Registered Identity-Based Expressive Asymmetric Searchable Encryption

Jiaming Yuan
Center for Cyber Security and Privacy
UNIVERSITY OF OREGON

Introduction

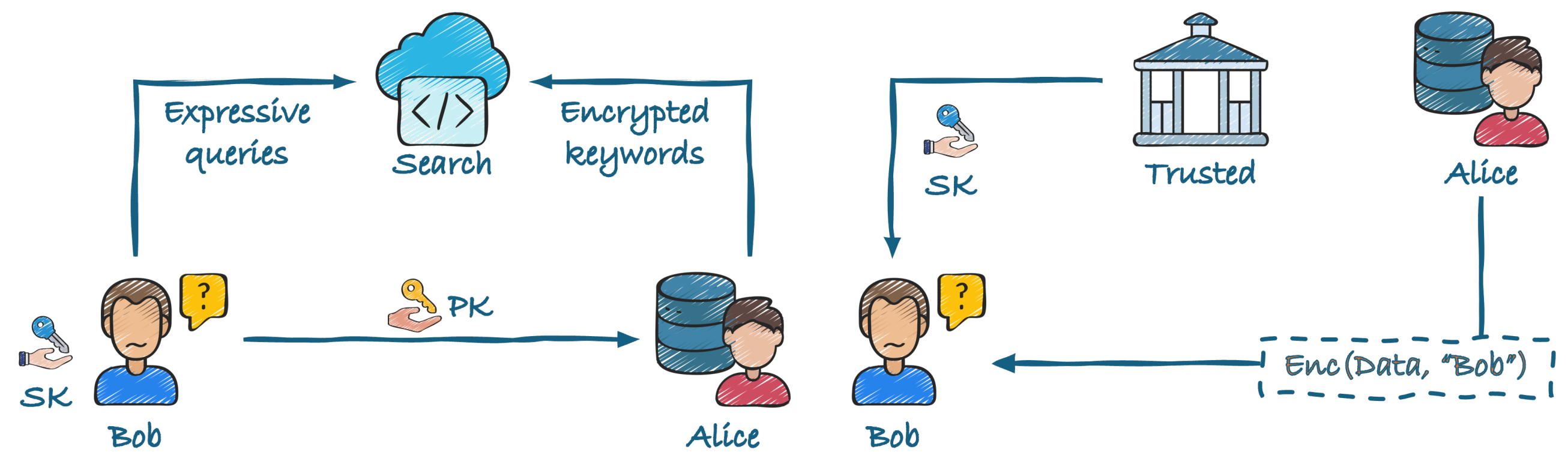
Registered Identity-Based Expressive Asymmetric Searchable Encryption (RIBEASE) enables inquirers to outsource expressive queries to a semi-trusted cloud server over encrypted data shared by data owners.

- RIBEASE supports expressive queries that are conjunctive, disjunctive or any monotonic boolean formulas.
- It employs Identity-Based Encryption (IBE), wherein data is encrypted using users' *identities* rather than public keys, thereby eliminating *public key distribution overhead*.
- A semi-trusted key curator is introduced to register users' identities and their public keys, effectively mitigating the *key escrow problem* inherent from IBE.

Related Work

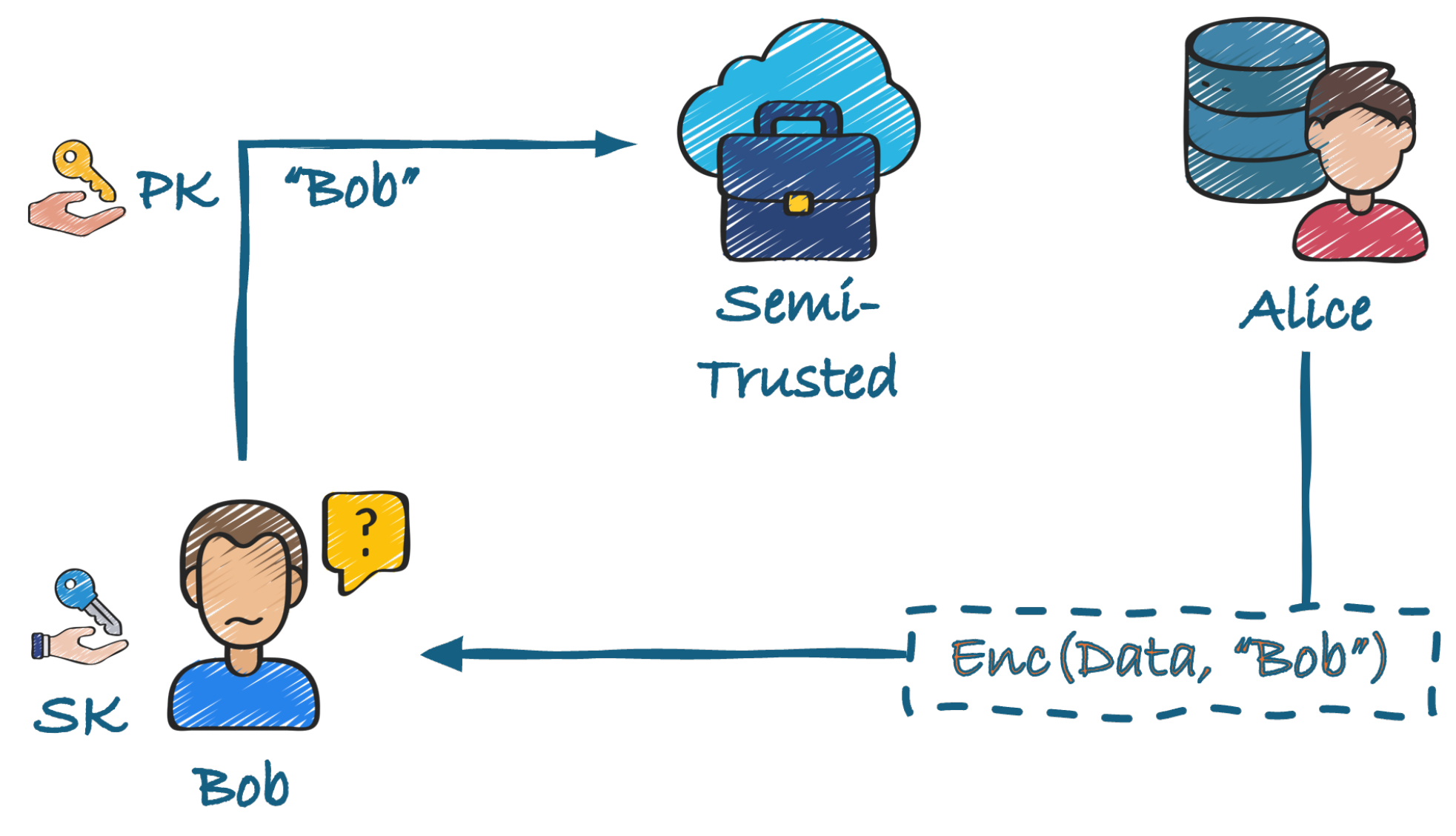
Existing Expressive Asymmetric Searchable Encryption (EASE) suffers from significant public key distribution overhead, as data owners must encrypt data using the inquirers' public keys.

IBE addresses this overhead by allowing encryption directly with users' identities, thereby eliminating the need for public key distribution. However, IBE requires a fully trusted third party to issue secret keys to inquirers, which introduces the well-known key escrow problem.



(a) Expressive Asymmetric Searchable Encryption (b) Identity-Based Encryption

Registration-Based Encryption (RBE) extends the IBE framework by introducing a registered encryption model to mitigate the key escrow problem. It replaces the fully trusted third party with a semi-trusted key curator, who manages user registrations instead of issuing secret keys directly.

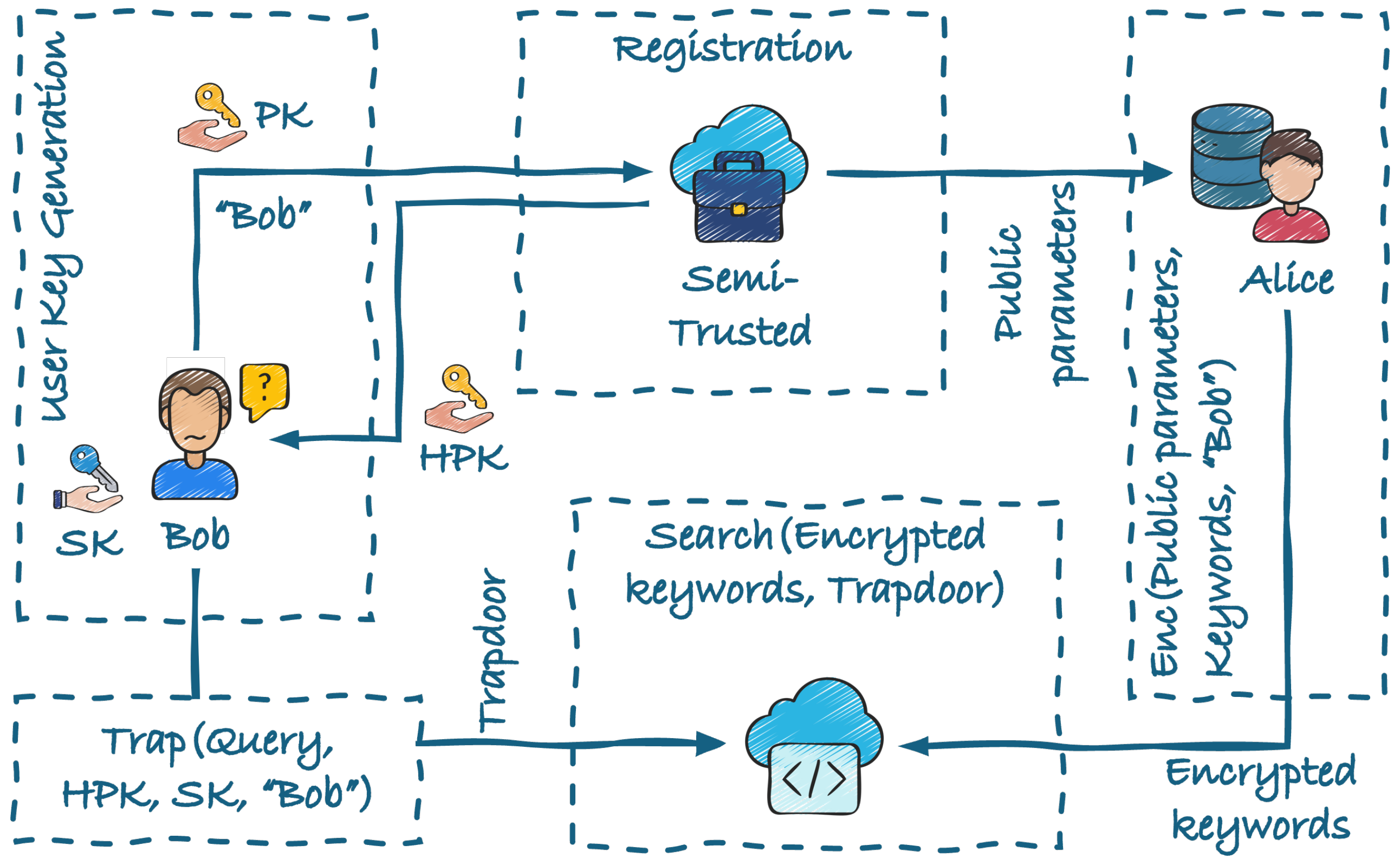


Registration-Based Encryption

Challenges

- Designing an efficient Identity-Based Expressive Searchable Encryption (IBESE) scheme remains a non-trivial task due to the complexity of supporting expressive queries under identity-based settings.
- Extending IBESE to RIBESE further increases the complexity, requiring secure and scalable identity registration without relying on fully trusted authorities.
- Asymmetric Searchable Encryption schemes are vulnerable to Keyword Guessing Attacks (KGA). Effectively and efficiently mitigating KGA within the RIBESE framework poses a significant security challenge.

Registered Identity-Based Expressive Asymmetric Searchable Encryption



RIBEASE Framework

Setup Phase

- **System Setup:** A one-time fully trusted setup process generates public parameters, which are shared with all entities throughout the system's lifetime.
- **User Key Generation:** Bob (inquirer) locally generates a public/secret key pair.
- **User Registration:** Bob submits his public key and identity to the semi-trusted key curator, which aggregates the identity and public key into the public parameters.
- **Key Update:** Bob derives a helper key from the public parameters using his identity and keeps it up to date for secure trapdoor generation.

Query Phase

- **Data Encryption:** Alice (data owner) encrypts a set of keywords using Bob's identity and public parameters, then uploads the ciphertext to the cloud server.
- **Trapdoor Generation:** Bob uses his secret key, helper key, and identity to create a trapdoor for an expressive query and sends it to the cloud server.
- **Search:** The server uses the received ciphertext from Alice and the trapdoor from Bob to run a search algorithm that determines whether they match. It returns true if (1) the identities associated with the ciphertext and the trapdoor match, and (2) the query embedded in the trapdoor matches the keywords embedded in the ciphertext; otherwise, it returns false.

As long as each ciphertext is linked to its associated encrypted document or data entry in practice, RIBEASE can provide full search functionality over the encrypted content.

Methodology

We first construct an efficient IBEASE scheme by combining an EASE scheme [3] with an efficient IBE scheme [1]. We then transform IBEASE into RIBEASE by replacing IBE components with corrsponding RBE counterparts [2]. RIBEASE must satisfy the following requirements:

- **Compactness and efficiency:** Public parameters and helper keys remain compact and efficiently updatable, ideally growing only poly-logarithmically with the number of registered users.
- **Ciphertext indistinguishability:** Ciphertexts reveal no information about the encrypted keywords.
- **Trapdoor indistinguishability:** Trapdoors leak no information about query keywords.

KGA Defense. To resist Key Guessing Attacks (KGAs), we employ the matchmaking encryption (ME) primitive to enable mutual authentication between the inquirer and the data owner. Initially, only the intended inquirer can generate valid trapdoors. By integrating authentication into the trapdoor generation process, RIBEASE further ensures that only the intended data owner can produce ciphertexts accepted by those trapdoors. As a result, adversaries cannot craft valid ciphertexts to test trapdoors and infer the underlying queries.

Results

The registration requires $\mathcal{O}(\sqrt{n})$ computation. Trapdoor generation and decryption require $\mathcal{O}(|\text{Query}|)$, while encryption costs $\mathcal{O}(|\text{Kws}|)$. We are continuing our experimental evaluation of the system's performance.

The proposed RIBEASE scheme incurs the following sizes (in group elements): $2\sqrt{n}$ in the public parameters, $\sqrt{n}$ in the helper key, $|\text{Query}| + 2 + 4 \times \max(|\text{KwOccur}|)$ in the trapdoor, and $5|\text{Kws}| + 3$ in the ciphertext.

References

[1] Dan Boneh and Matt Franklin.
Identity-based encryption from the weil pairing.
In *Crypto*. Springer, 2001.

[2] Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, and Ahmadreza Rahimi.
Efficient registration-based encryption.
In *CCS*, 2023.

[3] Long Meng, Liqun Chen, Yangguang Tian, Mark Manulis, and Suhui Liu.
FEASE: Fast and expressive asymmetric searchable encryption.
In *USENIX Security*, 2024.

https://uoregongo.github.io/

UO-CS Graduate Research Open House 2025, May 28