NYU

CENTER FOR
CYBER SECURITY

Hardware Evaluation of NIST PQC Round-2 Algorithms

Deepraj Soni[1], Kanad Basu[2], Mohammed Nabeel[3], Ramesh Karri[1]
New York University

[1]New York University - New York, NY, USA
[2]University of Texas at Dallas - Dallas, Texas, USA
[3]New York University - Abu Dhabi, Abu Dhabi, UAE

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Outline

- High-Level Synthesis (HLS)
- Design Space Exploration (DSE)
- HLS-based Design flow
- Design Space Exploration example for a PQC algorithm
- Security level-2 Signature schemes comparison
- FPGA Demo
- Conclusion
- Future Work
- Acknowledgement

Motivation for High Level Synthesis (HLS)

Two approaches: (1) Register-Transfer Level (RTL) - based implementation and (2) High Level Synthesis (HLS) - based implementation.

RTL-Based Implementation:

- Better performance and less resource utilization (area overhead).
- Requires more time for implementation and verification.
- The architecture is fixed.

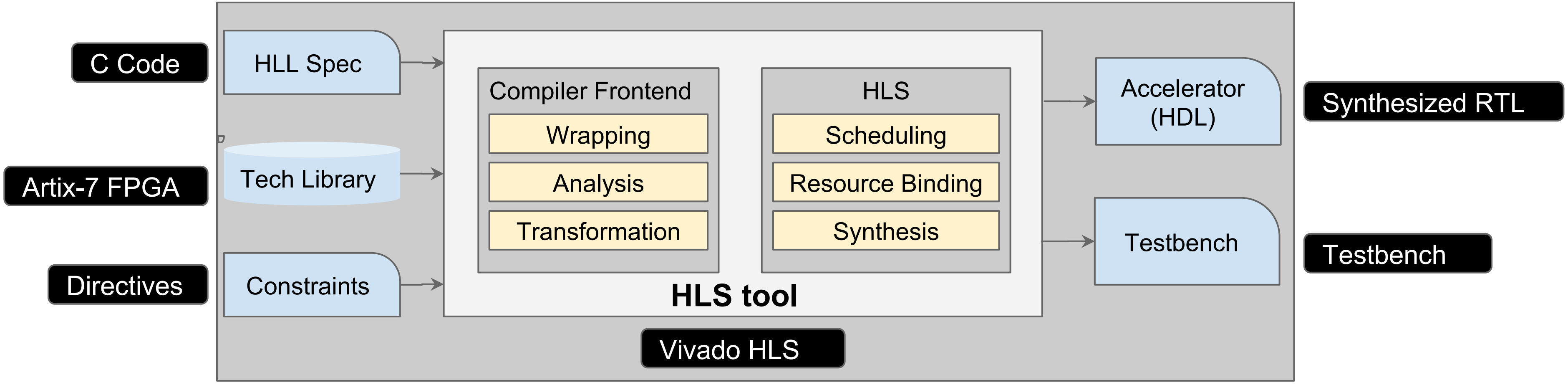
HLS-Based Implementation:

- Might be less efficient and customizable.
  - Depends upon application, skill of the engineer, etc.
- Faster and easier implementation due to algorithmic approach.
- Easy to change the design and architecture.
  - Useful for Design-space exploration.

High Level Synthesis (HLS)

High-Level Synthesis (HLS) is used to automatically generate RTL designs starting from a high-level specification.

- It leverages state-of-the-art compilers (e.g., GCC or LLVM).
- It implements several hardware-oriented and technology-aware optimizations.



HLS based design process

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

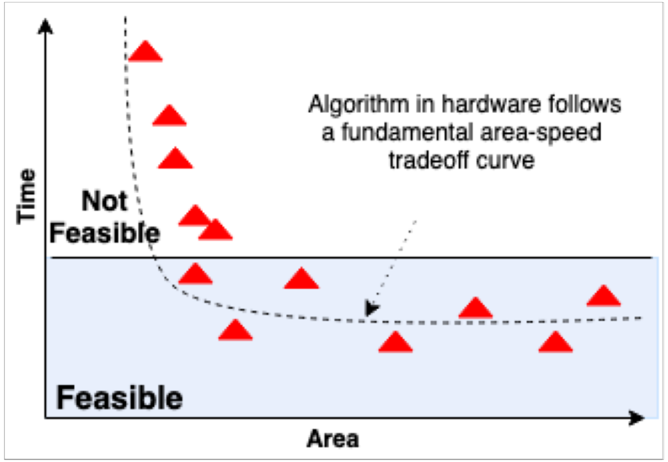
Design Space Exploration

Design Space Exploration (DSE) refers to systematic analysis and removing of unwanted design points based on parameters of interest.

It helps to evaluate the trade-off between parameters of interest.

For IoT devices, area is the most important parameter.

For Servers, speed is the most important parameter.



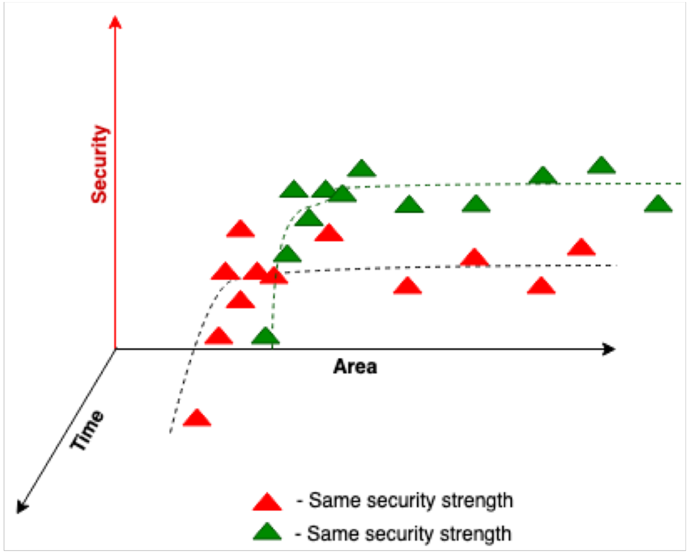
Design-space exploration

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Design Space Exploration (DSE)

We are focusing on three parameters: Security, Time and Area.

For each algorithm security level, tens of different design points are identified.

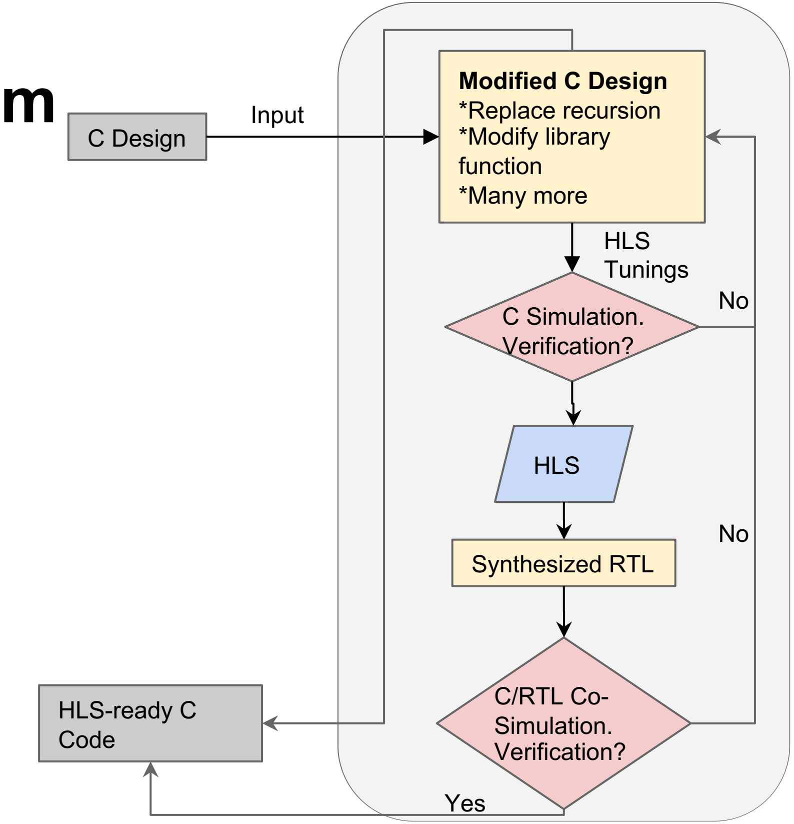


3-D Design-space exploration

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

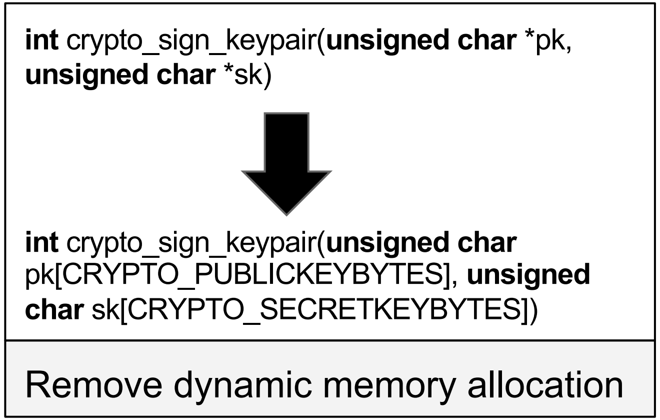
Design Flow for PQC algorithm Part-1: Preparing the C code

- Input C design is taken from NIST PQC Round-2 submission.
- The C code has to go through lot of changes to make it HLS-ready. NIST PQC Round-2 developers provided required help for this.
- NIST KATs are used for verification.
- For qTesla security level -1, we have to make around 40 modifications.



HLS-based implementation of PQC algorithms.

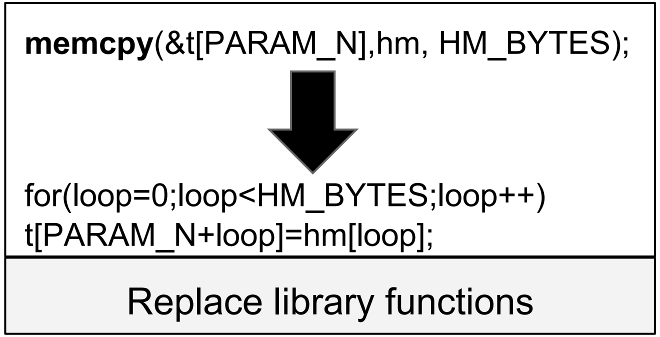
Examples of C code changes



```
int crypto_sign_keypair(unsigned char *pk,
unsigned char *sk)
```

```
int crypto_sign_keypair(unsigned char
pk[CRYPTO_PUBLICKEYBYTES], unsigned
char sk[CRYPTO_SECRETKEYBYTES])
```

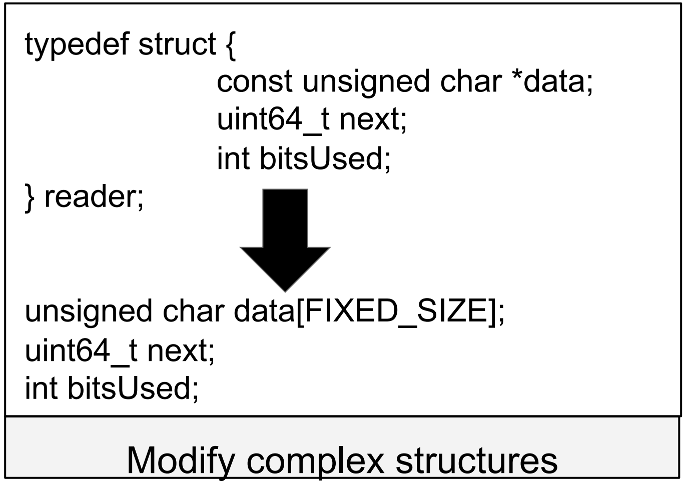
Remove dynamic memory allocation



```
memcpy(&t[PARAM_N],hm, HM_BYTES);
```

```
for(loop=0;loop<HM_BYTES;loop++)
t[PARAM_N+loop]=hm[loop];
```

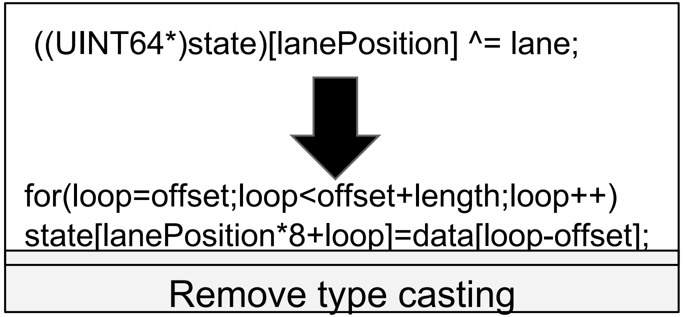
Replace library functions



```
typedef struct {
                    const unsigned char *data;
                    uint64_t next;
                    int bitsUsed;
} reader;
```

```
unsigned char data[FIXED_SIZE];
uint64_t next;
int bitsUsed;
```

Modify complex structures



```
 ((UINT64*)state)[lanePosition] ^= lane;
```

```
for(loop=offset;loop<offset+length;loop++)
state[lanePosition*8+loop]=data[loop-offset];
```

Remove type casting

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

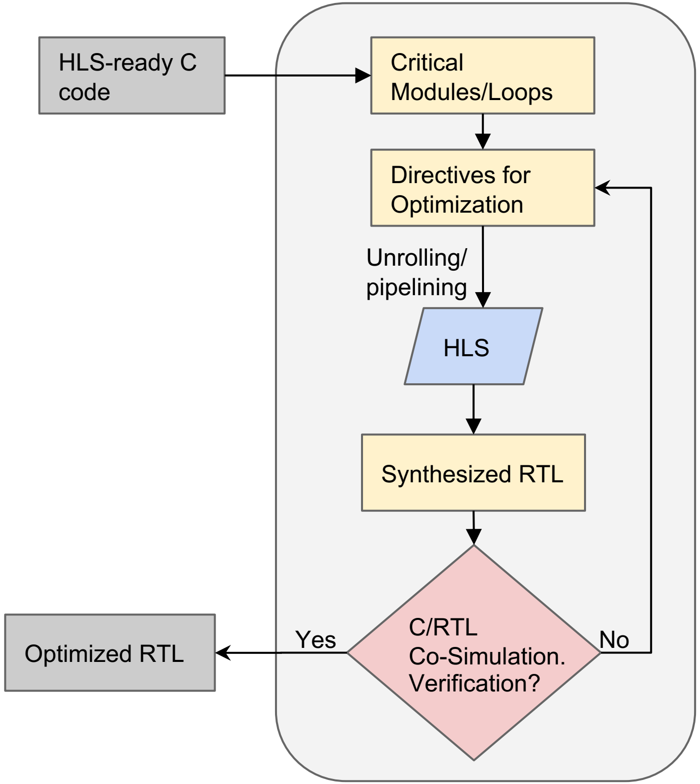
Design Flow for PQC algorithm Part-2: Generation of RTL

- The modules/loops/functions which take more time or area is defined as critical modules/loops/functions.

- Loop Unrolling and Pipelining improves performance.

- C/RTL co-simulation for verification of Hardware.

- Final optimized RTL verified with KATs.



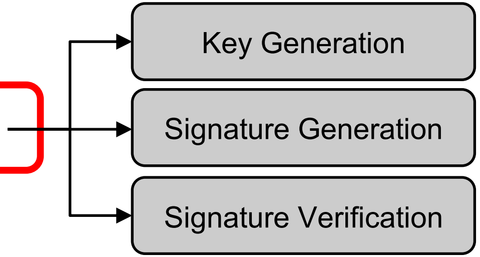
HLS-based design exploration flow of PQC algorithms.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Scope of the ongoing study

- 17 KEMs.
- 9 Signature schemes.

Algorithm	Security Level 1	Security Level 2	Security Level 3	Security Level 4	Security Level 5
Crystals-Dilithium	X	X	X	X	
qTESLA	X	X	X		X
MQDSS		X		X	
LUOV		X		X	X
SPHINCS+	X		X		X
PICNIC	X		X		X
FALCON	X		X		X
GeMSS	X		X		X
Rainbow	X		X		X



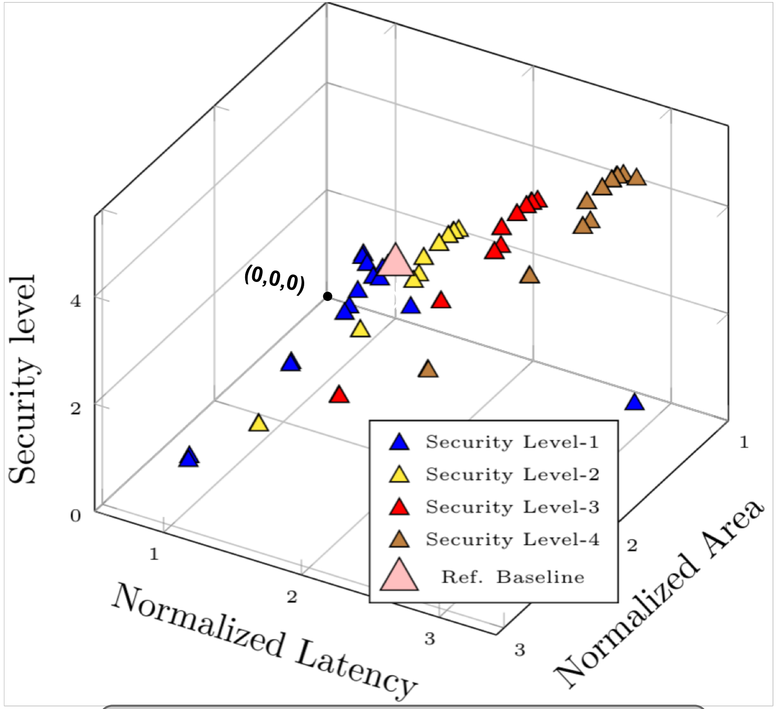
Key Generation

Signature Generation

Signature Verification

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Design Space Exploration (DSE) of CRYSTALS-Dilithium

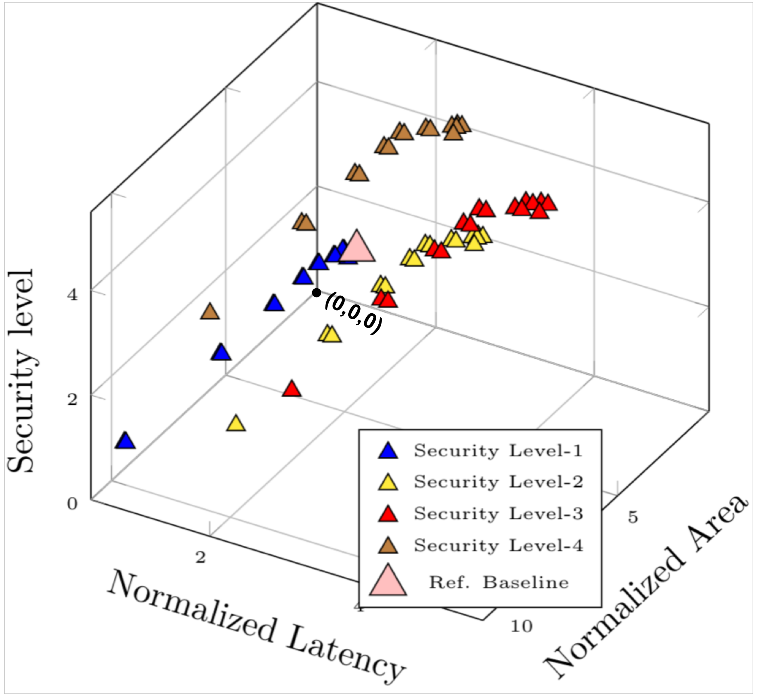


Key Generation

- Design-space exploration of CRYSTALS-Dilithium is normalised with baseline security level-1 LUT and latency.
- The area overhead is similar for different security level.
- The Latency increases as security strength increases.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

DSE of CRYSTALS-Dilithium

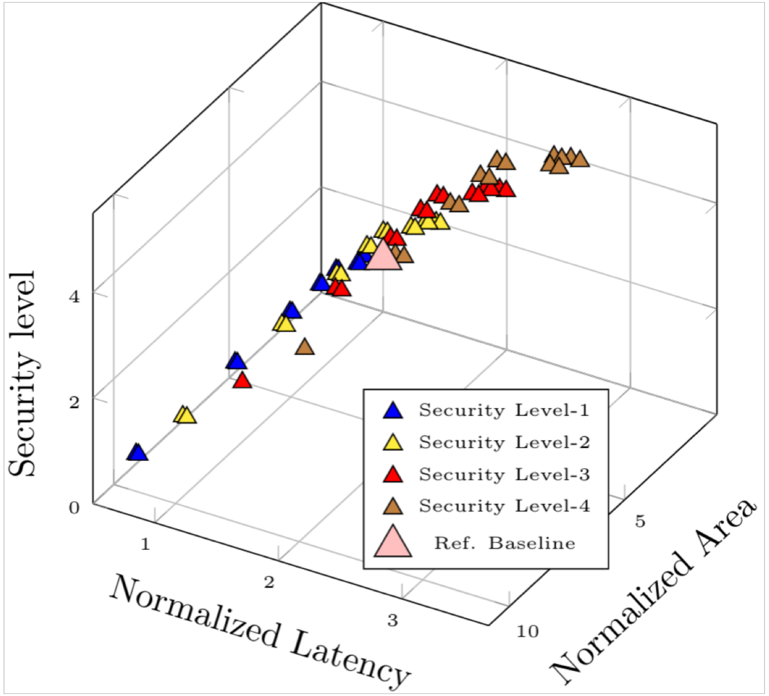


Signature Generation

- Design-space exploration of CRYSTALS-Dilithium is normalised with baseline security level-1 LUT and latency.
- The optimization directives improves the performance and area in hardware compared to baseline implementation.
- The area overhead is similar for different security level.
- The Latency increases as security strength increases.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

DSE of CRYSTALS-Dilithium

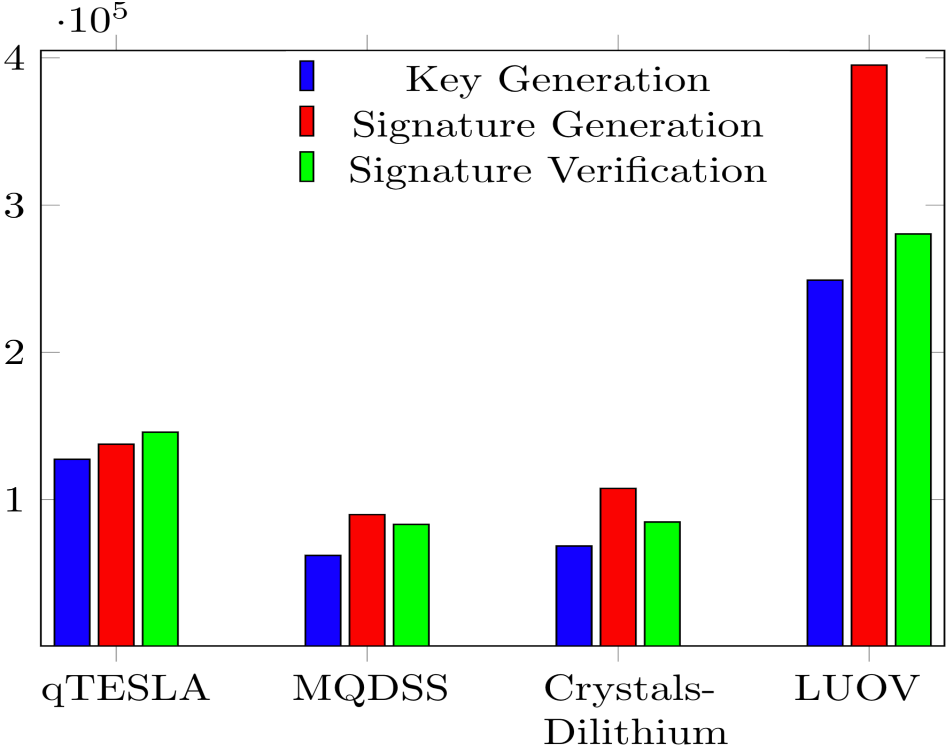


Signature Verification

- Design-space exploration of CRYSTALS-Dilithium is normalised with baseline security level-1 LUT and latency.
- The difference in area and latency is less as the points are closer to each other.
- The Latency increases as security strength increases.

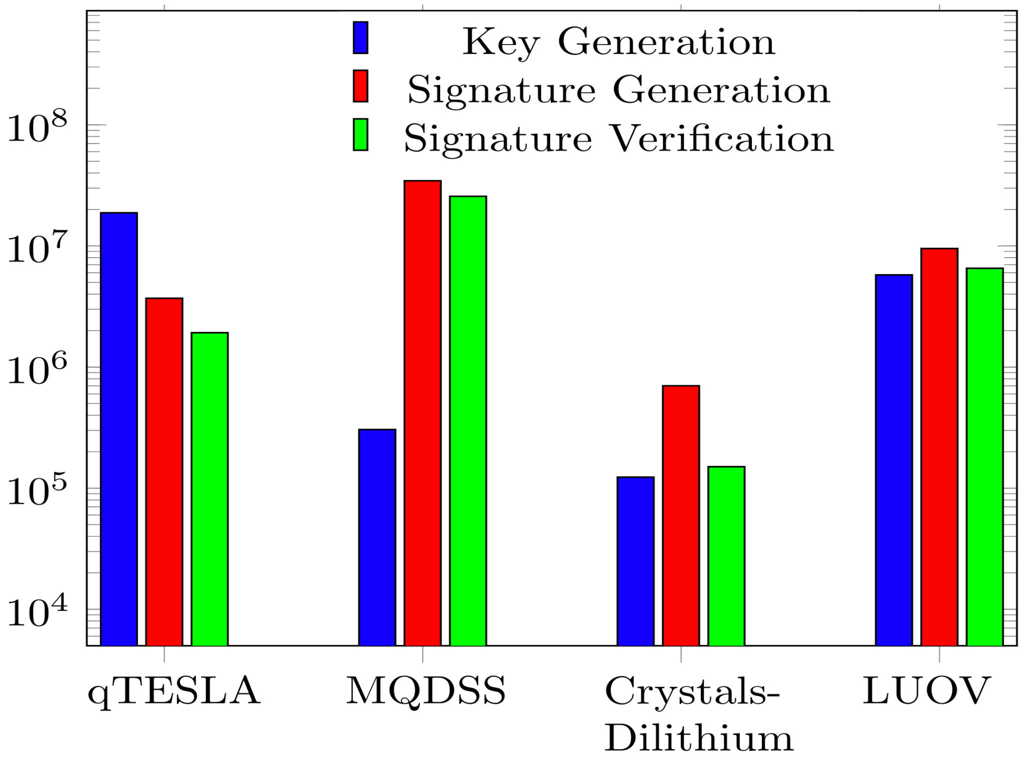
Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Area Comparison for Security level-2 Signature Schemes



LookUp Table comparison for security level-2 of signature schemes.

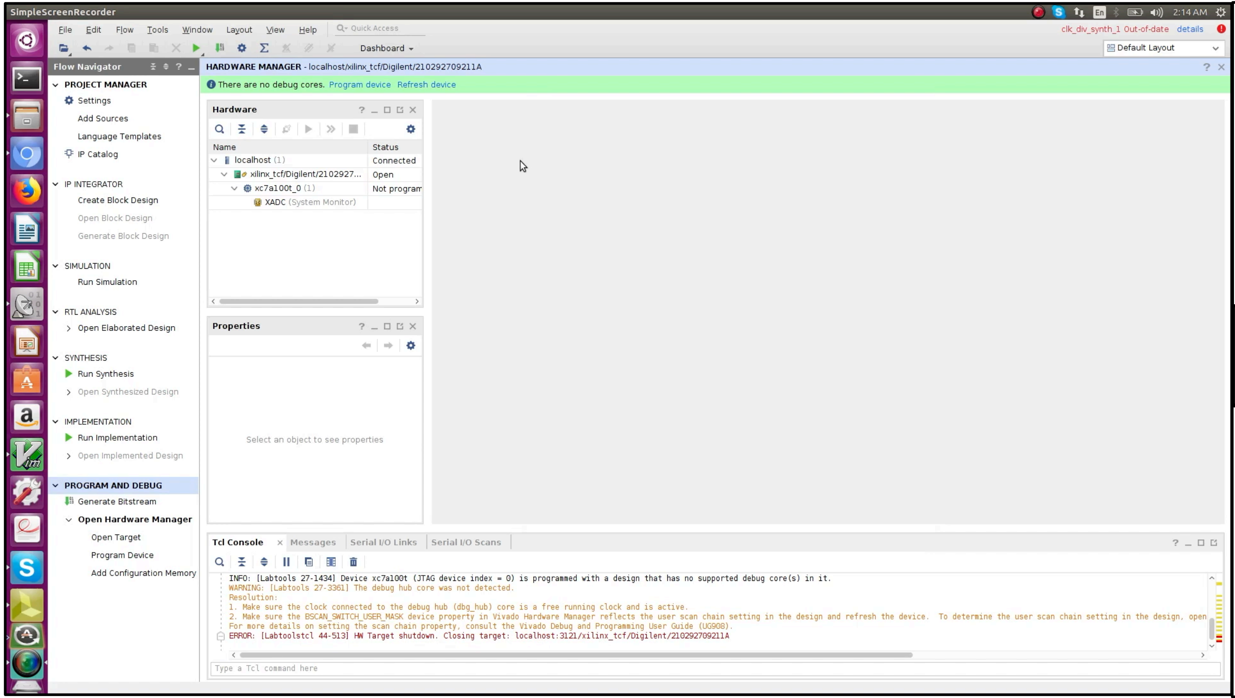
Performance Comparison for Security level-2 Signature Schemes



Latency comparison for security level-2 of signature schemes.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

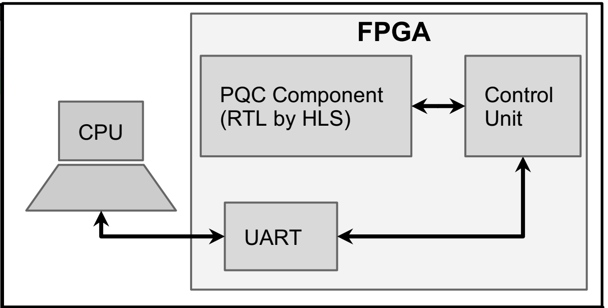
FPGA Demo for CRYSTALS-Dilithium Signature Generation



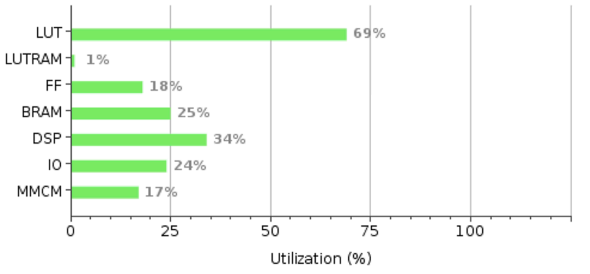
There are no debug cores. Program device Refresh device

Name	Status
localhost (1)	Connected
xilinx_tcf/Digilent/2102927...	Open
xc7a100t_0 (1)	Not program
XADC (System Monitor)	

```
INFO: [Labtools 27-1434] Device xc7a100t (JTAG device index = 0) is programmed with a design that has no supported debug core(s) in it.
WARNING: [Labtools 27-3361] The debug hub core was not detected.
Resolution:
1. Make sure the clock connected to the debug hub (dbg_hub) core is a free running clock and is active.
2. Make sure the BSCAN_SWITCH_USER_MASK device property in Vivado Hardware Manager reflects the user scan chain setting in the design and refresh the device.  To determine the user scan chain setting in the design, open
For more details on setting the scan chain property, consult the Vivado Debug and Programming User Guide (UG908).
ERROR: [Labtoolstcl 44-513] HW Target shutdown. Closing target: localhost:3121/xilinx_tcf/Digilent/210292709211A
```



Latency clock cycle = 701166
Clock Frequency = 50MHz



*Artix-7 FPGA is recommended by NIST.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Conclusion

- The RTL generated by HLS can be used for hardware design of the PQC algorithm. It can be used as first implementation of hardware. Manual implementation can further improve the design.
- Other teams are focusing on software/hardware co-design and speed up or implementing some part of the design in hardware. We are focusing on complete hardware design and its evaluation.
- For Security level-2
  - CRYSTALS-Dilithium has the best performance in signature schemes.
  - CRYSTALS-Dilithium and MQDSS have less area while LUOV area overhead is significantly more.
- With HLS, design-space exploration is analyzed. Design-Space exploration helps to estimate performance and area of hardware architecture.

Paper: https://eprint.iacr.org/2019/047.pdf
Website: https://wp.nyu.edu/hipqccheck/

Future Research

- For design-space exploration, **POWER** would be added as one more parameter.
- FPGA implementation and analysis of the PQC algorithms.
- Automate the HLS-synthesizable C generation process.
- Evaluate the hardware implementations against side-channel attacks.

Acknowledgement

Special thanks to NIST PQC algorithm Developers for helping us realize the hardware by answering questions while implementation.

- Dr. Nina Bindel for qTESLA.
- Dr. Ward Beullens for LUOV.
- Dr. Greg Zaverucha and Dr. Sebastian Ramacher for Picnic.
- Dr. Jintai Ding and Dr. Ming-Shing Chen for RAINBOW.
- Dr. Alessandro Barenghi for LEDAcrypt.
- Dr. Xianhui Lu for LAC.
- Dr. Ludovic Perret for GeMSS
- Dr. Marc Manzano and Dr. Najwa Aaraj of DarkMatter inc. Abu Dhabi, UAE offered timely and insightful feedback (especially to explore the security-informed trade-offs) on the early drafts of the report.