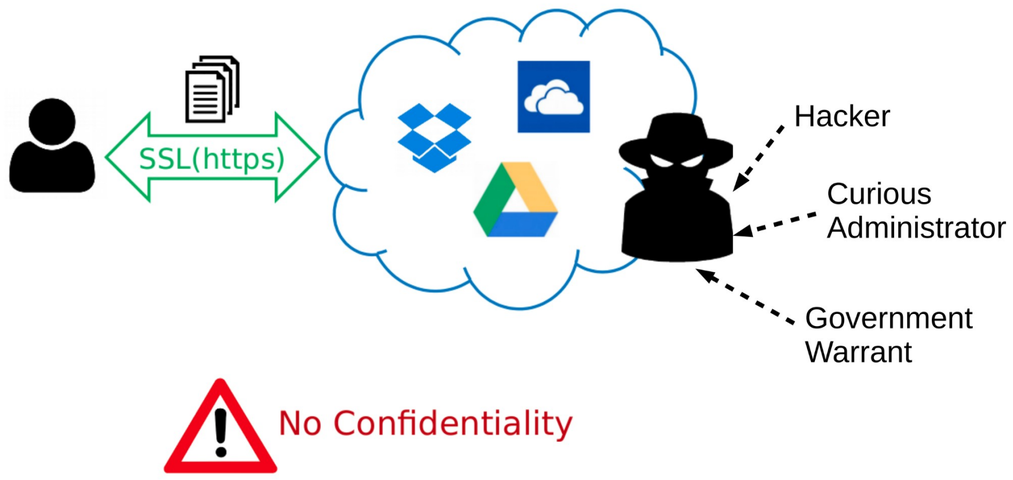
Towards Efficient Cryptographic Group Access Control Systems

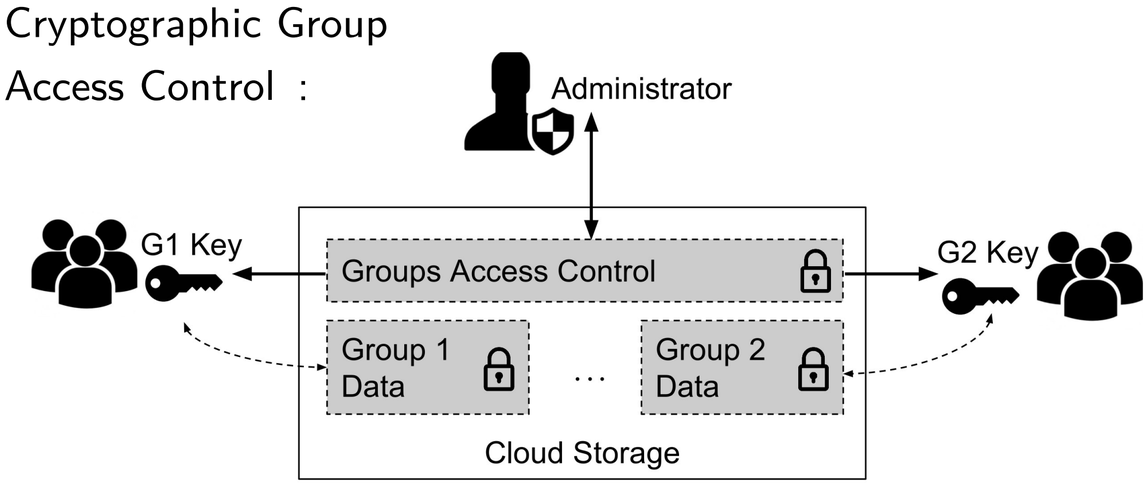
Stefan Contiu[1,2], Laurent Réveillère[2]

[1]University of Bordeaux, [2]Scille SAS, France – first.last@u-bordeaux.fr

In collaboration with **University of Neuchâtel**, Switzerland and **Université catholique de Louvain**, Belgium.



Cryptographic Group Access Control :

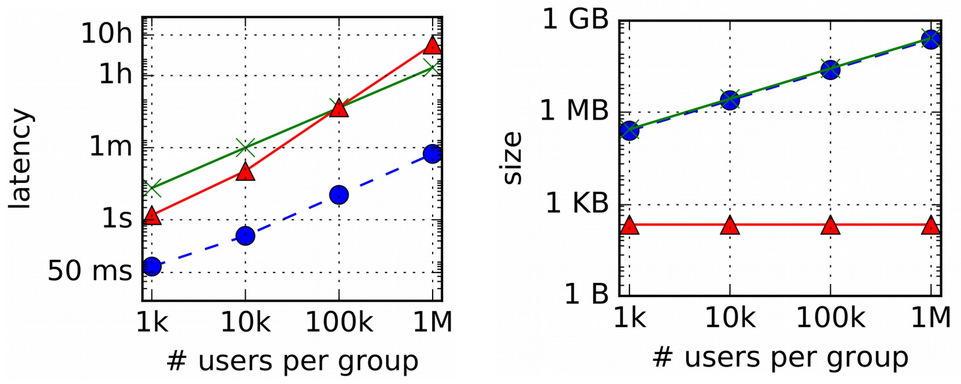


What's already out there ?

Hybrid Encryption with Public Key Infrastructure

Hybrid Encryption with Identity Based Encryption

Identitity Based Broadcast Encryption



None of the schmes have **low latency** and **low storage overhead** !

IBBE-SGX [1]

Use Trusted Execution Environments (**SGX**) to cache secrets and speed-up computations.

Use a group **partitioning mechanism** to speed-up membership updates time.

Operation	IBBE-SGX	IBBE [29]
System Setup	$O(\|p\|)$	$O(\|S\|)$
Extract User Key	$O(1)$	$O(1)$
Create Group Key	$\|P\| \times O(\|p\|)$	$O(\|S\|^2)$
Add User to Group	$O(1)$	
Remove User from Group	$\|P\| \times O(1)$	
Decrypt Group Key	$O(\|p\|^2)$	$O(\|S\|^2)$

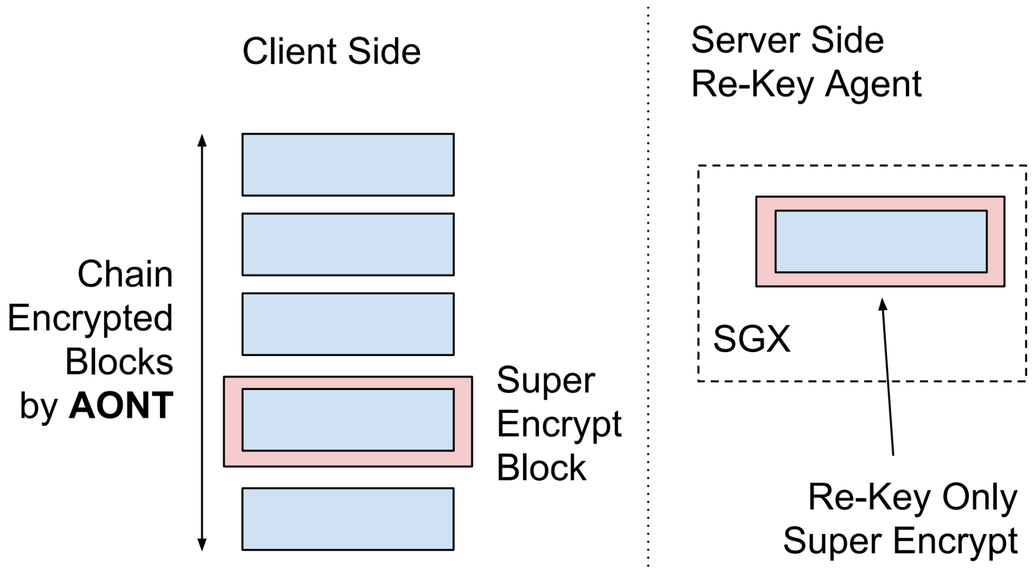
S: set of Users, *P:* set of partitions

IBBE-SGX has **low latency** and **low storage overhead**.
(better than HE-PKI by 1.2 OM for latency and 6 OM for storage)

Active Revocation Efficiency

Full re-encryption by client is **unpractical**.

Use SGX and All or Nothing Transform (AONT)



Anonymous Cryptographic Group Access Control

What if group members are secret?

Use Anonymous Broadcast Encryption with SGX?

Shared Commanding by Multiple Administrators

What if multiple administrators are required for a membership decision?

Use Secret Voting and Blockchain?

[1] Stefan Contiu, Rafael Pires, Sèbastien Vaucher, Marcelo Pasin, Pascal Felber, and Laurent Réveillère. *IBBE-SGX: Cryptographic Group Access Control using Trusted Execution Environments.* In 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018.