Kryptallage: a Unified FHE Scheme and its Threshold Protocol Layer

Presented by Erin Hales on behalf of Team Kryptallage

Ghada Almashaqbeh, Sonia Belaïd, Nicolas Bon, Ilaria Chillotti, Mariana Gama, Antonio Guimarães, Erin Hales, Hyojun Kim, Elena Kirshanova, Damien Ligier, Ryan Orendorff, Emmanuela Orsini, Matthieu Rivain, Luisa Siniscalchi, Ravital Solomon, Rick Weber

30 September 2026 @ TCPT3 workshop

Agenda

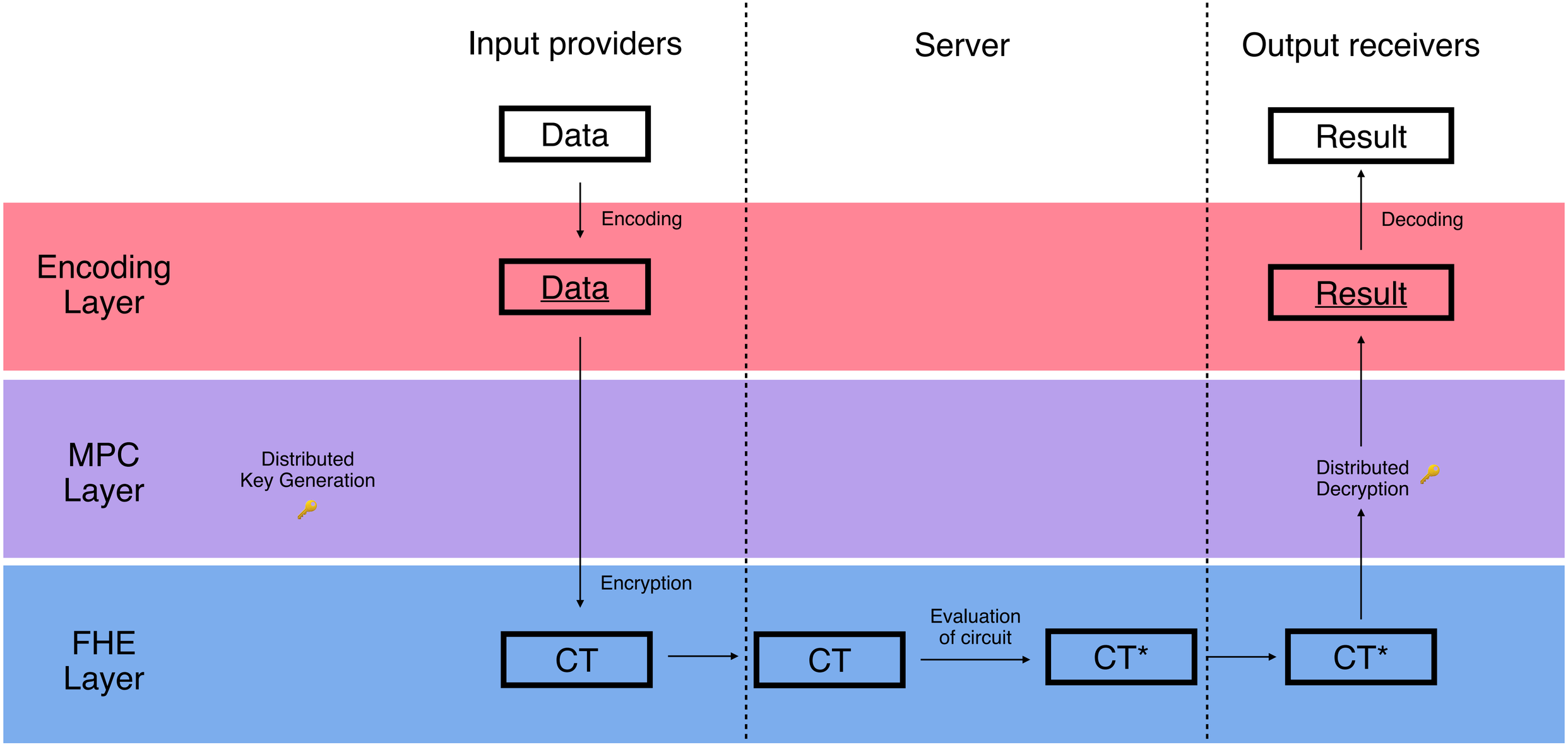
1. FHE and Threshold context
2. Scheme switching
3. Tools needed
4. Application to multi-unit auction



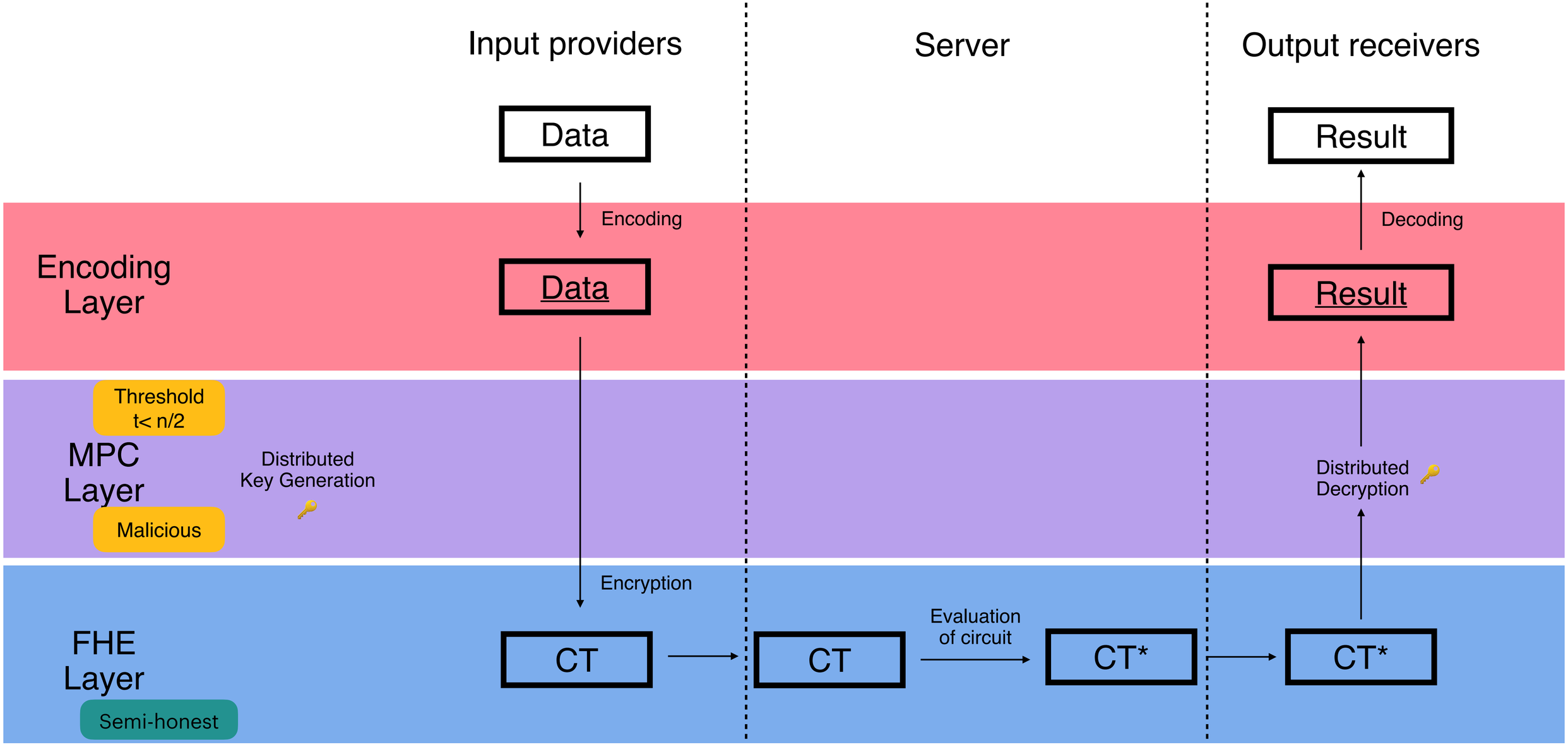


FHE and Threshold context

FHE computation layer and threshold protocol layer

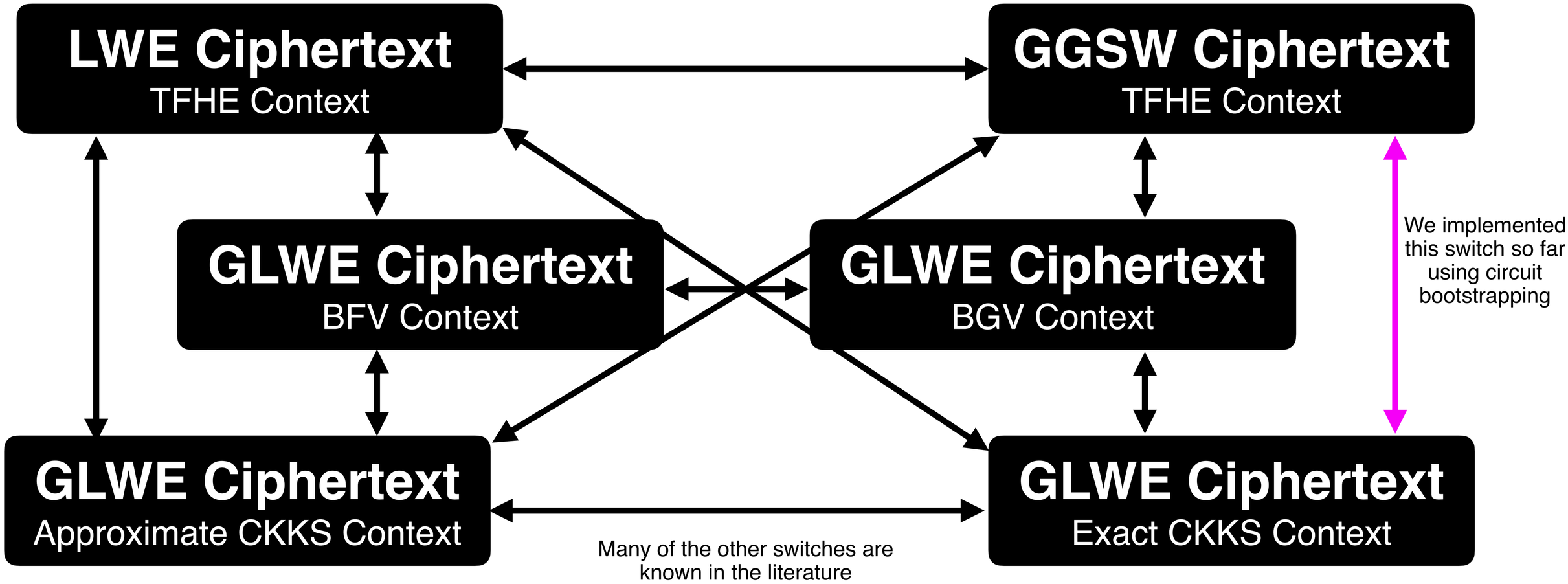


What models do we use?

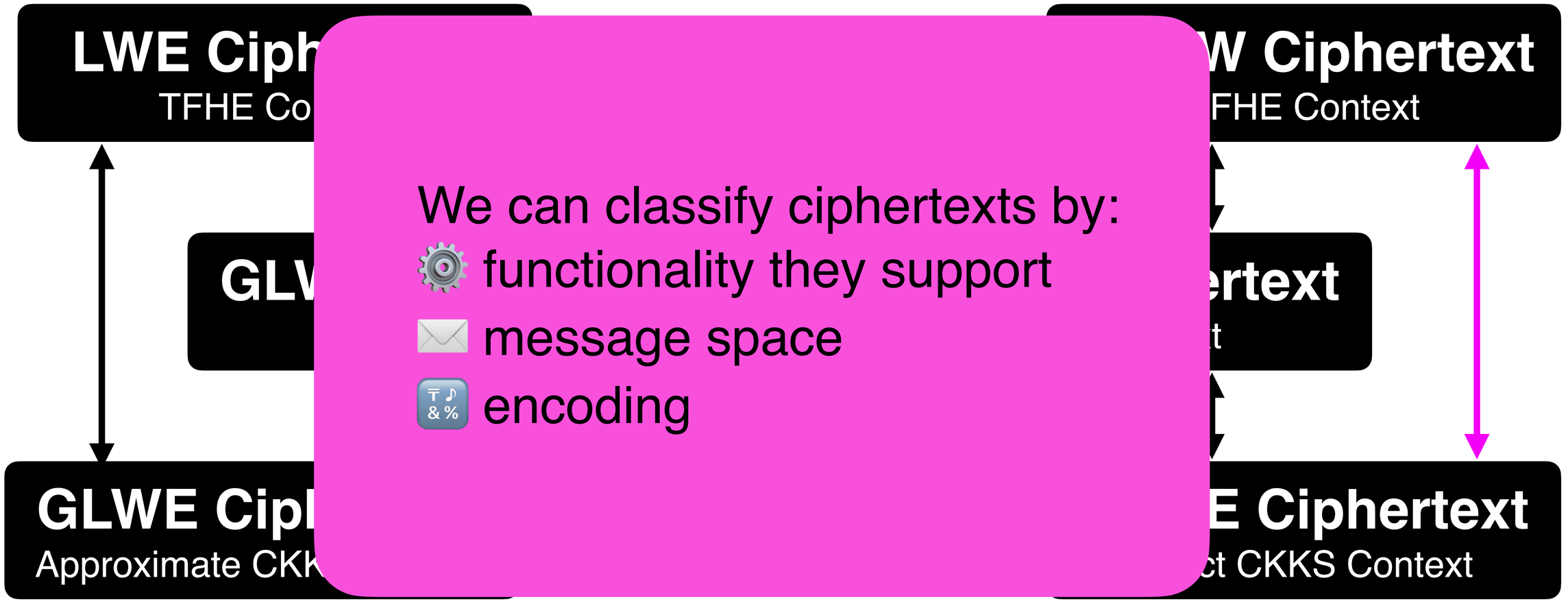



Scheme Switching

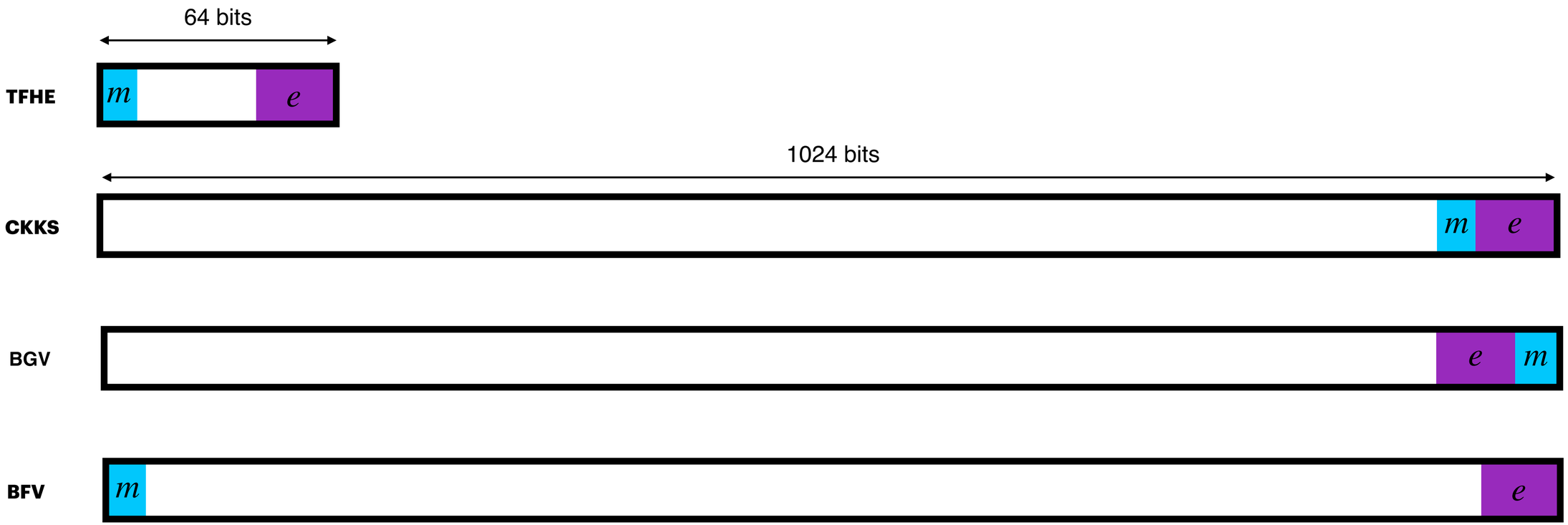
Switching between cipher text types



Our scheme switching philosophy

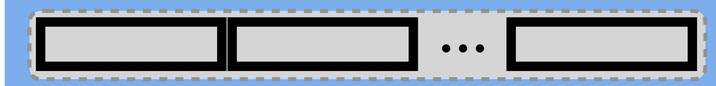


What do ciphertexts really contain?



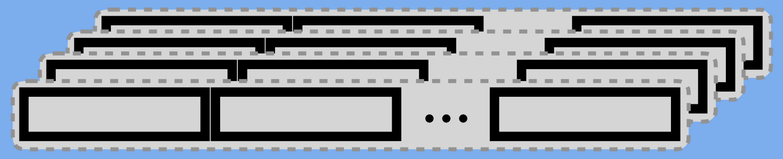
What ciphertext formats are there?

GLWE



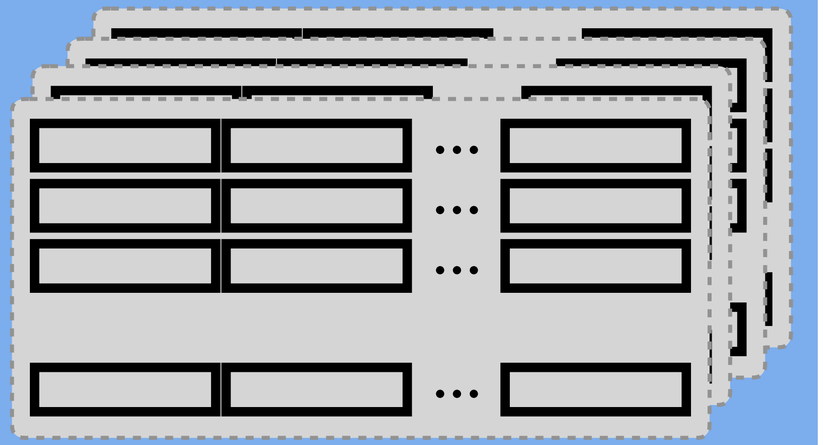
✅ Compact
✅ SIMD possible
✅ Easier to bootstrap

GLev



✅ Key switching functionality
✅ Useful for relinearisation

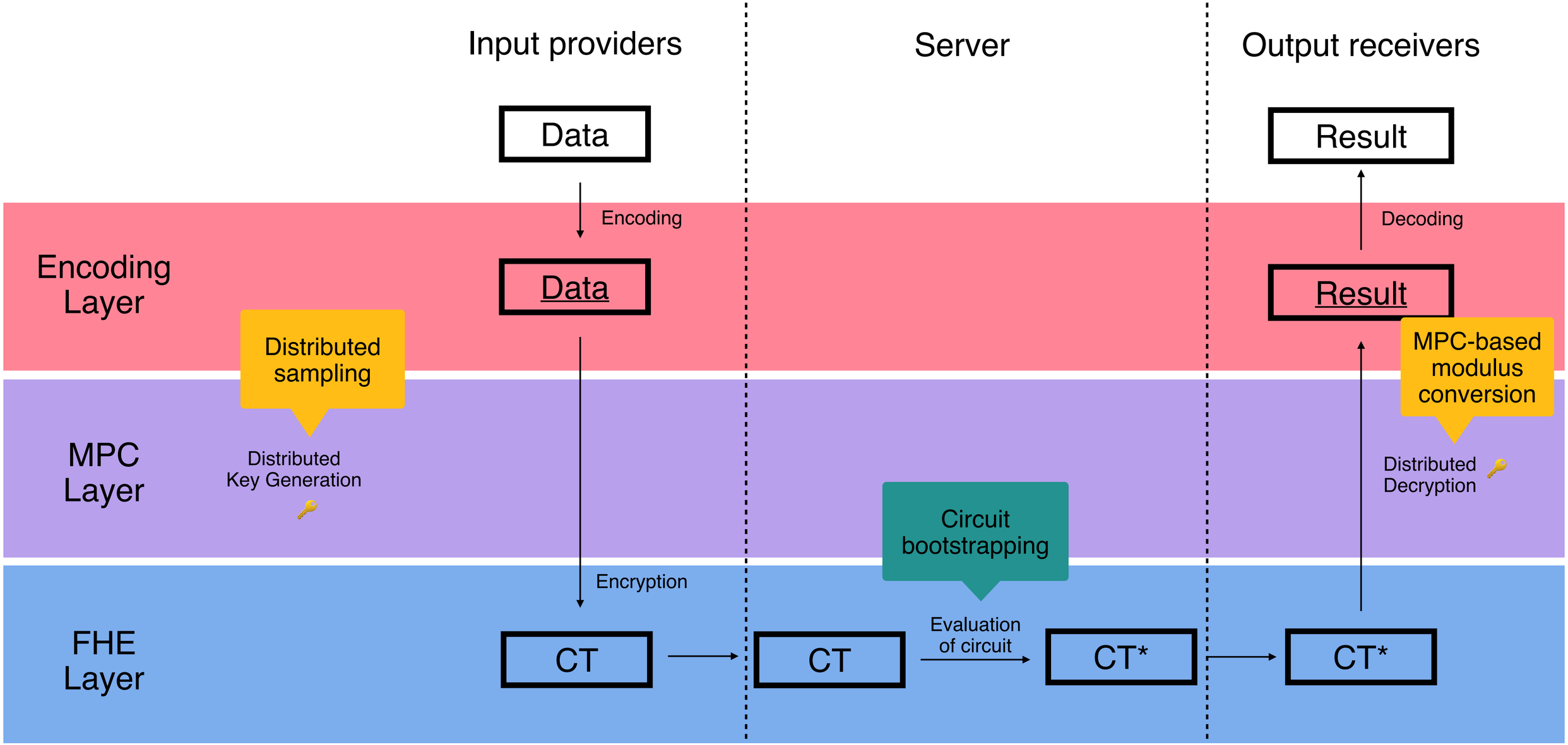
GGSW



✅ Good for bootstrapping
✅ Good for cmux
✅ Good homomorphic product noise growth
⚠️ Large so can pose challenges for transferring ciphertexts


Tools from FHE and MPC

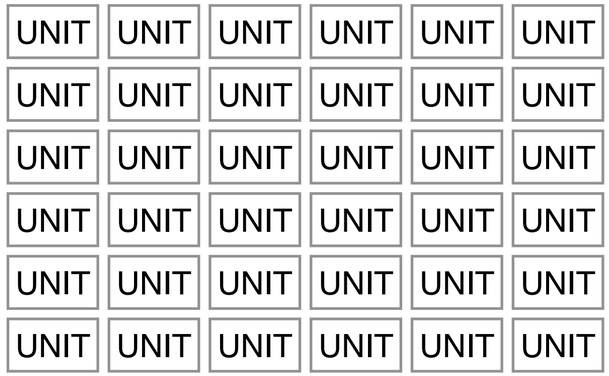
What tools will we use?



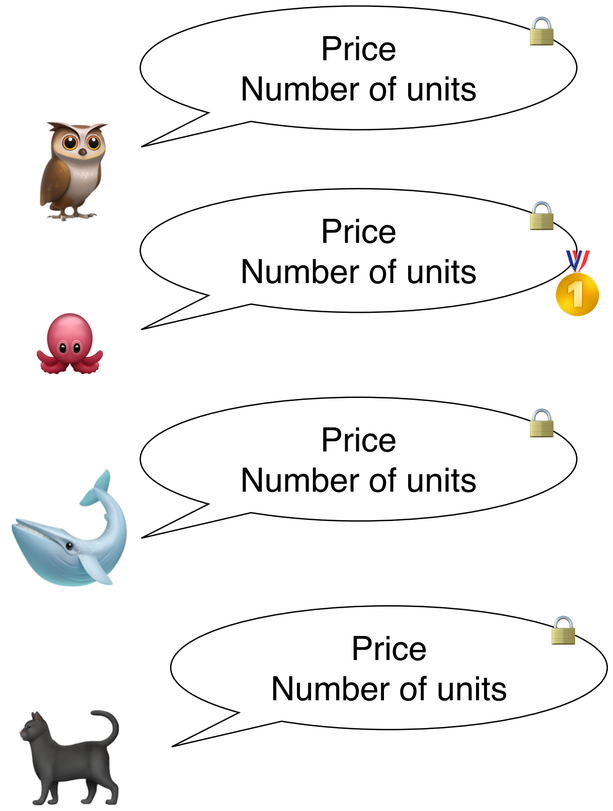


Use case: Multi-Unit Auction

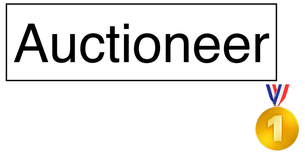
What is a multi-unit auction?



Multiple units for sale



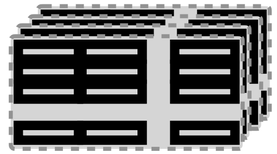
Each participant decided what price they will pay
and number of units they want to buy and keeps this private

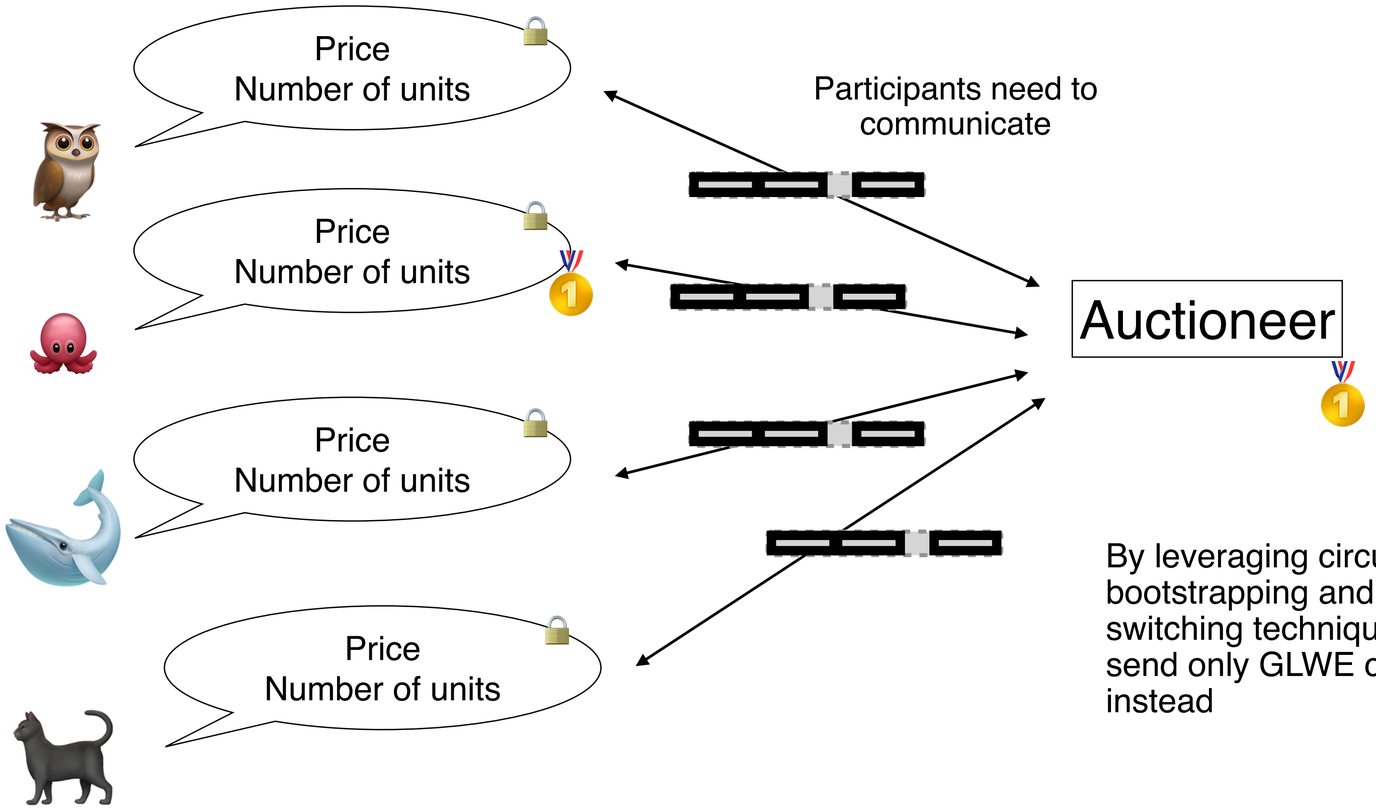


Decides who bid the most, and allocates them
their requested number of units.
Continues to next highest bidder, and so on.

Why is kryptallage a good solution?

Implementation of auction protocols using FHE usually involves many GGSW ciphertexts





By leveraging circuit bootstrapping and other scheme switching techniques we can send only GLWE ciphertexts instead

Participants do not trust one another


What next?

contact-kryptallage@desilo.ai

What next?

