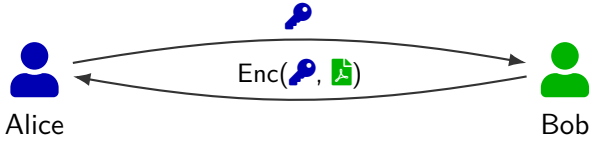
# Scalable Registration-Based Encryption from Lattices

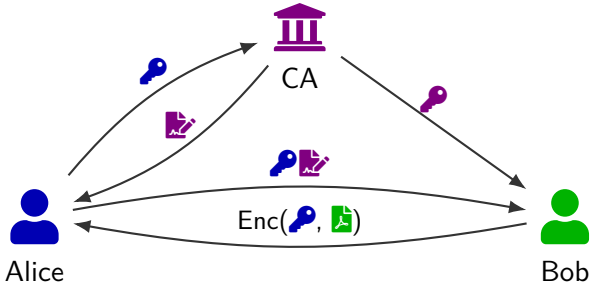
**Michael Klooß[1], Russell W. F. Lai[2], Jan Niklas Siemer[3], Monisha Swarnakar[2]**
[1]Karlsruhe Institute of Technology & KASTEL Security Research Labs
[2]Aalto University
[3]King's College London
May 20, 2026



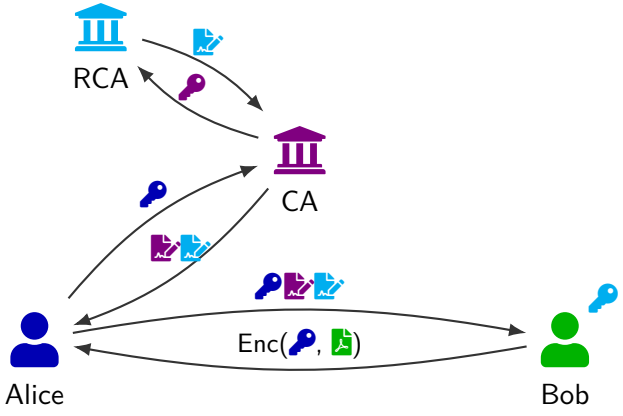
# PKI based on Public-Key Encryption



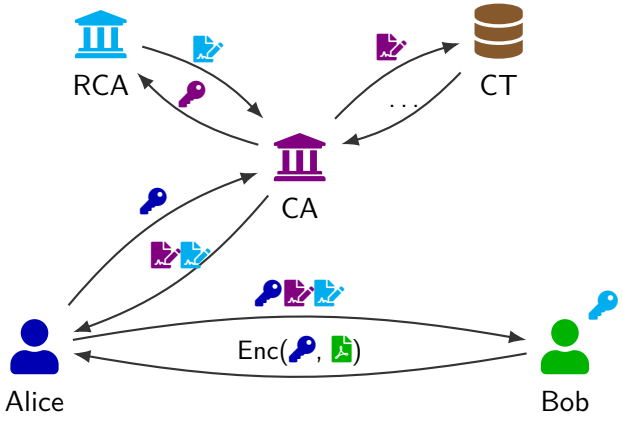
# PKI based on Public-Key Encryption



# PKI based on Public-Key Encryption



# PKI based on Public-Key Encryption



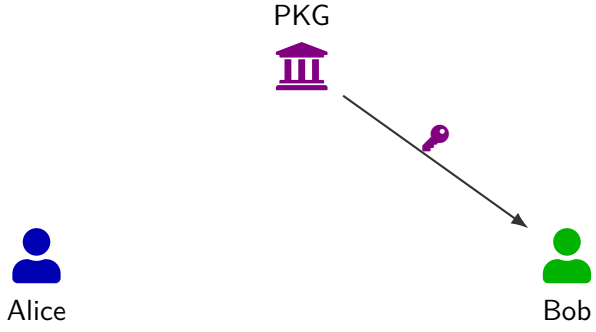
# PKI based on Identity-Based Encryption [Sha84]

PKG

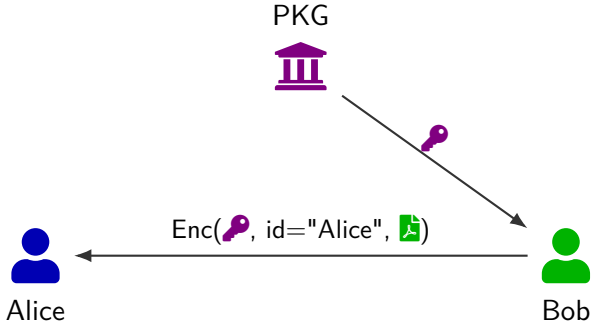
Alice

Bob

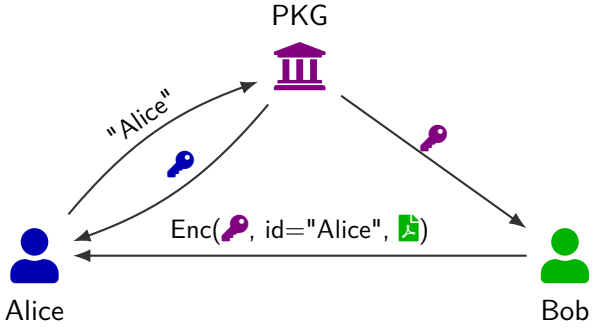
# PKI based on Identity-Based Encryption [Sha84]



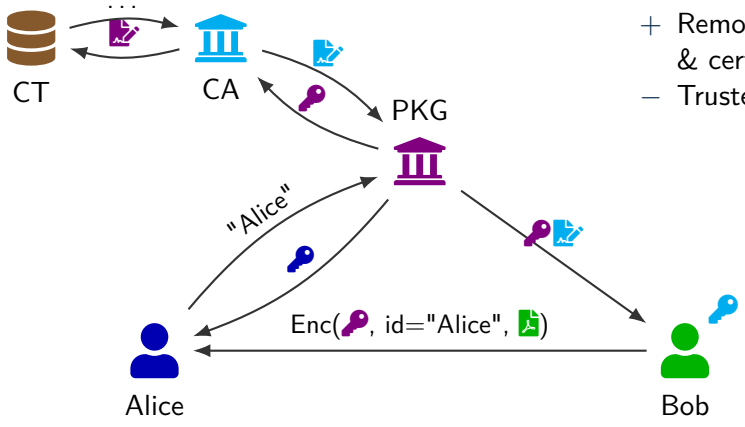
# PKI based on Identity-Based Encryption [Sha84]



# PKI based on Identity-Based Encryption [Sha84]

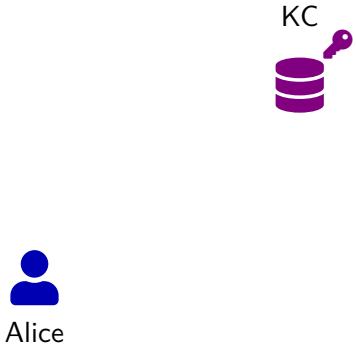


# PKI based on Identity-Based Encryption [Sha84]

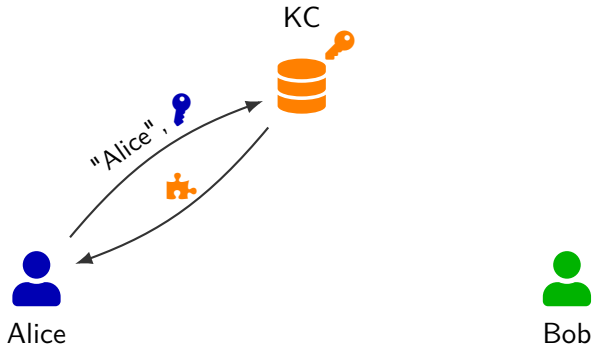



+ Removes individual keys & certificates
− Trusted PKG

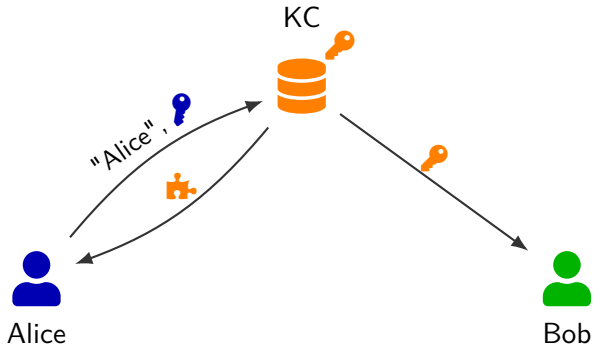
# PKI based on Registration-Based Encryption [GHMR18]



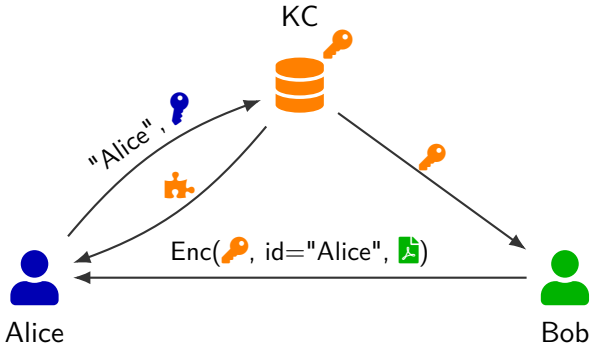
# PKI based on Registration-Based Encryption [GHMR18]



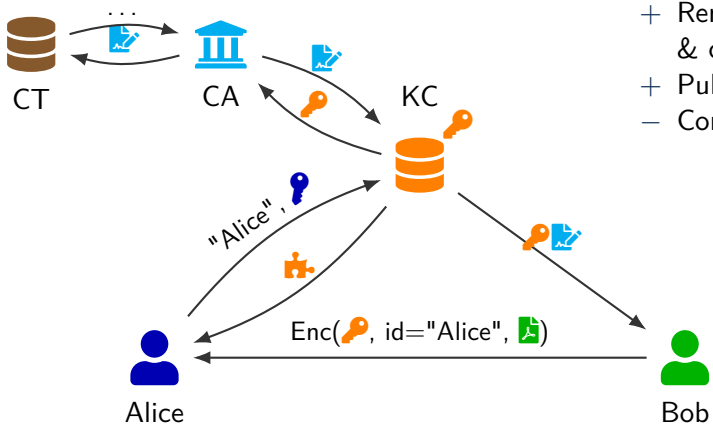
# PKI based on Registration-Based Encryption [GHMR18]



# PKI based on Registration-Based Encryption [GHMR18]



# PKI based on Registration-Based Encryption [GHMR18]




+ Removes individual keys & certificates
+ Publically auditable KC
− Communication overhead

# Constructing an RBE

Generic compiler: Derive RBE from multi-instance of Laconic Encryption (LE)

**Recipe to Construct Laconic Encryption**

Ingredients

- Vector Commitment (VC)
- Public-Key Encryption (PKE)

Instructions

- Enter public key of id in the id-th entry of VC
- Encrypt with respect to that entry

$\Rightarrow$ Decryption works only with corr. opening and secret key of corr. entry

# Our Work

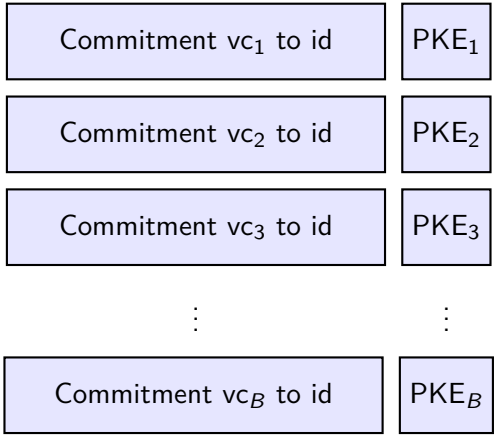
# Foundation

Build on DKLLMR scheme [DKL+23]

+ Security based on SIS and LWE
+ Transparent setup
+ Naturally extends to support arbitrary identity spaces
+ Only known post-quantum construction
− Ciphertext size of 7.2 GB for our setting

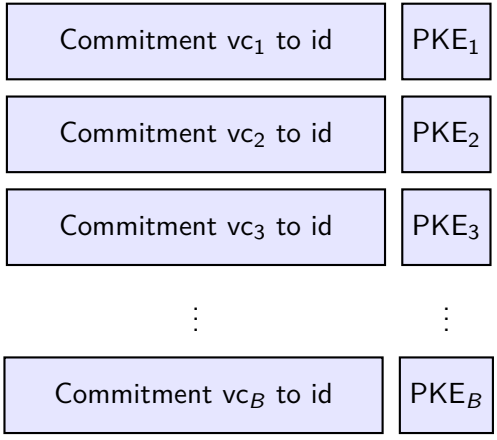
# Optimisation 1: Batching Parts of Ciphertext

**Shape of Ciphertext**

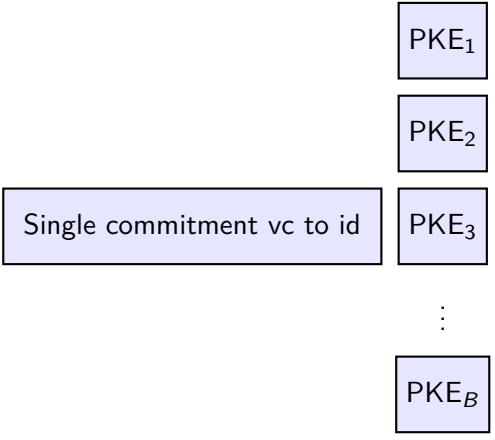


# Optimisation 1: Batching Parts of Ciphertext

**Shape of Ciphertext**




**Batch Commitments to same** id by sharing randomness across LE instances



# Further Optimisations

2. Remove lower-order bits of ciphertext
3. Replace statistical arguments in security proof by computational ones
4. Utilise approximate gadget matrices rather than exact ones

$\Rightarrow$ Ciphertext size of 7.0 MB for 128-bit security

# Further Optimisations

2. Remove lower-order bits of ciphertext
3. Replace statistical arguments in security proof by computational ones
4. Utilise approximate gadget matrices rather than exact ones

$\Rightarrow$ Ciphertext size of 7.0 MB for 128-bit security

- Scalable: Increase number of users to $2^{128}$ $\Rightarrow$ Ciphertext size of 7.1 MB

# Practical Confirmation of Approach

Practical confirmation via open-source prototype in Rust

Further practical optimisations

- Hardware-accelerated NTT multiplication
- Optimised memory layout of registry, minimising numbers of NTT transforms
- Multi-Threading of Enc

| | | Time (milliseconds) | | | | | |
|---|---|---|---|---|---|---|---|
| | $\varphi$ | Setup | KeyGen | Upd | Enc | WGen | Dec |
| Ours | 256 | 9.98 | 0.12 | 33.24 | 15.56 | 3.38 | 10.43 |

Table: Benchmarks for RBE schemes in comparison.

## Closing Remarks

**Open Problem**

- Ciphertext size is dominated by length of identity due to choice of VC

$\Rightarrow$ Replace VC by more succinct VC

## Closing Remarks

**Open Problem**

- Ciphertext size is dominated by length of identity due to choice of VC

$\Rightarrow$ Replace VC by more succinct VC

**Thanks for your Attention!**

**Paper**

https://ia.cr/2026/717

**Implementation**

jnsiemer/scalable_rbe_prototype

# Main References



Nico Döttling, Dimitris Kolonelos, Russell WF Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi.
Efficient laconic cryptography from learning with errors.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 417–446. Springer, 2023.


Dario Fiore, Dimitris Kolonelos, and Paola de Perthuis.
Cuckoo commitments: registration-based encryption and key-value map commitments for large spaces.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 166–200. Springer, 2023.


Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ahmadreza Rahimi.
Registration-based encryption: removing private-key generator from IBE.
In *Theory of Cryptography Conference*, pages 689–718. Springer, 2018.

# Main References



Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, and Ahmadreza Rahimi.
Efficient registration-based encryption.
In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 1065–1079, 2023.


Russell Lai, Monisha Swarnakar, and Ivy Woo.
Leaky lwe: Learning with errors with semi-adaptive secret-and error-leakage.
*IACR Communications in Cryptology*, pages 1–23, 2025.


Adi Shamir.
Identity-based cryptosystems and signature schemes.
In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.