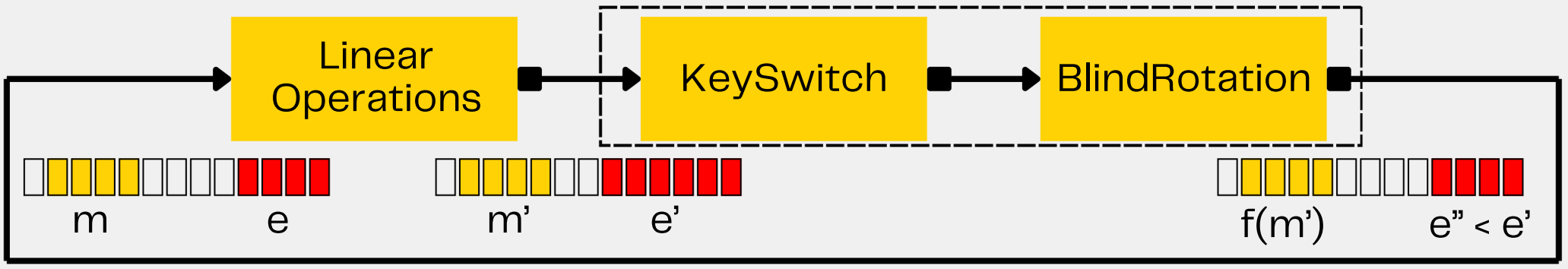
Let's Talk: How TFHE Became Practical

Pierre Gardrat, Agnès Leroy, Arthur Meyre, Jean-Baptiste Orfila and Samuel Tap

TFHE Bootstrapping = Noise Reduction & Function Evaluation



Specfic PBS / Hardware Backend

CPU
[92x2 cores @2.6GHz]
32-bit Keyswitch
FFT-based

GPU
[8xH100 SXM5]
Parallel BlindRotation
FFT-based

HPU
[AMD Alveo V80]
21-bit Keyswitch
NTT-based

64-bit OpsPBS	4-bits	15.1 ms	1.2 ms	0.6 ms
	+	96.2 ms	9.1 ms	8.4 ms
	x	363 ms	32.8 ms	122 ms
	/	4.9 s	514 ms	912 ms

TFHE-rs =
1 API for all backends

Threshold Compliant

Public Key Encryption
Proofs of encryption (ZkPoK)
Distributed Decryption Friendly

Production Compliant

Default (s)Ind-CPA-D security
Compression pre/post computing

Resources
zama.org/blog
github.com/zama-ai