{G}^{2n+d+1}.$$

Define $p(x) = p_d x^d + \cdots p_1 x + p_0$, $f(x) = f_d x^d + \cdots f_1 x + f_0$
Define $F : \mathbb{Z}_p \to \mathbb{G}$ by $F(x) = g_n{}^{p(x)} g^{f(x)} = \prod_{j=1}^{d} h_j{}^{x^j}$.

Extract(i, ω): Given $i \in \{1, \ldots, n\}$ and set ω of attributes.
For $j \in \omega$, choose $r_j \leftarrow \mathbb{Z}_p$.
Choose random poly $q(x)$ of degree d with $q(0) = \alpha^i$.

$$d_{i,\omega} = \left(\underbrace{g^{\left(\gamma \cdot q(j)\right)} \cdot F(j)^{r_j}}_{BE \otimes ABE}, \underbrace{g^{r_j}}_{ABE} \;\middle|\; j \in \omega \right) \in \mathbb{G}^{2|\omega|}.$$

Construction (2/2)

Encrypt$(\mathsf{pk}, R, \omega')$: Choose $t \leftarrow \mathbb{Z}_p$. Set KEM-key $K = e(g_n, g_1)^t$. Set

$$\mathsf{Hdr} = \left(g^t,\ \underbrace{(v \cdot \prod_{k \in \mathcal{U} \setminus R} g_{n+1-k})^t}_{BE},\ \underbrace{\left(F(j)^t \mid j \in \omega' \right)}_{ABE} \right)$$

$\in \mathbb{G}^{|\omega'|+2}$ as a header.

Decrypt$(\mathsf{pk}, i, \omega, d_{i,\omega}, R, \omega', \mathsf{Hdr})$: Decryptable if $|\omega \cap \omega'| \geq d+1$. Choose $T \in \omega \cap \omega'$ that $|T| = d+1$. Parse $d_{i,\omega} = (a_j, b_j \mid j \in \omega)$, $\mathsf{Hdr} = (C_0, C_1, (A_j \mid j \in \omega'))$. Compute

$$K = \frac{e(g_i, C_1)}{e(\prod_{\substack{k \in \mathcal{U} \setminus R \\ k \neq i}} g_{n+1-k+i},\ C_0)} \cdot \prod_{j \in T} \left(\frac{e(A_j, b_j)}{e(a_j,\ C_0)} \right)^{\Delta_{j,T}(0)}.$$

where $\Delta_{j,T}(x) = \prod_{\substack{k \in T \\ k \neq j}} \frac{(x-k)}{(j-k)}$ (Lagrange Interpolation Coef).

- Here, we formulate as KEM. In usage, ciphertext is $\mathsf{Hdr} || \mathsf{Enc}_K(\mathsf{Msg})$.

Results

	Revocable CP-ABE	Revocable KP-ABE
Previous	[OSW07] |Cipher|= [BSW07] +r |Key|= [BSW07] · (log m)	None
This work	|Cipher|= [BSW07] +1 |Key|= [BSW07] +1	|Cipher|=[GPSW07]+1 |Key|=[GPSW07]

- Selective security in the standard model under Decision BDHE assumption [BGW05].
- Drawback: large public key (as in [BGW05]-BE). But can be reused for all instances.

Conclusions

- Attribute-based encryption can be used as a flexible access control tool over encrypted data
  - Applications: Secure remote file sharing, Flexible Pay-TV system, etc.
- For Key-policy ABE, we propose the first revocable scheme ever.
- For Ciphertext-policy ABE, we propose a revocable scheme which is much more efficient than [OSW07].

Thank you!

Disclaimer: This presentation was originally created using Apple iWork'08 Keynote and then converted to PDF. The font and some structures may seem strange.