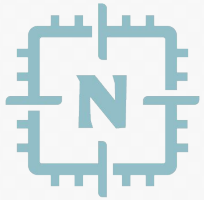


NIOBIUM MICROSYSTEMS

Integrated Hardware Acceleration for BGV, CKKS, and BFV Fully Homomorphic Encryption

March 24, 2024

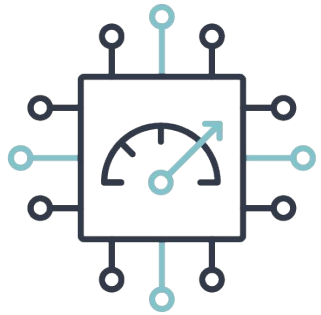
Dr. David W. Archer, CTO

COSIC

galois

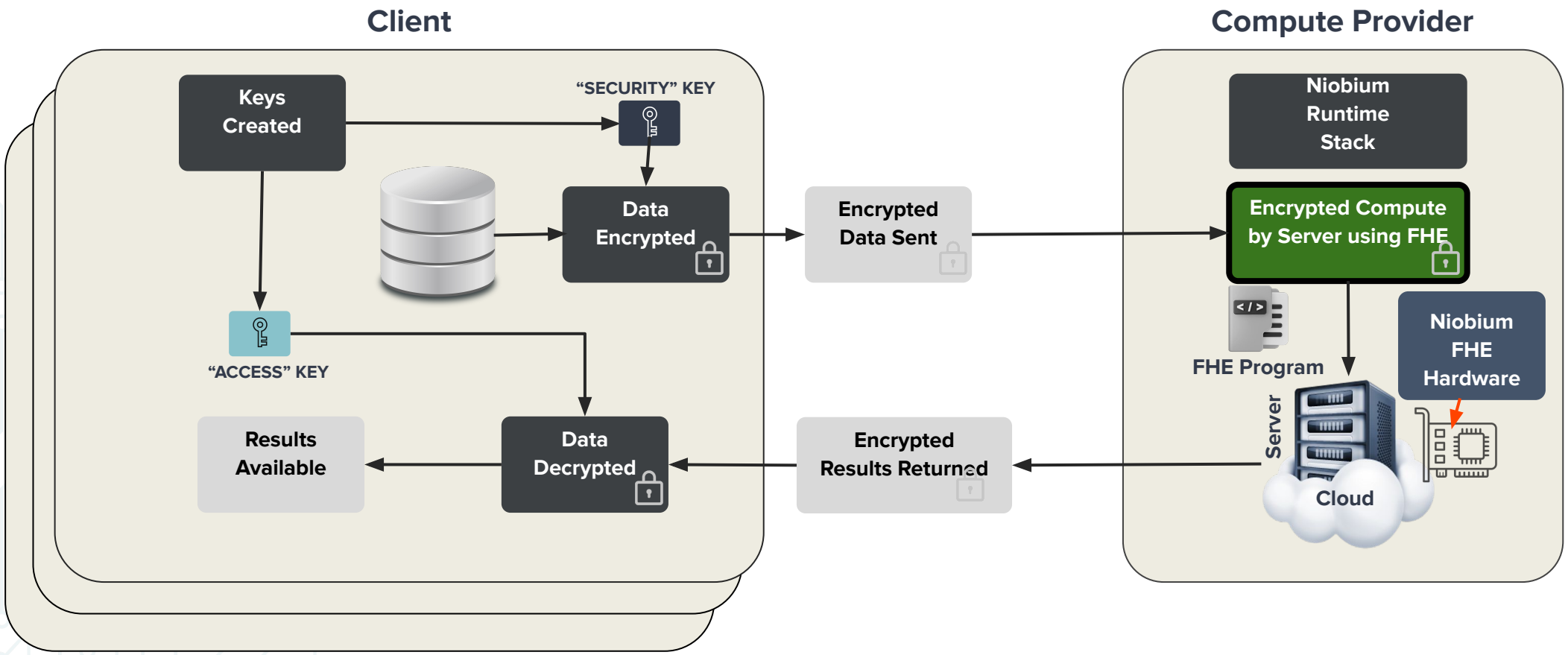
/ What Does Niobium Do?

Unlock the value of data
while preserving privacy
by way of Zero Trust Computing Technologies
(FHE, MPC, ZK Proofs, and others)



Our first product: Integrated Fully Homomorphic Encryption (FHE) Hardware Accelerator

/ Our FHE Solution - User's View



Emerging: Multiple Clients Provide Data

Emerging: Choice of Which Clients Can Decrypt

/ Challenges of FHE Computation

- Data expands (a LOT) when encrypted for FHE computation
  - Thousands to millions of times more space to represent same data
- Execution is blindingly slow on CPUs and GPUs
  - Must do extra work to manage the encrypted computation
  - Need fast and big (wider word) additions and multiplications
- Ease of use
  - Programming style unfamiliar to all but a few experts
  - Complicated trade-offs between security, precision, and speed

/ Niobium Solves for the Challenges

Technical Advantages / Patents Filed

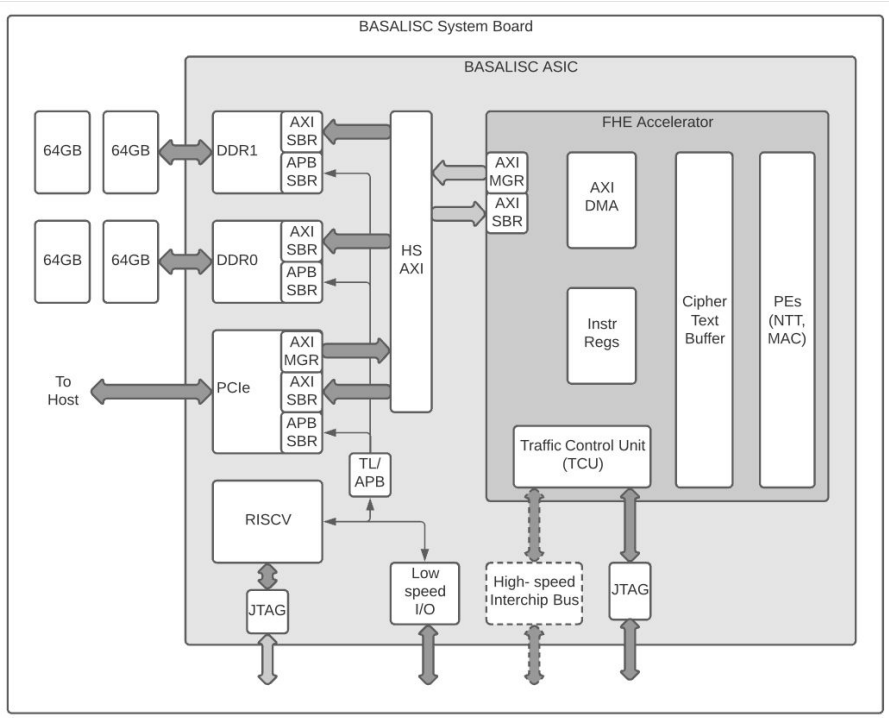
- On-chip generation of “management” data significantly boosts performance
  - NTT twiddle factors
  - Key-switching keys
- Bespoke multi-dimensional data store avoids NTT matrix transpositions
- Specialized “Montgomery-modular” bootstrapping reduces chip area, power
- Highly parallel *modular arithmetic* datapaths & register file free-run @ 2X core clock speed
- RISC architecture
  - One data type: *residue polynomial*
  - Two data addressing modes: *register*, *immediate*
  - Load/Store “cacheless” architecture

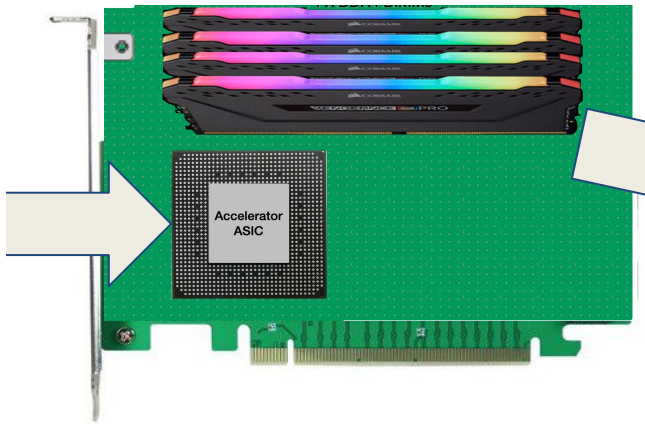
/ FHE Scheme Support

- Optimized for BGV, CKKS, BFV
- Parameter ranges
  - Plaintext modulus: 2 → 127^3
  - Ring dimension: 2^{16}
  - Ciphertext modulus: 20 → 1800 bits
  - Native math: up to 64 bits
  - Achievable security: > 128 bits
- Native operations: Add, Multiply, NTT, INTT, Automorphisms

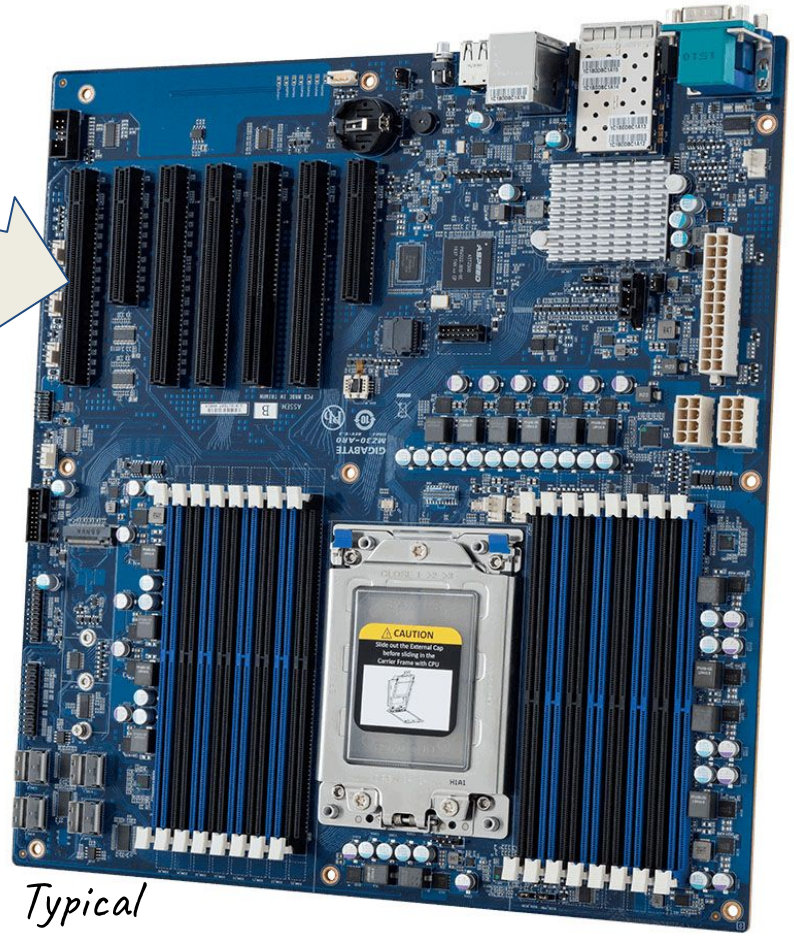
/ Simple, Cost-effective Deployment to Infrastructure

Niobium's
FHE Acceleration Processor

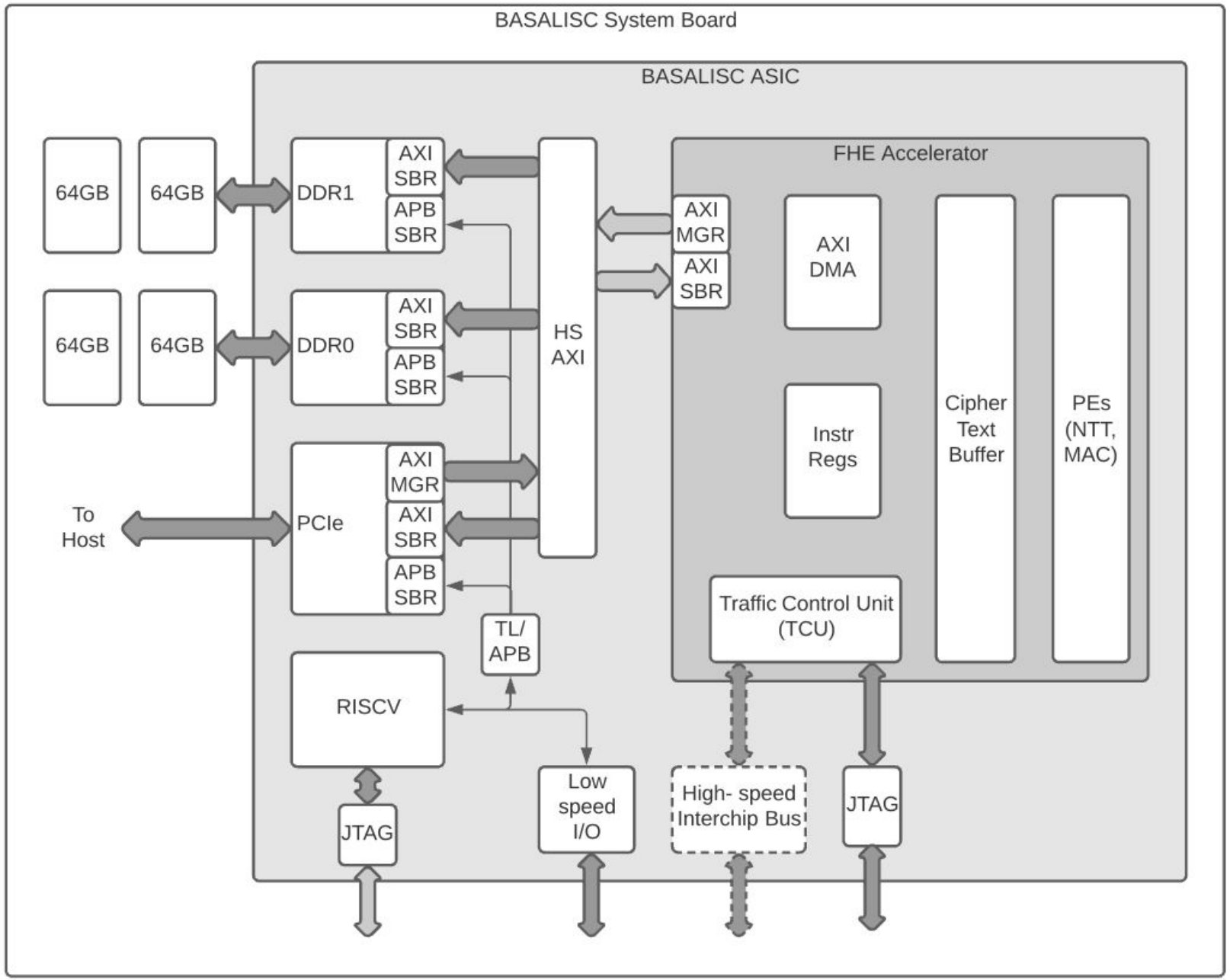




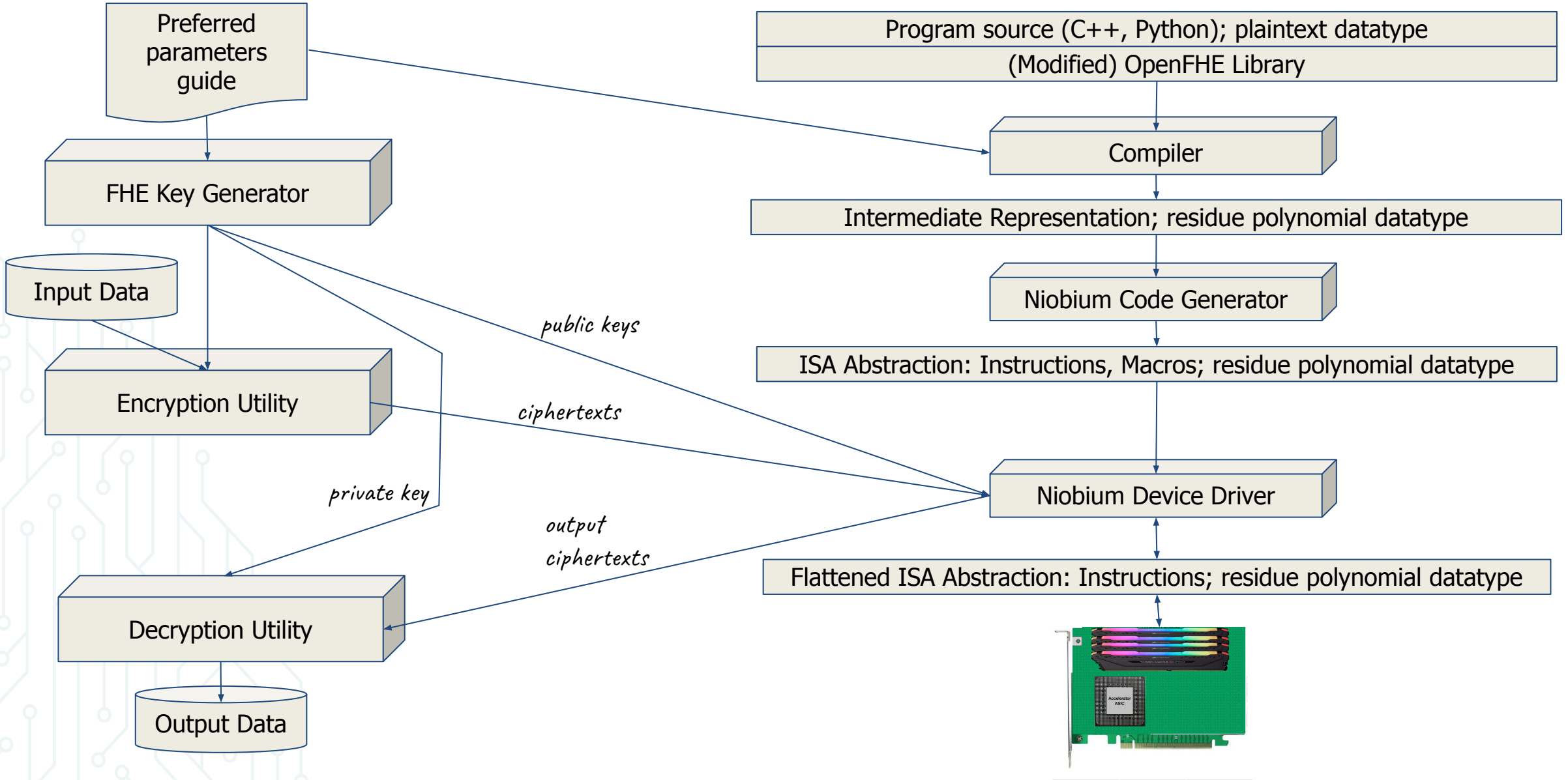
Standard PCIe
Form factor



Typical
Single-board Server


BASALISC System Board
BASALISC ASIC
64GB
64GB
64GB
64GB
DDR1
DDR0
AXI SBR
APB SBR
AXI SBR
APB SBR
HS AXI
FHE Accelerator
AXI MGR
AXI SBR
AXI DMA
Instr Regs
Cipher Text Buffer
PEs (NTT, MAC)
To Host
PCIe
AXI MGR
AXI SBR
APB SBR
Traffic Control Unit (TCU)
TL/ APB
RISCV
JTAG
Low speed I/O
High- speed Interchip Bus
JTAG

/ Software Development Stack



/ Availability Timetable

- Niobium Early Access Program opens summer 2024
  - Including availability for Cloud providers, Server OEMs and end users
  - Options for remote access as well as on-prem (PCIe boards)
- Measured application results - late Fall 2024
- Client access through Early Access Program - Early 2025

/ Acknowledging Our Roots

This research was, in part, funded by the Defense Advanced Research Projects Agency (DARPA) through contract HR0011-21-C0034. The views, opinions, and findings expressed are those of the authors and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. Distribution Statement ‘A’ (Approved for Public Release,Distribution Unlimited).

Thank you!