# Project Topic Choice

1

## Project

✓**Cryptography Projects** - proposed by the Instructor

✓ **Projects in your domain of expertise**, e.g.,
Machine Learning, Big Data, DSP,
Remote Sensing & Image Processing,
Bioengineering, etc.

- ✓ you will be responsible for defining and specifying a topic & scope of these projects by yourselves
- ✓ an additional advisor, such as your MS/PhD Thesis advisor or manager at work highly recommended

2

## Cryptography Projects

- ✓related to the research project conducted by Cryptographic Engineering Research Group (CERG) at GMU
- ✓ supporting NIST (National Institute of Standards and Technology) in the evaluation of candidates for new cryptographic standards
- ✓ do not require knowledge of cryptography!

3

## Three Project Types

1. **Lightweight Cryptography (LWC)**
2. **Post-Quantum Cryptography (PQC)**
3. **Other domains proposed by you**

4

## Type 1: Lightweight Cryptography (LWC)

One of the following Round 2 candidates in the NIST Lightweight Cryptography standardization process:

1. DryGASCON
2. ForkAE
3. ORANGE
4. SAEAES
5. SpoC
6. Spook
7. Subterranean 2.0, or
8. SUNDAE-GIFT

**No known hardware design or VHDL code**

5

## Type 1: Lightweight Cryptography (LWC)

**Given:**

1. **Specification, including pseudocode**
2. **Reference implementation in C**
3. **Hardware API, including the interface**
4. Verilog code
   (all except ORANGE, SAEAES, SUNDAE-GIFT)
5. Results of the Verilog implementation
   (all except ORANGE, SAEAES, SUNDAE-GIFT)

Lightweight Cryptography, Round 2 Candidates
https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates

6

# LWC Hardware API proposed by GMU, TUM, & VT

## 1. Minimum Compliance Criteria

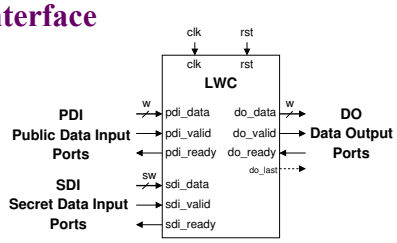
- Supported operations
- Permitted input sizes
- Decrypted plaintext release
- Permitted data port widths

etc.

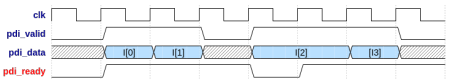
## 3. Communication Protocol

| instruction = ACTKEY |
|---|
| instruction = ENC |
| seg_0_header |
| seg_0 = Npub |
| seg_1_header |
| seg_1 = AD |
| seg_2_header |
| seg_2 = Plaintext |

## 2. Interface




## 4. Timing Characteristics

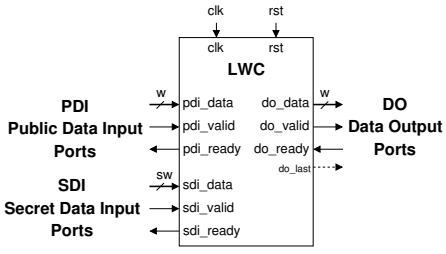



Hardware API for Lightweight Cryptography
https://cryptography.gmu.edu/athena/LWC/LWC_HW_API.pdf

7

# LWC Hardware Development Package by GMU, TUM, & VT

## Helpful for all designers



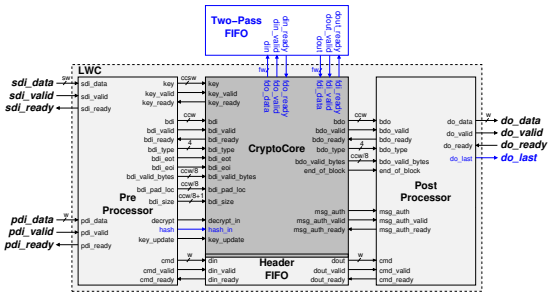

- **Universal testbench (LWC_TB)**
- **Test vector generator (cryptotvgen)**

Implementer's Guide + Development Package
https://cryptography.gmu.edu/athena/index.php?id=LWC

8

## LWC Hardware Development Package by GMU, TUM, & VT

**Helpful for designers following the recommended design flow**




- **VHDL code of a generic PreProcessor, PostProcessor, and Header FIFO**
- **CryptoCore of a dummy authenticated cipher with hash functionality**

Implementer's Guide + Development Package
https://cryptography.gmu.edu/athena/index.php?id=LWC

9

## Type 2: Post-Quantum Cryptography

A basic building block of a Post-Quantum Cryptography algorithm, e.g.,

1. Schoolbook polynomial multiplier
2. Toom-Cook polynomial multiplier
3. Fast Fourier Transform
4. Number Theoretic Transform
5. Arithmetic Masking to Boolean Masking Converter
6. Boolean Masking to Arithmetic Masking Converter

**No known hardware design or VHDL code**

10

## Type 2: Post-Quantum Cryptography

**Given:**

1. **Specification, including pseudocode**
2. **Reference implementation in C**
3. Simplified block diagrams
   (for some blocks only)
4. HDL code
   (for some blocks only)

Post-Quantum Cryptography, Round 3 Submissions
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

11

## Type 3: Other Domains Proposed by You

Primarily directed at students who do hardware development as a part of your
- Graduate Research Assistantship
- Master's Thesis research
- Ph.D. Thesis research
- full-time or part-time job
- hobby, etc.

A co-advising of the project by your GRA supervisor, thesis advisor, or your manager at work, who is an expert in a given domain, is highly recommended.

**No known hardware design or VHDL code**

12

## Project Declaration by Monday, October 11

If you already have a partner:
**GROUP {**
**<Name 1>**
**<Name 2>**
**}**

If you do not have a partner, but you are open to working as a part of a group:
**<Your Name>, <Preferred e-mail address> - open to forming a group**

If you prefer to work individually:
**<Your Name> - working individually**

**If you would like to work on project type 3, please send me an e-mail explaining an idea for your project.**

13

## Individual vs. Team Projects

**Individual:**

You will be expected to design, implement, verify, and benchmark
- **one architecture of a single algorithm**.

**Team of 2:**

You will be expected to design, implement, verify, and benchmark
- **two architectures of a single algorithm**
  (with different trade-offs between speed and area)
  **or**
- **one architecture supporting two related algorithms**
  with resource sharing (e.g., an authenticated cipher and a hash function of a single LWC candidate).

14

## The First Project Tasks

**(recommended to be completed within 2 weeks of the project assignment)**

1. **Get familiar with the algorithm specification (without security analysis)**
2. **Get familiar with the reference implementation in C**
3. **Get familiar with the required hardware API or develop it by yourself**
4. **Draw a block diagram of the Datapath**

15

## Project Choice

**Choose**

1. Project Type
2. Project Partner (if any)

**Deadline**

**Monday, October 11, 11:59 PM**

**Specify your preferences in the following Google Doc**

https://docs.google.com/document/d/1O8SOPjv79TGHXxgJvRyL5cJK9qkNH2xOm6j1CwKtv-Y/edit?usp=sharing

16