Worked with In-Q-Tel & Blue Bastion, pen tested for 3 months
• Red team had full access to all IP
• 2-person years effort to build, fuzz test, and verify
• TrustForge competes with
  • Homomorphic encryption (HE and FHE)
  • Multiparty computation (MPC)
  • Bottom line: Much faster than comparable frameworks, much more secure than TEEs

This 190k-gate functional unit implements always-encrypted computation, nullifying hacking and advancing privacy technology.

TrustForge Enclave Advances Privacy Tech
• Enables zero-trust data sharing
• No trust in any system security, software, programmers or IT staff
• Enables privacy-enhanced computation, without a valid data contract
• Unauthorized enclaves gen exception
• Expired contracts gen exception
• Unauthorized codes destroy data
• Only authorized results are visible
• Provides hardware capabilities of homomorphic encryption and zero knowledge proofs
• Available on Amazon AWS and Microsoft Azure

A Recipe for Cryptographic TEEs...
1. Eliminate all software vulnerabilities
   • But all software is (eventually) hackable!
   • Approach: no S/W in the enclave
2. Silence side channels
   • Control, memory, timing, and uArch
   • Approach: provably side-channel free enclave
3. Encrypt sensitive data everywhere else
   • Eliminates trust for all remaining S/W and H/W
   • Approach: encrypt on exit of enclave

Use Case: Medical Data Sharing
• Privacy-preserving smartwatch-based heart monitoring
  - Data encryption: biometric data is encrypted at the sensor, sent to server encrypted
  - Encrypted computation: analysis of biometric data is performed on encrypted data, without giving access to the server or its operators
  - Guardrails: attacker cannot manipulate analysis algorithms to trigger false warnings
  - Safe datagates: arithmetic analysis algorithms can expose potential health warnings to permit notification/text message to the user

Programming for the TrustForge Enclave
• TrustForge extends development language with encrypted variables
• Bit-for-bit compatible, but encrypted
• Support for integers, floating-point, Booleans, and strings
• Encrypted ops return encrypted results
• Decision processing on encrypted variables implemented with $CMOV$ primitive
• Secret-dependent array indexing implemented with $ORAM$ primitives

TrustForge Security Analysis
• Worked with In-Q-Tel & Blue Bastion, pen tested for 3 months
• Red team had full access to all IP
• Zero vulnerabilities found
• Formal verification with Princeton
• Secure for any program on a specific implementation
• Zero vulnerabilities found
• Proofs to appear in ACM CCS 2023

TrustForge: Inside the Zone of Trust
• TrustForge enclave exports a public key, PKI-encrypted keys are decrypted in enclave
• Enclave supports RISC-like operations that operate directly on encrypted data
• Enclave is decrypting, processing, checking, and re-encrypting secret data without S/W vulnerabilities or digital side channels
• Enclave is protected from physical attacks, and data is encrypted everywhere else

TrustForge Enclave for Azure and AWS
• Deployed on FPGA nodes in the cloud
• % of total UltraScale+ FPGA used: ~6%, ~190k gates
• Logic locked, watermarked and with forward secrecy
• Bubbles lock; much harder than comparable frameworks, much more secure than TEEs

TrustForge Performance Comparison
• TrustForge enclave exports a public key, PKI-encrypted keys are decrypted in enclave
• Enclave supports RISC-like operations that operate directly on encrypted data
• Enclave is encrypting, processing, checking, and re-encrypting secret data without S/W vulnerabilities or digital side channels
• Enclave is protected from physical attacks, and data is encrypted everywhere else

TrustForge Performance Headroom (vs. Native)

Cryptographic Data Contracts:
• Who can perform analyses
• What analytics are allowed
• When can they be run

Massively multi-tenant multi-tenant
• Section 4.2
• Implementation
• Section 4.4
• Section 4.5
• Section 4.6

Digital smartwatch heart rate monitor

Intel SGX

Multiparty computation (MPC)

Zero vulnerabilities found

Secure Enclave

Multiparty computation (MPC)

Zero vulnerabilities found

Secure Enclave

Multiparty computation (MPC)

Zero vulnerabilities found

Secure Enclave

Multiparty computation (MPC)

Zero vulnerabilities found

Secure Enclave