VIP-Bench

A Benchmark Suite for Evaluating Privacy-Enhanced Computation Frameworks

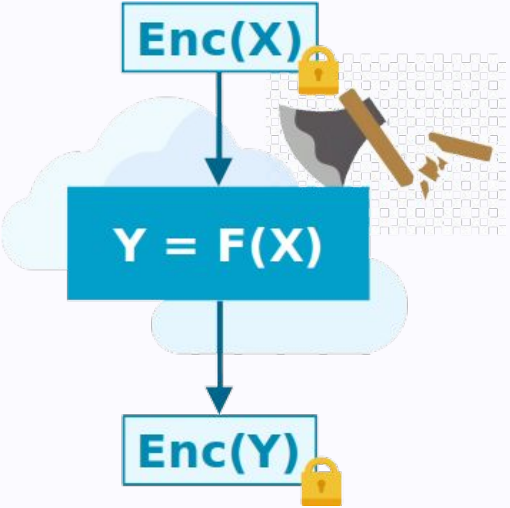
Lauren Biernacki, Meron Zerihun Demissie, Kidus Birkayehu Workneh,Galane Basha Namomsa, Plato Gebremedhin,Fitsum Assamnew Andargie,Brandon Reagen,Todd Austin

Group 10

Donayam Nega, Biniyam Tiruye

Privacy Enhanced Computation (PEC)

- Computing directly on encrypted data.
- A fast growing field.
- Holds a great promise for the future of computing.



PEC Frameworks

- Homomorphic Encryption (HE)
- Multi-Party Computation (MPC)
- Trusted Execution Environment (TEE)

VIP-Bench

- Computation capability comparison benchmark for PEC frameworks.
- Defines a central computation model to which all benchmarks adhere.
- Provides 18 benchmarks that were selected to be representative of applications that would benefit from enhanced privacy.

VIP Benchmark

Has 18 workloads organized by

A. Operation Complexity
B. Depth of Computation

VIP-Bench Variants	Low Operational Complexity	High Operational Complexity
Shallow Computation	*X-Gradient* *Linear-Regression* *Roberts-Cross*	*Nonlinear-NN*
Deep Computation	*Hamming-Distance* *Dot-Product* *Poly-Regression* *Eulers-Approx* *Triangle-Count* *Mersenne*	*Bubble-Sort* *Edit-Distance* *FFT-Int* *NR-Solver* *LDA* *Kepler* *Parrondo* *MNIST-CNN*

Modes of Operation

1) Native (NA)
2) Data Oblivious (DO)
3) Encrypted (ENC)

Unified PEC Programming Interface

VIP COMPUTATION MODEL

- Makes three assumptions about the PEC frameworks:
  - Sensitive data is **always encrypted**, including in registers and memory.
  - **Encrypted variables** cannot be used to r**esolve branches.**
  - **Encrypted variables** cannot be used to compute **memory addresses.**

VIP COMPUTATION MODEL

Encrypted variable definitions

Type Class	VIP Data Types
Boolean	VIP_ENCBOOL
Character	VIP_ENCCHAR, VIP_ENCUCHAR
Integer	VIP_ENCINT, VIP_ENCUINT, VIP_ENCINT64, VIP_ENCUINT64
Floating Point	VIP_ENCFLOAT, VIP_ENCDOUBLE

Operations on encrypted variables

Operator Class	Example Semantics
Linear Arithmetic *e.g.,* +, -, *	x = enc(dec(y) + dec(z))
Nonlinear Arithmetic *e.g.,* /, %	x = enc(dec(y) % dec(z))
Nonlinear Relational *e.g.,* ==, >, >=, <, <=	x = enc(dec(y) < dec(z))
Nonlinear Boolean *e.g.,* &, |, ^, ~, &&, ||, !	x = enc(dec(y) & dec(z))
Type Cast Operators *e.g.,* (VIP_ENCINT)	x = enc((int)dec(y))
Conditional *e.g.,* VIP_CMOV(p, x, z)	x = enc(dec(p) ? dec(x) : dec(y))
Control Flow	n/a
Memory Access	n/a

VIP COMPUTATIONAL MODEL

Transformation to use data oblivious operations

Transform

a) Program control flow and
b) Memory accesses

Program Control Flow Transformation

```
if ((x & 1) == 1) {
    odd = odd + 1;
}

else {
    even = even + 1;
}
```

(a) Unsafe Conditional Logic.

```
VIP_ENCBOOL cond =
              (x & 1) == 1;
odd = VIP_CMOV(cond,
               odd+1,
               odd);
even = VIP_CMOV(!cond,
                even+1,
                even);
```

(b) Safe Conditional Logic.

Memory accesses Transformation

Prevents inferring of the encrypted variable

Idx -> encrypted

```
// Unsafe Memory Access
arr[idx]++;
```

```
// Safe Memory Access
for(int i=0; i<N; i++;) {
    arr[i] = enc_cmov(i==idx,
                      arr[i]+1,
                      arr[i]);
}
```

Results

Computed on

Native,Data Oblivious and Encrypted (ENC)

Compared using

Instruction count and execution time

Benchmark	Mode	Insn. Count	Runtime (μs)		VSZ (kB)
Hamming-Distance	NA	571,746	258		14,160
	DO	571,746	258		14,160
	ENC-BFV	379,721,213	50,553	*(196x)*	135,692
	ENC-CKKS	203,778,393	30,038	*(116x)*	148,292
Dot-Product	NA	589,272	167		14,160
	DO	589,272	167		14,160
	ENC-BFV	213,441,935	30,089	*(180x)*	112,804
	ENC-CKKS	235,657,417	34,125	*(204x)*	148,292
X-Gradient	NA	35,688	4		14,160
	DO	35,688	4		14,160
	ENC-BFV	357,762,502	42,439	*(10,427x)*	112,292
	ENC-CKKS	555,413,370	65,828	*(16,174x)*	148,032
Linear-Regression	NA	556,518	149		14,160
	DO	556,518	149		14,160
	ENC-BFV	255,475,787	36,883	*(248x)*	130,048
	ENC-CKKS	132,301,587	21,769	*(147x)*	146,368
Parrondo	NA	25,047,453	9,535		14,012
	DO	143,643,026	24,058		14,012
	ENC-VIP	71,487,961,658	9,028,822	*(947x)*	14,036

Commentary

- Best
  - First PEC benchmark/programming model

- Limitations
  - Small number of test programs
  - Doesn’t evaluate security
  - Manual algorithm conversion to data oblivious mode