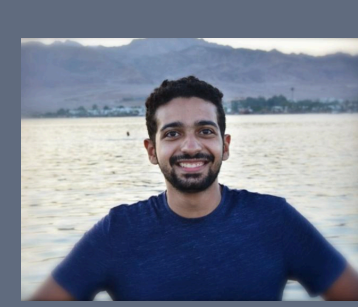
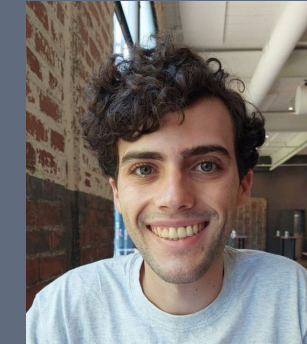




Muhammad Faisal



Alessandra Lanz



Sam Buxbaum



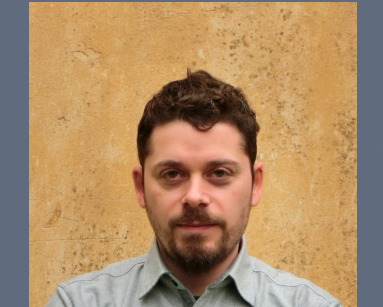
Adam Godel



Vasiliki Kalavri



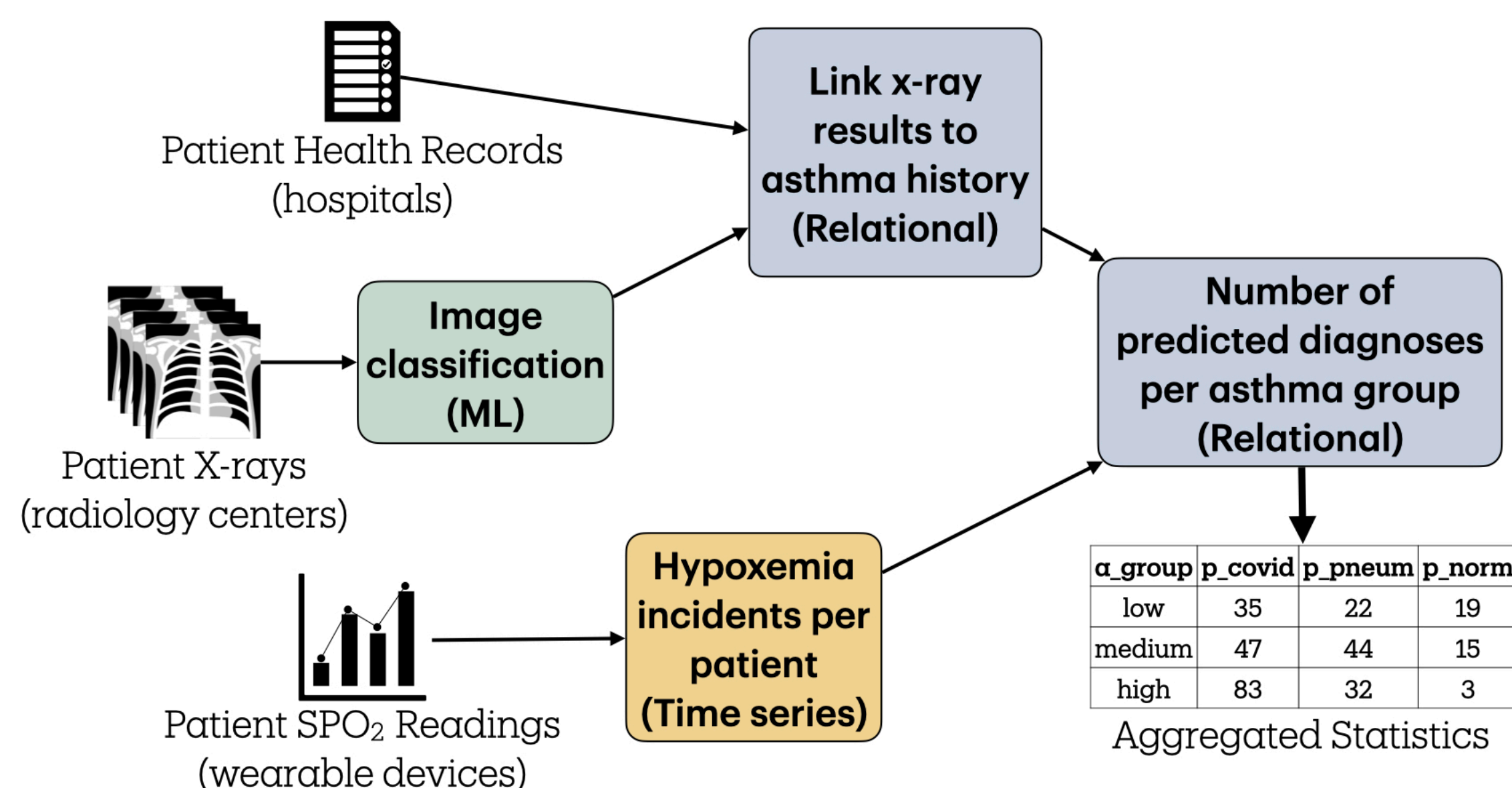
Mayank Varia



John Liagouris

Secure computation requires rethinking the entire system stack

Secure multiparty computation (MPC) enables collaborative analytics on secret data



Lessons learned from MPC applications in the wild:

- Threat models and security requirements vary across use cases
- Data analysis pipelines typically include diverse workloads
- Deploying MPC jobs currently requires cryptographic expertise

Limitations of existing MPC systems:

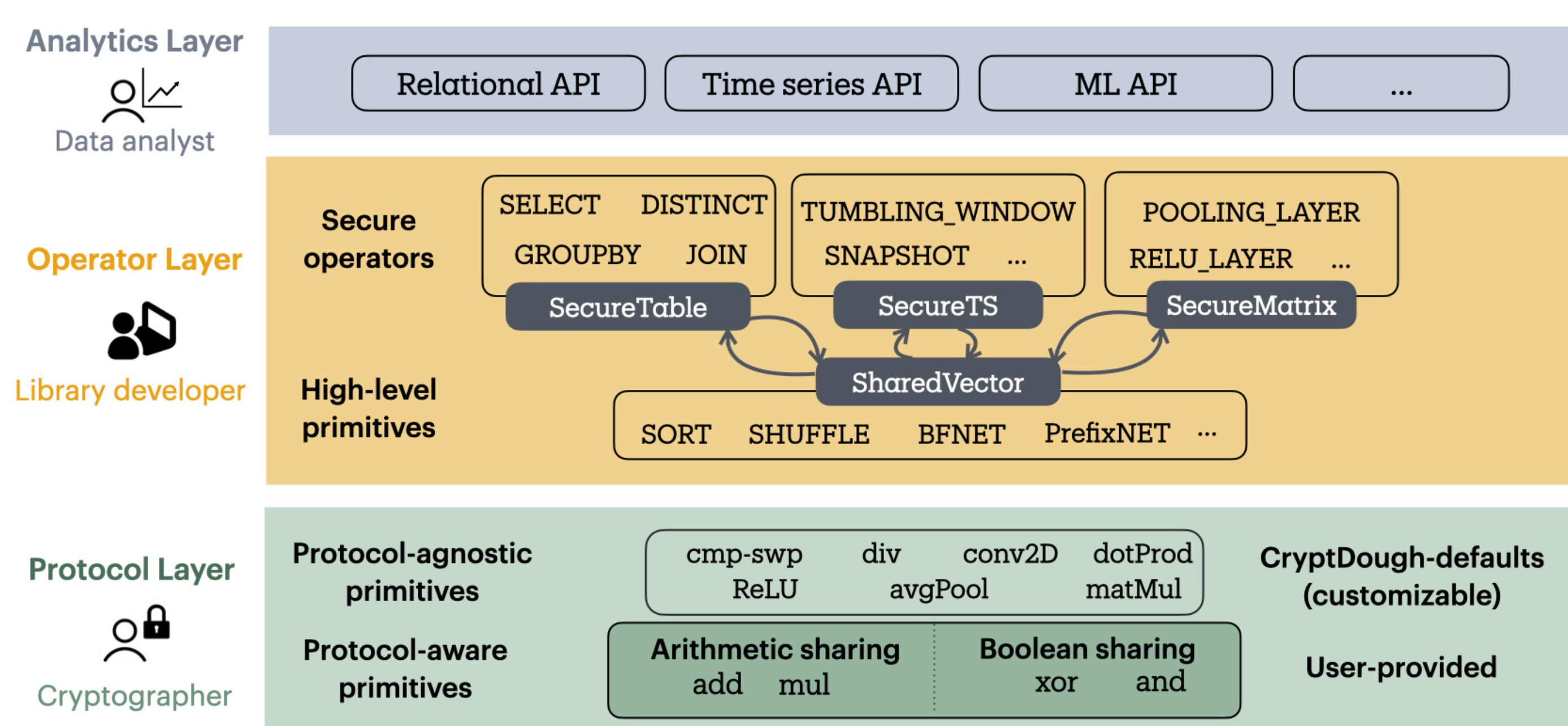
- No built-in support for mixed workloads (ML, relational, time series)
- Non-extensible system designs (tailored to specific threat models)
- Limited interoperability (no standardized interfaces)

Key challenge: How to architect an extensible software stack that does not deteriorate into a “wrapper” of external MPC libraries?

CryptDough: The first unified analytics engine for MPC

CryptDough's architecture: Prioritizing extensibility across the stack through progressive lowering of abstractions

CryptDough's key programming abstraction: Virtual Vectors

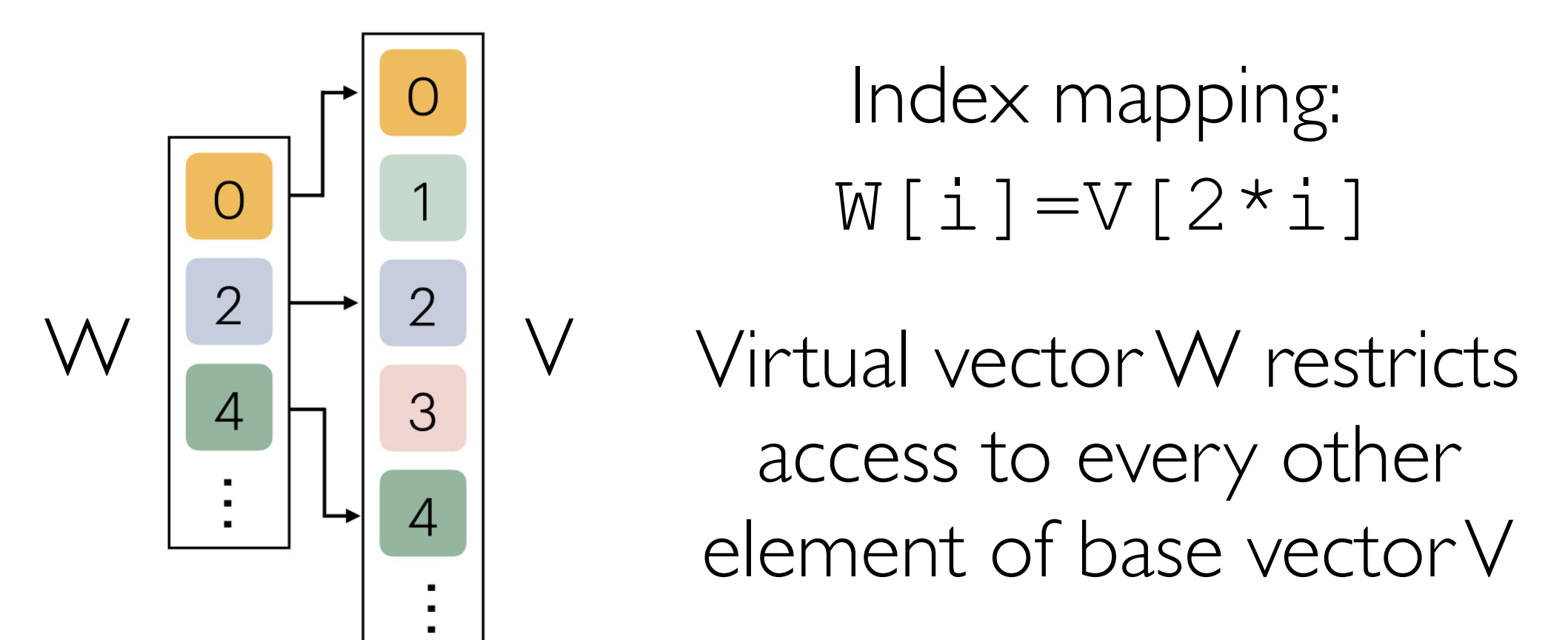


No systems or cryptography background

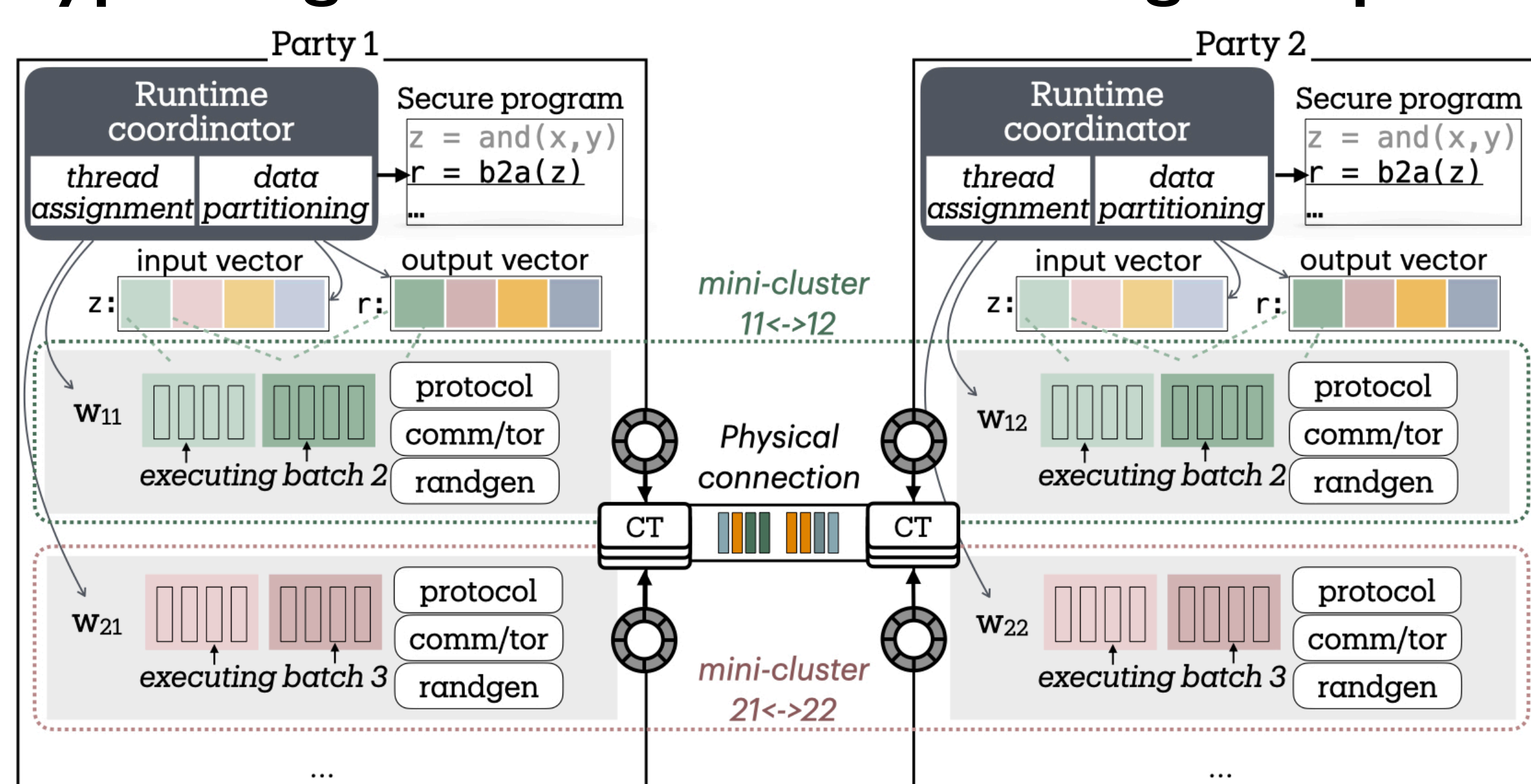
Domain expert who can design oblivious algorithms
No systems or MPC protocol expertise

MPC expert
No systems or domain expertise

A virtual vector is a restricted view of a base vector with an internal index mapping



CryptDough's execution model using two parties



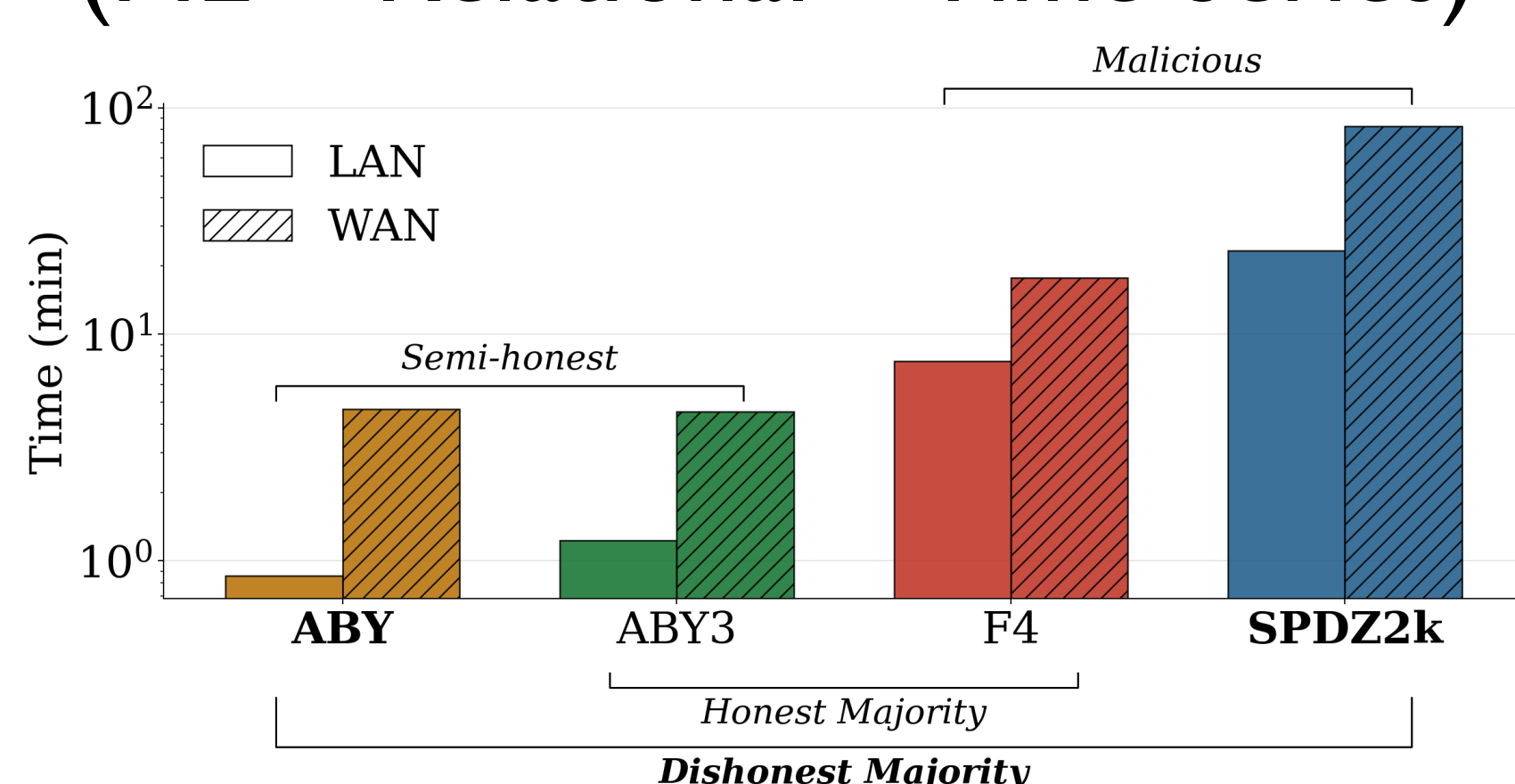
Pairs of worker threads across computing parties form independent MPC "mini-clusters"

CryptDough uses virtual vectors to automatically parallelize oblivious operators with irregular access patterns

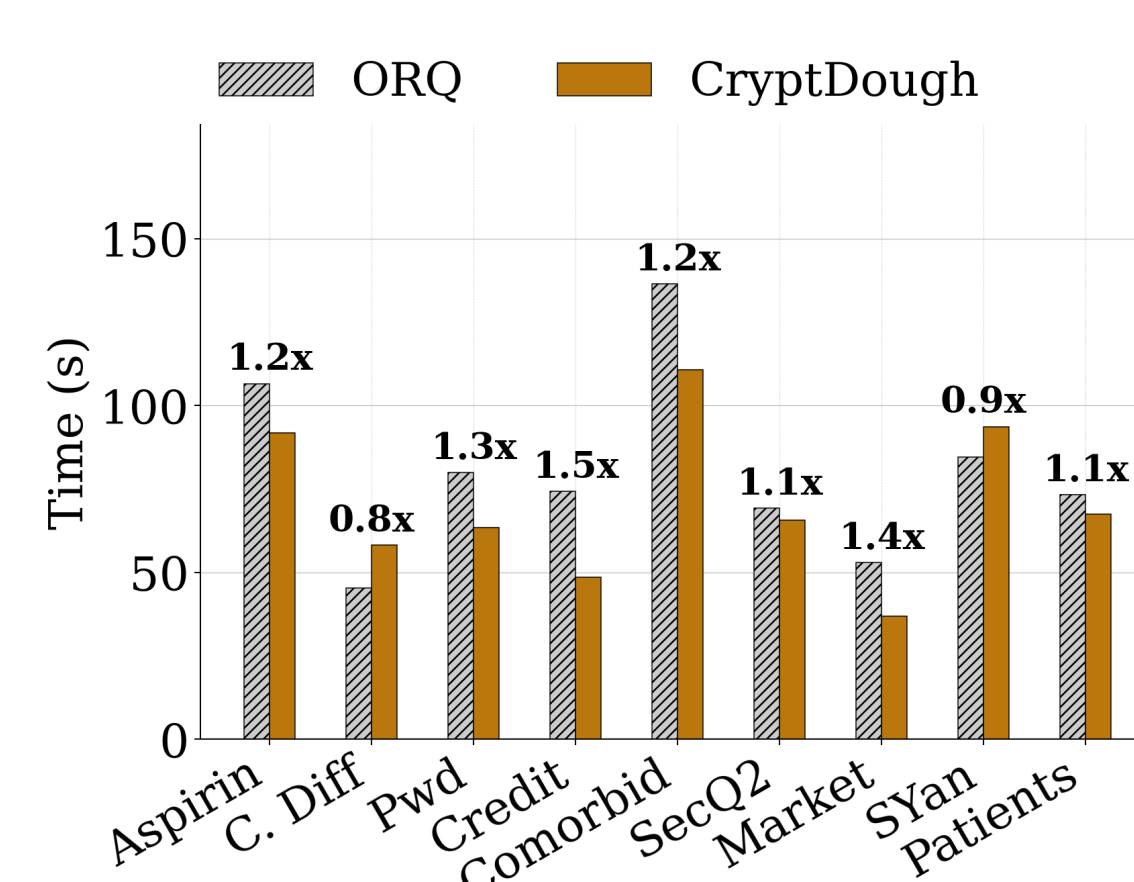
- 1 Example oblivious operation on vector V with an irregular access pattern
- 2 Goal: reuse vectorized `cmp-swap()` primitive and parallelize independent operations across worker threads
- 3 Reusing the existing vectorized primitive through virtual vectors
- 4 Virtual vectors are transparently partitioned by the system runtime as if they were contiguous vectors

CryptDough achieves generality without sacrificing security or performance

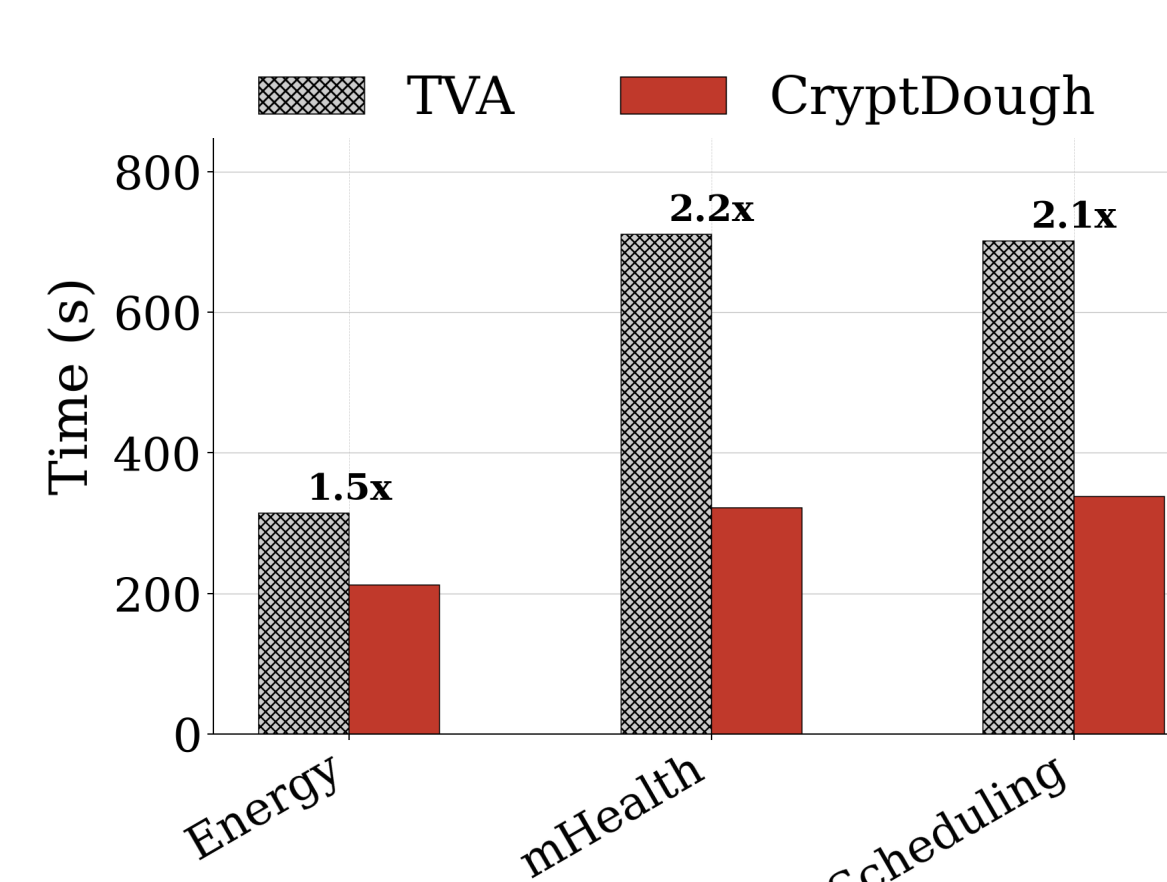
Mixed workload (ML + Relational + Time Series)



Relational (2PC, LAN)



Time Series (4PC, LAN)



CNN Inference (2PC, LAN)

	AlexNet (CIFAR-10)	VGG16 (CIFAR-10)	VGG16 (ImageNet)
LAN			
Piranha	0.57 s	31.6 s	47.3 s
CryptDough	0.46 s	14.2 s	30.1 s
Speedup	1.2x	2.2x	1.6x
WAN			
Piranha	3.58 s	80.2 s	164.4 s
CryptDough	9.20 s	56.2 s	92.3 s
Speedup	0.4x	1.4x	1.8x

First MPC analytics system to report results for mixed workloads across the entire spectrum of threat models

CryptDough remains competitive with specialized MPC systems and often outperforms them by more than 2x