encrypt

A scalable and practical privacy-preserving framework

Hybrid Protection Services

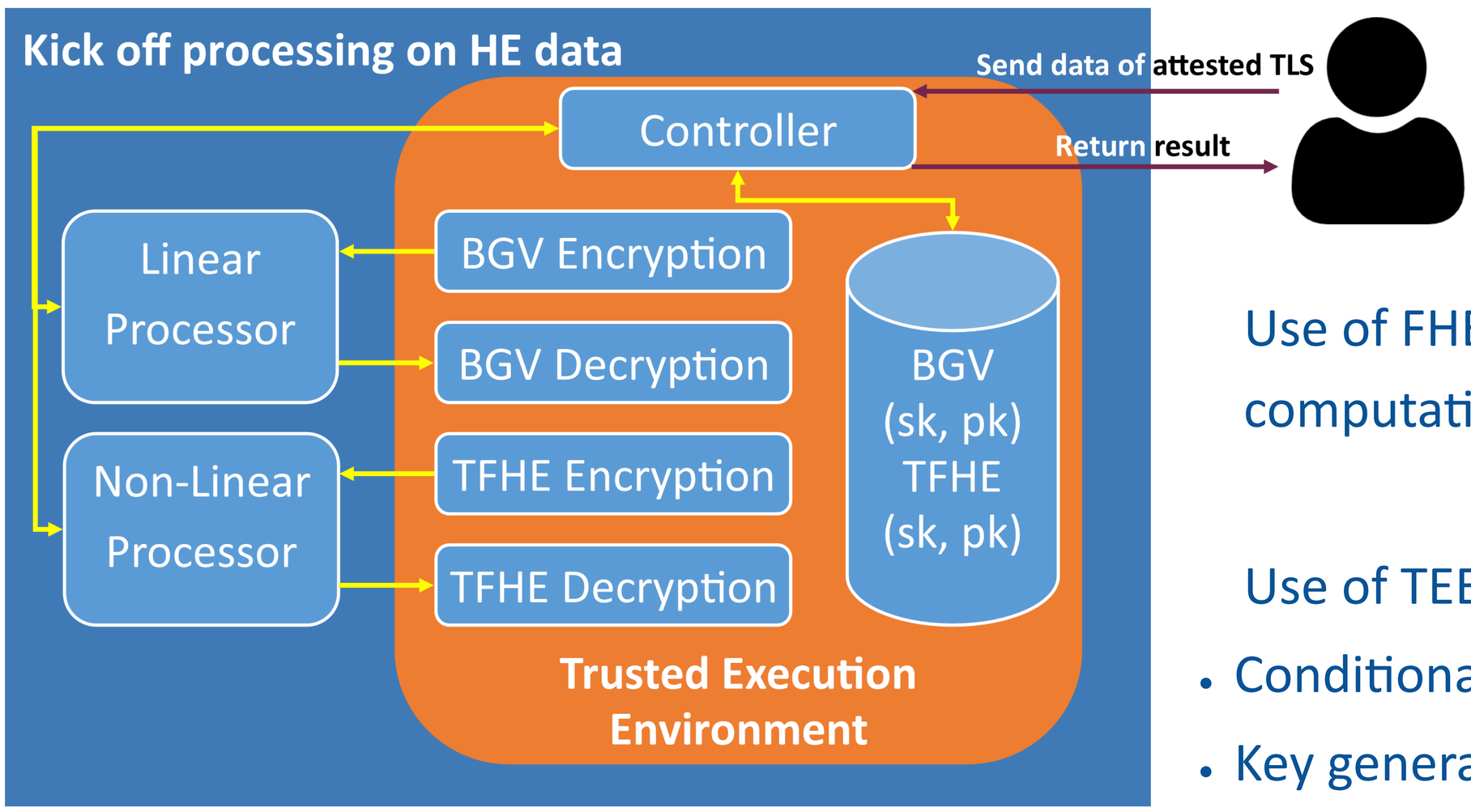
Combining FHE and TEE for Practical, Secure Privacy-Preserving Computation

Data in use remains vulnerable, even with encrypted-at-rest or -in-transit protections

- FHE allows computation on encrypted data, but suffers from:
  - High computational overhead, Ciphertext Expansion, Unverifiable Conditionals
- Trusted Execution Environment executes fast, but:
  - Is subject to side-channel attacks, Requires full trust in hardware vendor

Goal: Combine FHE's privacy guarantees with TEE's performance in a hybrid architecture that reduces risks and improves efficiency

Solution: **SOTERIA** - Hybrid Processing Framework for Secure, Practical FHE/TEE Integration



Use of FHE for encrypted computation

Use of TEE only for:

- Conditional checks
- Key generation/sealing

Benefits

- Side-channel window minimized (TEE used "on-demand" only)
- HE decryption/encryption standardized → reusable countermeasures
- Ciphertext never revealed outside TEE

Funded by the European Union

This work is supported by the European Union's Horizon Europe programme under grant agreement No 101070670.