An Integrated Privacy Preserving Attribute Based Access Control Framework

Runhua Xu & James Joshi

University of Pittsburgh

runhua.xu@pitt.edu

Cloud Storage

Top Cloud Storage Providers

Google Cloud

Amazon Web Service

Microsoft Azure…

Take MS Azure as an Example

2012, 4 Trillion Objects

2015 Jan, 10 Trillion Objects

Source: https://www.nasuni.com/infographic-2015-state-of-cloud-storage/

Cloud Storage

Recent advances have enabled applications that generate/collect *huge amounts of personal data*.

Cloud Storage Providers

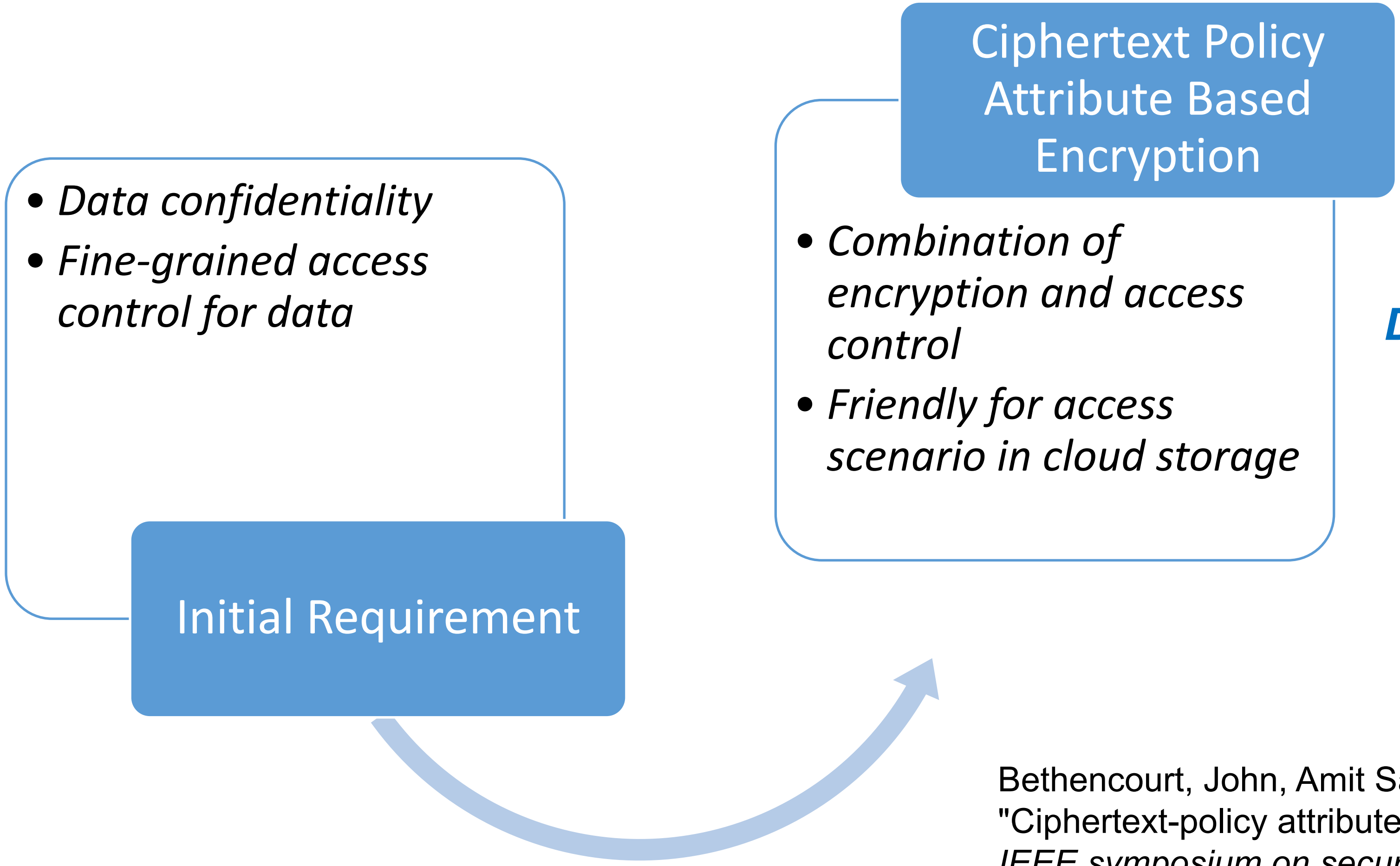
Honest-but-Curious

-- run the programs and algorithms correctly
but gather information related to the stored data and access records.

Gartner, Inc. is the world's leading information technology research and advisory company.

Security & Privacy Concerns: Personal Data / Sensitive Data

Initial Solution



Data : self-protection

Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." *2007 IEEE symposium on security and privacy (S&P'07)*. IEEE, 2007.

Scenario

A patient-centric health application

-- that allows a patient/user to store and manage all his Electronic Health Records (EHRs) by storing them in Cloud Storage

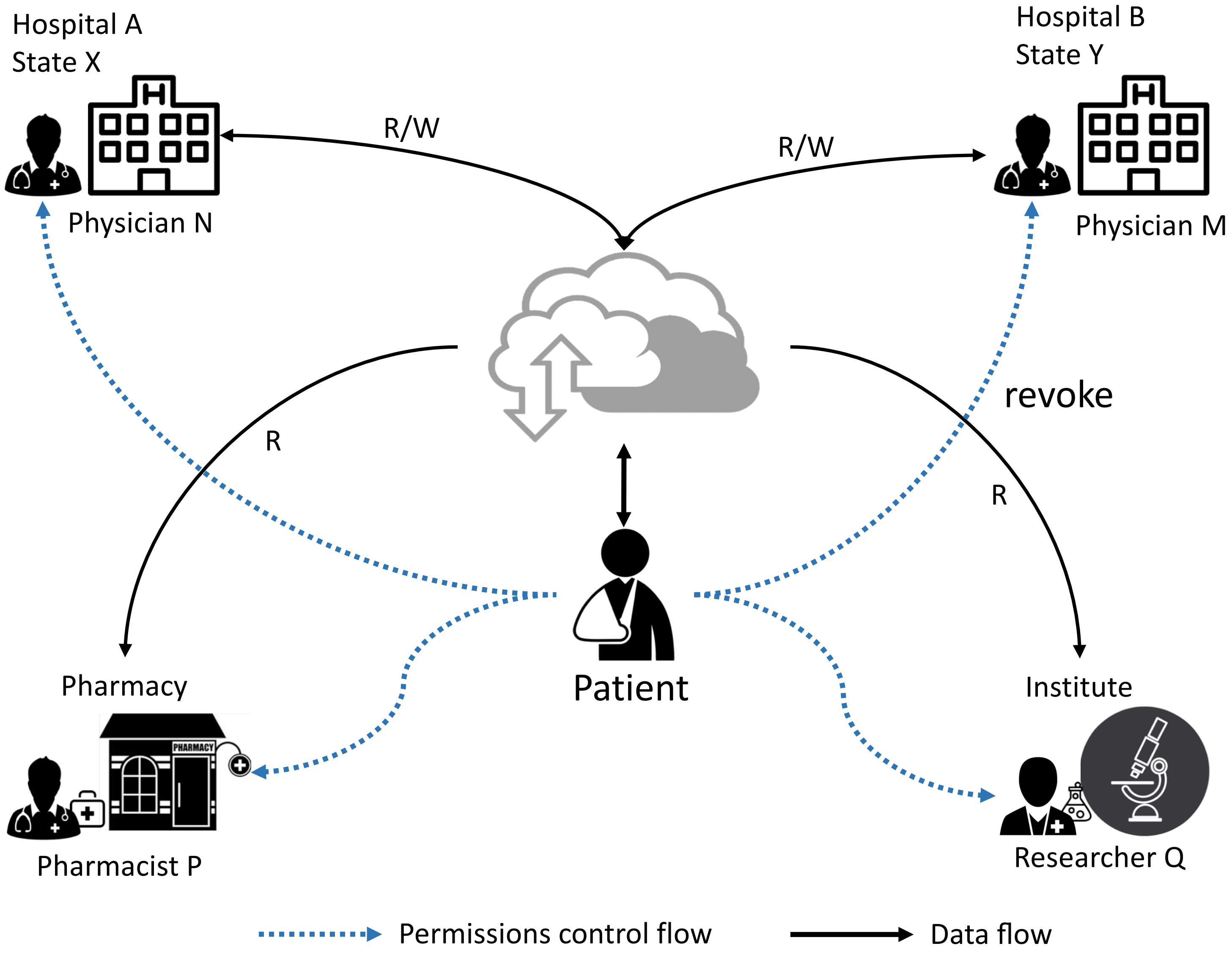
Similar scenarios:

User-centric applications

Organization-centric applications

Hospital-centric applications

How to protect user-sensitive data in the public cloud ?



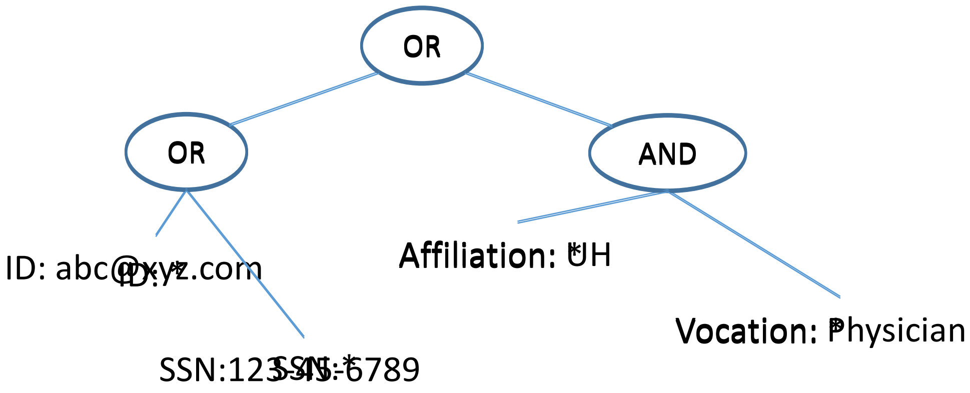
Challenges

- Challenges of applying CP-ABE to the Scenarios
  - *Support both revocation and privacy-preserving policy*
  - *Limitation of all CP-ABE schemes*
    - Only support read access
    - But don’t support write access & policy update
  - *Access patterns leak*
    - Data is protected by encryption, it doesn’t matter ?
      - E.g., encrypted data in the cloud, which is often accessed from hospitals, may be identified as EHRs, then link to a specific patient.

Social engineering
Enough time
Powerful machine

The key contributions

- A privacy-preserving revocable CP-ABE scheme (PR-CP-ABE)
  - *Privacy-preserving Access Structure*
    - Linear Secret Sharing Scheme (LSSS)
  - *Supports immediate attribute revocation*



(ID: abc@xyz.com OR *SSN: 123-45-6789)* OR
(Affiliation: University Hospital AND *Vocation: Physician)*

*(ID: ** OR *SSN: *)* OR *(Affiliation: ** AND *Vocation: *)*

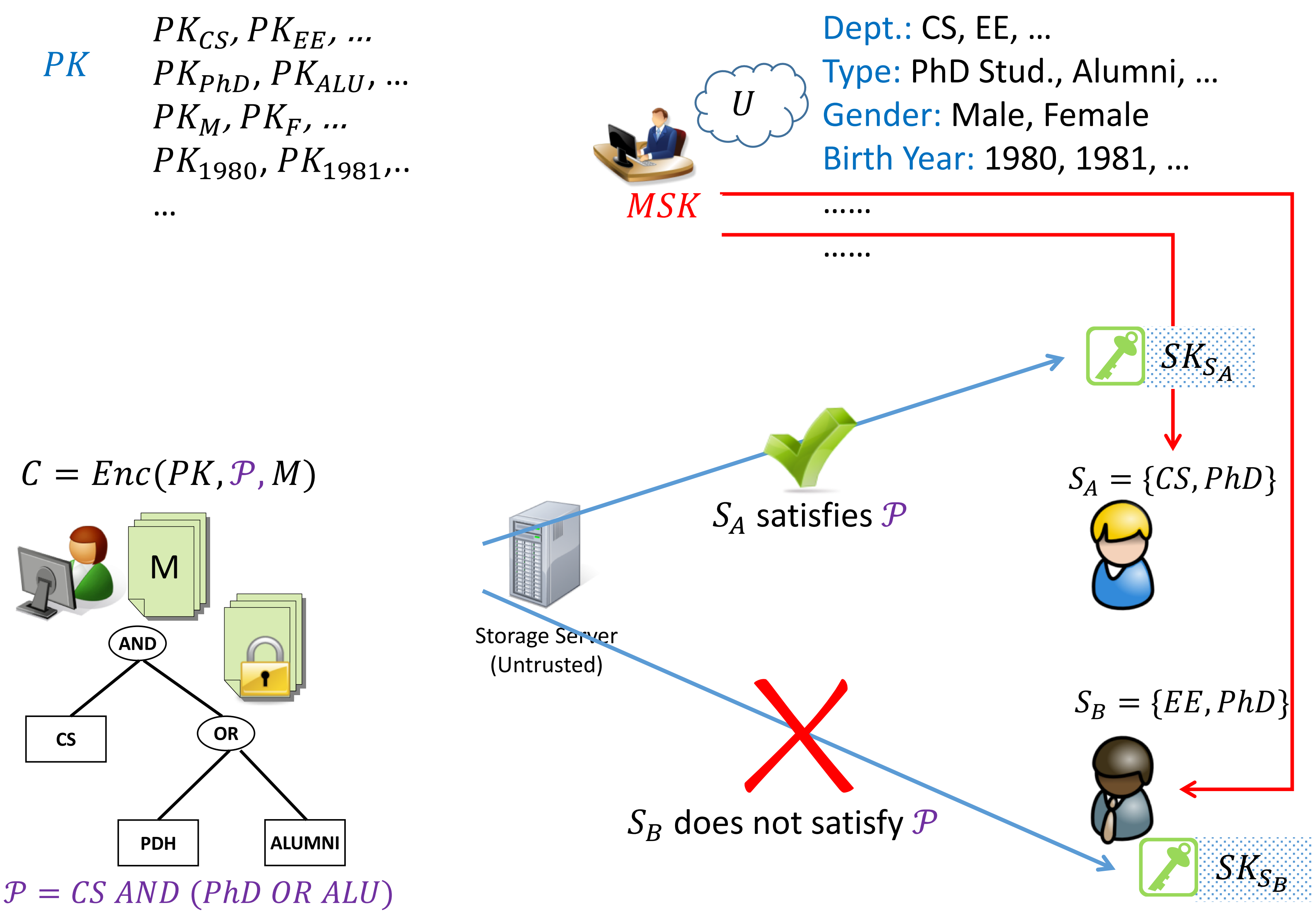
The key contributions

- An extended path oblivious RAM (ePath-ORAM) protocol
  - *Prevents privacy disclosure of access patterns*
  - *Supports data/policy update*
- Security proof of the PR-CP-ABE scheme

Preliminaries: What's CP-ABE

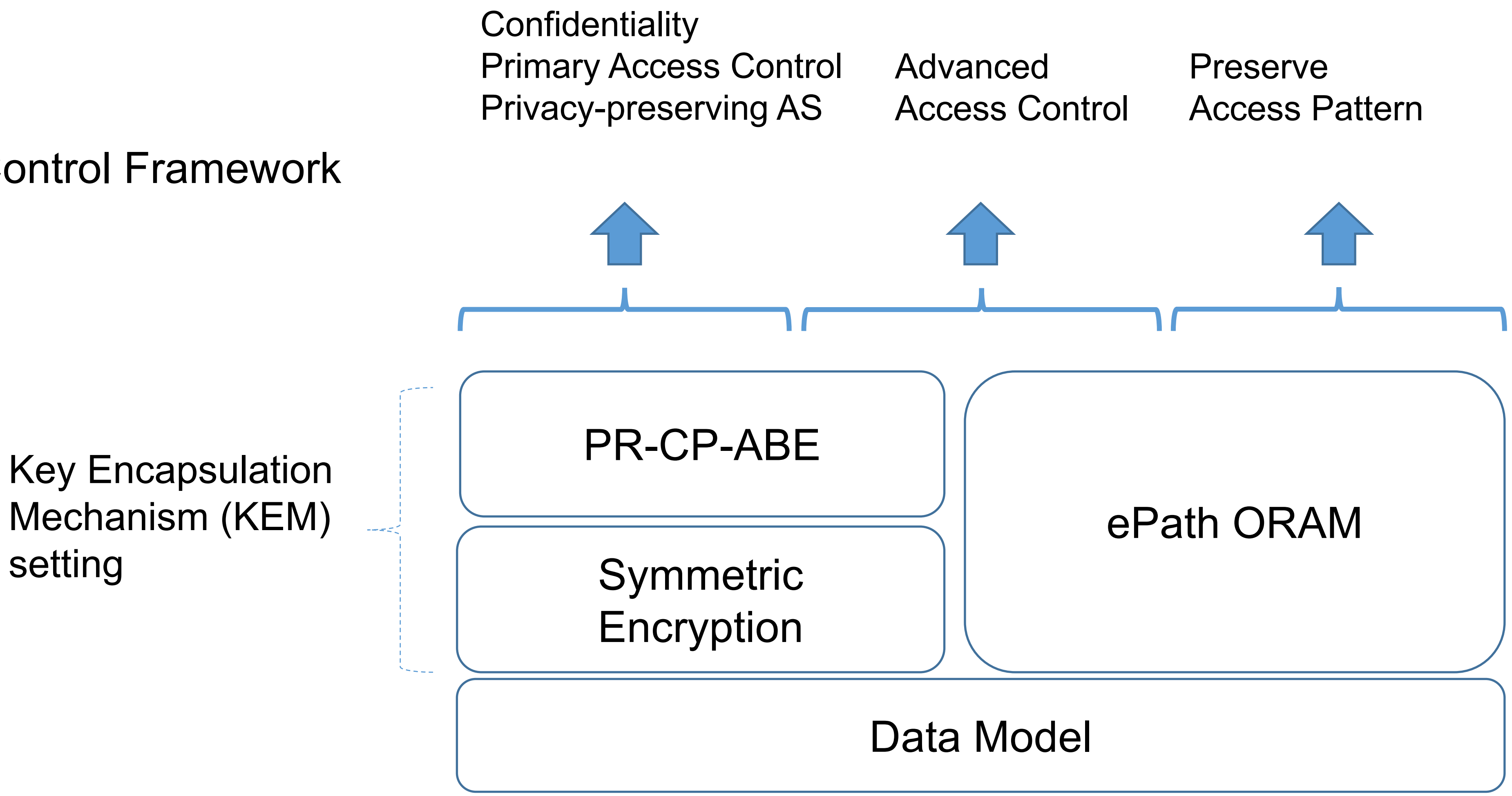
Slide from ESORICS

CP-ABE in detail



Overview

of Access Control Framework



Data Model

$$\mathcal{D} = (id, \mathcal{P}_r, \mathcal{P}_w, \mathcal{P}_o, Enc_{k_\delta}(data)),$$

where

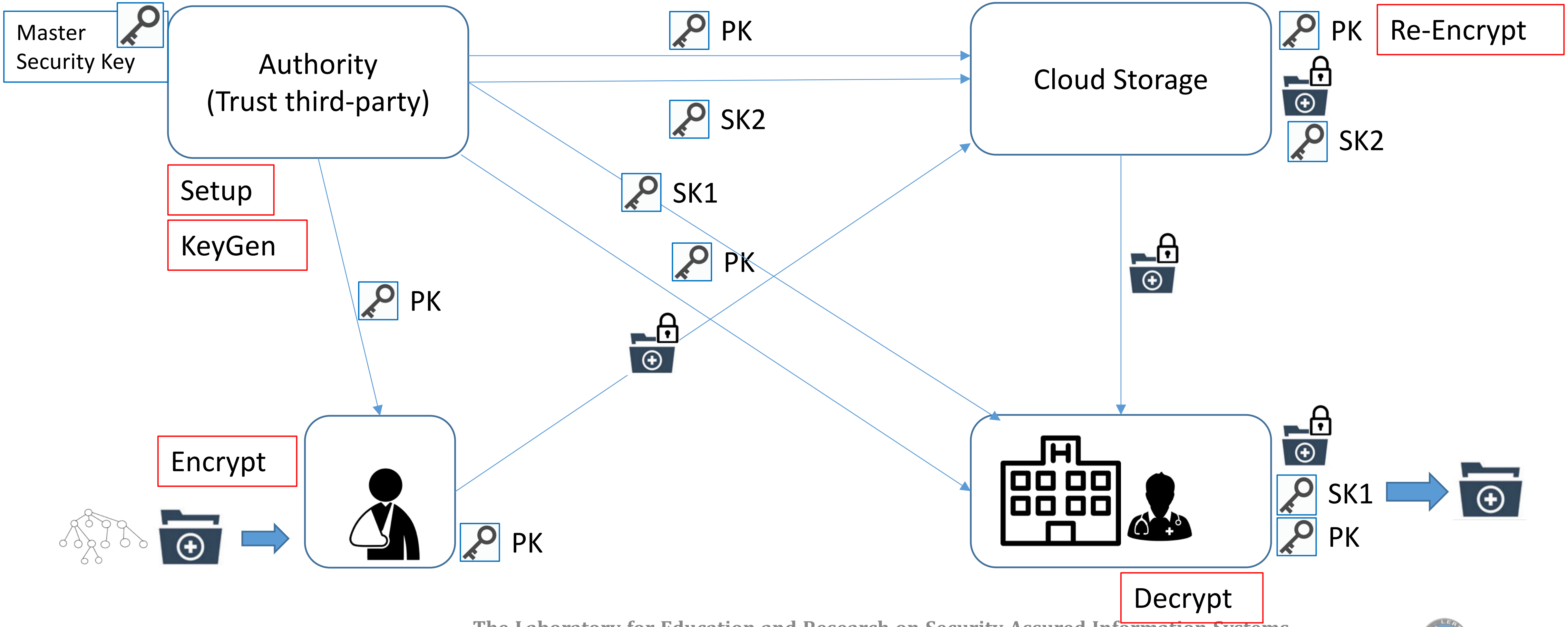
$$\mathcal{P}_r = (< A_r, \rho_r >, Enc_\gamma(k_\delta)),$$
$$\mathcal{P}_w = (< A_w, \rho_w >, Enc_\gamma(s_w), s_w),$$
$$\mathcal{P}_o = (< A_o, \rho_o >, Enc_\gamma(s_o), s_o).$$

Encrypted data under KEM setting

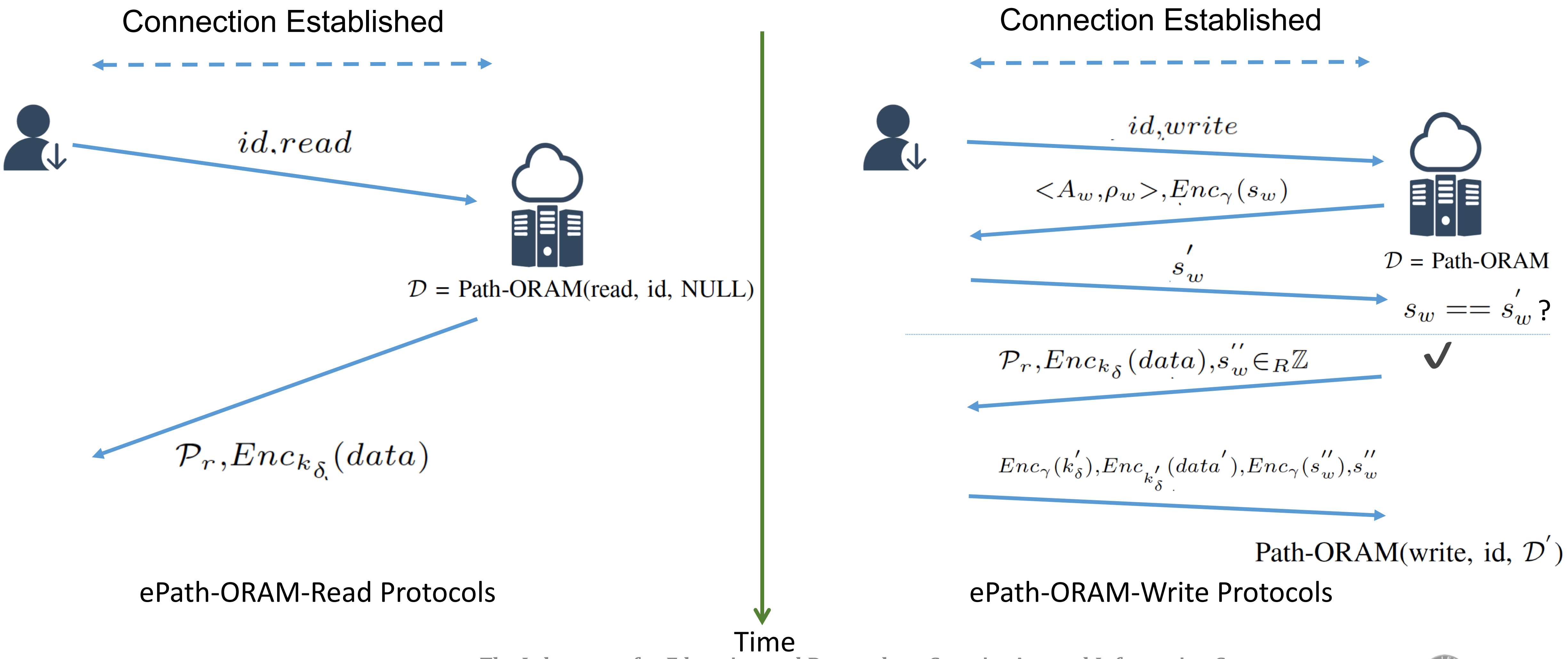
Used to verify a user's write permission
By checking decryption ability on a random seed

Three access structure (hide value)

Instance of PR-CP-ABE



ePath ORAM Protocols



Analysis

- Tricks behind PR-CP-ABE construction
  - *Composite Order Bilinear Groups*
    - Introduce random elements from a subgroup into algorithms to perturb/hide ciphtertext components ←→ attributes
    - Use the property to eliminate random elements

$$\left\{\begin{array}{l} h_r \in \mathbb{G}_r \\ h_p \in \mathbb{G}_p \end{array}\right. \Rightarrow e(h_r, h_p) = 1$$

  - *Re-encrypt technology*
    - Divide the initial secret element $\alpha = \alpha_1 + \alpha_2$
    - One is corresponding to user, the other is for delegation (CSP)

Analysis

- Forward Security
  - *Protects past ciphertext against future compromises of secret keys.*
  - *If attribute is revoked*
    - Users can not update the corresponding private key
    - Thus they can not decrypt again
- Backward Security
  - *A new user joins in an attribute group that satisfies the policy*
  - *Suppose he has a previous ciphtertext*
  - *Even if he can update private key, he can not decrypt it*
    - Random elements in previous component D' ←X→ new user's private key

Analysis

- Key features

Table 1: Comparison of key features

Schemes	Access Structure (AS)	Immediate Revocation	Privacy-preserving AS
[39]	LSSS Matrix	Yes	No
[38]	And-gate	Yes	No
[15]	Tree-based	Yes	No
[20]	LSSS Matrix	No	Yes
[23]	And-gate	No	Yes
Ours	LSSS Matrix	Yes	Yes

Analysis

- Performance
  - *As shown in previous experiments.*
    - Encryption/decryption → milliseconds level
    - Key Application (network communication) → seconds level

Table 2: Comparison of communication cost

Entities	Our scheme	[39]	[38]	[15]
Authority ↔ User	$(2+n_{a,i})\|g\|$	$(2+n_{a,i})\|g\|$	$(1+2n_{a,i})\|g\|$	$(1+2n_{a,i})\|g\|$
Authority ↔ Owner	$(2+n)\|g\|+\|g_T\|$	$2\|g\|+\|g_T\|$	$(1+3n_{a,i})\|g\|+\|g_T\|$	$2\|g\|+\|g_T\|$
CSP ↔ User	$(4l+3)\|g\|+2\|g_T\|$	$(2l+3)\|g\|+\|g_T\|+l\|p\|$	$(3l+2n_{a,i})\|g\|+\|g_T\|$	$(3l+2n_{a,i})\|g\|+\|g_T\|$ $+(l/2\times\|n_u\|+log(n_u+1))\|p\|$
CSP ↔ Owner	$2((2l+1)\|g\|+\|g_T\|)$	$(2l+1)\|g\|+\|g_T\|$	$3l\|g\|+\|g_T\|$	$2l\|g\|+(l+1)\|g_T\|$

[1] $|p|$, $|g|$ and $|g_T|$ are the elements size in $\mathbb{Z}_p, \mathbb{G}$ and $\mathbb{G}_T$, respectively.
[2] $n_{a,i}$ is the number of attributes that the user i possess.
[3] l represents the number of attributes associated with the ciphertext.

Our scheme makes a compromise on performance for privacy-preserving policy, compared with [39]
However, our scheme's performance is better than others

Security Proof

- Methodology
  - *Suppose that adversary has advantage to break our scheme*
  - *Adversary's advantage ←→ break q-parallel BDHE assumption*
  - *However, no-polynomial time algorithm has advantage to break assumption*
  - *Thus no adversary has advantage to break our scheme*

Please find the detail proof in Appendix.

Conclusion

- A novel privacy-preserving attribute-based access control framework
  - *PR-CP-ABE*
    - Privacy-preserving
    - Revocation
    - Security Proof: CPA
  - *ePath-ORAM Protocol*
    - Preserve access pattern
    - Extend PR-CP-ABE to support r/w/o access
  - *Features*
    - User-centric data and policy management
    - Immediate privilege revocation
    - Privacy protection

Q & A

Thanks