# MSc Project Demonstration

EEE8097

**Michael Walker**

(130623935)

10:00am Thursday 25th October 2014

# Concept

Physically Unclonable Functions (PUFs)

for

Networked Device Authentication

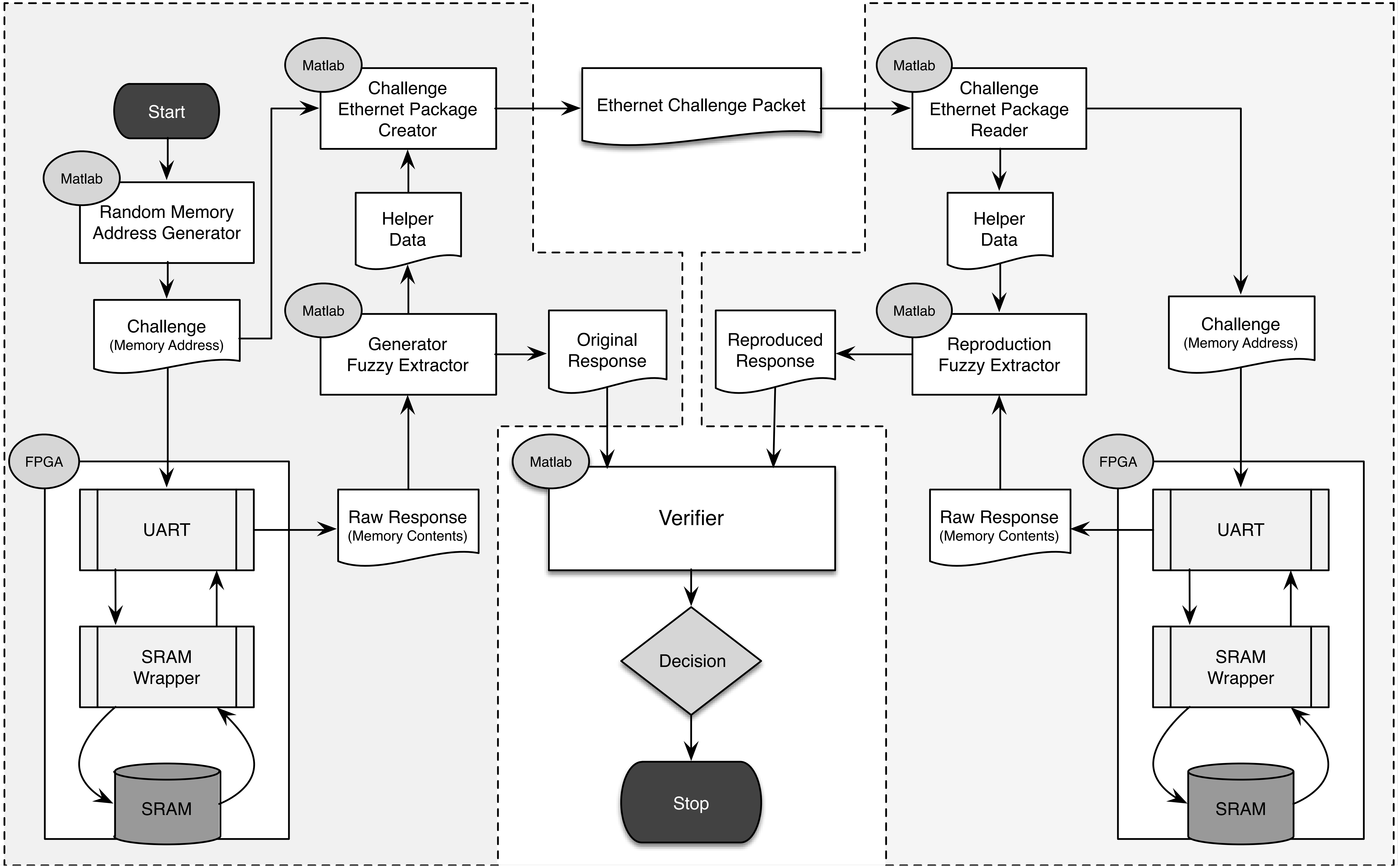
# Concept Breakdown

- Complex Project
  - Many substantial subcomponents
  - Too big for three month Masters project
- Requires Hybrid Development
  - Partial Physical Implementation (FPGA)
  - Partial Simulation (Matlab)

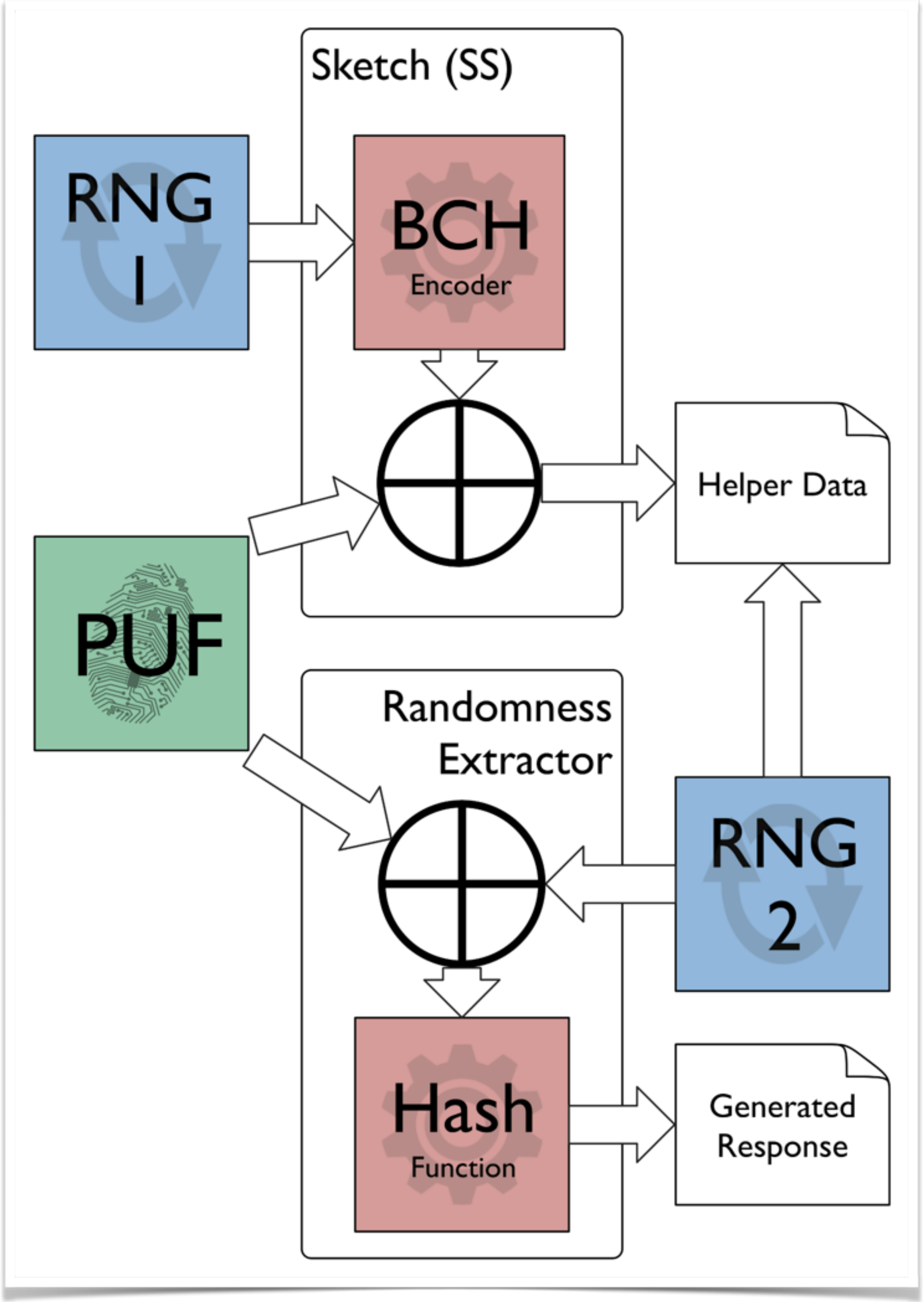
# Demonstration Overview

- Two Processes:
  - **Generation** Process (Enrolment in factory)
  - **Reproduction** Process (Validation in field)
- Three main modules per process:
  - **Ethernet** Security Protocol
  - **Fuzzy Extractor** Secure Sketch and Recovery
  - **SRAM-PUF** Wrapper

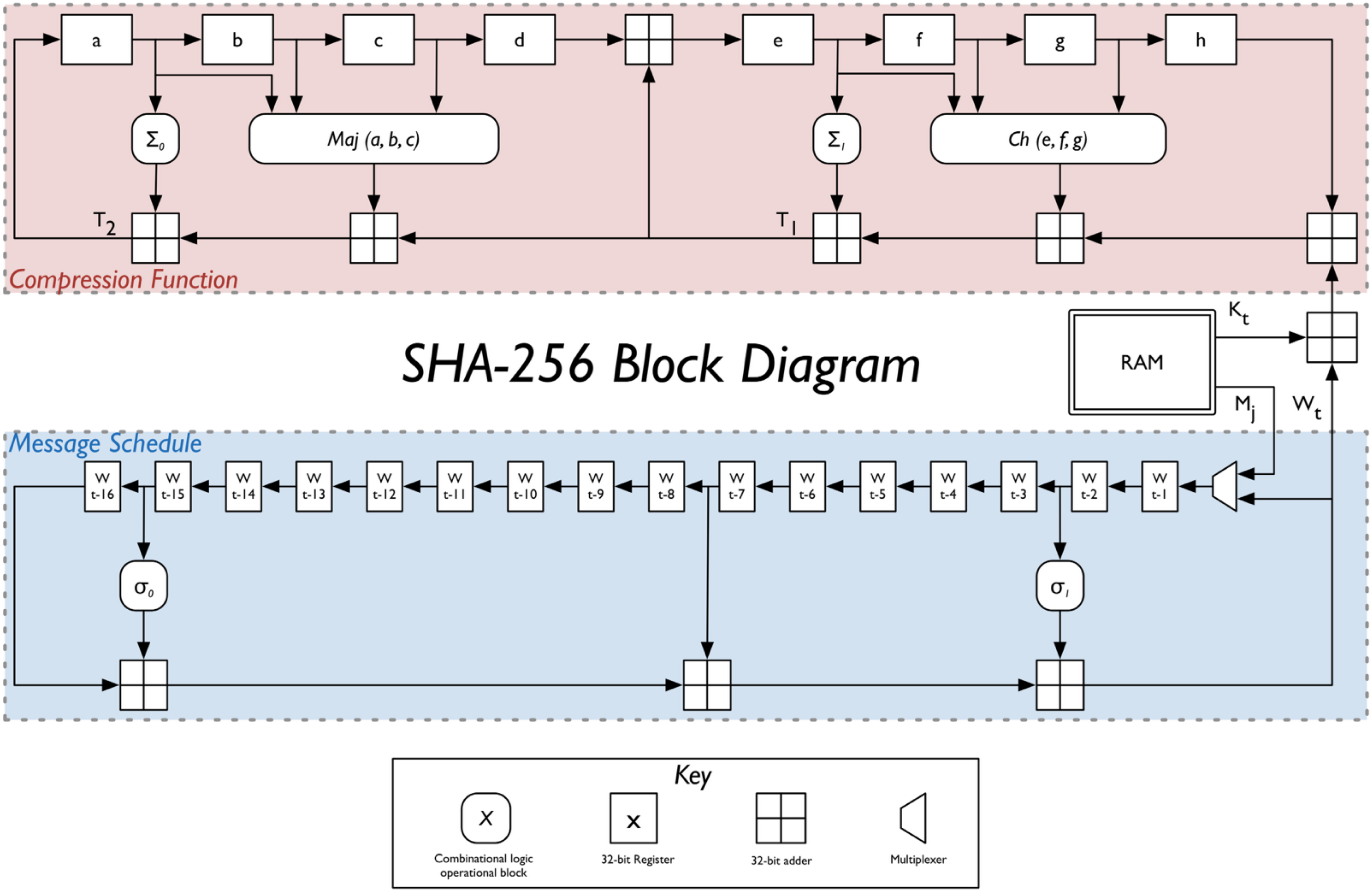
# Project Demonstration Flowchart


Start
Matlab
Random Memory Address Generator
Challenge (Memory Address)
Matlab
Challenge Ethernet Package Creator
Helper Data
Matlab
Generator Fuzzy Extractor
Original Response
FPGA
UART
SRAM Wrapper
SRAM
Raw Response (Memory Contents)
Ethernet Challenge Packet
Matlab
Verifier
Decision
Stop
Matlab
Challenge Ethernet Package Reader
Helper Data
Matlab
Reproduction Fuzzy Extractor
Reproduced Response
Challenge (Memory Address)
FPGA
UART
SRAM Wrapper
SRAM
Raw Response (Memory Contents)

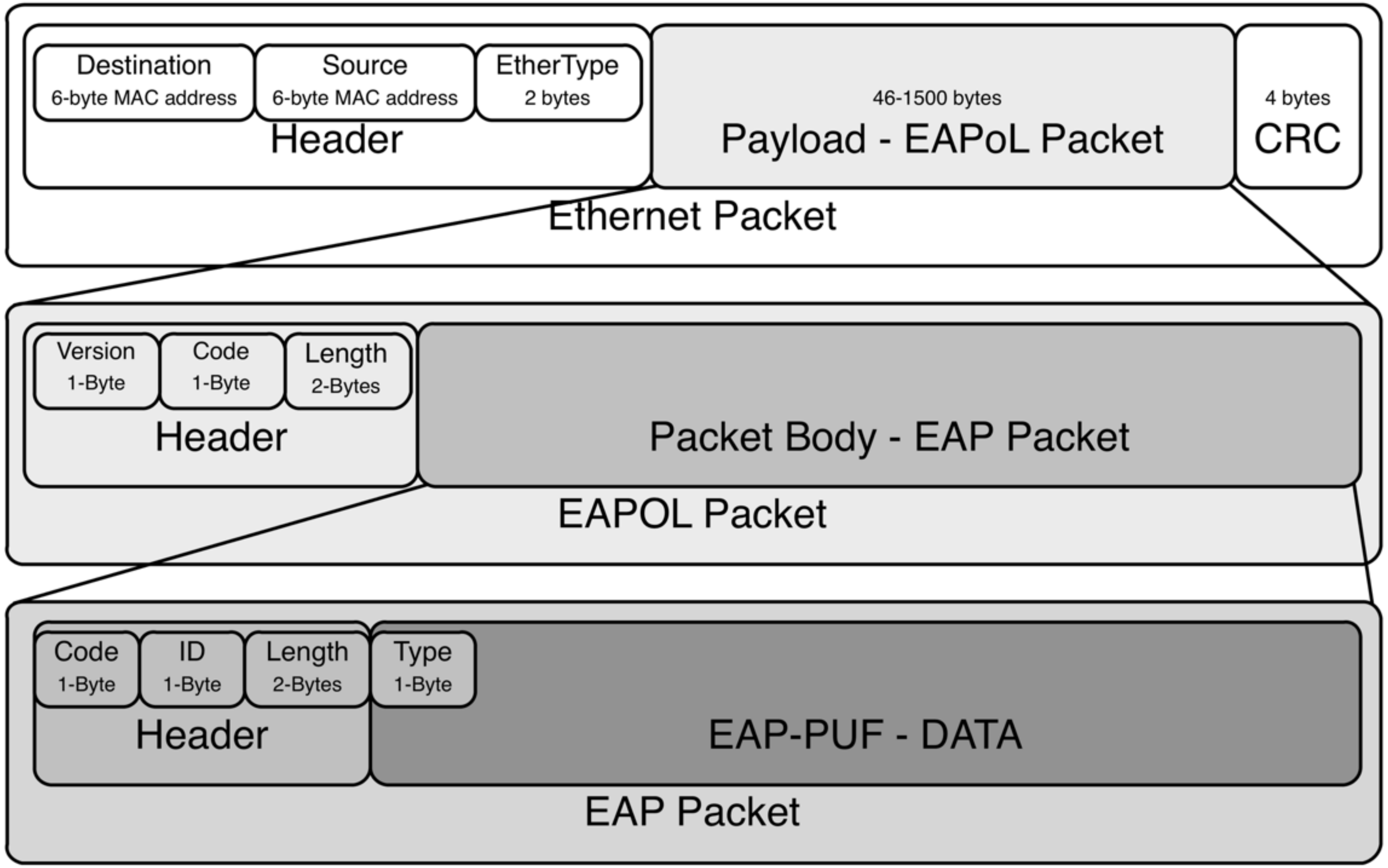
# Generation Process



# SHA-256 Block Diagram



# Ethernet Packet Structure



Destination
6-byte MAC address

Source
6-byte MAC address

EtherType
2 bytes

Header

46-1500 bytes
Payload - EAPoL Packet

4 bytes
CRC

Ethernet Packet

Version
1-Byte

Code
1-Byte

Length
2-Bytes

Header

Packet Body - EAP Packet

EAPOL Packet

Code
1-Byte

ID
1-Byte

Length
2-Bytes

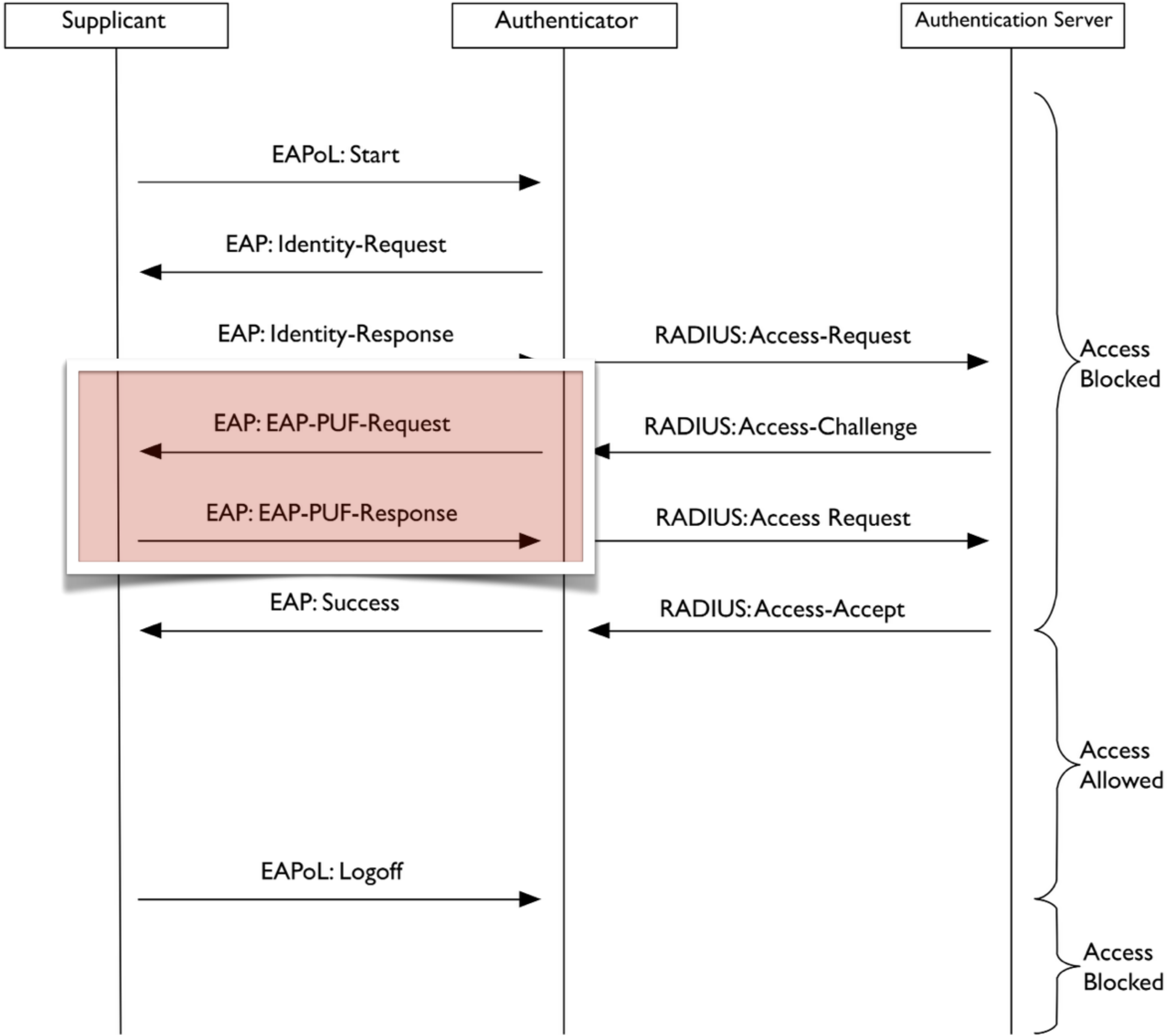
Header

Type
1-Byte

EAP-PUF - DATA

EAP Packet

# Full EAP-PUF Authentication Protocol Sequence



# Calculating Ethernet Packets Involved in Authentication via EAP-PUF

```
Pre-assigned values for demo:
-----------------------------
Supplicant MAC address   : 00005E005301 (reserved for documentation purposes)
Authenticator MAC Address: 00005E0053FF (reserved for documentation purposes)

EAPoL PAE Broadcast MAC  : 0180C2000003 (reserved group-multicast MAC address
                                         used for contacting 802.1x PAEs)
EAP type of EAP-PUF      : B0           (in unassigned types list decimal=192)

Ethertype for 802.1x     : 888E
EAP Identifier           : 55           (Authenticator generates this at start)

Sizes are constant for the protocol (also EAP and EAPoL lengths always same)
--------------------------------------------------------------------------------
- Start and Logoff  -  0 Bytes - 0000 -(No EAP content so 0 Bytes)
- Identity Request  -  6 Bytes - 0006 -(4 Byte header + Identity type Byte +
                                        EAP-PUF type Byte)
- Identity Response - 11 Bytes - 000B -(4 Byte header + Identity type Byte +
                                        6 Byte MAC of supplicant)
- PUF  Request      - 53 Bytes - 0035 -(4 Byte header + PUF type Byte +
                                       16 Byte Challenge + 32 Bytes helper data)
- PUF  Response     - 37 Bytes - 0025 -(4 Byte header + PUF type Byte +
                                       32 Byte SHA-256 Response)
- EAP Success       -  4 Bytes - 0004 -(4 Byte Header only)
```

## Message Sequence

- EAPoL Start Packet (From Supplicant)
- 0180C200000300005E005301888E02010000…
- + 4 Byte CRC

- EAP Identity Request Packet (From Authenticator)
- 00005E00530100005E0053FF888E020000060155000601B0…
- + 4 Byte CRC

- EAP Identity Response Packet (From Supplicant)
- 00005E0053FF00005E005301888E0200000B0255000B0100005E005301…
- + 4 Byte CRC

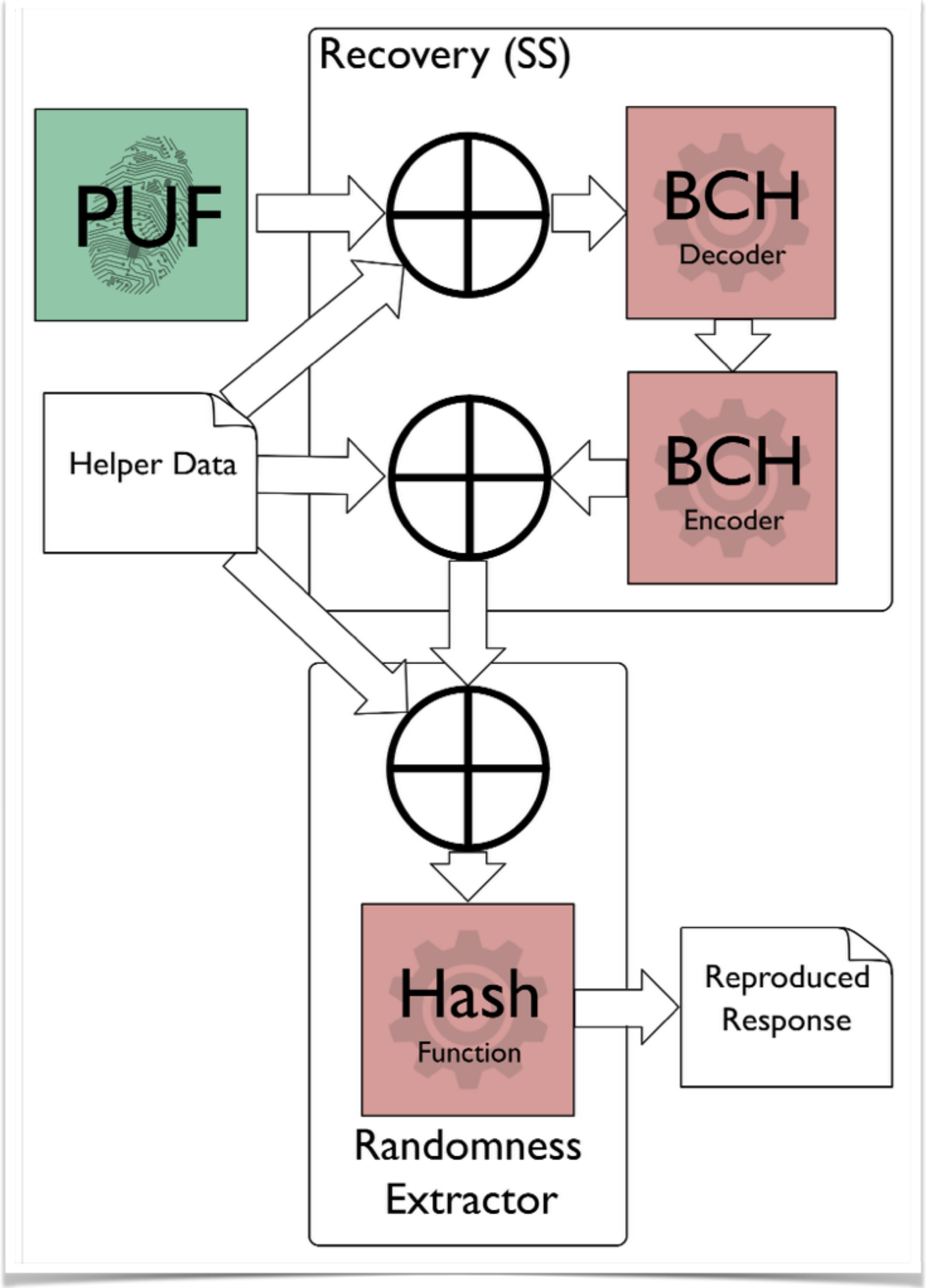
- **EAP EAP-PUF Request Packet (From Authenticator)**
- **00005E00530100005E0053FF888E0200003501550035B0…**
- **+ Challenge(16 Bytes) + Helper Data(32 Bytes) + 4 Byte CRC**

- **EAP EAP_PUF Response Packet (From Supplicant)**
- **00005E0053FF00005E005301888E0200002502550025B0…**
- **+ Response(32 Bytes) + 4 Byte CRC**

- EAP Success Packet (From Authenticator)
- 00005E00530100005E0053FF888E0200000403550004…
- + 4 Byte CRC

- EAPoL Logoff Packet (From Supplicant)
- 0180C200000300005E005301888E02020000
- + 4 Byte CRC

# Reproduction Process


Recovery (SS)
PUF
BCH
Decoder
Helper Data
BCH
Encoder
Hash
Function
Reproduced Response
Randomness Extractor