Considerations When Designing Sponge-based Extendable-Output Functions for Lightweight and Mobile Devices

Meaad Tori, David Paul, William Billlingsley
School of Science & Technology
University of New England
Armidale, Australia
email: mtori@myune.edu.au, David.Paul@une.edu.au, wbilling@une.edu.au

Date 25/05/2022

Presenter Name : Meaad Tori

Meaad Tori has a Masters of Information Technology from the University of New England , Australia in 2014. She is currently a doctoral student at school of science and Technology in the area of lightweight cryptography.

research interest

Designing a lightweight sponge-based extendable output function (XOF) that should allow correctly balanced security and performance in environments where compute power, available memory, and battery life may all be limited, also for various wireless or mobile systems.

une University of New England

Faculty of Science, Agriculture, Business and Law

Aims

- General consideration of existing lightweight XOFs

- Deep analysis of three:
  - Ascon
  - Gimli
  - Xoodyak

University of New England

Faculty of Science, Agriculture, Business and Law

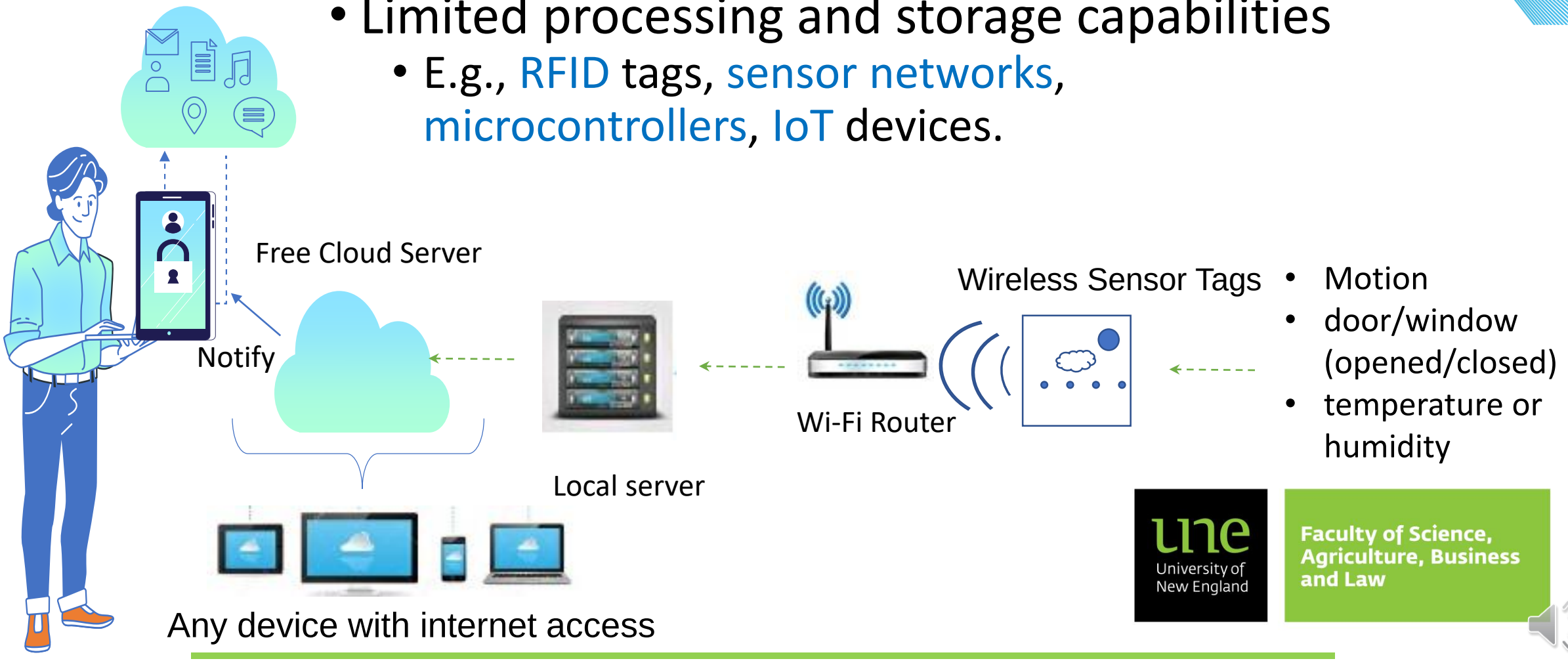
Contributions

- A set of design considerations
  - Round function width
  - Number of rounds
  - Round constants
  - Rate
  - Linear layer
  - Nonlinear layer
  - Security claim

une University of New England
Faculty of Science, Agriculture, Business and Law

What is a Resource-constrained Device?

- Limited processing and storage capabilities
  - E.g., RFID tags, sensor networks, microcontrollers, IoT devices.



- Motion
- door/window (opened/closed)
- temperature or humidity

une University of New England

Faculty of Science, Agriculture, Business and Law

Some Applications

01

Automobiles

•In-vehicle, vehicle-to-vehicle and road-to-vehicle communication, driving assistance systems.

02

Medical sensors

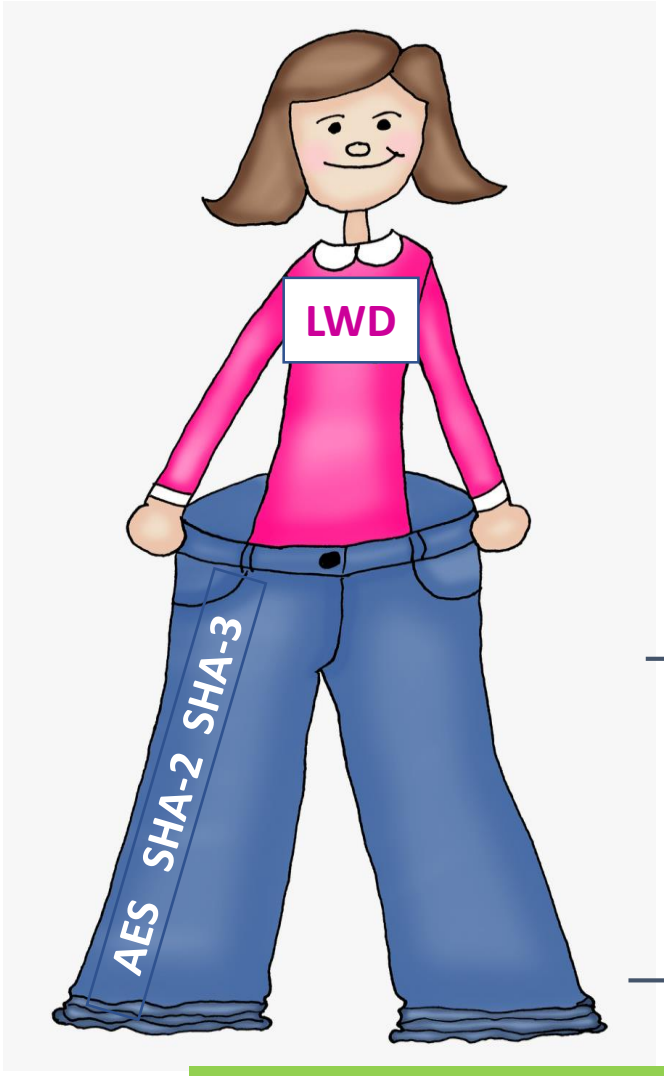
•Measuring blood pressure, blood sugar etc.

03

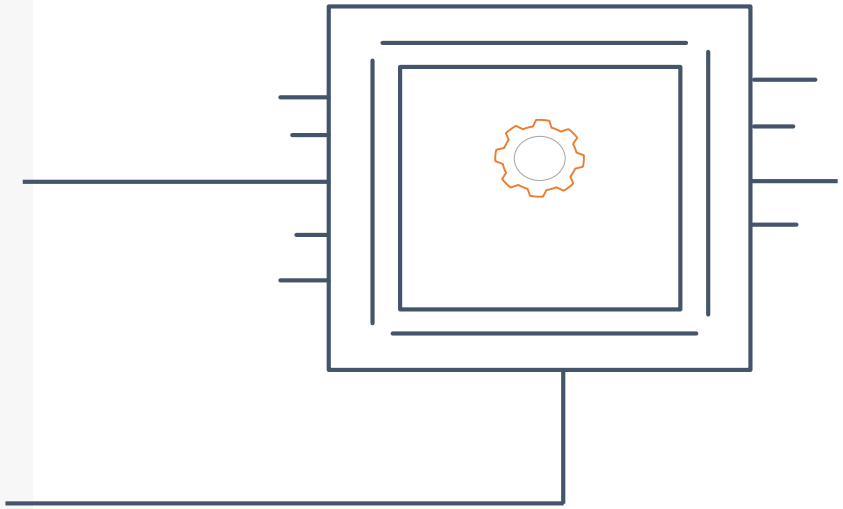
Smart Home Appliances

•Smart Heating, Door Locks, smart gardening

Why is it Difficult to Secure Lightweight Devices?



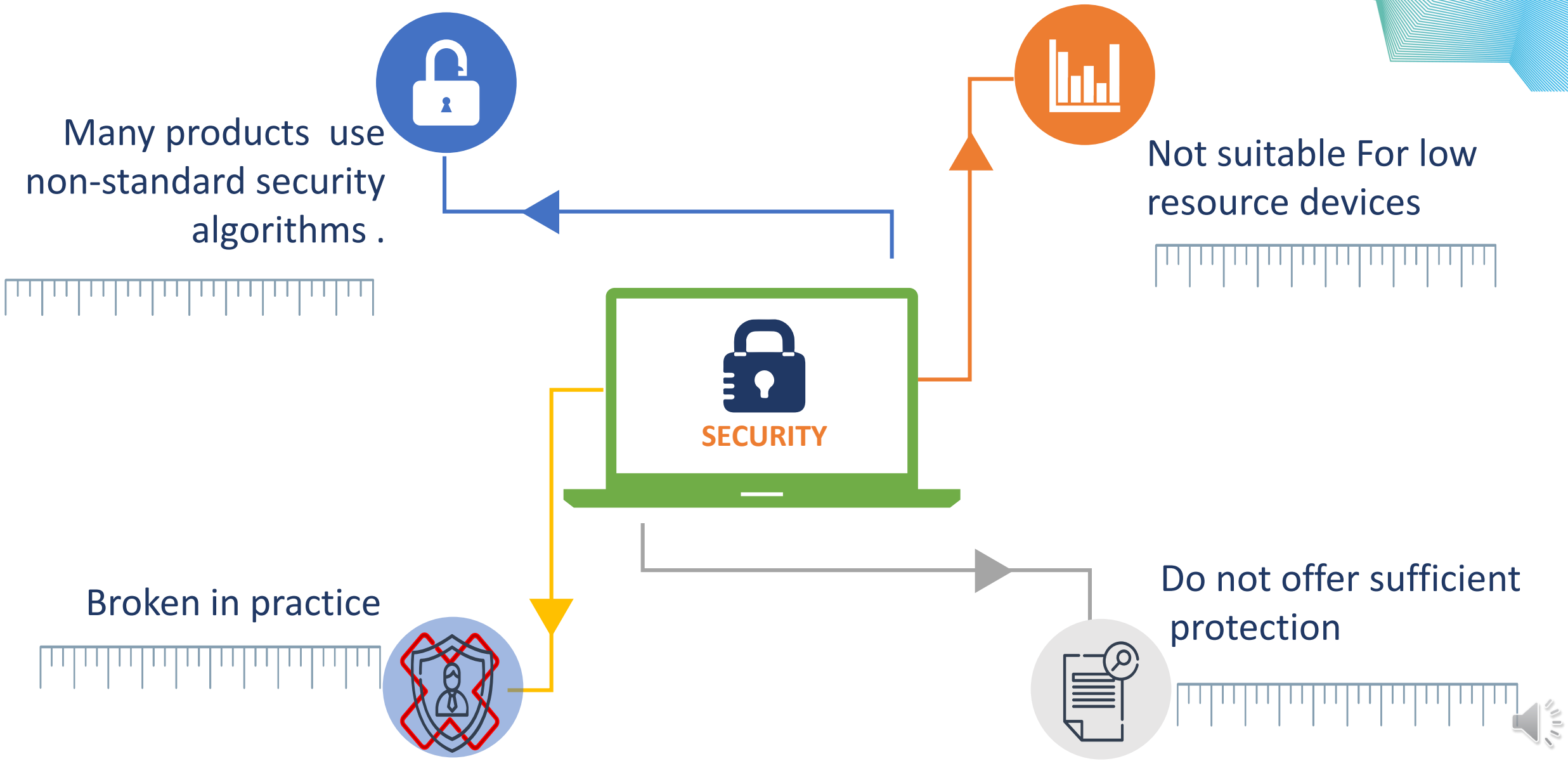
- Limited Memory.
- Limited Computational Power.
- Limited Power.



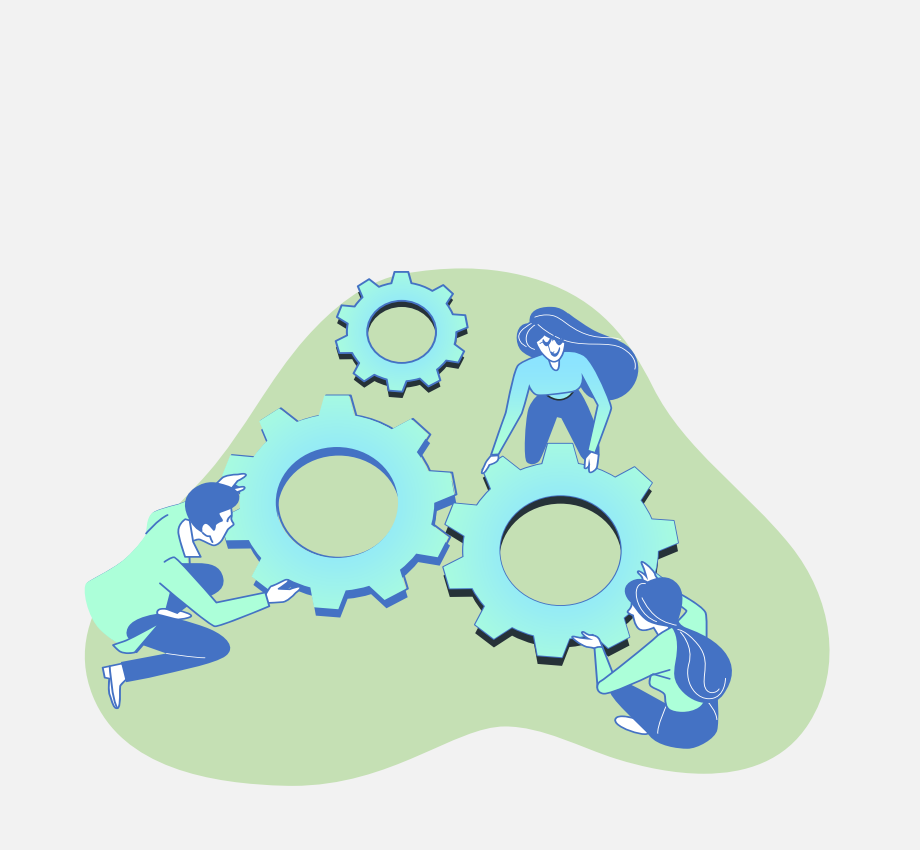
une University of New England

Faculty of Science, Agriculture, Business and Law

Lack of Suitable Cryptographic Solutions



Lightweight devices need right-sized cryptography



Urgent need for suitable crypto!

une University of New England

Faculty of Science, Agriculture, Business and Law

Lightweight cryptography

Lightweight Cryptography is a Subfield of cryptography that aims to provide crypto solutions optimized for constrained environments

The US National Institute of Standards and Technology (***NIST***) **competition** .

Cryptographic Hash function ***Vs*** an eXtendable-Output Function

NIST Lightweight Cryptography competition

- 12 of the 32 second-round candidates include a hash algorithm.

- With the exception of SATURNIN, each

of these candidates uses a sponge construction (or derivative which allows for XOFs.)

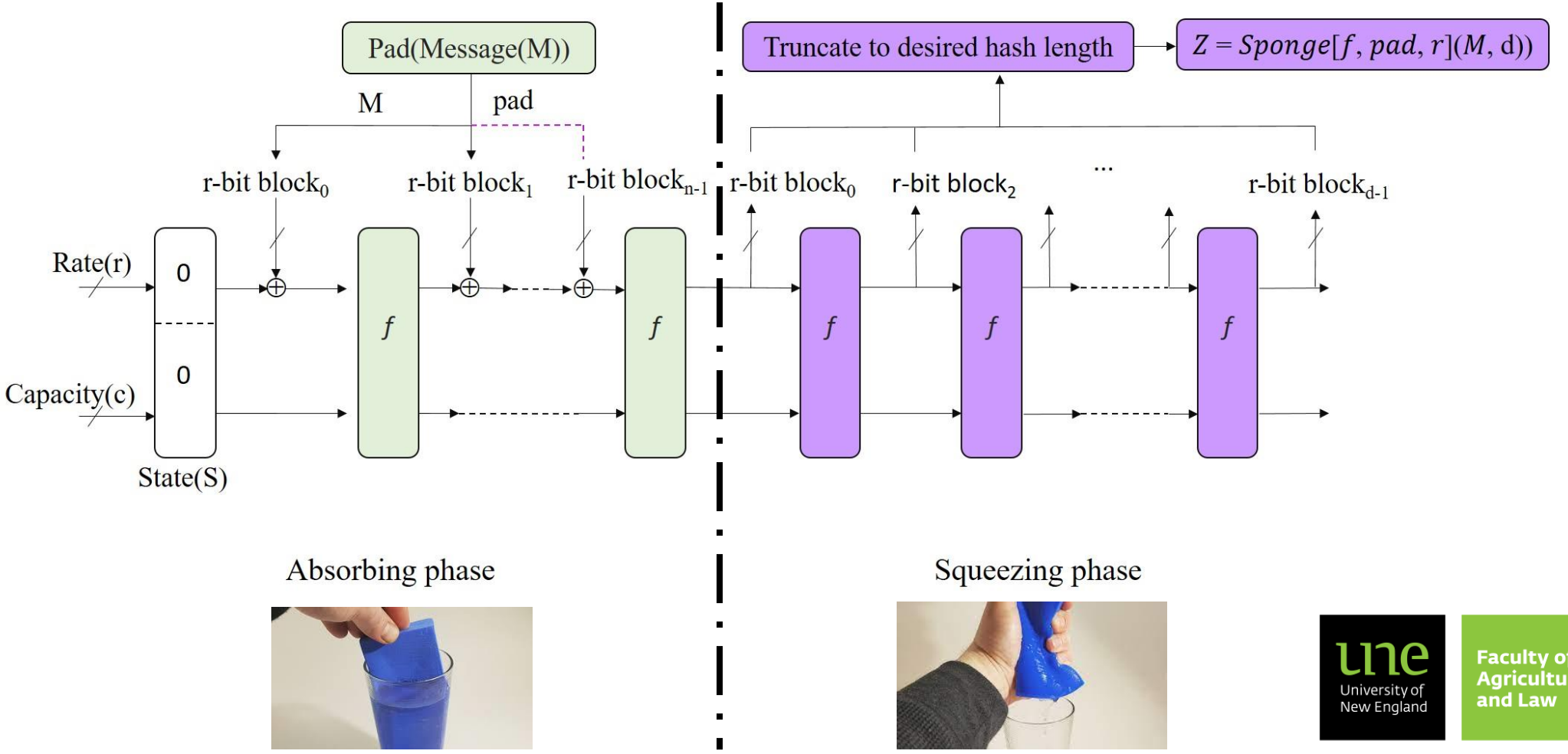
- Our analysis includes two of the finalists (Ascon and Xoodyak) and one did not make it to the final (Gimli).

NIST
National Institute of Standards and Technology

une University of New England

Faculty of Science, Agriculture, Business and Law

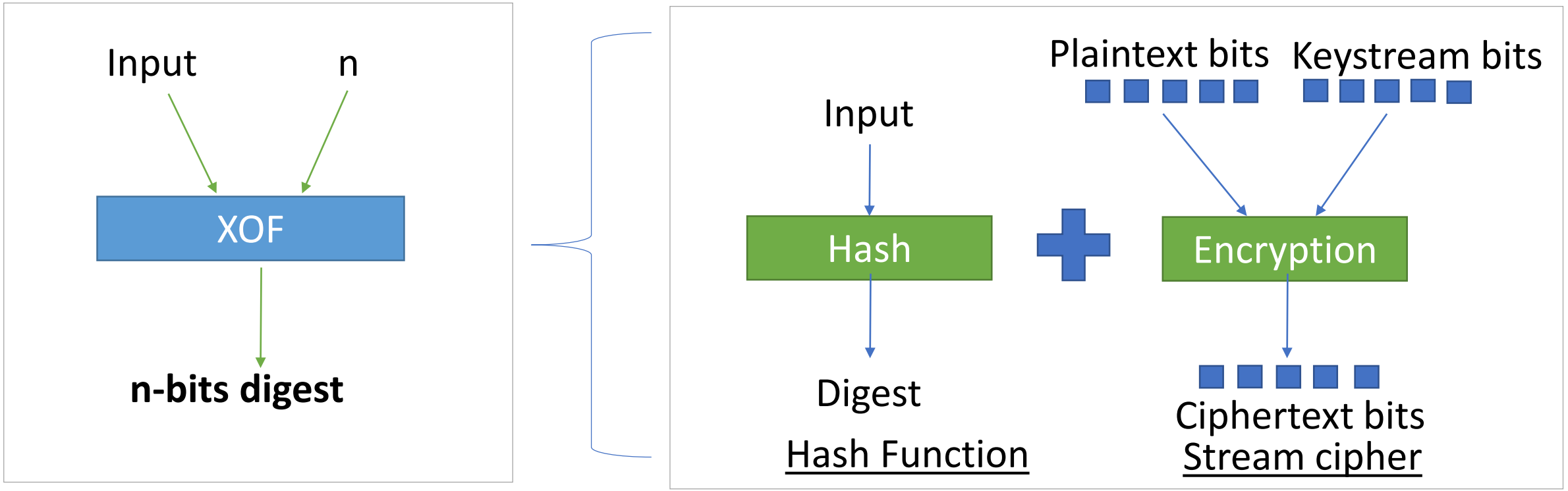
The Sponge Construction



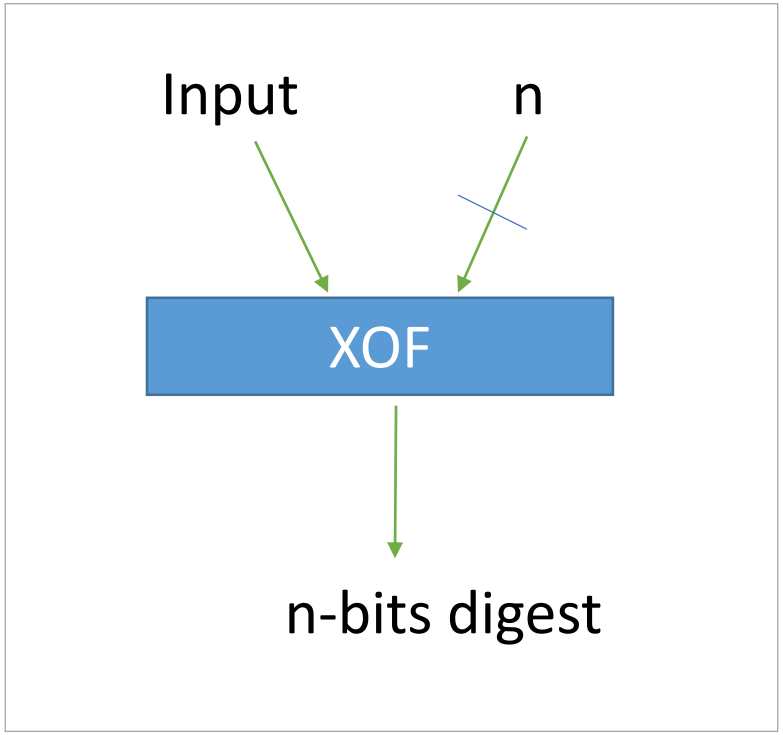
une University of New England

Faculty of Science, Agriculture, Business and Law

Complexity of an XOF



Some Applications of an XOFs



Application 1

Key derivation

Application 2

Signature message hashing.

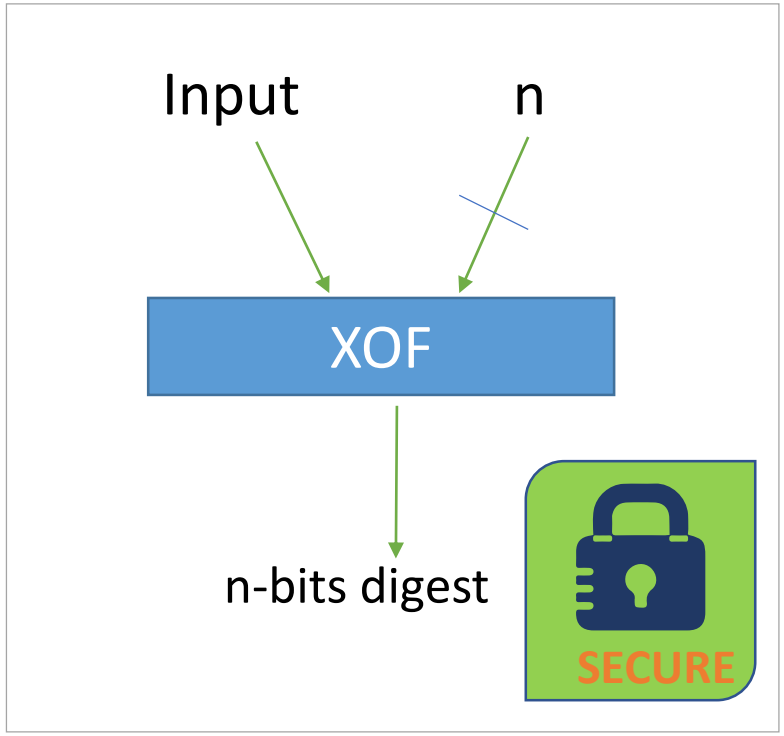
Application 3

Easier instantiation of random oracles

Application 4

Stream ciphers

Security of an XOF mode



- Collision (n/2 bits of security)
- Preimage (n bits of Security)
- Second-Preimage (n bits of Security)
- Relies on the chosen underlying construction .

Ascon-XOF Analysis

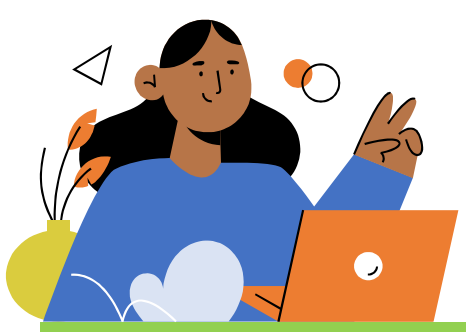
Ascon–XOF has received significant third –party analysis

Advantages

- Fast Diffusion
- Strong word structure
- Good choice of round constants
- Good security margin against collision attacks

Limitation

- Consecutive dependent bits.



University of New England

Faculty of Science, Agriculture, Business and Law

Gimli-XOF Analysis

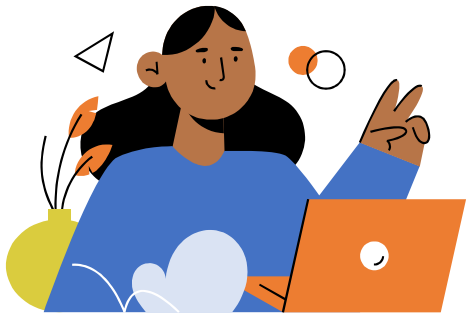
Gimli–XOF has a theoretical pre-image attack

Advantages

- Very simple
- Good cross-platform performance

Limitations

- Slow diffusion



une University of New England

Faculty of Science, Agriculture, Business and Law

Xoodyak-Hash Analysis

Xoodyak-hash

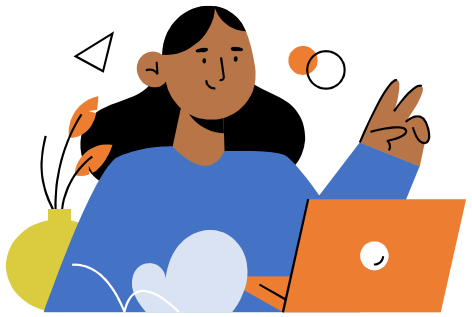
a deep learning pre-image attack on reduced Xoodyak–Hash .

Advantages

- Good Diffusion
- Strong and efficient permutation (Xoodo).

Limitations

- ***Slow speed for short messages***



une University of New England

Faculty of Science, Agriculture, Business and Law

General Guidelines to Design a Secure Lightweight XOF

✓Apply parallel computation (using wide round function width such as Ascon (320-bit state), Gimli (384-bit state) and Xoodyak (384-bit).

✓ Minimal rounds is better in LWA

- If an n-round attack exists, consider using 2n rounds

✓ Good Round constants

une University of New England

Faculty of Science, Agriculture, Business and Law

General Guidelines to Design a Secure Lightweight XOF

✓Use a low rate

- Less susceptible to pre-image and differential cryptanalysis attacks

✓Use smaller optimal 4X4 s-boxes

- Or larger suboptimal s-boxes

✓ Ensure weak alignment of the primitive

✓Use a capacity of at least 255 bits and a digest length of at least 128 bits

- A security strength of 128 bits

une University of New England
Faculty of Science, Agriculture, Business and Law

Future Work

- Automatic security analysis of XOFs
  - Created using these guidelines
- Use evolutionary computing to design XOFs.

une University of New England
Faculty of Science, Agriculture, Business and Law