MindCrypt: The Brain as a Random Number Generator for SoC-Based Brain-Computer Interfaces

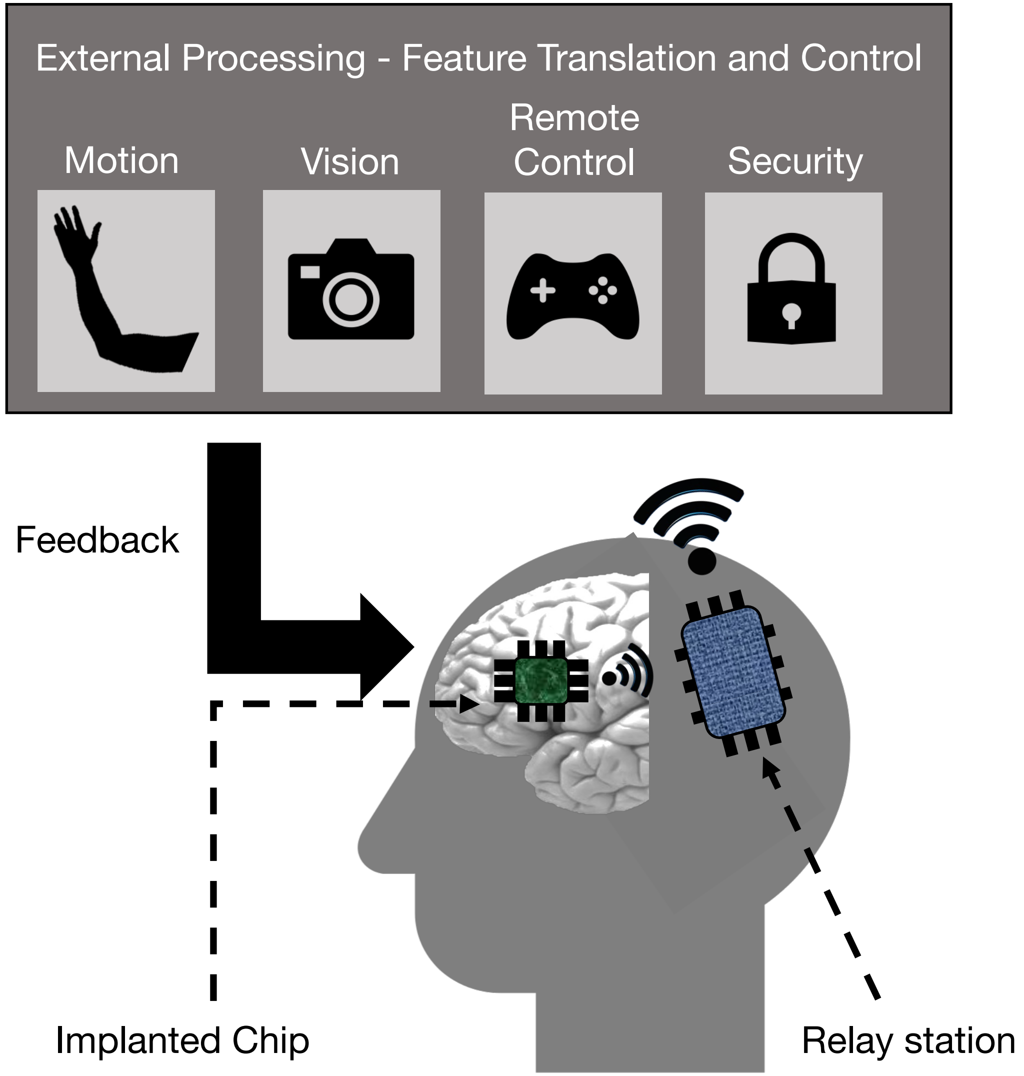
Guy Eichler
Biruk Seyoum
Kuan-Lin Chiu
Luca Carloni

ICCD 2023

Columbia University
CS@CU Computer Science

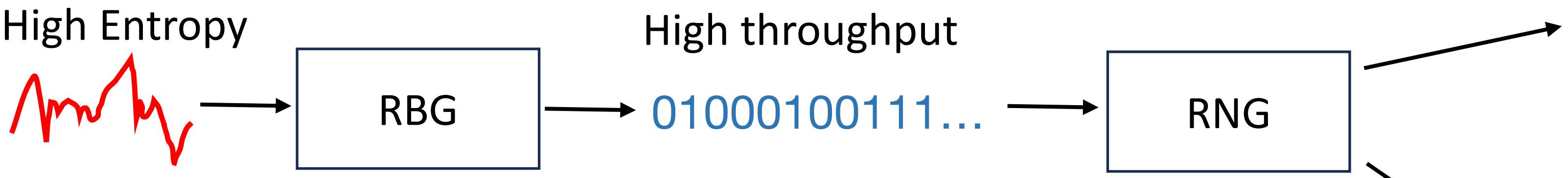
Brain-Computer Interfaces?

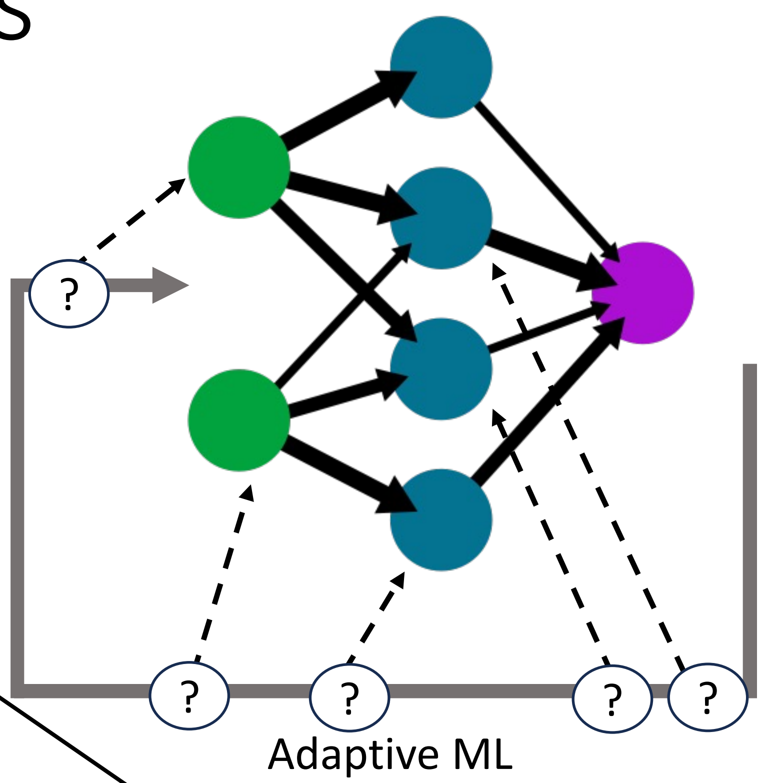
- A Brain-Computer Interface (BCI) is a system that establishes a connection between the brain and the outside world
  - The goal: improve the quality of life – aid with disabilities
- Main components:
  - Implanted **neural Interface** (ECoG) – recording and stimulation
  - Wearable **relay-station** for real-time computations
  - Additional high-performance processing in a distant machine
- Main guidelines when designing BCI systems:
  - Sufficient **resolution and throughput** of neural data
  - **Real-time** computation within the boundaries of the reaction time of the brain for BCI applications
  - Meet **low-power** constraints for wearable devices in a body-area network (BAN)

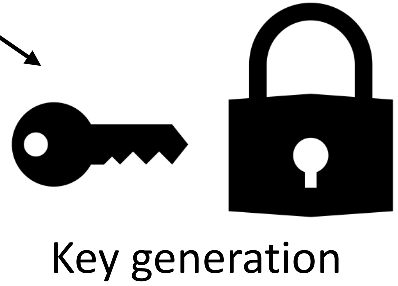


Randomness and BCI applications

- BCI applications running on BCI devices –
  - Adaptive ML – Reinforcement Learning uses randomness
  - Secure communication – random keys







- **Physically Unclonable Functions (PUFs)** for Internet-of-Things –
  - Problem: unstable under a constantly changing environment
- **Sensor-based PUFs**
  - Lightweight and based on random bit generation algorithms – compute on sensor data
- **Can we create a sensor-based PUF in the BCI system?**

Brain Data into Random Bits

- BrainBit algorithm – Szczepanski et al. 2004
- **BrainMod** algorithm – MindCrypt`23 (this work)
  - Hardware efficient
- **Real brain data** from the visual cortex of a non-human primate
  - 78 million data points, 64 electrodes, 41 minutes
- Evaluation with the NIST statistical test suite
  - NIST SP 800-22

global variables: σ, μ, R, L, d, h

function BrainBit(x)
  Initialize: $result = None$
  if $|x - \mu| \leq R\sigma$ **then**
    $y = x - (\mu - R\sigma)$
    $z = 2 \times R\sigma$
    $w = \lfloor (y/z) \times L) \rfloor$
    $result = w \mod 2$
  return $result$

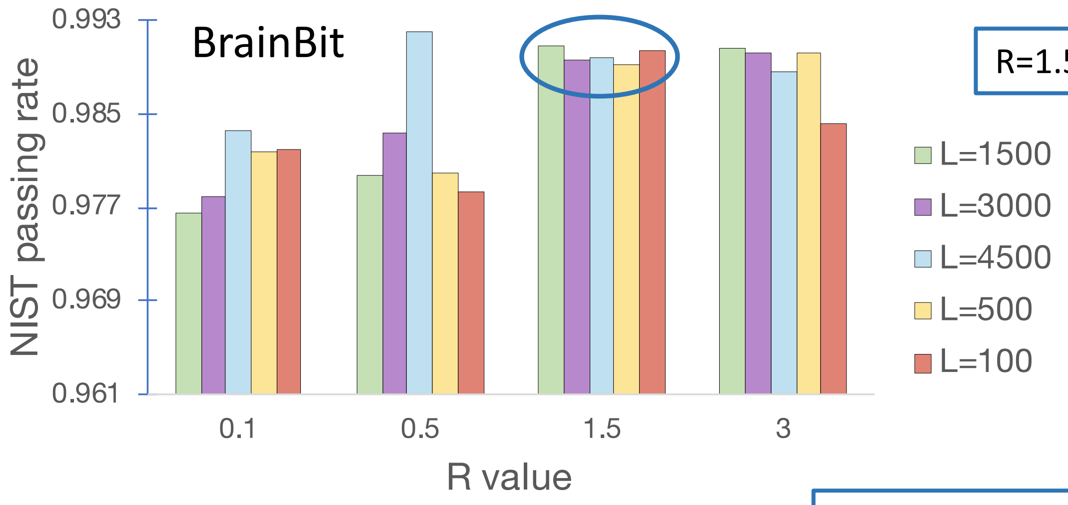
function BrainMod(x)
  Initialize: $result = None$
  if $|x - \mu| \leq R\sigma$ **then**
    $y = x - \mu$
    $z = y \times 2^d$
    $w = \lfloor z \rfloor \mod 2^h$
    $result = (\sum_h w_b) \mod 2$
  return $result$

Notations:
R, L, d, h are user defined parameters
μ is the estimated average over all values
σ is the estimated standard deviation over all values
w_b are the bits of the variable w

Random Bit Generation Algorithms - Performance

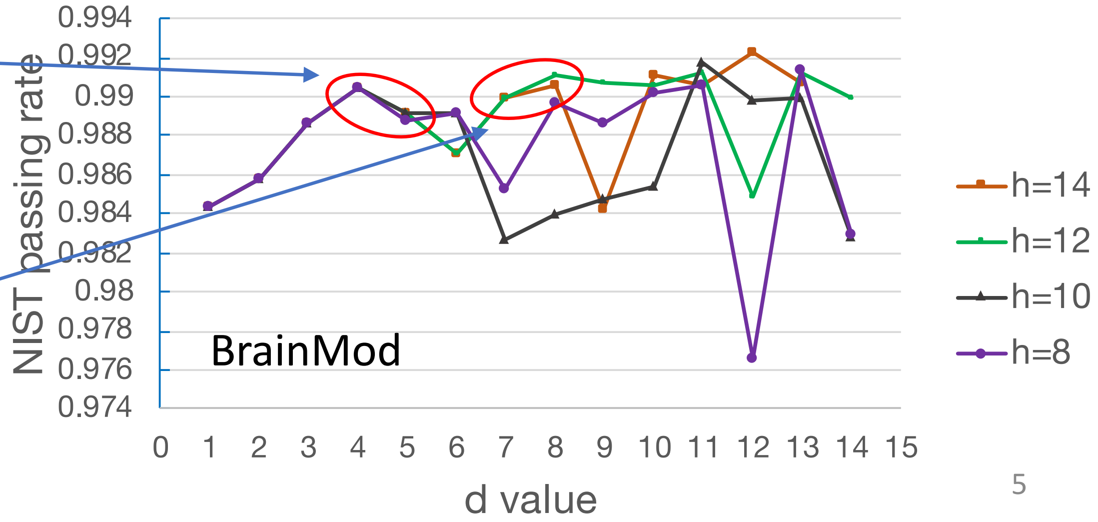
BrainBit has over 96% pass rate

R=1.5 was most consistent



Value of ‘d’ starts making a difference

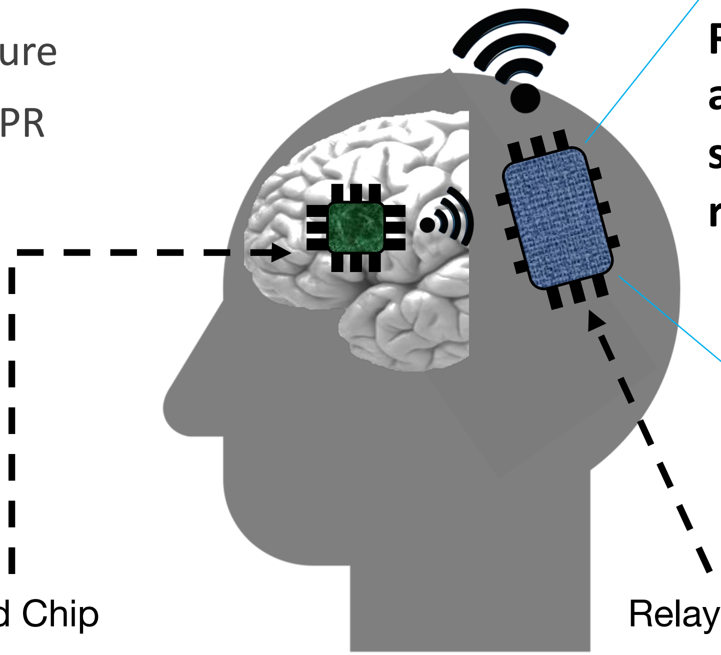
Good performance vs. pass rate



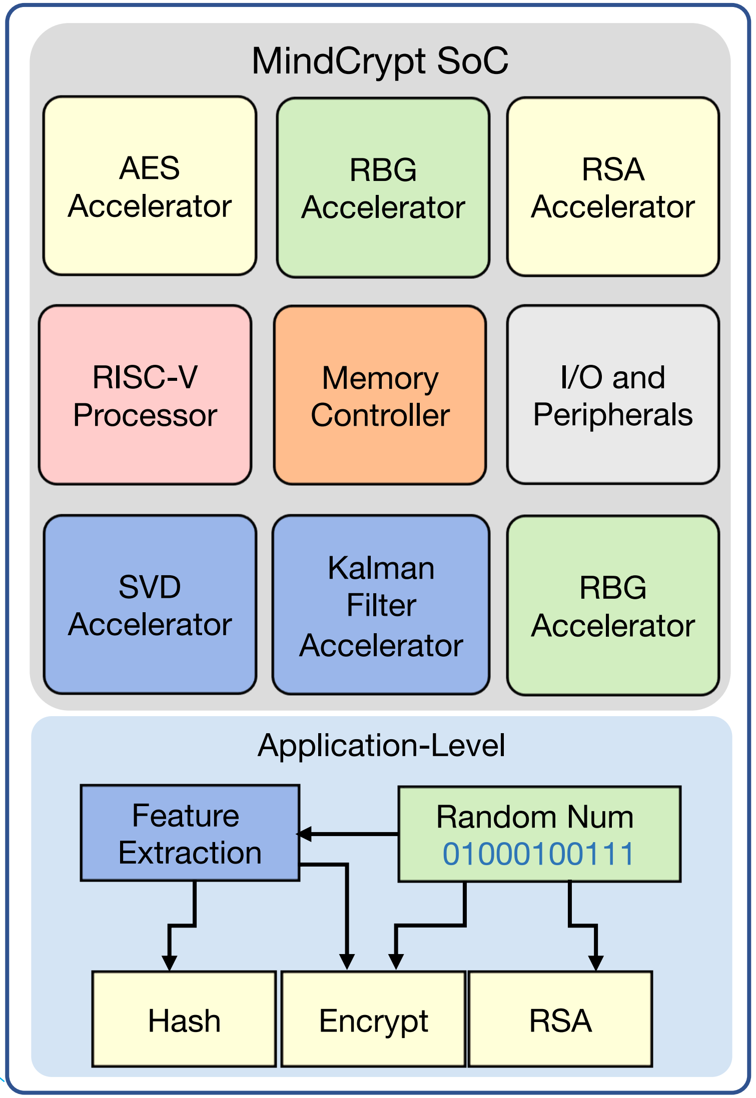
System-on-Chip for BCI – MindCrypt SoC

- BCI is a subset of the Internet-of-Things (IoT) domain
- Mobile edge devices – constraints in area in power
  - How to get real-time performance?
- Solution: Design heterogeneous Systems-on-Chip (SoCs) with hardware accelerators for BCI - MindCrypt
- SoC design platform – ESP
  - Tile-based architecture
  - Supports P2P and DPR

ESP - https://esp.cs.columbia.edu/

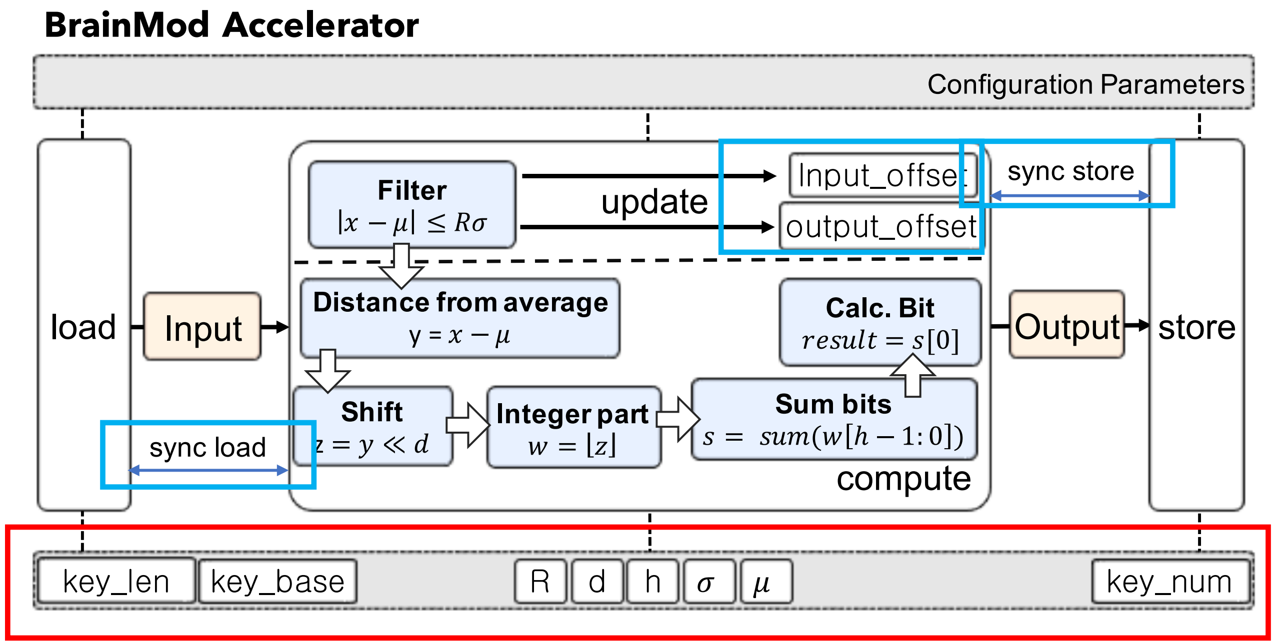


Run BCI applications and support randomness!



RBG Hardware Accelerator – BrainMod (BrainBit)

- C/C++ Vivado HLS
- 3-modules structure: *load, compute, store*
- Generates random bit-streams of configurable fixed-lengths (**keys**)
- Configuration registers:
  - key_len – bit-length of the key
  - key_base – upper bound for number of keys
  - key_num – number of keys to generate
  - $R, d, h, \sigma, \mu \ (, L)$ – configure the computation
- Input/output offset control – in case certain values didn't pass the filter condition
- Synchronization between the modules



Evaluation – MindCrypt SoC

- Prototypes of the MindCrypt SoC on Xilinx Virtex UltraScale+ VCU118 FPGA
  - @ 78MHz, 64-bit CVA6 RISC-V
  - RBG accelerators:
    - BrainMod, BrainBit
  - Crypto accelerators:
    - AES, RSA, SHA2 (from HARDROID`22)

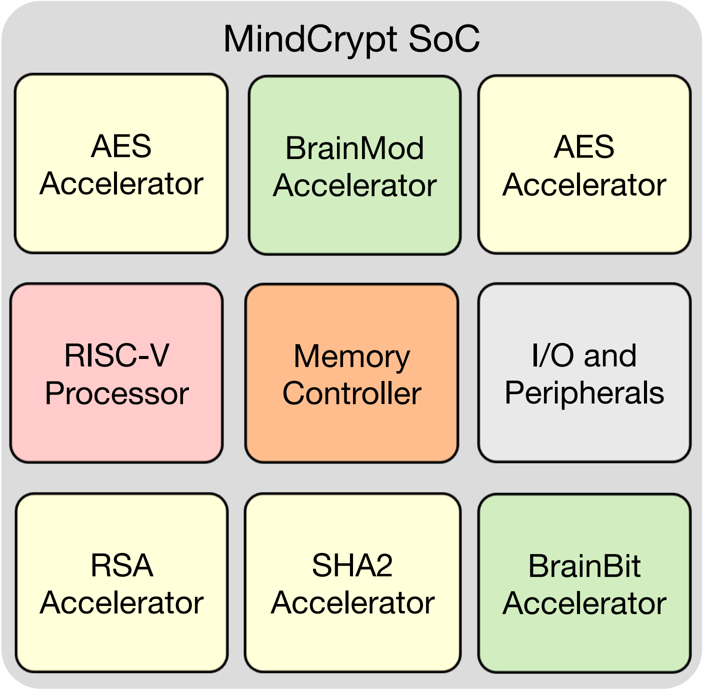


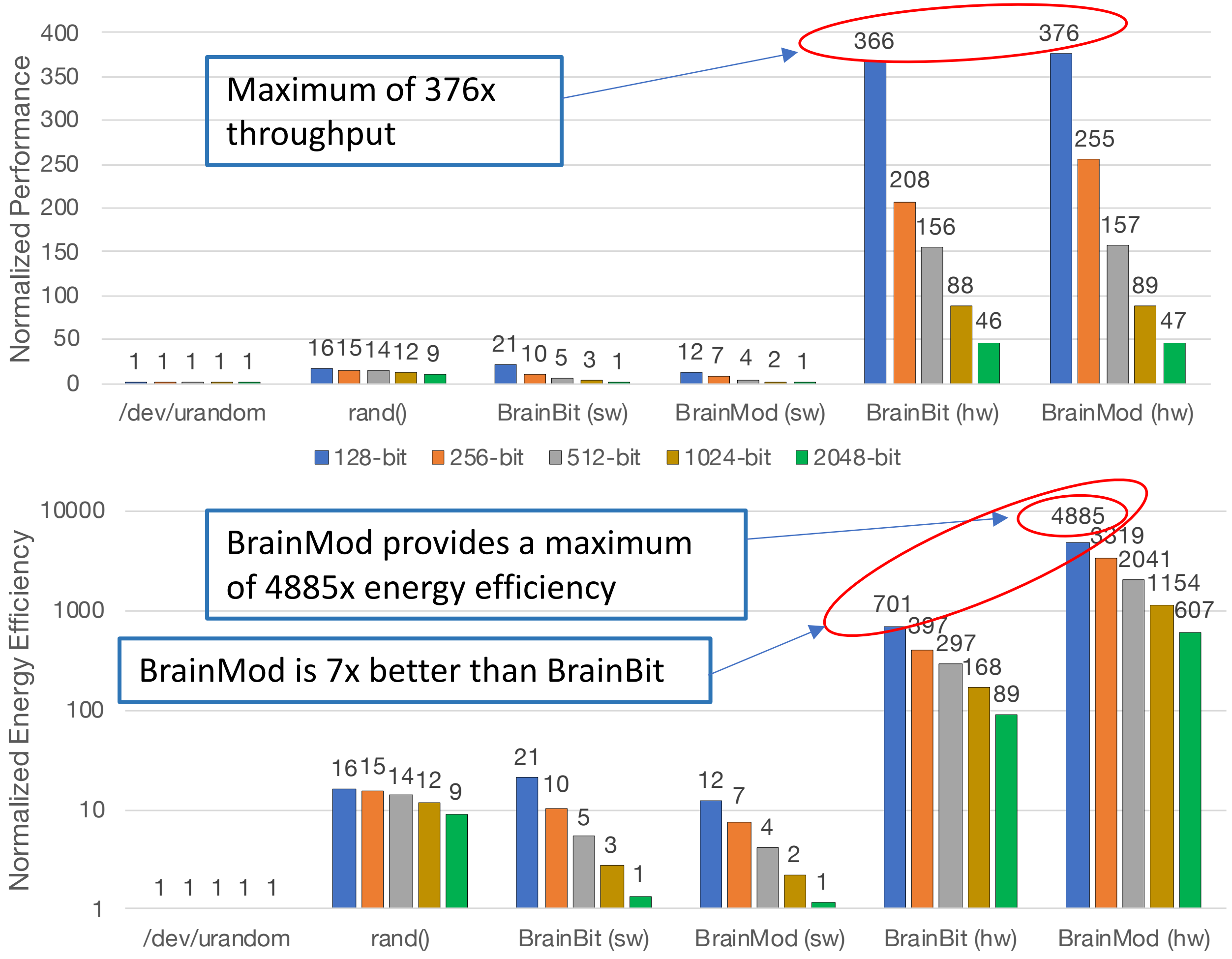
TABLE I: Resource and Power consumption in MindCrypt SoC.

Component	LUT	FF	BRAM	DSP	Power[W]	Time[ms]
BrainBit	11441	6730	4	22	0.068	89.8
BrainMod	5929	2379	4	16	0.01	88.3
CVA6	56191	35752	36	27	0.128	N/A
AES	69075	28290	14	3	0.108	4.9
RSA	126973	57941	0	0	0.277	6874.4
SHA2	32796	20756	2	0	0.408	5.1

*Execution time is for 1536 bits

Evaluation – Random Number Generation

- Compared the performance and energy efficiency of random number generation:
  - BrainMod HW and SW
  - BrainBit HW and SW
  - /dev/urandom
  - rand()



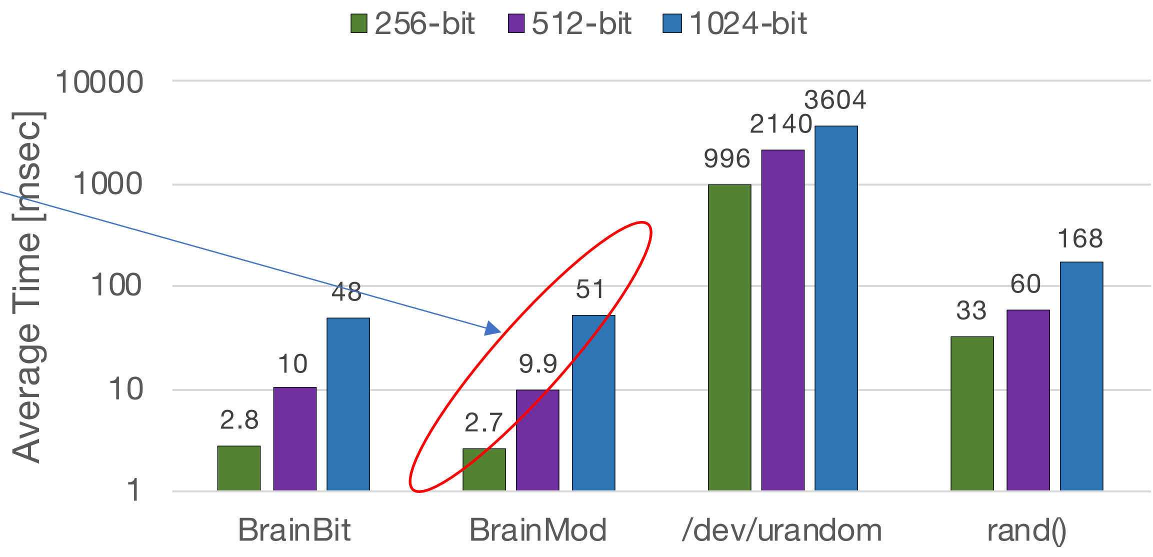
Evaluation – Prime Number Generation

- Prime numbers are important for the RSA algorithm
- MindCrypt integrates an RSA accelerator
  - The longest runtime among all accelerators
- Random prime number generation is usually a costly operation

TABLE II: Average Amount of Prime Numbers / 1000 Numbers

bit length	BrainBit	BrainMod	/dev/urandom	rand()
256-bit	5.47	5.51	5.6	11
512-bit	2.87	2.83	2.59	6.65
1024-bit	1.16	1.46	1.08	2.74

The time that takes BrainMod to generate a prime number of a fixed-length



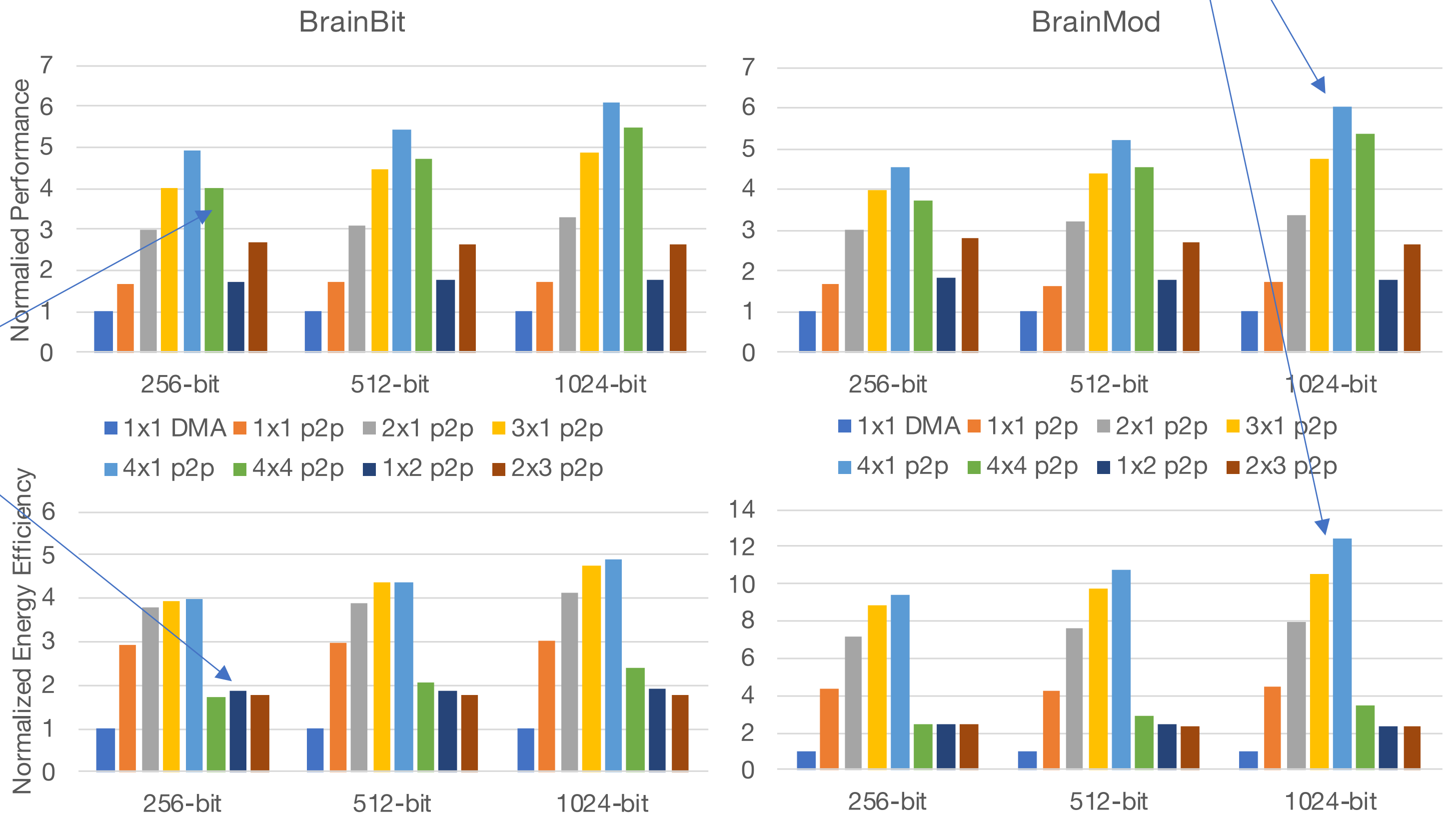
- BrainMod provides throughput gains of up to 368x – **enables fast prime number generation!**

Evaluation – Point-to-Point Communication

- Direct point-to-point (P2P) communication between AES and the RBG accelerators compared to communication through DMA
- Up to 4 instances for each: BrainMod, BrainBit, and AES

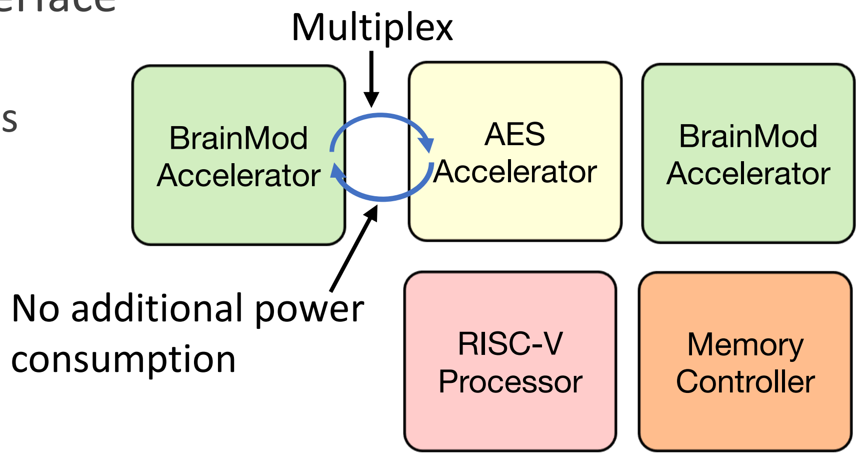
4 RBGs with 1 AES provide a maximum of 6.1x speedup and 12.4x energy efficiency

4 RBGs with more than 1 AES causes diminishing returns



Evaluation – FPGA Implementation with DPR

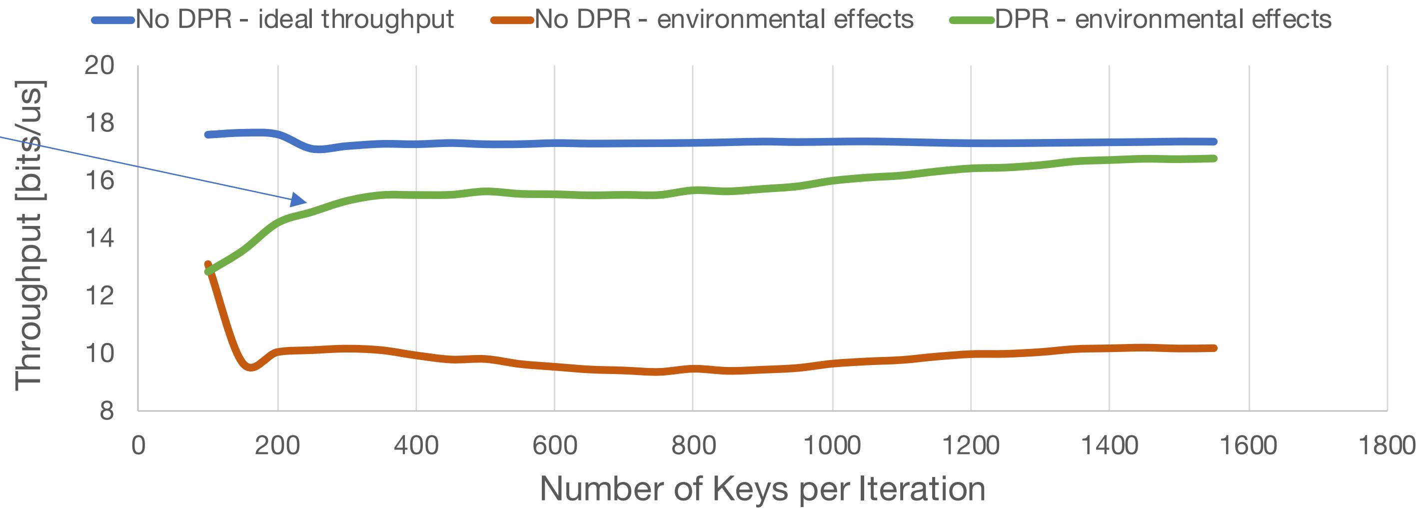
- Environmental factors can affect the performance of the neural interface – More data will be discarded by BrainMod (filter condition)
  - Solution: Increase RBG throughput by adding more BrainMod instances
  - Problem: BCI SoCs are constrained in area and power



- Low RBG throughout is detected – triggers a partial reconfiguration to replace an unused accelerator with BrainMod

- Altered brain data – 60% of the values are expected to be discarded

DPR is able to improve RBG throughput – the more random numbers the better the throughput



Conclusions and Future Research

- MindCrypt is the first work to provide a complete flow that enables brain-based configurable random number generation for applications on BCI SoCs

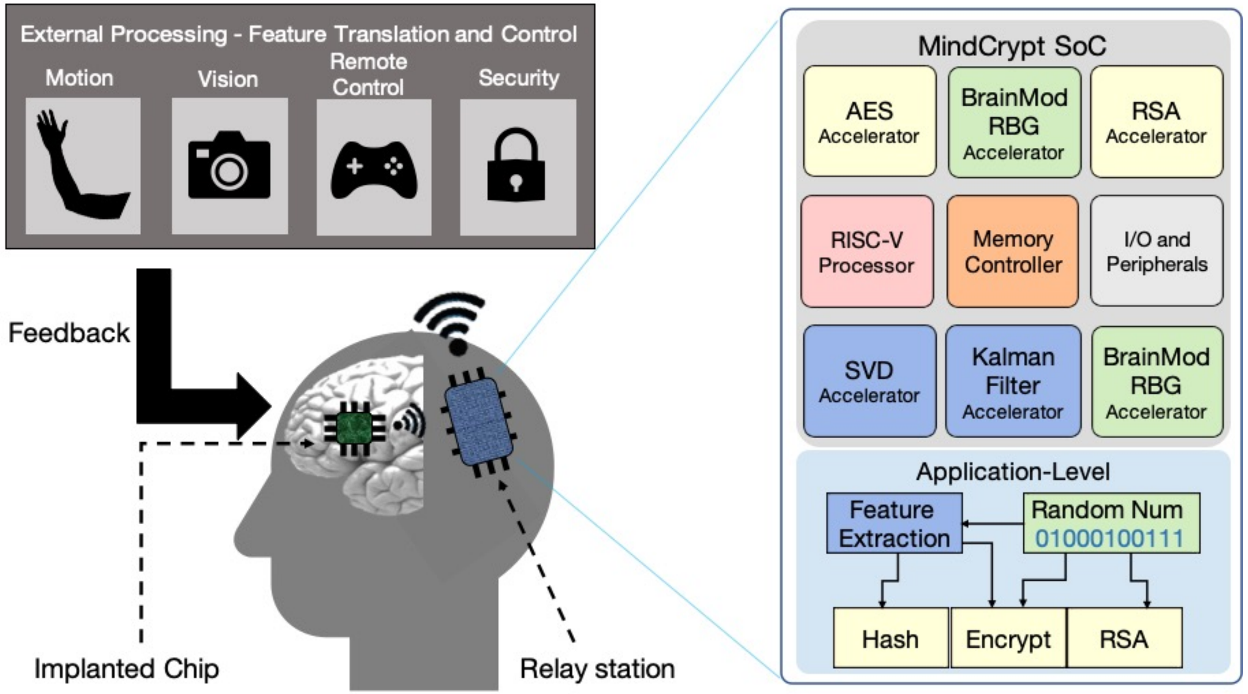
- We were able to design and test MindCrypt following the availability of open-source, modern, high-resolution, and high-throughout brain data
- MindCrypt unlocks more research opportunities on brain data by showing how it can be used in a full system

- Potential research directions include:
  - Randomness from the brain under different states (sleep, awake, walking, running, etc.)
  - Randomness extraction from different regions of the brain
  - Statistical analysis of brain data with Cryptanalysis
  - Should we use brain data for randomness outside of the BCI field?

https://github.com/GuyEichler/esp/tree/mindcrypt

Thank you!

Questions?



https://github.com/GuyEichler/esp/tree/mindcrypt