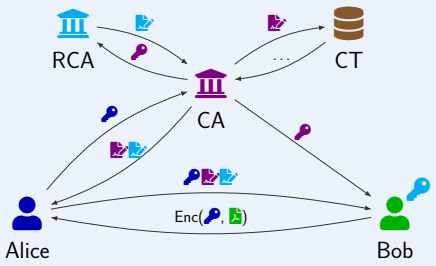
Registration-Based Encryption

Towards More Robust Public-Key Infrastructure

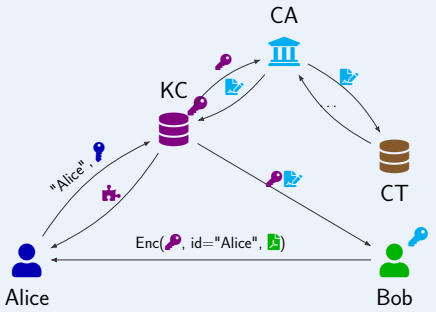
Towards Sturdier Public-Key Infrastructure

PKE



+ Lightweight
− Individual public-keys ⇒ individual certificates
− Heavily relies on fragile certificate infrastructure

RBE



+ Aggregated public-keys ⇒ no individual certificates
+ Alleviates dependency on certificate infrastructure
+ No trusted authority
− Update frequency

Primitives

Laconic Encryption (LE)

- $(\mathsf{pp}, \mathsf{st}, \mathsf{reg}) \leftarrow \mathsf{Setup}(1^n)$: generates initial state 🔑 and registry 🗄
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\mathsf{pp})$: generates a key-pair with pk 🔑
- $\mathsf{ctxt} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{st}, \mathsf{id}, \mathsf{msg})$: encrypts msg for identity id
- $\mathsf{msg} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{wit}, \mathsf{ctxt})$
- $\mathsf{st}' \leftarrow \mathsf{Upd}^{\mathsf{reg}}(\mathsf{pp}, \mathsf{st}, \mathsf{id}, \mathsf{pk})$: updates state 🔑 and registry 🗄 upon registration of a new identity id according to its pk 🔑
- $\mathsf{wit} \leftarrow \mathsf{WGen}^{\mathsf{reg}}(\mathsf{pp}, \mathsf{st}, \mathsf{id})$: generates 🧩 called witness

Laconic Encryption can be built from:

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

RBE

LE + Efficiency Requirement: Each identity's witness wit 🧩 updates at most $O(\log N)$ times; N defines the maximum number of registered identites.

Transforming LE to RBE

Encryption against B LE instances ⇒ |ctxt| scales **linearly** with B

Take B LE instances for a max. number of users $N = 2^B$. On registry of a new user, add it to an empty LE. Iteratively merge two LEs if there are two LE instances with the same number of users, leaving one empty.
⇒ Max. number of merges (witness updates) per identity $\leq \log N$.

Batched LE

LE with reg containing B sub-registries + *Efficiency Requirement:* only *small parts* of |ctxt| allowed to scale linearly with B

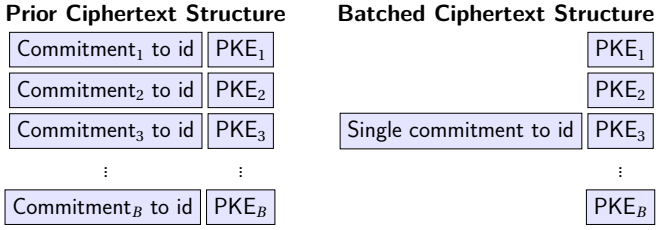
Prior State-Of-The-Art Construction [1]

✓ Naturally extends to arbitrary identity spaces (e.g. emails as identities)
✓ Based on lattice assumption ⇒ **Post-Quantum Secure**
✗ Ciphertext size of **7.2 GB**

Optimisations in our Paper

1. BLE reuses $\mathbf{c}^T$ to share randomness along path to id across all B vector commitments

Optimise Structure of Ciphertext



2. Utilise approximate bit decompositions rather than exact ones
3. Replace statistical arguments in game hops by computational ones
4. Lossy compression of ciphertext

Practical Implementation

Open-source implementation in Rust supporting hardware-accelerated NTT and discrete Gaussian sampler with high throughput.

	Time (ms)				Size (MB)	
	Upd	Enc	WGen	Dec	ctxt	st
[1]	$5 \cdot 1565$	$150 \cdot 2.95$	$5 \cdot 0.061$	$5 \cdot 6.27$	$150 \cdot 49$	8
Our RBE	33.24	15.56	3.38	10.43	7.0	0.34

Fig. 1: Benchmarks on laptop for $N = 2^{30}$, $|ID| \geq 2^{256}$, and $n = 1{,}000$. LE of [1] scaled to RBE.

Conclusion

Reduced ciphertext size by a factor of 1,000 from 7.2 GB to 7.0 MB

- Reduction of ciphertext size from 7.2 **G**B [1] to 7.0 **M**B
- Highly scalable: $N = 2^{128}$ users results in |ctxt| = 7.1 MB
- Currently realistic use-cases: Low frequency, high bandwidth applications such as emails in companies
- Further improvements will require different vector commitment

References & Further Details

[1] N. Döttling et al. *Efficient laconic cryptography from learning with errors.* EUROCRYPT'23. DOI: 10.1007/978-3-031-30620-4_14

- Paper: https://ia.cr/2026/717
- Implementation: jnsiemer/scalable_rbe_prototype

Michael Klooß, Russell W. F. Lai, Jan Niklas Siemer & Monisha Swarnakar
Karlsruhe Institute of Technology & KASTEL | Aalto University | King's College London