VASA: Vector AES Instructions for Security Applications
Jean-Pierre Münch, Thomas Schneider, Hossein Yalame
ACSAC’21
Motivation – Security Applications

- AES is the most ubiquitous symmetric cipher and used in many applications
  - Disk encryption / Transmission encryption
  - Post-quantum signature schemes [DGK21]
  - Secure two-party computation (STPC)
- STPC protocols are implemented with AES
Motivation - Some Use Cases of Parallel AES

- Disk Encryption / Transmission Encryption [DGK19]
  - Trivial parallelism
  - Solve once

- Post-Quantum Signatures [DG19a, DG19b, DGK21]
  - Accelerate PRFs
  - and PRGs

- Secure Two Party Computation
  - Complex data dependencies from circuits

This work:

Our challenge: Batch enough independent AES calls together for the AES hardware units
Our goal: Improve efficiency of STPC protocol implementations using VAES
Preliminaries - Secure Two-Party Computation (STPC)

- Compute arbitrary function $f$
- On private data $x$, $y$
- Without trusted third party
- Reveal nothing but the result $z = f(x,y)$

Free-XOR [KS08]

Fixed-key Garbling [BHK13] Via AES

[Yao86]
Privacy-preserving Machine Learning (PPML) and Oblivious Transfer (OT)

Privacy-preserving Machine Learning (PPML)

Private DL Model $f$

Private Classification Input $x$

Privately obtains $f(x)$

Learn nothing about model $f$

Oblivious Transfer (OT) Protocol

Alice

Data $x_0, x_1$

Bit $c$

Aladdin

$xc$
AES

AES State

AES-128: $n=10$
AES-192: $n=12$
AES-256: $n=14$
Vectorized AES (VAES) [DGK19]

- Importance of batching data and microarchitectural properties [DGK19]
  - Block ciphers: AES-CTR, AES-CBC, AES-GCM, and AES-GCM-SI.
    - Up to 4× performance improvements

![Diagram of AES process]

- VXOR
- VAESNC
- VAESNCLAST
## AES-NI vs. VAES [Fog]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Haswell</td>
<td>AES-NI</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>2015</td>
<td>Sky lake</td>
<td>AES-NI</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2019</td>
<td>Ice lake</td>
<td>VAES</td>
<td>1/2/4</td>
<td>3/3/3</td>
<td>0.5/0.5/1</td>
<td>6/12/12</td>
</tr>
</tbody>
</table>

**Process Technologies**
- MEROM: 65nm
- NEHALEM: 45nm
- SANDY BRIDGE: 32nm
- HASWELL: 22nm
- SKY LAKE: 14nm
- [DGK19]: 10nm
- ICE LAKE: 10nm
Our Contributions

➢ Automatic batch identification and computation techniques for efficient use of AES in complex security applications

➢ First performance measurements for VAES in the area of STPC
  ➢ STPC frameworks: ABY [DSZ15], EMP-OT [Emptool]
  ➢ PPML framework: CrypTFlow2 [RRKC+20]

➢ Open-source implementation at https://encrypto.de/code/VASA
Parallelization - Baseline Scenario

- Fetch next gate
- Fast Process
- AND?
  - Yes: Process AND
  - No: Fast Process

ACSAC '21 | VASA: Vector AES Instructions for Security Applications | Jean-Pierre Münch, Thomas Schneider, Hossein Yalame | Slide 10
Parallelization - Dynamic Batching

- Fetch next gate
- Use queued? → Yes
  - Process queued ANDs
  - Enqueue AND
- Use queued? → No
  - Fast process
  - AND? → No
  - AND?
  - Yes

Parallelization - Static Batching

1. SIMD
2. Layering
3. Smart Arrangement
Benchmarking – Evaluation Platform

➢ Apple Macbook Pro
  ➢ Intel Core i7-1068NG7, 2x16GB dual rank RAM

❖ Oblivious Transfer in EMP [EMPtool]

❖ Yao’s Garbled Circuit in ABY [DSZ15]

❖ PPML in CrypTFlow2 [RRKC+20]
Benchmarking – OT in EMP Framework

- Passive OT Extension [ALSZ13]: 27% faster
- Active OT Extension [ALSZ15]: 25% faster
- Passive Silent OT [YWLZW20]: 17% faster
- Active Silent OT [YWLZW20]: 17% faster

Reference: VAES
Benchmarking - Yao Garbling in ABY

- PRF Security [GLNP15] +51%
- Circular Security [ZRE15] +56%
- Multi Instance Security [GKWWY20] +47%
- Public Random Permutation [ZRE15] +27%

Average runtimes for applications AES, SHA-1, SCS-PSI, and Phasing-PSI.
Benchmarking - Yao Evaluation in ABY

Average runtimes for applications AES, SHA-1, SCS-PSI, and Phasing-PSI.
Benchmarking – PPML in CrypTFlow2 Framework

Conclusion

✓ Computation in STPC protocols can be accelerated with VAES
✓ Automatic batching of AES calls to the hardware units
✓ VAES yields significant performance improvements for parallel circuits

Future Work

✓ VAES in further MPC protocols
Thank You!

That was VASA:
Vector AES Instructions for Security Applications

Paper: https://ia.cr/2021/1493

Code: https://encrypto.de/code/VASA

Questions?
https://encrypto.de/yalame
Bibliography


