The Fifteenth International Conference on Advances in Circuits, Electronics and Micro-electronics
CENICS 2022
October 16, 2022 to October 20, 2022 - Lisbon, Portugal

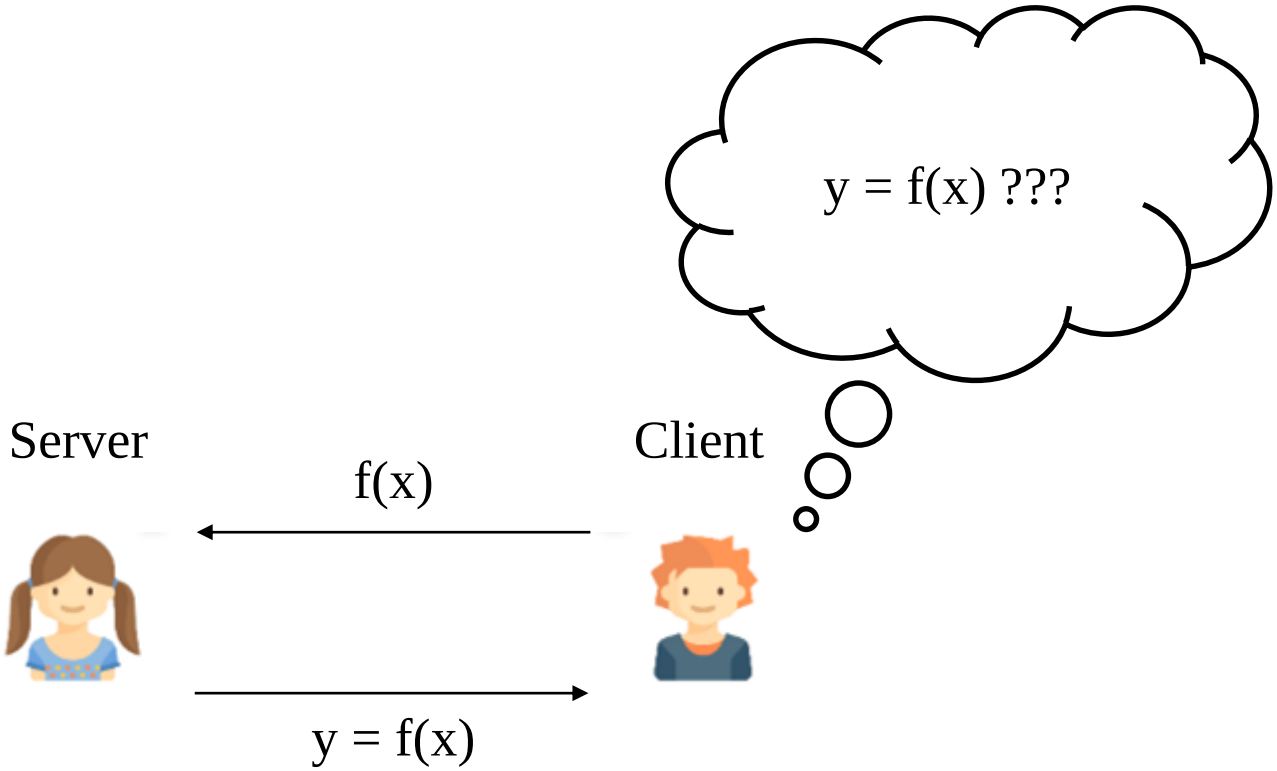
Correct Execution Environment: Hardware-Assisted Verifiable Computation

Junghee Lee, Korea University
(j_lee@korea.ac.kr)

Your Speaker

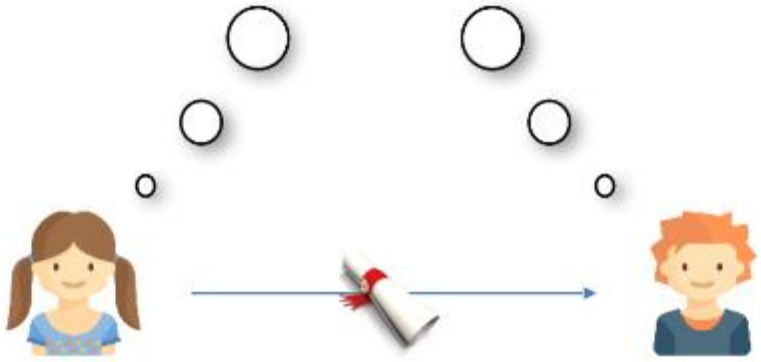
- Education
  - Ph.D Georgia Institute of Technology (2013)
  - M.S. Seoul National University (2003)
  - B.S. Seoul National University (2000)
- Appointments
  - Assistant/Associate Professor
    Korea University (2019-Present)
  - Assistant Professor
    University of Texas at San Antonio (2014-2019)
  - Engineer
    Samsung Electronics (2003-2008)
- Research area
  - Hardware security (processor, memory, non-volatile memory, storage, dedicated hardware)

Verifiable Computation



Cryptographic VC

$EK, VK \leftarrow KeyGen(1^{\lambda})$



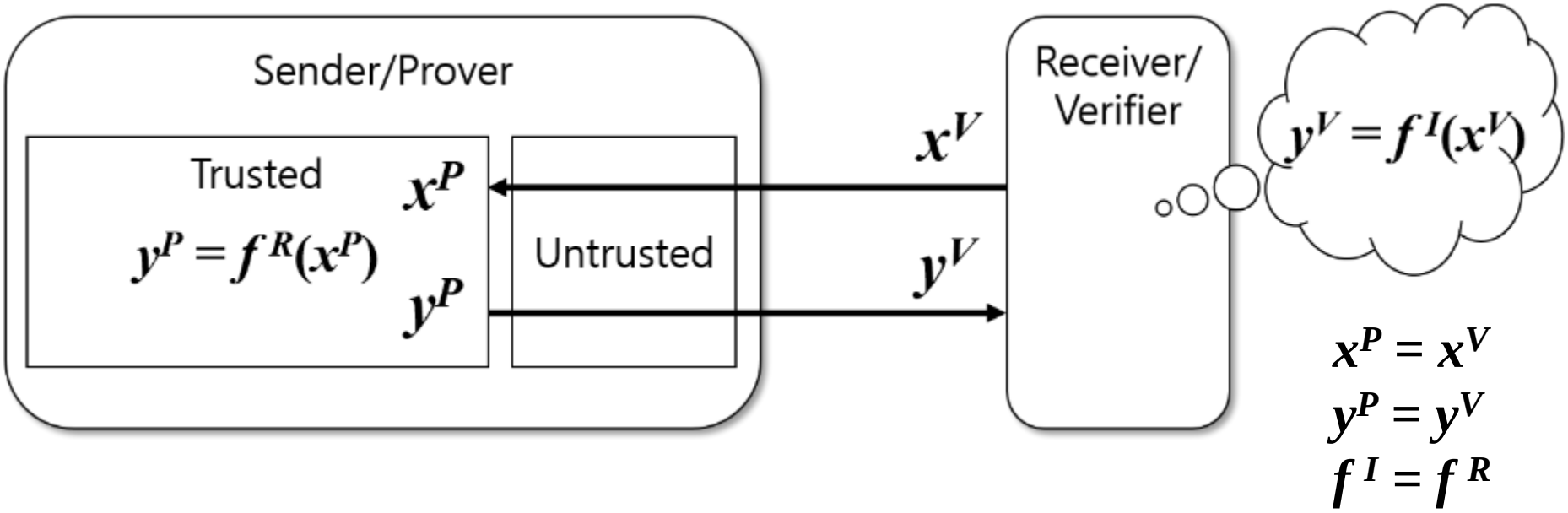
Prover

Verifier

$y, \pi \leftarrow compute(EK, F, x)$

$verify(VK, F, x, y, \pi)==1$

Hardware-Assisted VC



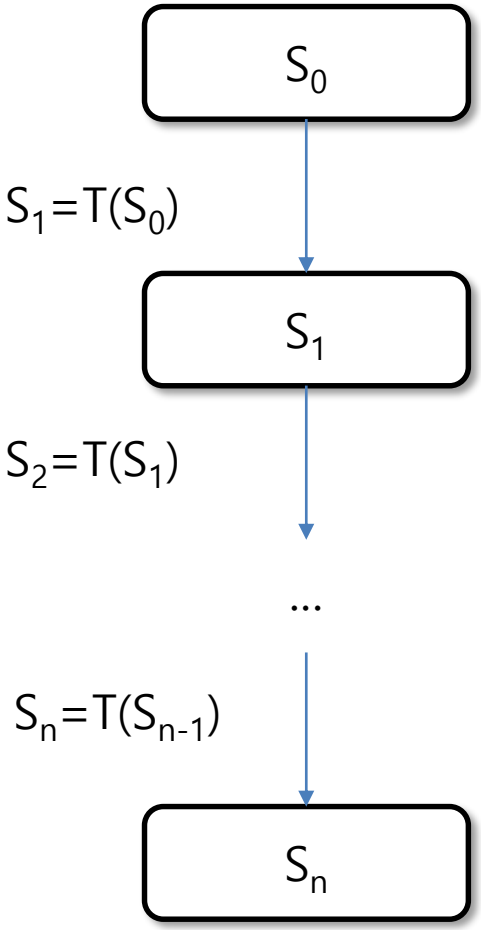
Contents

- Introduction
- Background and Motivation
- Correct Execution Environment
- Evaluation
- Conclusions

VC Construction

- For y=f(x)
- Three algorithms
  - (EK, VK) ← KeyGen(1^{λ})
  - (y, π) ← Compute(EK, f, x)
  - {0,1} ← Verify(VK, f, x, y, π)
- Guaranteed properties
  - Completeness
  - Soundness

Cryptographic Approach



- Verifies every step of computation
  - Checks the hash of the previous state
  - Generates the proof of every instruction
- Extremely slow
  - 10,000 ~ 100,000 times slower

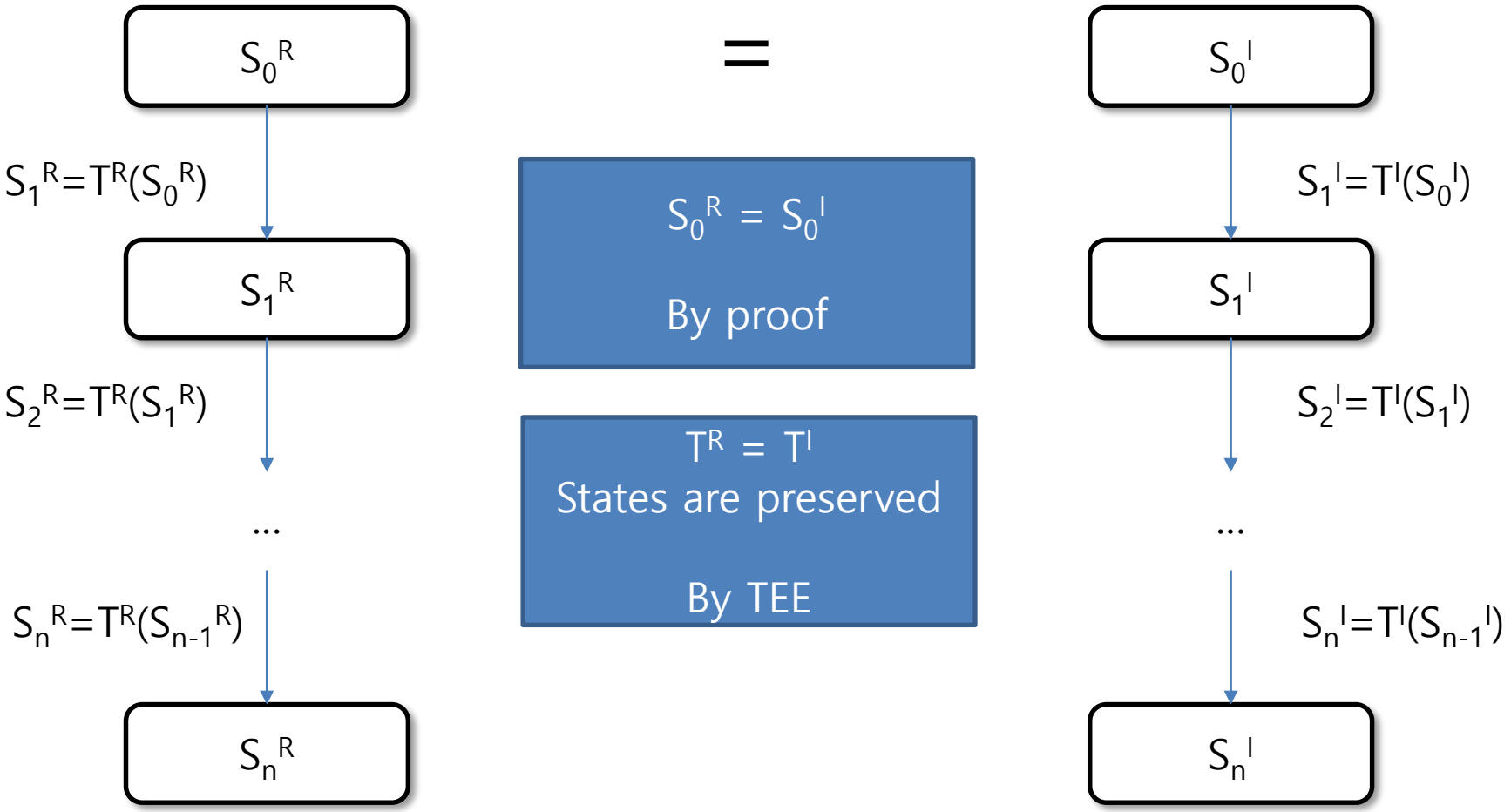
Trusted Hardware

- Trusted Execution Environment (TEE)
  - Hardware guarantees the correct execution of a protected application by isolation and attestation
- TEE for VC
  - If the hardware guarantees correct execution, we do not have to verify every step
- Formality
  - We need to define what exactly the hardware guarantees and what should be included to the proof

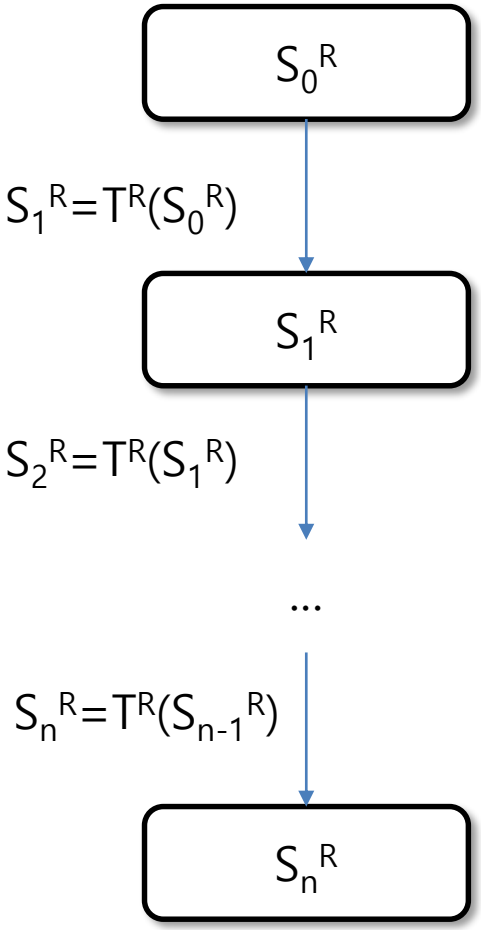
Contents

- Introduction
- Background and Motivation
- Correct Execution Environment
- Evaluation
- Conclusions

Correct Execution Environment



State Preservation



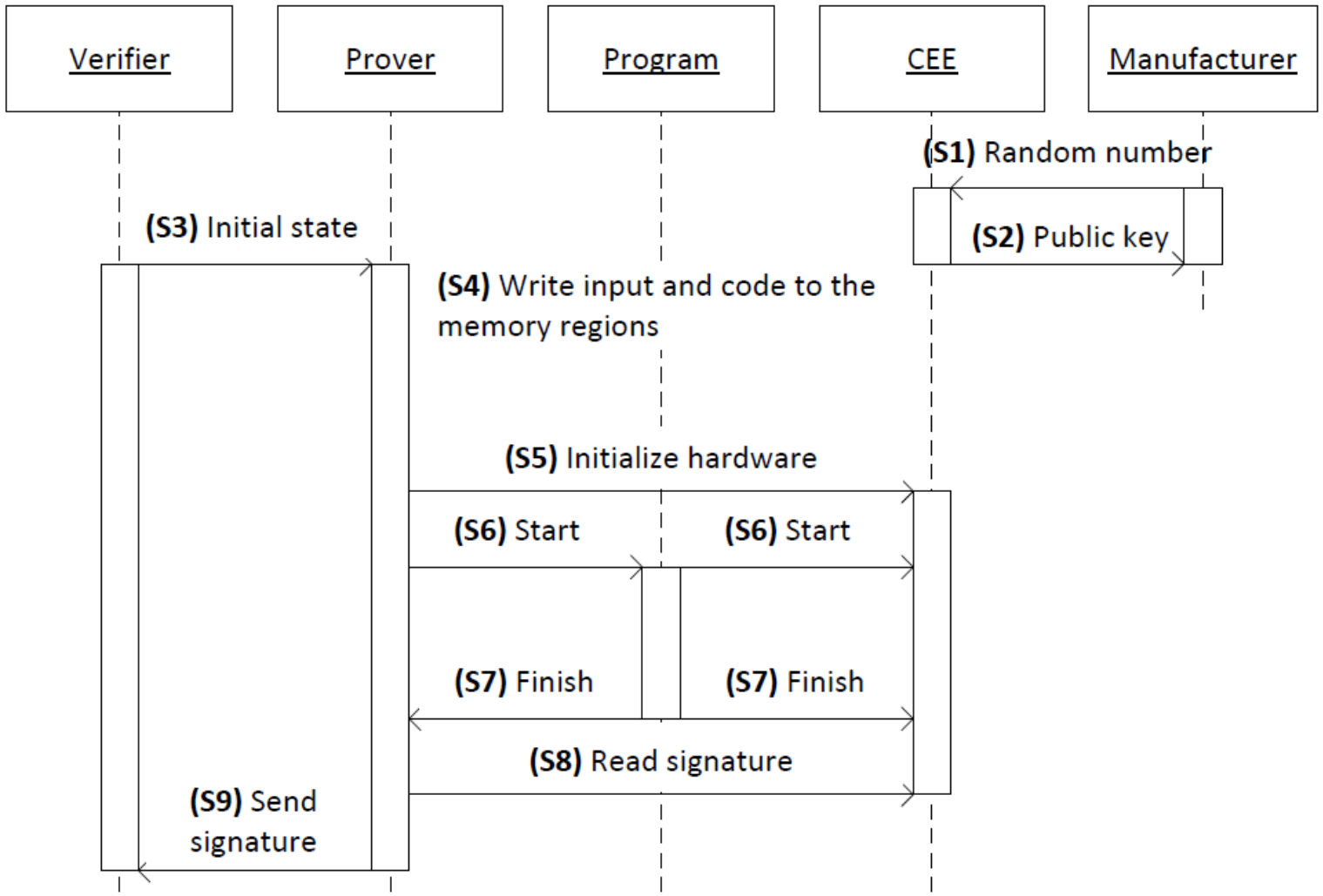
Preventing memory access to physical pages used by the protected application
➔ OS services cannot be used

A shared memory region may be allowed
➔ Its integrity should be managed by the developer

CEE VC Construction

- Digital signature scheme
  - $(SK, PK) \leftarrow Gen(1^{\lambda})$
  - $\sigma \leftarrow Sig(m, SK)$
  - $\{0,1\} \leftarrow Ver(m, \sigma, PK)$
- CEE VC construction
  - KeyGen
    - $(EK, VK) \leftarrow Gen$
  - Compute
    - $\pi \leftarrow Sig(S_0 || S_n, EK)$
  - Verify
    - $\{0,1\} \leftarrow Ver(S_0 || S_n, \pi, VK)$

CEE VC Scheme



Contents

- Introduction
- Background and Motivation
- Correct Execution Environment
- Evaluation
- Conclusions

Prototype

- By modifying AMBER processor
  - ARM-compatible open-source processor written in Verilog
- Tools
  - Xilinx ISE Verilog simulator
  - Synopsys Design Compiler

MiBench Suite

Benchmark	Executed	Program size	Input size
ADPCM	121,672	5,116 B	3,072 B
BitCount	115,895	4,828 B	292 B
BlowFish	372,860	4,820 B	4,258 B
CRC32	137,460	4,576 B	1,136 B
QuickSort	126,712	4,320 B	528 B
SHA	239,833	5,968 B	672 B
StringSearch	167,549	4,444 B	2,852 B

Prover Overhead

Benchmark	Original	Proposed	No-limit[1)]	Limit[2)]
ADPCM	1.82 ms	2.01 ms	885.50 h	3.00 h
BitCount	1.99 ms	2.06 ms	843.45 h	2.86 h
BlowFish	5.41 ms	5.68 ms	2,713.59 h	N/A
CRC32	2.55 ms	2.67 ms	1,000.40 h	3.39 h
QuickSort	1.91 ms	1.98 ms	922.18 h	3.13 h
SHA	3.62 ms	3.75 ms	1,745.45 h	6.58 h
StringSearch	2.45 ms	2.60 ms	1,219.38 h	4.60 h

1) E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable zero knowledge via cycles of elliptic curves," Algorithmica, vol. 79, Dec. 2017.
2) E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct noninteractive zero knowledge for a von neumann architecture," in Proceedings of the 23rd USENIX Conference on Security Symposium. USENIX Association, 2014.

Verifier Overhead

Benchmark	Original	Proposed	No-limit[1)]	Limit[2)]
ADPCM	1.82 ms	1.43 ms	59.69 ms	43.26 ms
BitCount	1.99 ms	1.56 ms	57.67 ms	41.19 ms
BlowFish	5.41 ms	1.52 ms	57.61 ms	N/A
CRC32	2.55 ms	1.73 ms	55.90 ms	44.14 ms
QuickSort	1.91 ms	1.24 ms	54.10 ms	41.37 ms
SHA	3.62 ms	1.30 ms	65.67 ms	41.48 ms
StringSearch	2.45 ms	1.35 ms	54.97 ms	43.09 ms

1) E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable zero knowledge via cycles of elliptic curves," Algorithmica, vol. 79, Dec. 2017.
2) E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct noninteractive zero knowledge for a von neumann architecture," in Proceedings of the 23rd USENIX Conference on Security Symposium. USENIX Association, 2014.

Hardware Cost

Hardware Cost

Component	Original	Modified	Overhead
Register file	0.023 mm^2	0.032 mm^2	41.47 %
Execution stage	0.021 mm^2	0.025 mm^2	19.86 %
Cache controller	0.002 mm^2	0.006 mm^2	209.71 %
Signature	-	0.257 mm^2	-
Interface	-	0.004 mm^2	-
Unchanged	0.085 mm^2	0.085 mm^2	-
Total	0.131 mm^2	0.409 mm^2	213.72 %

Conclusions

- A trusted hardware-based verifiable computation scheme is proposed.
- It offers order-of-magnitude shorter execution time compared to cryptographic approaches.
- The required properties for the hardware and security properties guaranteed by the hardware are formally defined.