VOLtA: Voltage Over-scaling Based Lightweight Authentication for IoT Applications

Md Tanvir Arafin, Mingze Gao, and Gang Qu
University of Maryland, College Park

{marafin, mgao1, gangqu}@umd.edu

Internet of Things

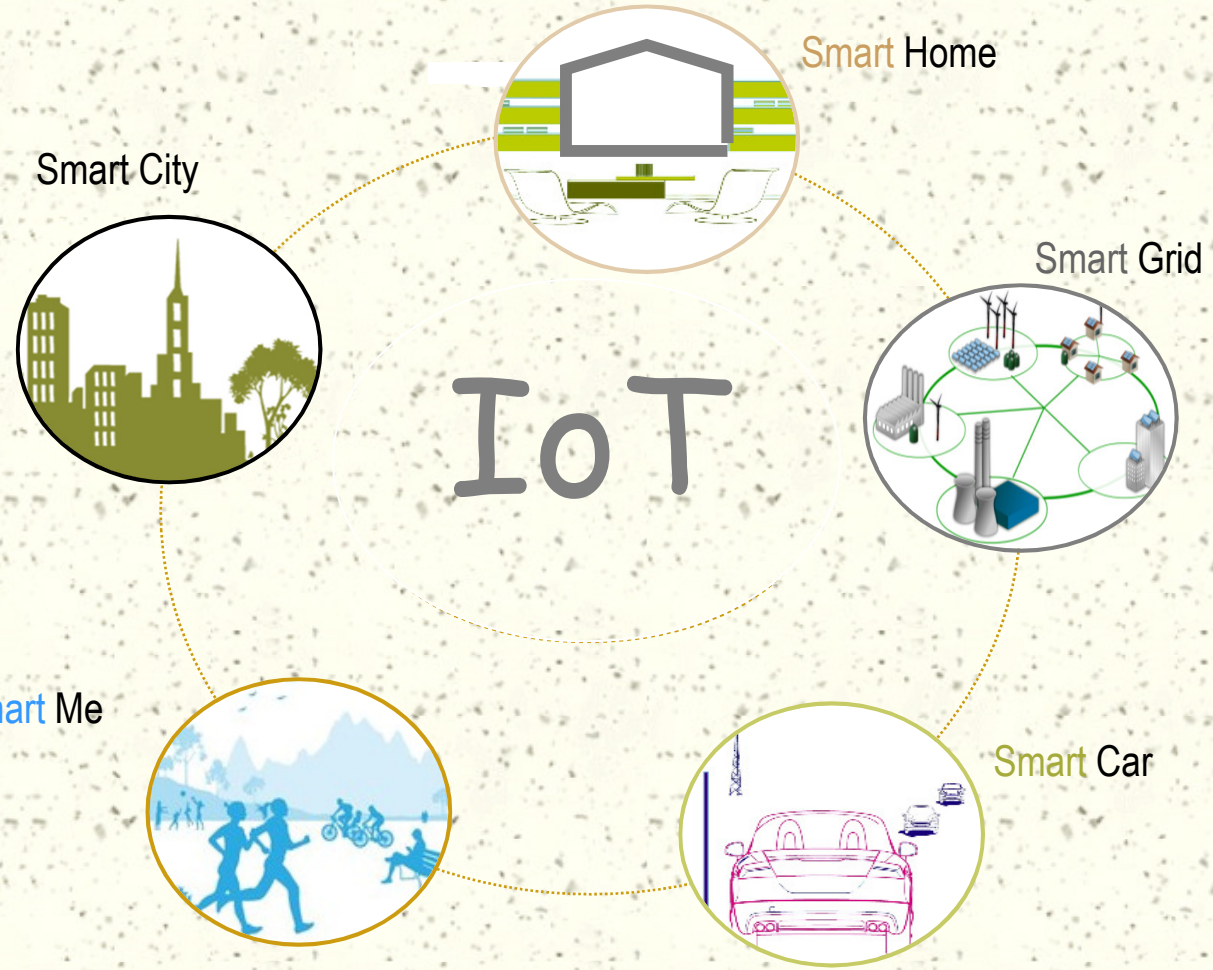


Image source: ST Microelectronics

Authentication: Why and What?

- Why authentication?

- What to authenticate?
  - device, user, data, and process

Voltage Over-Scaling

- Reducing V_{dd} for power reduction
  - $P=P_{stat}+P_{dyn}=C_{eff}V_{dd}^2f+V_{dd}(I_{sub}+I_{gate})$
  - Quadratic dependence of power to V_{dd}
- Critical Voltage
  - Cell delay $d_{gate} \propto V_{dd}/\beta(V_{dd}-V_t)^{\alpha}$
- Scaling below critical voltage
  - Error due to path delay
  - Incorrect computation

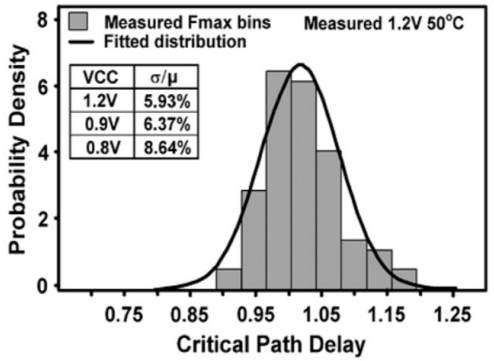


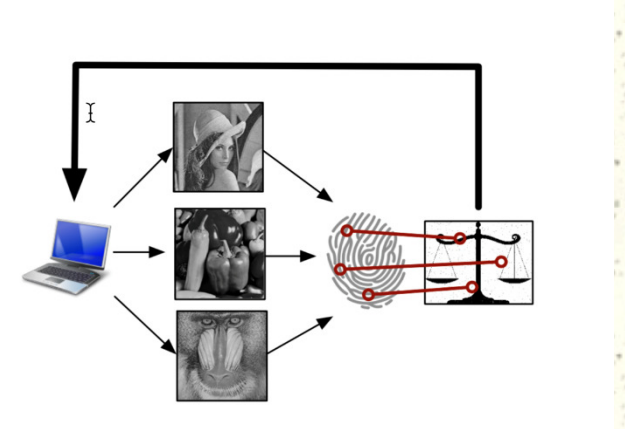
Figure 1: Impact of voltage scaling on path delay distribution. Mean and sigma of delay distribution and number of paths failing to meet target delay increase (80-core processor in 65nm [2]).

Han et al. ETS'13

Dr. Gang Qu (gangqu@umd.edu)

VOS for DRAM Deanonymization

- Key idea:
  - Use DRAM at a lower voltage
  - Cell decay rate is a function of process variation
  - Lowering V_{dd} will create errors in the data
  - Similar error pattern on the same chip
  - Profile the error for deanonymizing DRAMs



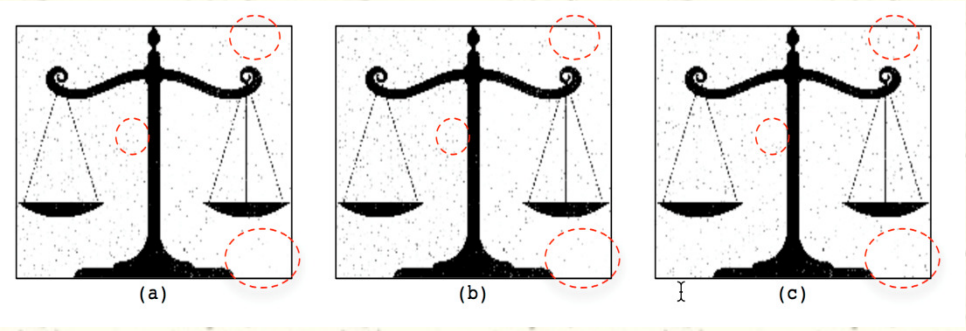


Figure 2: DRAM fingerprints on data

Motivation of the Work

- Fabrication variation impacts VOS
  - Transistor size shrinking makes V_t variation wider

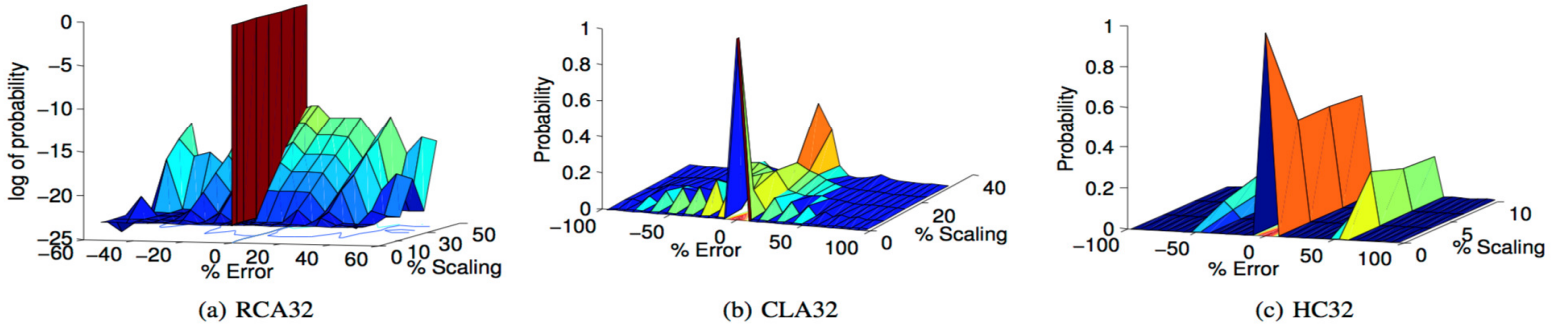
    $$\sigma_{\Delta Vt}=A_{\Delta Vt}/(WL)^{1/2}$$
  - Path delay error is a function of process variation

    $$d_{gate} \propto V_{dd}/\beta(V_{dd}-V_t)^{\alpha}$$
  - ➔observe (V_t) variation by VOS?!
  - *Variation is believed to be unique, random, unclonable*
- Security applications
  - Device fingerprint/identifier
  - Device authentication
  - Hardware PUF and other security primitives

Challenges

Where to Apply VOS?

- The circuit/device: simple, but …
- Small and common building blocks
- Existing VOS studies on different adders
  - Ripple Carry Adder
  - Carry Look ahead Adder
  - Han-Carlson Adder

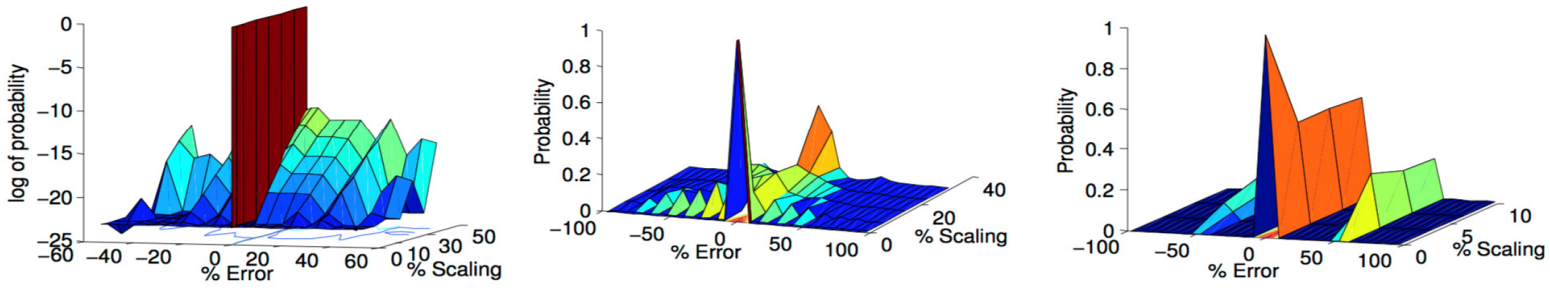


(a) RCA32 (b) CLA32 (c) HC32

Figure 3: Error Distribution for Different Adders [7]

VOS on Adders

- All inputs are equi-probable
- Error probability increase with scaling
- Output error depends on both current input and the previous input



(a) RCA32 (b) CLA32 (c) HC32

Dr. Gang Qu (gangqu@umd.edu)

Venkatesan et al. ICCAD'11

VOS Errors on RCA

- Why RCA?
  - One of the simplest designs
  - Error probability is higher with scaling
  - Show our proposed ideas only
  - 8-bit for reduced simulation time
- Goals of the experiment
  - Uniqueness
  - Robustness

Experimental Setup

- HSpice platform with FreePDK 45nm libraries
- 200 modified NMOS and PMOS models with a ±7.5% standard variation in V_t
- NMOS and PMOS transistor models are randomly chosen to build 100 different versions of each cell standard cell library.
- Circuits designed in Verilog and synthesized with Cadence Virtuoso RT compiler.
- The synthesized design is converted into an HSpice netlist with standard cells randomly chosen from the modified library

Experimental Parameters

Parameter Name	Value(s)
Supply voltage (V_{DD})	0.4V/0.45V/1V
NMOS threshold voltage (V_{tn})	0.322±0.02415V
PMOS threshold voltage (V_{tp})	-0.302±0.02265V
Operating temperature (T)	25 deg. C
Clock Period (T_{clk})	1ns

Uniqueness of Error under VOS

	A1	A2	A3	A4	A5	A6	A7	A8
A1	0	18.82	18.24	18.04	19.44	18.38	18.33	17.52
A2	18.82	0	5.36	5.21	5.67	5.65	3.89	5.39
A3	18.24	5.36	0	4.62	5.98	5.11	5	6.79
A4	18.04	5.21	4.62	0	5.73	3.53	4.13	6.44
A5	19.44	5.67	5.98	5.73	0	6.04	5.59	6.28
A6	18.38	5.65	5.11	3.53	6.04	0	4.96	6.64
A7	18.33	3.89	5	4.13	5.59	4.96	0	5.41
A8	17.52	5.39	6.79	6.44	6.28	6.64	5.41	0

Table 1. Pairwise Hamming distance (in percent) between the output from 8 devices at 0.4V.

Robustness with V_{dd} Variation

- With voltage increases
  - Error probability decreases
  - Output converges to the correct value
  - Noise in V_{dd} can have detrimental effect

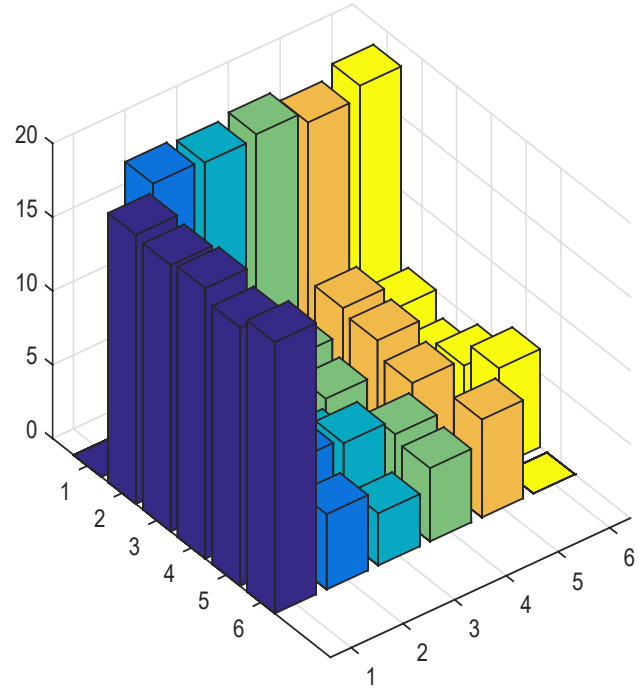


Figure 7. Hamming distance (in percent) between devices at 0.45V .

Robustness with Temperature Variation

- Error distribution is temperature sensitive
- No. of bit flips is relatively small with small temperature variations

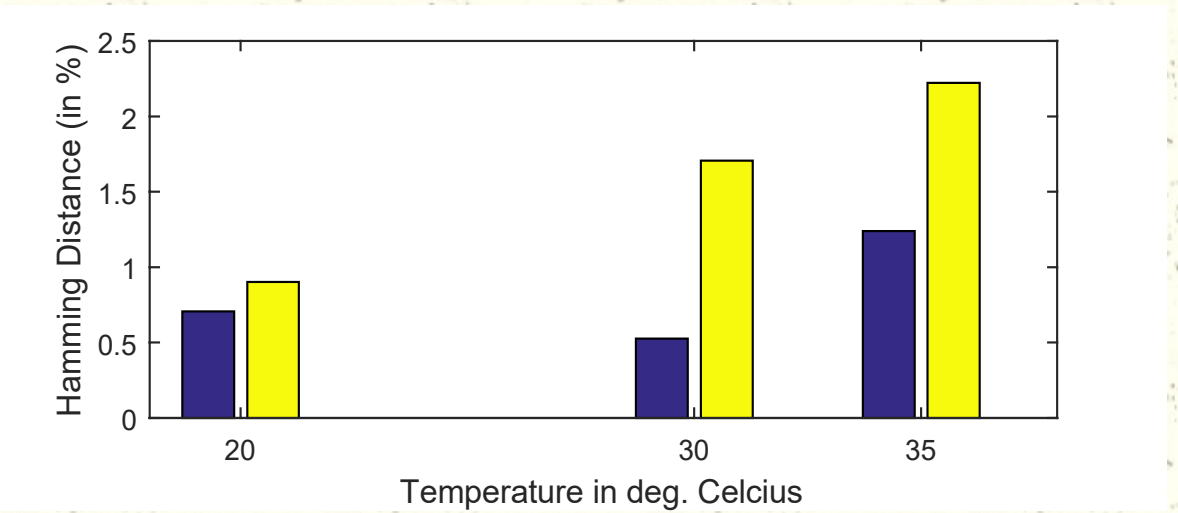


Figure 8. Temperature dependent bit flips for two different adders. The distance is calculated from the results produced at T=25 degree Celsius. The blue (left) bar represents the temperature dependent bit-flip for adder A2 and the yellow (right) bar represents the adder A3.

VOLtA: Protocol

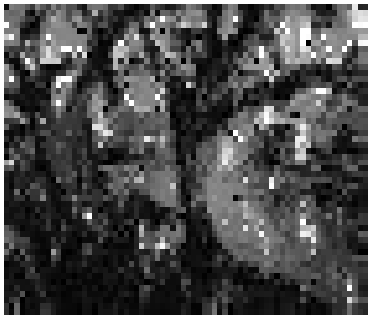
- Registration
  - Bob has a password K=(k1, k2)
  - Alice registers K=(k1, k2), and profiles or models the error pattern M.
- Authentication
  - Alice picks a random string R and sends it to Bob.
  - Bob calculated L=R+k1 using the adder and then calculates Y=L $\oplus$ k2 =(R+k1) $\oplus$ k2.
  - Bob sends Y to Alice.
  - Alice calculates L=Y $\oplus$ k2 and L'=M(R,k1). If *distance* (L',L) < *threshold*, Bob is authenticated.

VOLtA: Analysis

- Effectiveness
- Choice of Key
- Attacks
  - Random Guessing
  - Eavesdropping
  - Side-channel Attack
  - Learning Attack

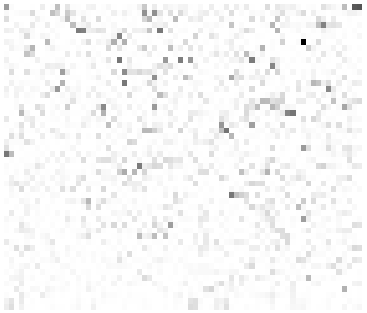
VOLtA: Illustrative Example

(a)

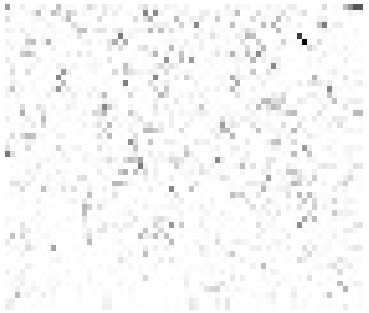


(b)

(c)



(d)



(e)

(f)

Measurements Metrics

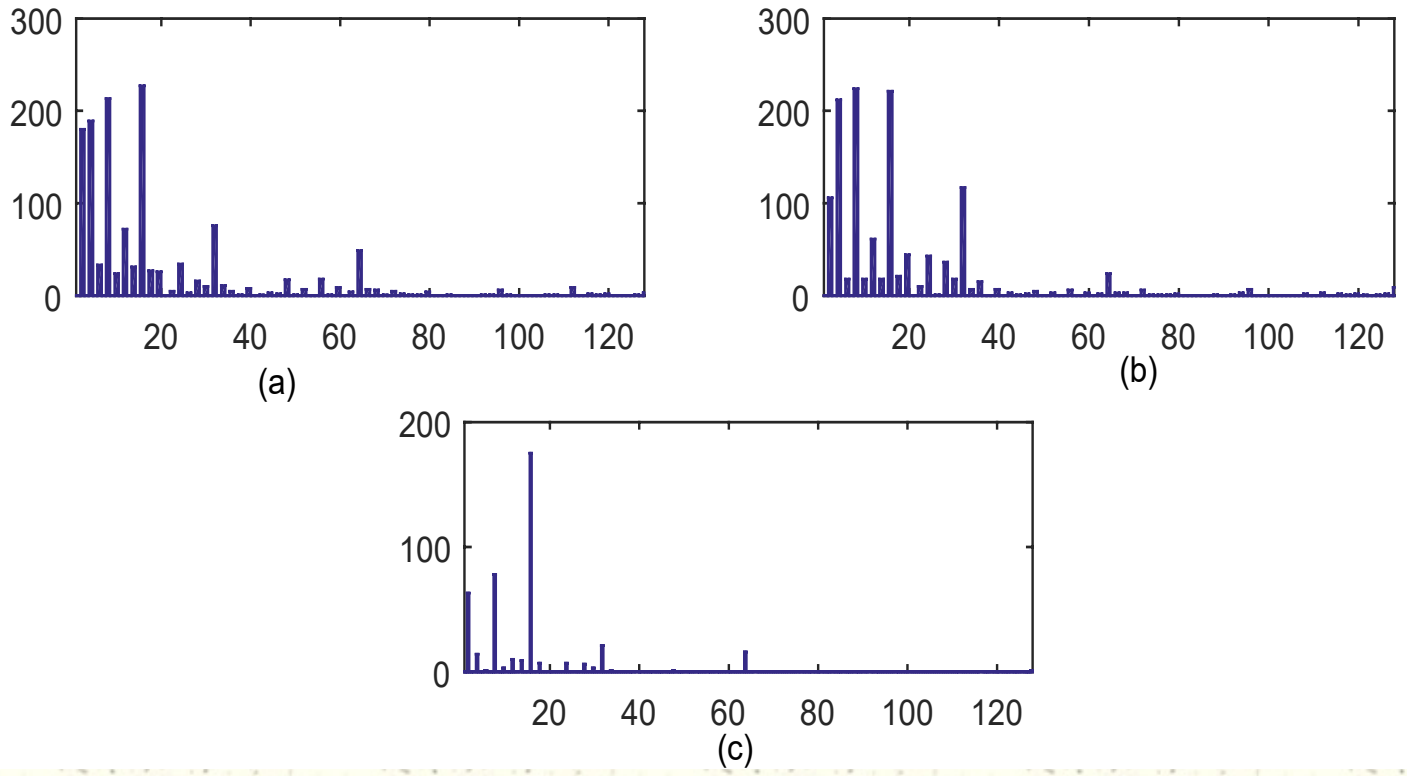


Figure 6. A histogram of the Euclidian distances (a) between the figures 5(a) and 5(b); (b) between the figures 5(a) and 5(c); between the figures 5(b) and 5(c)

Conclusions

- Hardware for lightweight security in IoT
- Voltage Over-Scaling
  - A popular approximate computing method
  - Leaves a process variation dependent device signature in the approximate results
  - Drawbacks: information leak, deanonymization

  ➔ A new security primitive!
- VOS based Device authentication
  - Lightweight: low cost, (low level of) security
  - Good for certain IoT applications

Thank You!

AFOSR MURI under award number FA9550-14-1-0351.

MeshSec Lab