CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

What Does Security Mean for Approximate Computing

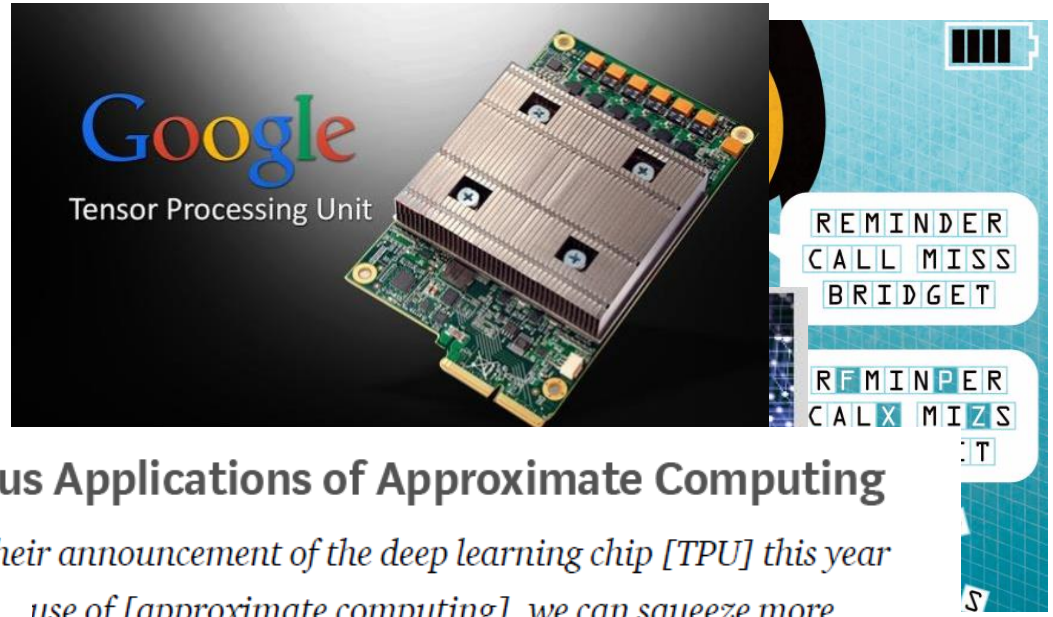
Dr Chongyan Gu

21 NOVEMBER 2019

Good-Enough Computing

We could **save energy** in everything from smartphones to super-computers by letting them make **m1stake5**

IBM, ARM, and Google are applying approximate computing to AI chip or processor design.



IBM

IBM Research Blog Topics Labs About

AI Hardware

EE Times

MIT Technology Review

Topics Magazine

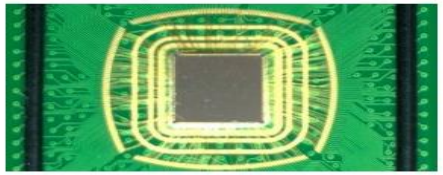
approximate computing 1 Story

Intelligent Machines

Why a Chip That's Bad at Math Can Help Computers Tackle Harder Problems

DARPA funded the development of a new computer chip that's hardwired to make simple mistakes but can help computers understand the world.

by Tom Simonite | 3 years ago



Numerous Applications of Approximate Computing

Google in their announcement of the deep learning chip [TPU] this year

use of [approximate computing], we can squeeze more

r second, use more sophisticated and powerful machine

els and apply these models more quickly, so users get more

ults more rapidly."

cusses

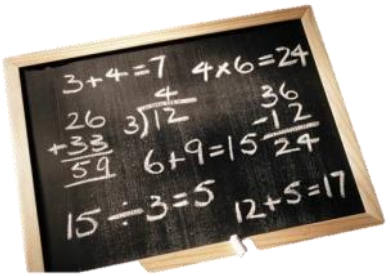
M scientists are
omized core
signed to increase
f AI systems,
the training and
esses of deep

ARM's lead processor architect has told us that the company has thought about creating an inexact processor; a processor that curtails precision in the interest of saving power.

*Source from Good-Enough Computing, IEEE Spectrum, Oct. 2013

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Approximate Computing



Change Exact Design into Approximate Design(s)

Leads to

Leads to

Reduced Complexity and Lower Power

Trade-off

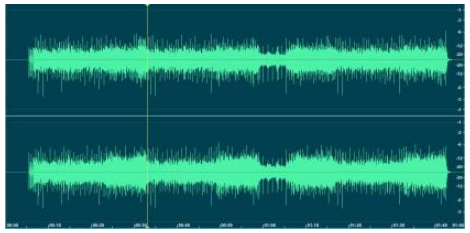
Lower Accuracy

$\pi \approx 3.14$

$e \approx 2.72$

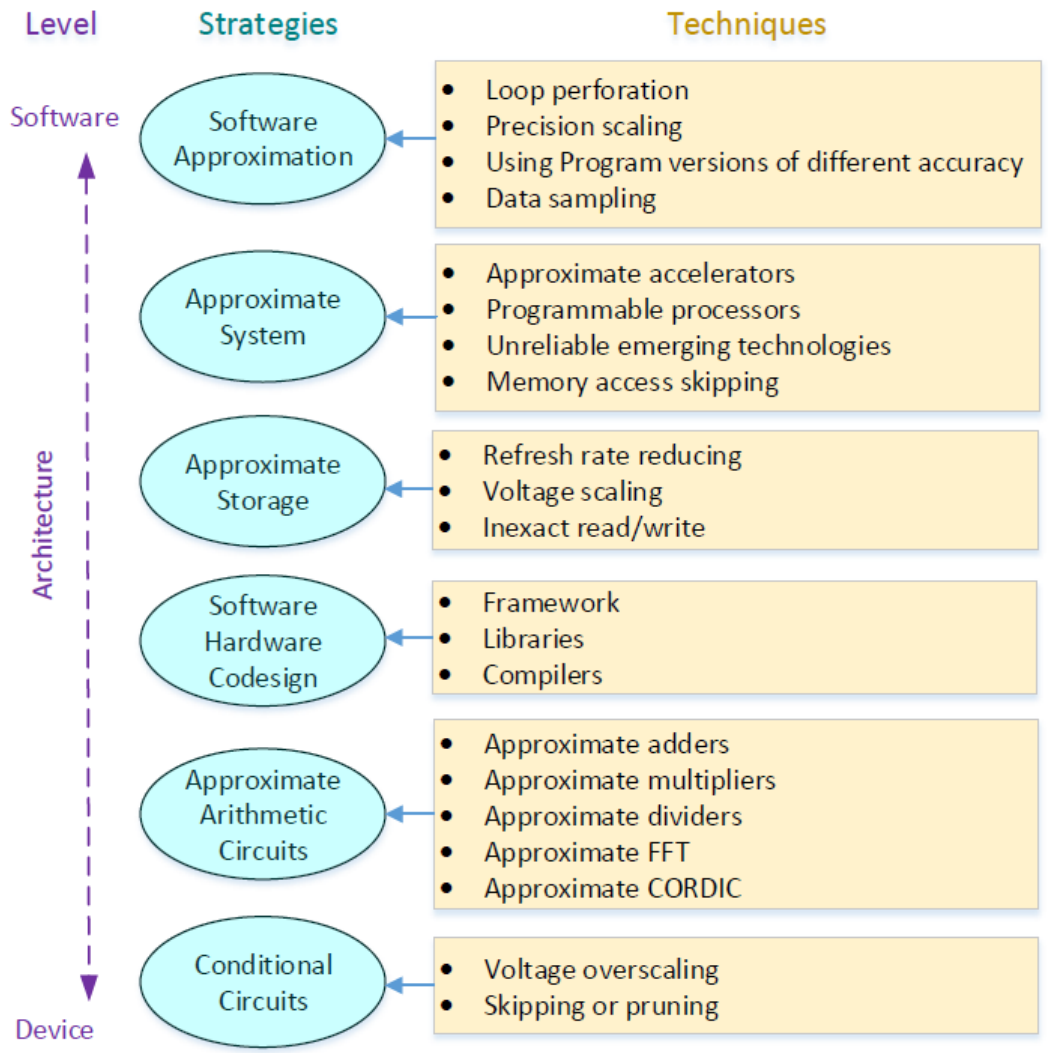
Good for

Acceptable for



Improved Performance for Error-Insensitive Applications

Approximate Computing Strategies



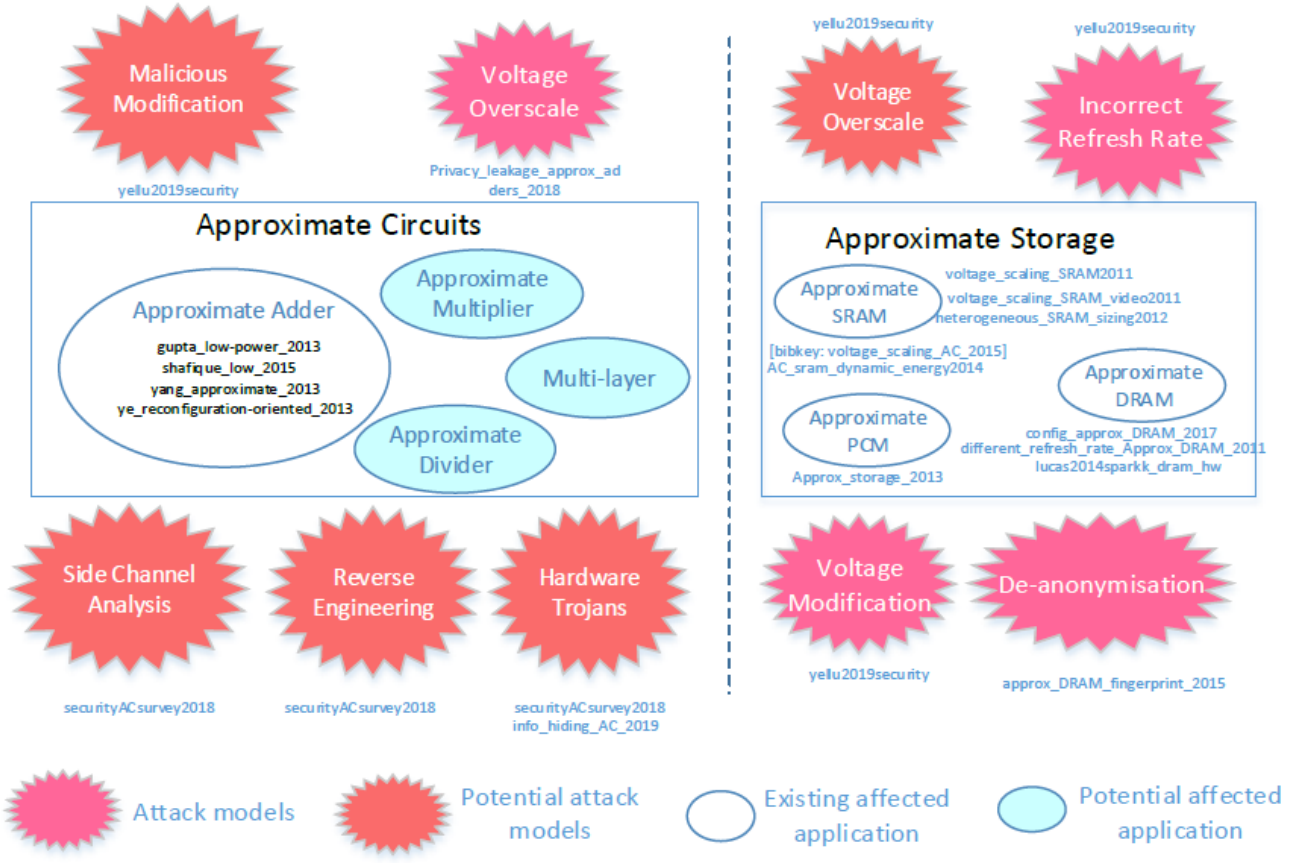
Approximate computing strategies and techniques

- Approximate computing can be utilised at different levels, from hardware to software.
- A system with approximation should have the same **security** as its non-approximated equivalent.
- However, the reality is that approximate computing introduces a new set of **vulnerablilities**.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security Threats in Approximate Computing

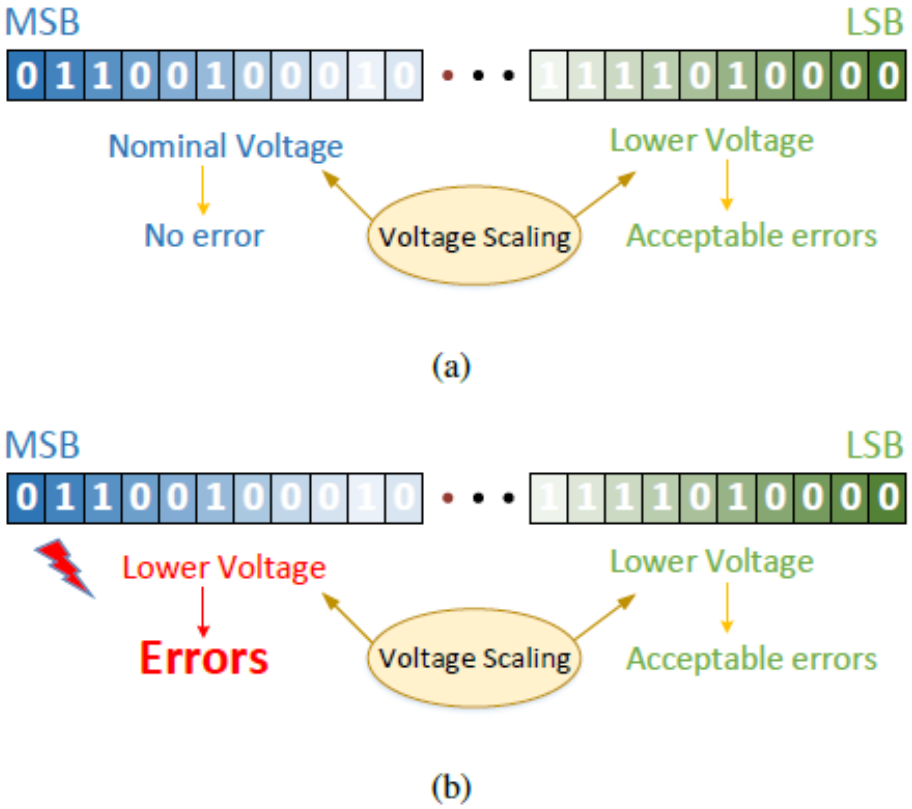
Approximate computing system circuits can be faster, more compact, with a lower power consumption. However, security threats have proven to be challenging to mitigate.



Systemization of security threats in approximate computing

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

An Example of Attacks on Approximate SRAM



An example of attacks on approximate SRAM:

(a) Normal voltage scaling technique for SRAM [1] to generate acceptable errors on the LSB and no errors on the MSB,

(b) Maliciously apply voltage scaling technique to the MSB to introduce unacceptable errors to the MSB.

MSB: the most significant bit
LSB: the least significant bit

[1] M. Cho, J. Schlessman, W. Wolf, and S. Mukhopadhyay, “Reconfigurable sram architecture with spatial voltage scaling for low power mobile multimedia applications,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 1, pp. 161–165, Jan 2011.

Take Away

Due to a high demand for low power but high performance computing systems, approximate computing has seen rapidly developments and deployment to computing architectures.

Approximate computing is beneficial for many applications, such as AI, machine learning, image processing, etc., where accurate results are not essential and intrinsic errors are tolerable for the calculation.

However, security threats are a challenge for approximate computing. Existing evidence shows that two popular approaches, approximate circuits and approximate storage, are affected.

It is expected that vulnerabilities should be applicable to more than these approaches. Security in/for approximate computing has not been widely studied.

Thank you

Any ideas or collaborations are welcome and please contact us.

Dr. Chongyan Gu
Email: c.gu@qub.ac.uk
Phone: +44(0)28 9097 1722
Address: ECIT, Queen's University Belfast,
Queen's Road,
Belfast, BT3 9DT

Research interests: Physical unclonable function (PUF), security in/for approximate computing, true random number generator (TRNG), hardware Trojan detection, logic obfuscation and machine learning attacks.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES