Physical Chip-ID based Encryption and Security in SSD Controller

Data governed IoT via Flash
presented by FOREMAY

Hiroshi Watanabe

World Demand on Data Free Flow

- Data is the New Oil.
  - BigData & AI
- Global Consensus on Data Governance
  - World Economic Forum, G20 Osaka
  - Data Free Flow with Trust (DFFT)
- Trusted Data Flow is really valuable

Data Free Flow with Trust (DFFT)

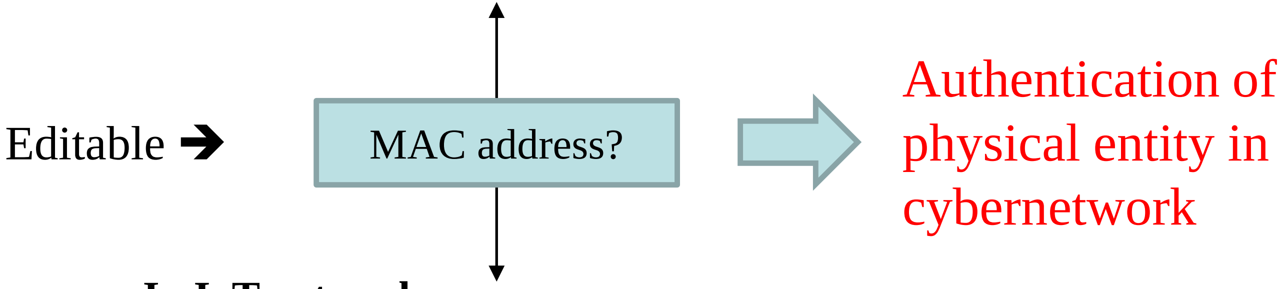
What can make us trust flowed data?

Blockchain

Trust → Traceability → When, Where, What → Recorded in a ledger

In Cyber network:

- **When → timestamp**
- **Where → IP address**



Editable →

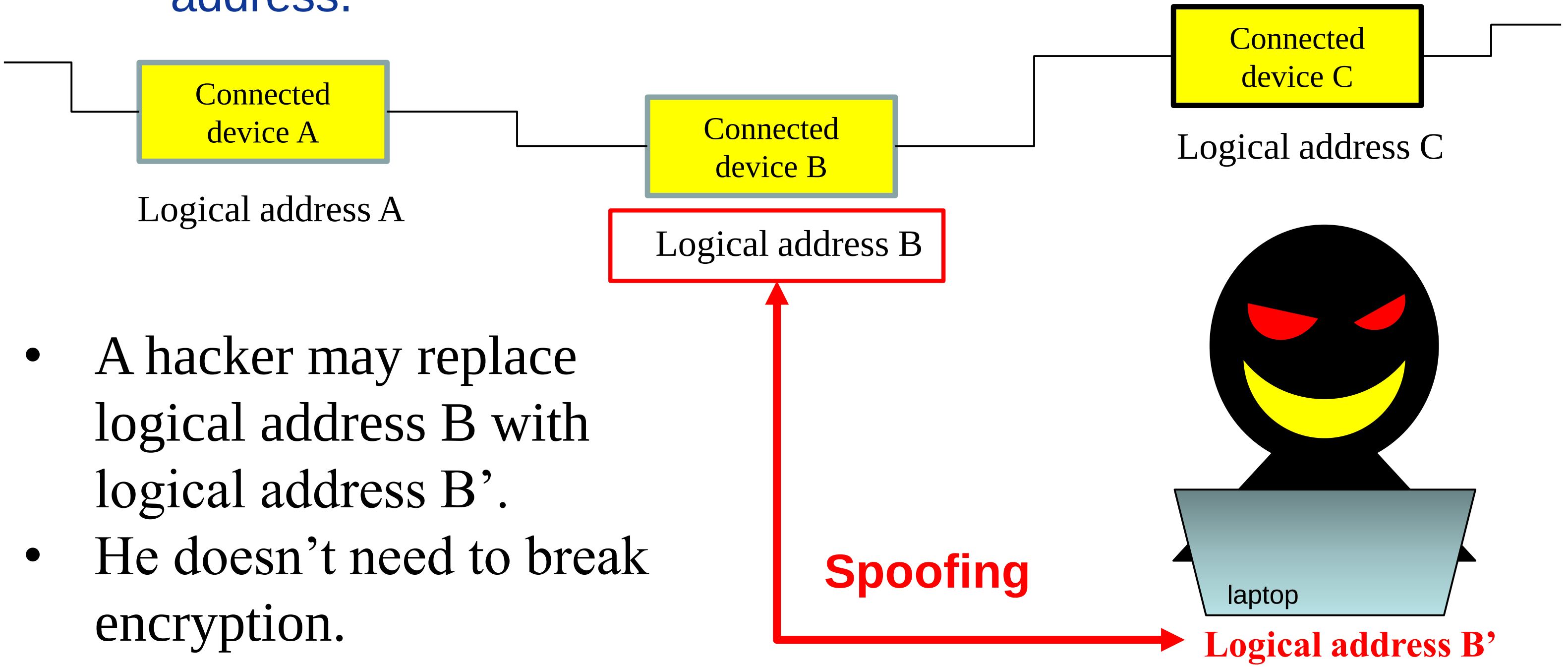
MAC address?

Authentication of physical entity in cybernetwork

In IoT network:

- **Where → which device**

Logical address is public in the network because it is address in the network. If it is protected by encryption, it cannot serve as address.



Connected device A

Logical address A

Connected device B

Logical address B

Connected device C

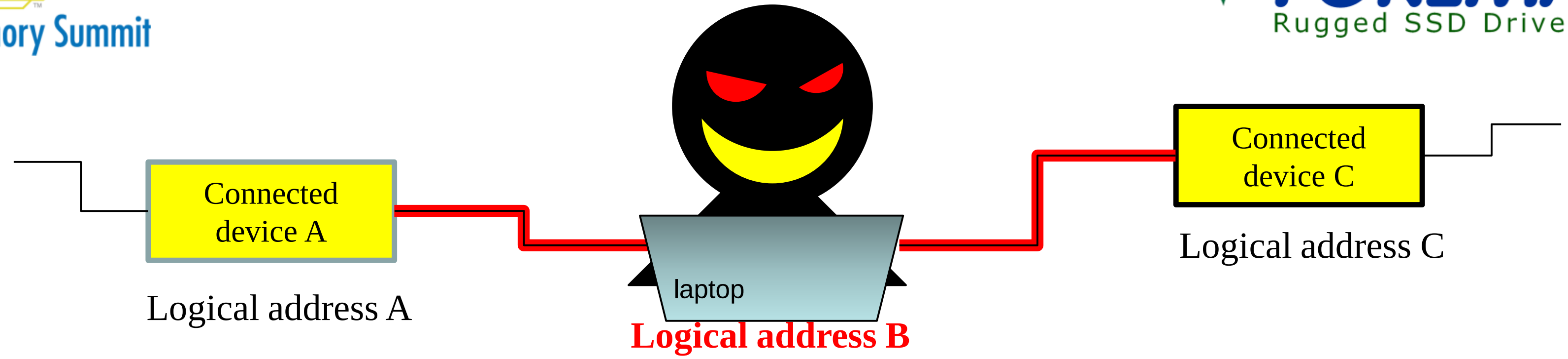
Logical address C

Spoofing

Logical address B’

- A hacker may replace logical address B with logical address B’.
- He doesn’t need to break encryption.

Man-in-the-middle attack



A hacker can, even though communication data is encrypted,

① INSERT an irregular data (e.g. noise) into between A and C.

② DELIVER an irregular data as a regular node.

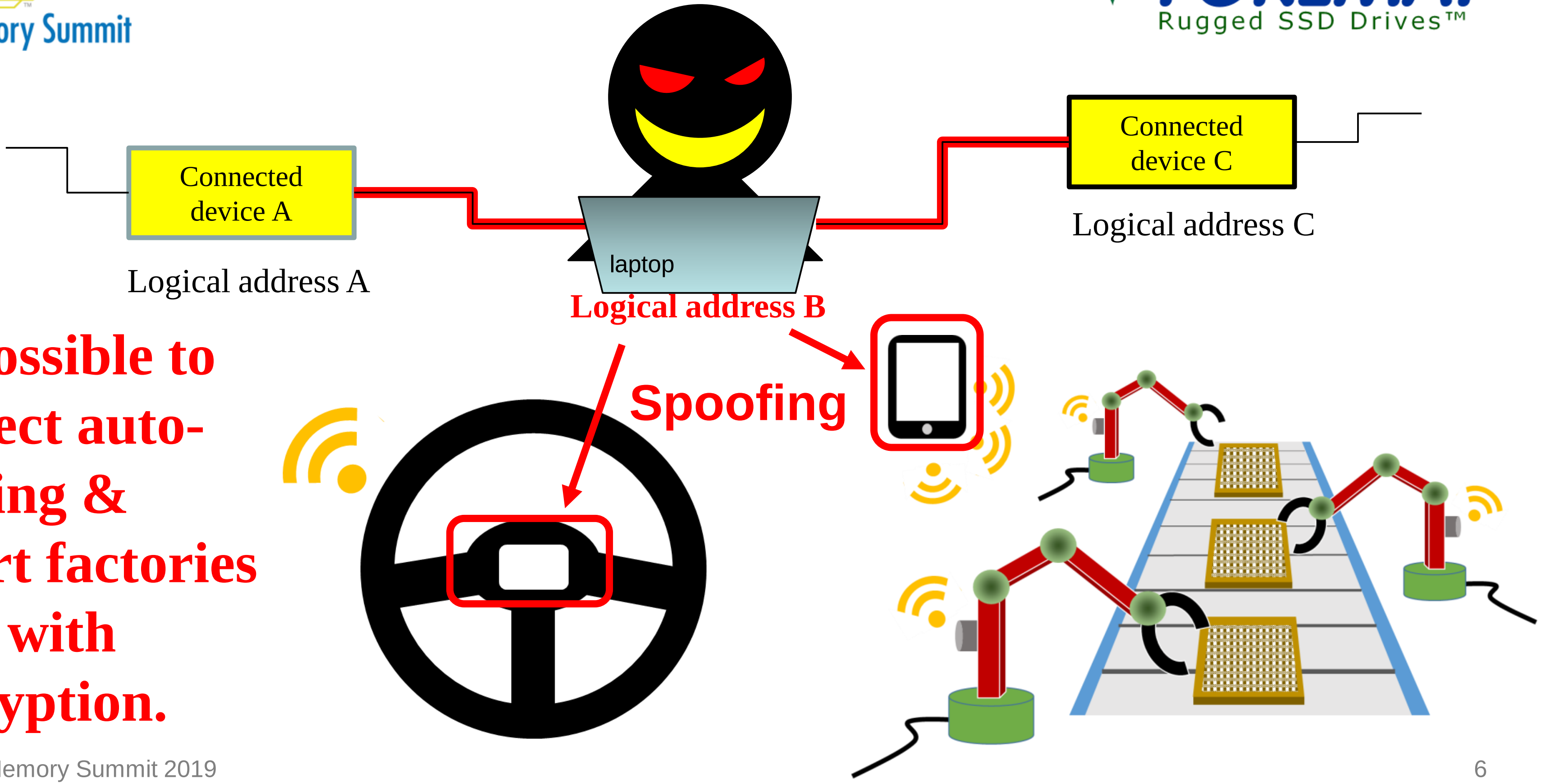
Ex1) Jamming

Ex3) fatal to BigData

Ex2) fake news

Impossible to assure data governance in IoT only with encryption.

Man-in-the-middle attack



Connected device A

Logical address A

laptop

Logical address B

Connected device C

Logical address C

Spoofing

Impossible to protect auto-driving & smart factories only with encryption.

Concept

Physical and logical addresses are connected uniquely in a chip.

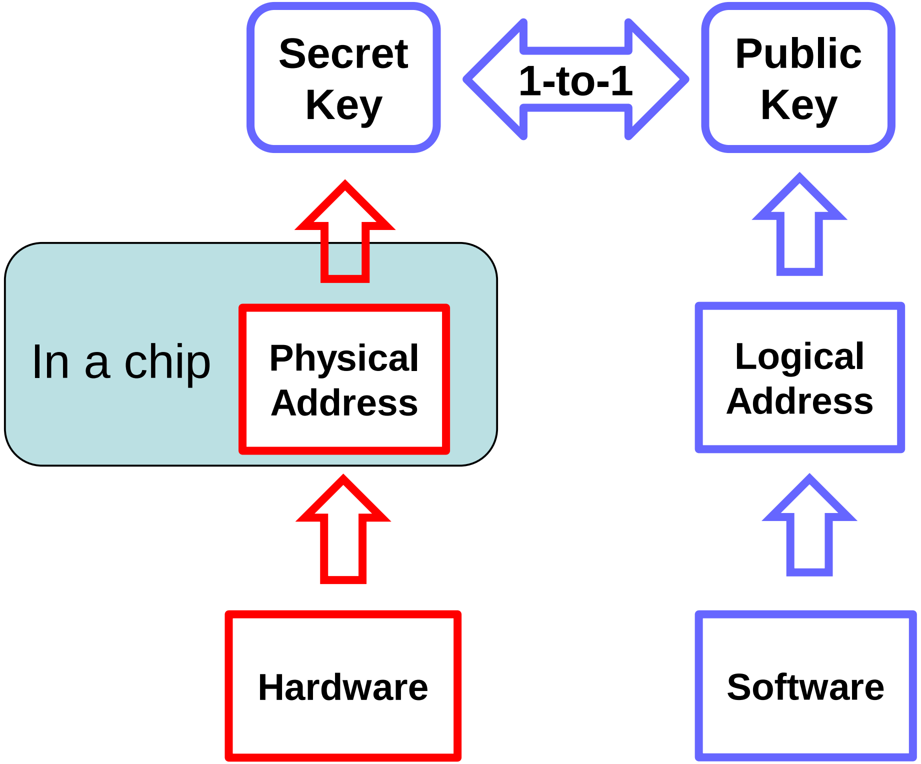
⇩

Physical network meets Cybernetwork.

⇩

Data-governed IoT

Public Key Encryption



Chip Experimental

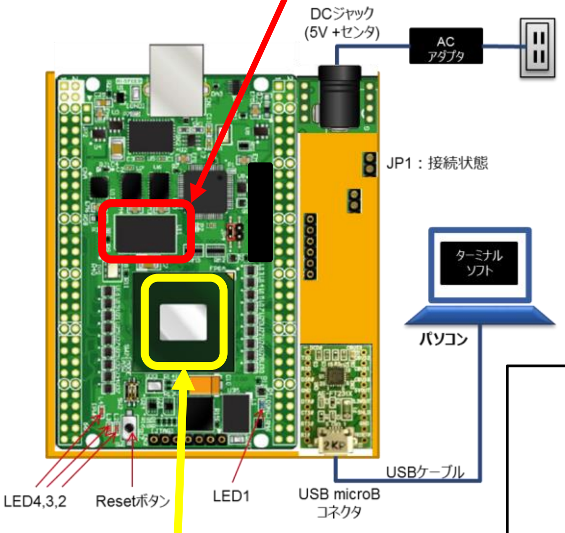
Stable shipment in large quantity	√
Longevity (>10 yrs)	√
Temperature (-40 ~105° C)	√
Humidity (0 ~ 100%)	Undergoing

5G requires stable volume shipment & environmental toughness.

Reference: Technologies 2019, 7(1), 2

FPGA test

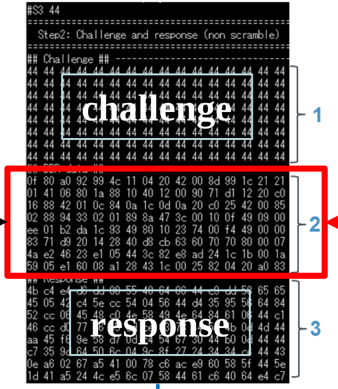
1Gb DDR3 DRAM
(in SSD controller)



FPGA

Module-1

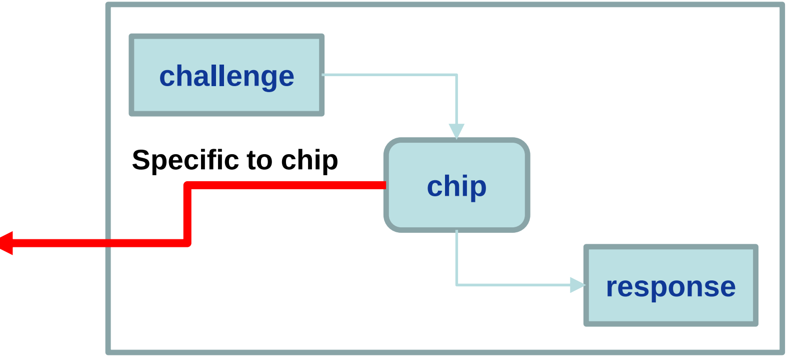
Terminal Image



```
#S3 44
==========================================================
  Step2: Challenge and response (non scramble)
==========================================================
## Challenge ## ------------------------------------------
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
44 44 44 44 44 44 44 44 44 44 44 44 44 44 44 44
## DDR data ##
0f 80 a0 92 99 4c 11 04 20 42 00 8d 99 1c 21 21
01 41 06 80 1a 88 10 40 12 00 90 71 d1 12 20 c0
16 88 42 01 0c 84 0a 1c 0d 0a 20 c0 25 42 00 85
02 88 94 33 02 01 89 8a 47 3c 00 10 0f 49 09 00
ee 01 b2 da 1c 93 49 80 10 23 74 00 f4 49 00 00
83 71 d9 20 14 28 40 d8 cb 63 60 70 70 80 00 07
4a e2 46 23 e1 05 44 3c 82 e8 ad 24 1c 1b 00 1a
59 05 e1 60 08 a1 28 43 1c 00 25 82 04 20 a0 83
## Response ##
4b c4 e4 d6 dd 08 55 40 64 06 44 c9 dd 58 65 65
45 05 42 c4 5e cc 54 04 56 44 d4 35 95 56 64 84
52 cc 06 45 48 c0 4e 58 49 4e 64 84 61 06 44 c1
46 cc d0 77 [illegible] 4b 0d 4d 44
aa 45 f6 9e 58 d7 0d c4 54 67 30 44 b0 0d 44 44
c7 35 9d 64 50 6c 04 9c 8f 27 24 34 34 c4 44 43
0e a6 02 67 a5 41 00 78 c6 ac e9 60 58 5f 44 5e
1d 41 a5 24 4c e5 6c 07 58 44 61 c6 40 64 e4 c7
```

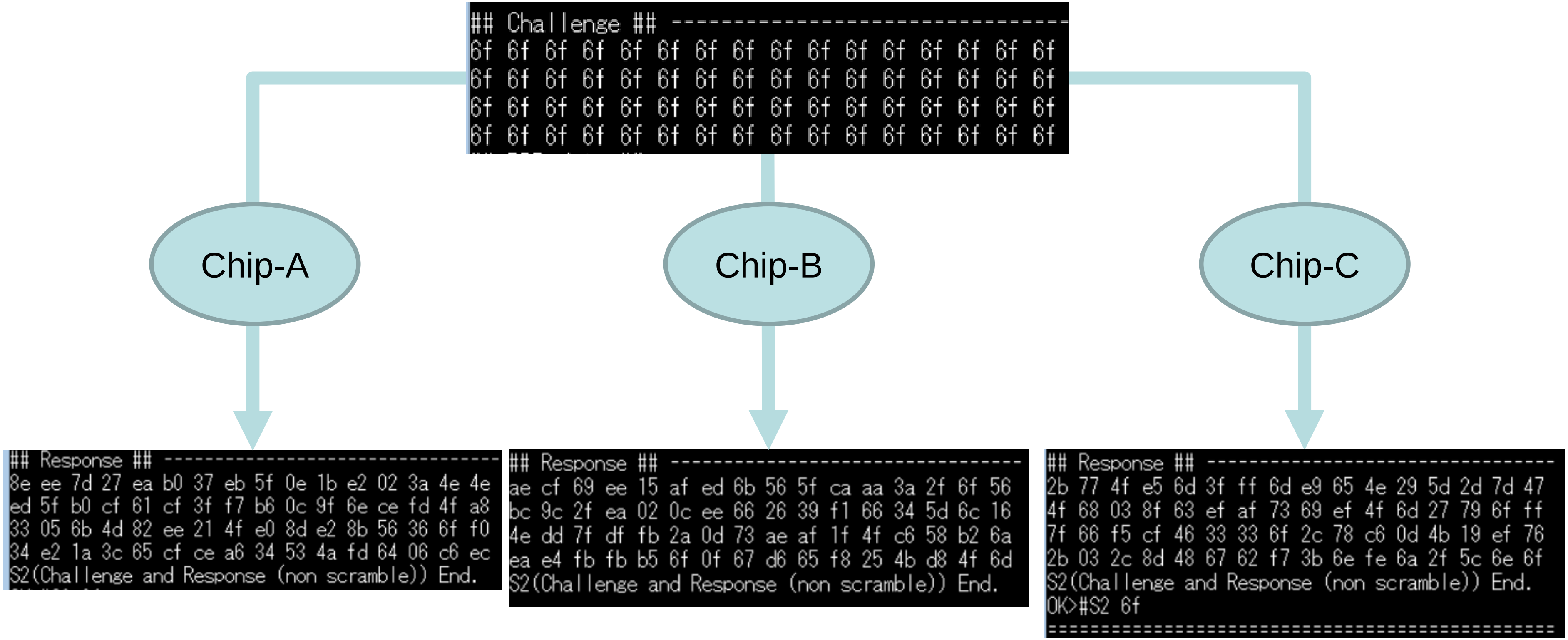
Chip physical random code using redundancy, converted to 2048bits.

Concept for Module-1



Output independency

Challenge to each chip

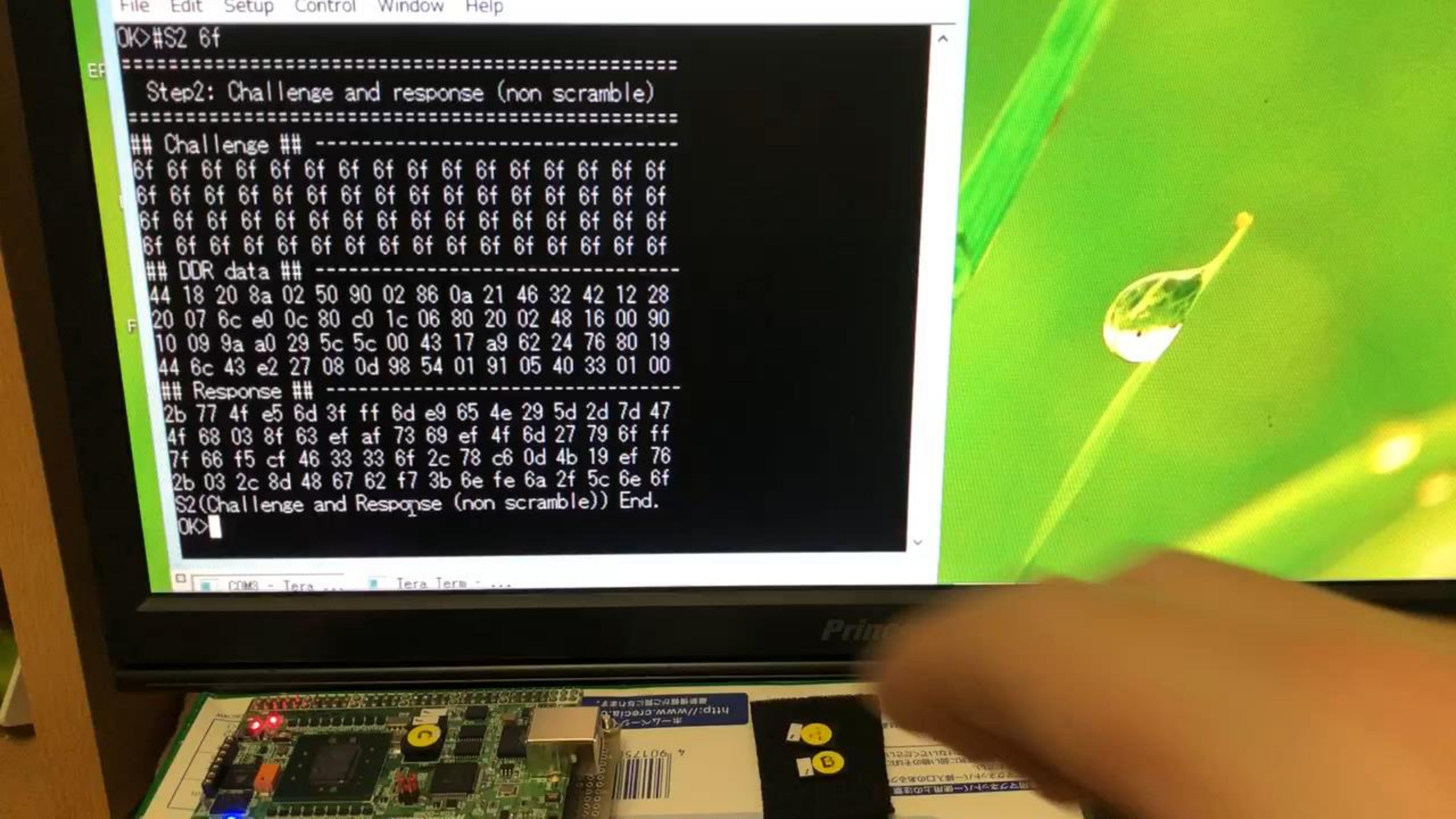


```
## Challenge ## ----------------------------------
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
```

```
## Response ## ------------------------------
8e ee 7d 27 ea b0 37 eb 5f 0e 1b e2 02 3a 4e 4e
ed 5f b0 cf 61 cf 3f f7 b6 0c 9f 6e ce fd 4f a8
33 05 6b 4d 82 ee 21 4f e0 8d e2 8b 56 36 6f f0
34 e2 1a 3c 65 cf ce a6 34 53 4a fd 64 06 c6 ec
S2(Challenge and Response (non scramble)) End.
```

```
## Response ## ------------------------------
ae cf 69 ee 15 af ed 6b 56 5f ca aa 3a 2f 6f 56
bc 9c 2f ea 02 0c ee 66 26 39 f1 66 34 5d 6c 16
4e dd 7f df fb 2a 0d 73 ae af 1f 4f c6 58 b2 6a
ea e4 fb fb b5 6f 0f 67 d6 65 f8 25 4b d8 4f 6d
S2(Challenge and Response (non scramble)) End.
```

```
## Response ## ------------------------------
2b 77 4f e5 6d 3f ff 6d e9 65 4e 29 5d 2d 7d 47
4f 68 03 8f 63 ef af 73 69 ef 4f 6d 27 79 6f ff
7f 66 f5 cf 46 33 33 6f 2c 78 c6 0d 4b 19 ef 76
2b 03 2c 8d 48 67 62 f7 3b 6e fe 6a 2f 5c 6e 6f
S2(Challenge and Response (non scramble)) End.
OK>#S2 6f
================================================
```



```
OK>#S2 6f
=================================================
  Step2: Challenge and response (non scramble)
=================================================
## Challenge ## ---------------------------------
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f
## DDR data ## ---------------------------------
44 18 20 8a 02 50 90 02 86 0a 21 46 32 42 12 28
20 07 6c e0 0c 80 c0 1c 06 80 20 02 48 16 00 90
10 09 9a a0 29 5c 5c 00 43 17 a9 62 24 76 80 19
44 6c 43 e2 27 08 0d 98 54 01 91 05 40 33 01 00
## Response ## ---------------------------------
2b 77 4f e5 6d 3f ff 6d e9 65 4e 29 5d 2d 7d 47
4f 68 03 8f 63 ef af 73 69 ef 4f 6d 27 79 6f ff
7f 66 f5 cf 46 33 33 6f 2c 78 c6 0d 4b 19 ef 76
2b 03 2c 8d 48 67 62 f7 3b 6e fe 6a 2f 5c 6e 6f
S2(Challenge and Response (non scramble)) End.
OK>
```

Summary

- Cybernetwork meets IoT Network via flash memory chip.
- Chip-level Trustworthy Data Free Flow by Flash memory
- Acknowledgement
  - Presented by FOREMAY
  - ROHM and LAPIS to co-work for FPGA test.