SAR ADCs for the discriminating host

An Update

National Nuclear Security Administration

CHARACTERIZING GAPS & CHALLENGES

Disarmament Treaties

GAPS & CHALLENGES

CVT Thrust Area

Bureau of Arms Control, Verification and Compliance (AVC) in DoS

AVC 2015

VERIFICATION TECHNOLOGY
RESEARCH AND DEVELOPMENT NEEDS

The following represents the priority needs of the Bureau of Arms Control, Verification and Compliance (AVC) for research and development programs to address critical arms control and nonproliferation technology requirements in the realm of verification and transparency. Responding to these priorities may involve the use of current technologies in unconventional ways, while others will require years of basic research, a properly resourced transition and acquisition process to build deployable systems, and diplomatic legwork on our part to create a feasible environment for deployment.

The top priorities for related verification technology research and development are:

Nuclear Test Ban Treaties, Agreements, and Moratoria

CTBT, Limited Test Ban Treaty (LTBT), Threshold Test Ban Treaty (TTBT), Peaceful Nuclear Explosion Treaty (PNET).

- Critical examination of the assumptions and methodologies that go into calculations to extract the yield of an underground test from **seismic** signals recorded at standoff distances.

- Capability to rapidly determine whether an explosion is nuclear or conventional. {seismic, infrasound, radionuclide, NTM, ….}

- Research is needed to explore the feasibility of "**information barriers**" to allow the collection and analysis of gamma-ray spectra associated with radionuclides without making the full spectral data available to inspectors (in the context of CTBT On-Site Inspections (OSI)).[2]

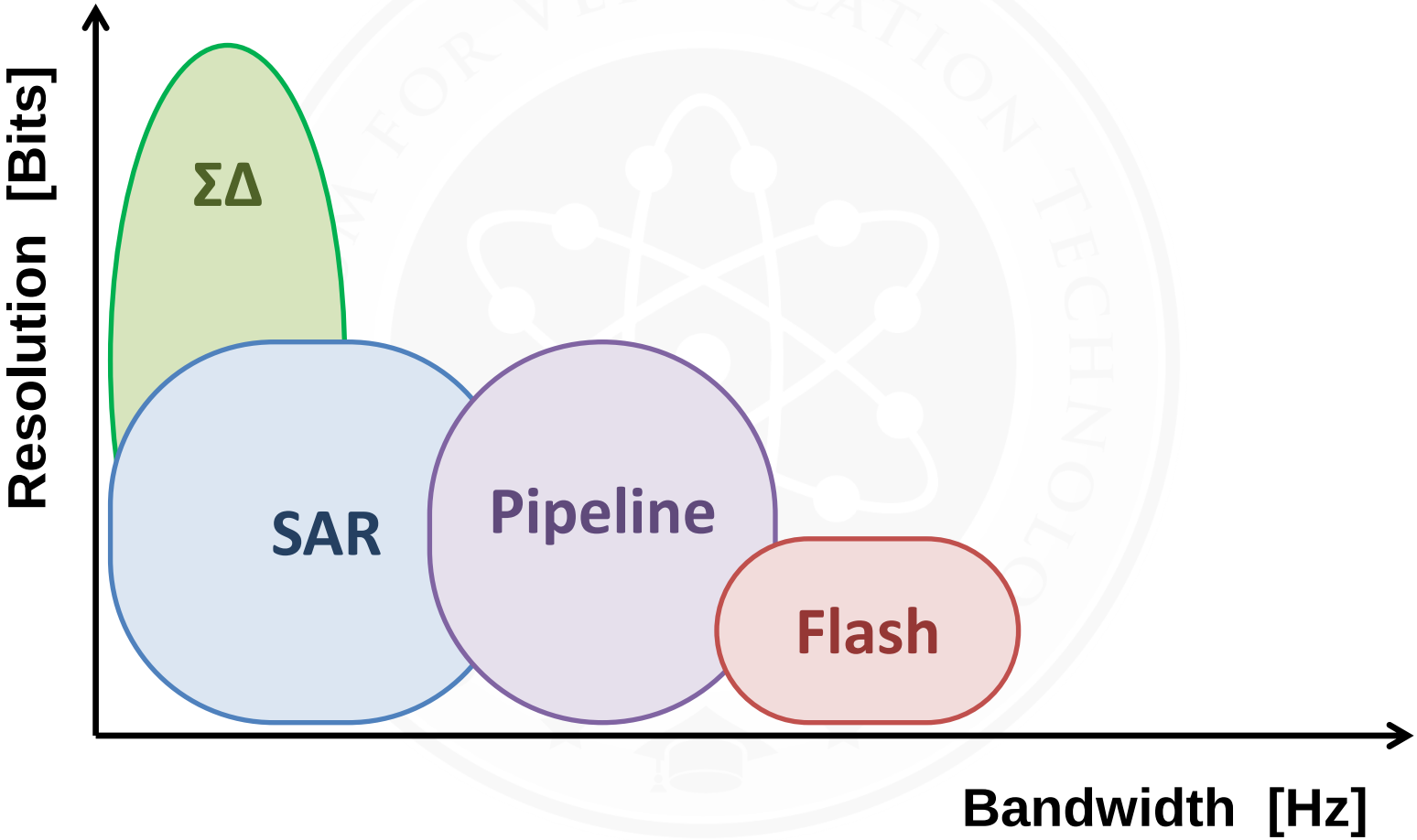
Future Nuclear Arms Reduction and Fissile Material Cutoff Treaties

AVC 2015

- Identify **aspects of the nuclear enterprise**, particularly involving the warhead life cycle, that would lend themselves to a control and/or transparency regime that is substantive, verifiable and improves U.S. National Security.
- Improved **detection of fissile materials**, particularly when they are shielded, at a standoff distance, and/or do not spontaneously emit neutrons.
- Strategies and/or technologies to **protect sensitive information** while verifying compliance with a nuclear warhead control or dismantlement regime.

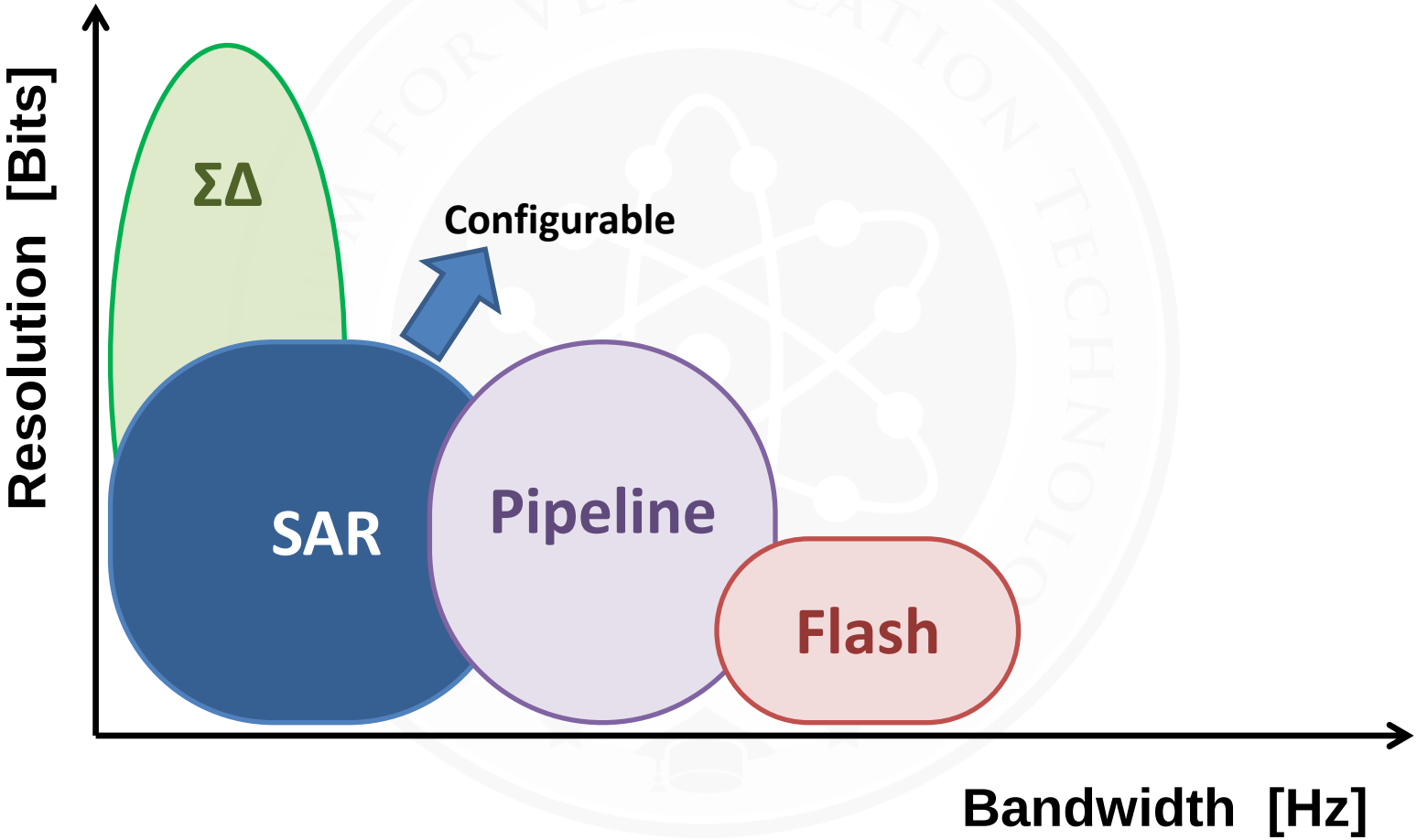
Understanding the problem

Fundamental Analog to Digital Converters (ADCs)



Understanding the problem

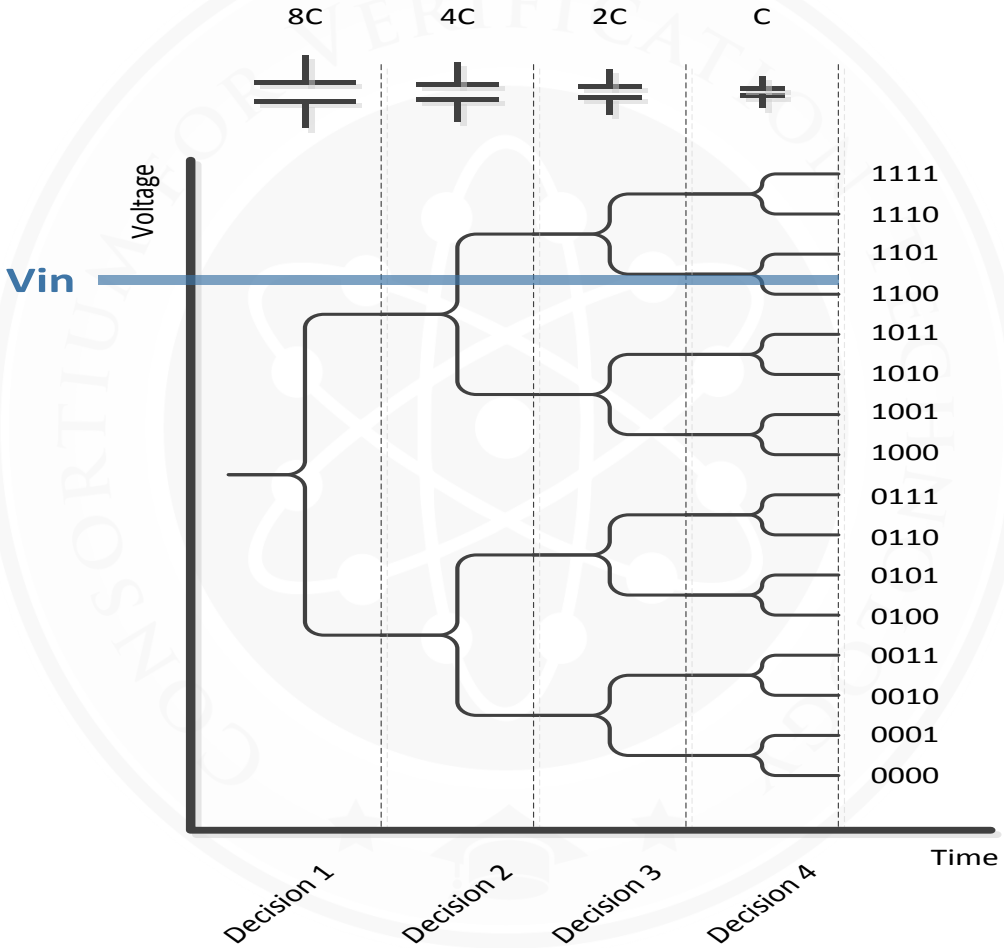
Fundamental Analog to Digital Converters (ADCs)



[Book of the Dead - Wikipedia]

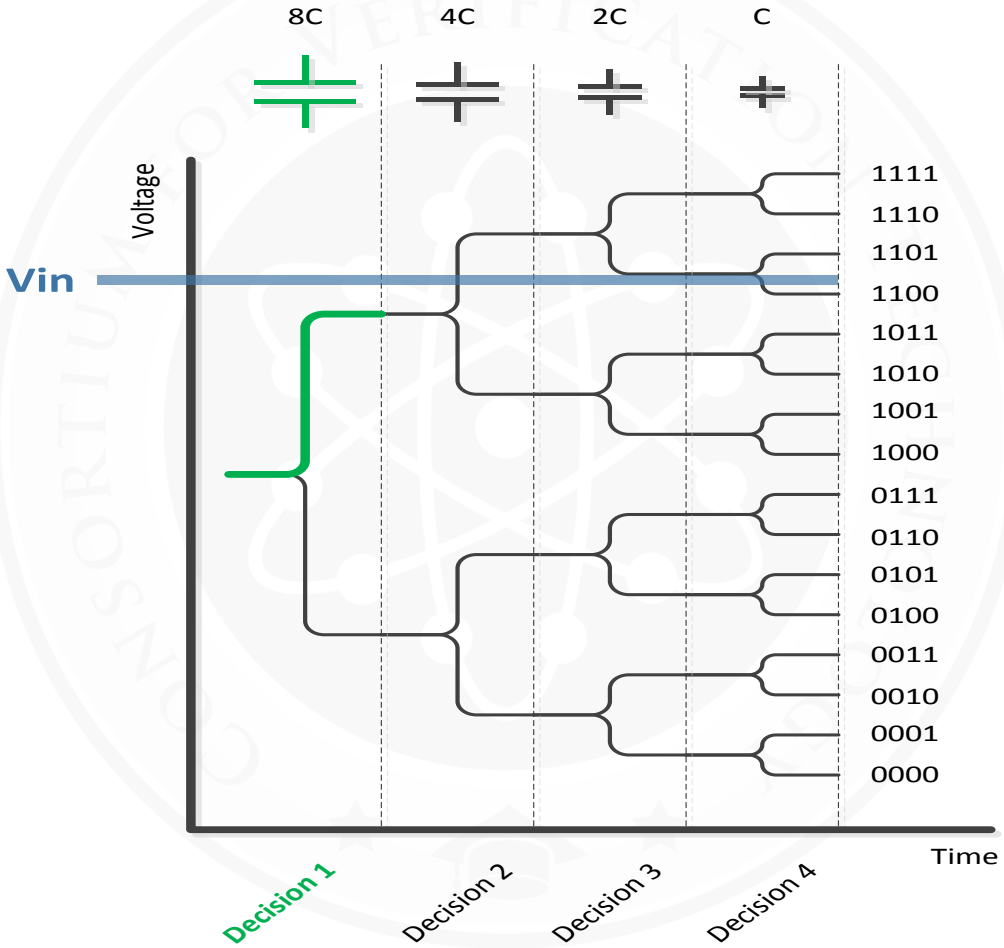
Basic Operation of SAR ADC (4-bit)

Decision 0/4



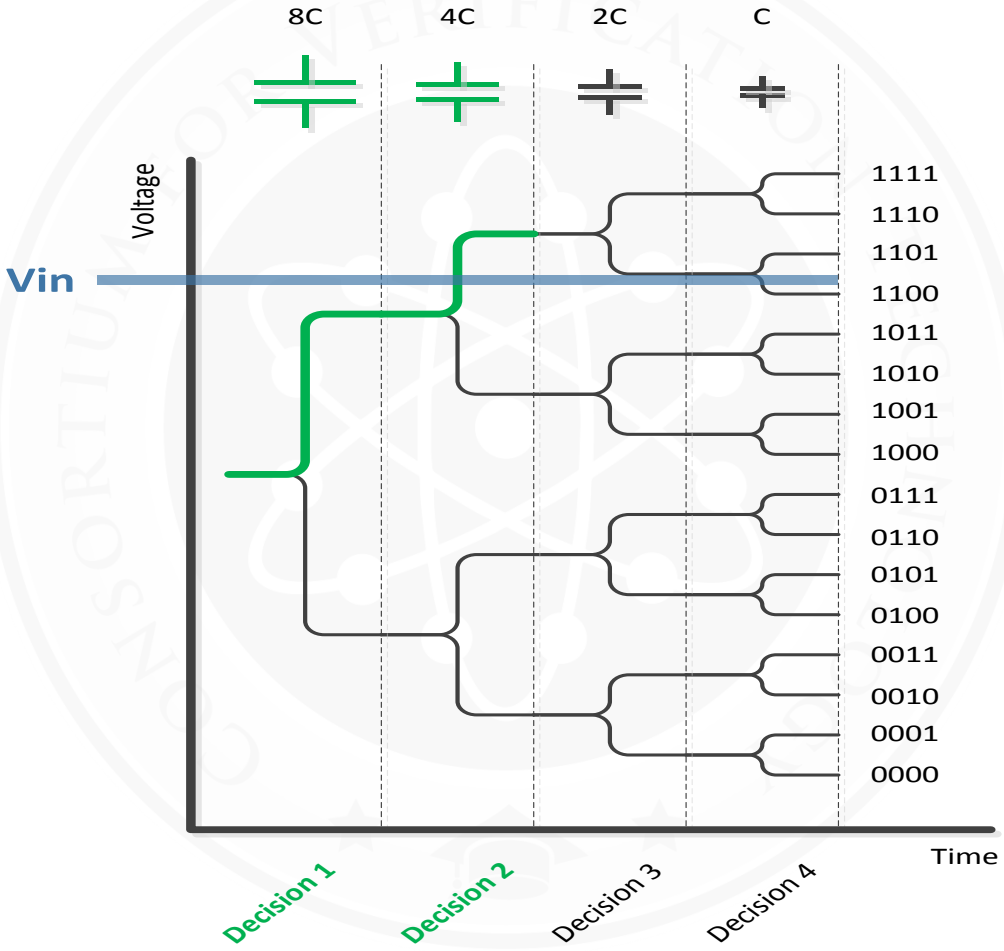
Basic Operation of SAR ADC (4-bit)

Decision 1/4



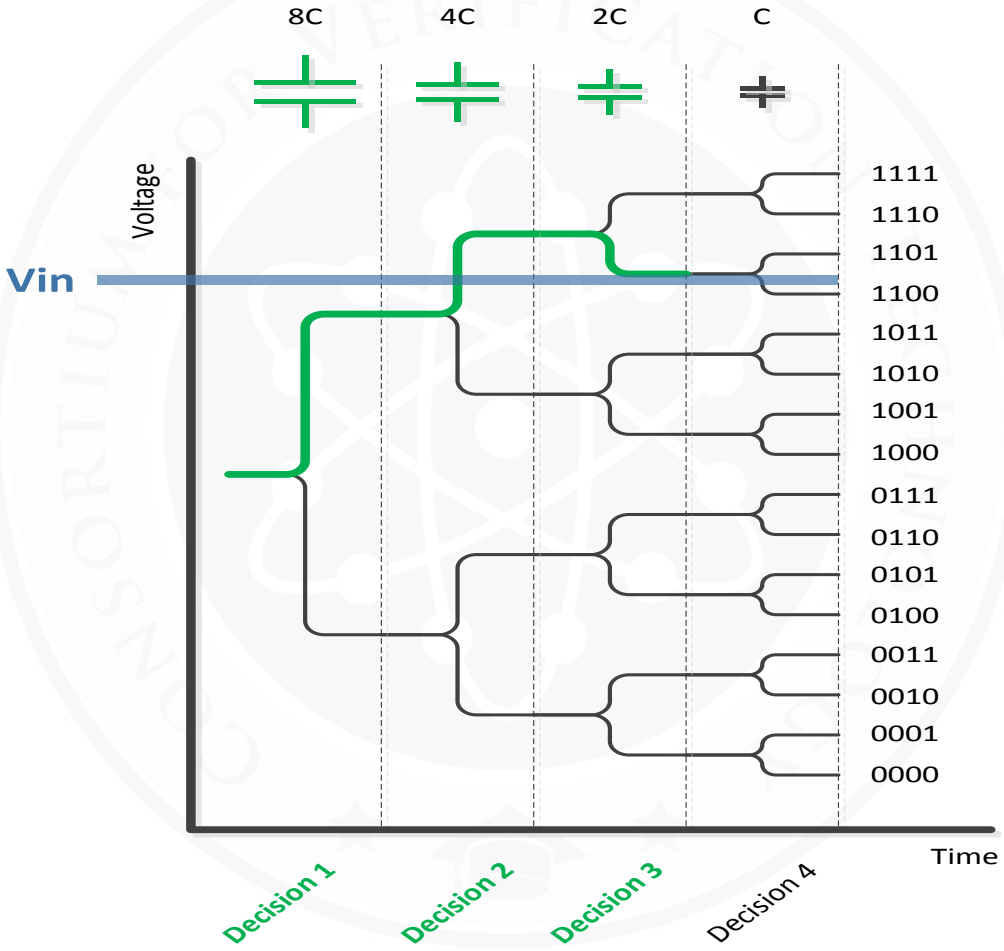
Basic Operation of SAR ADC (4-bit)

Decision 2/4



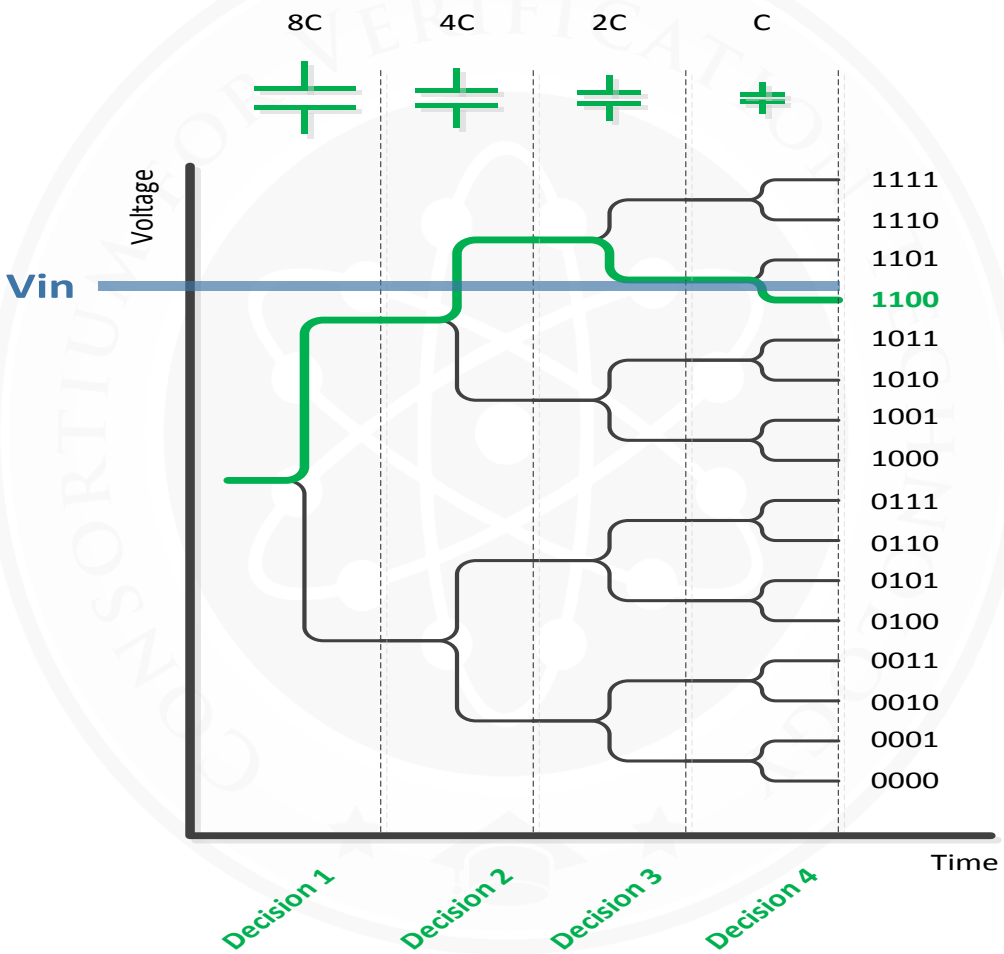
Basic Operation of SAR ADC (4-bit)

Decision 3/4

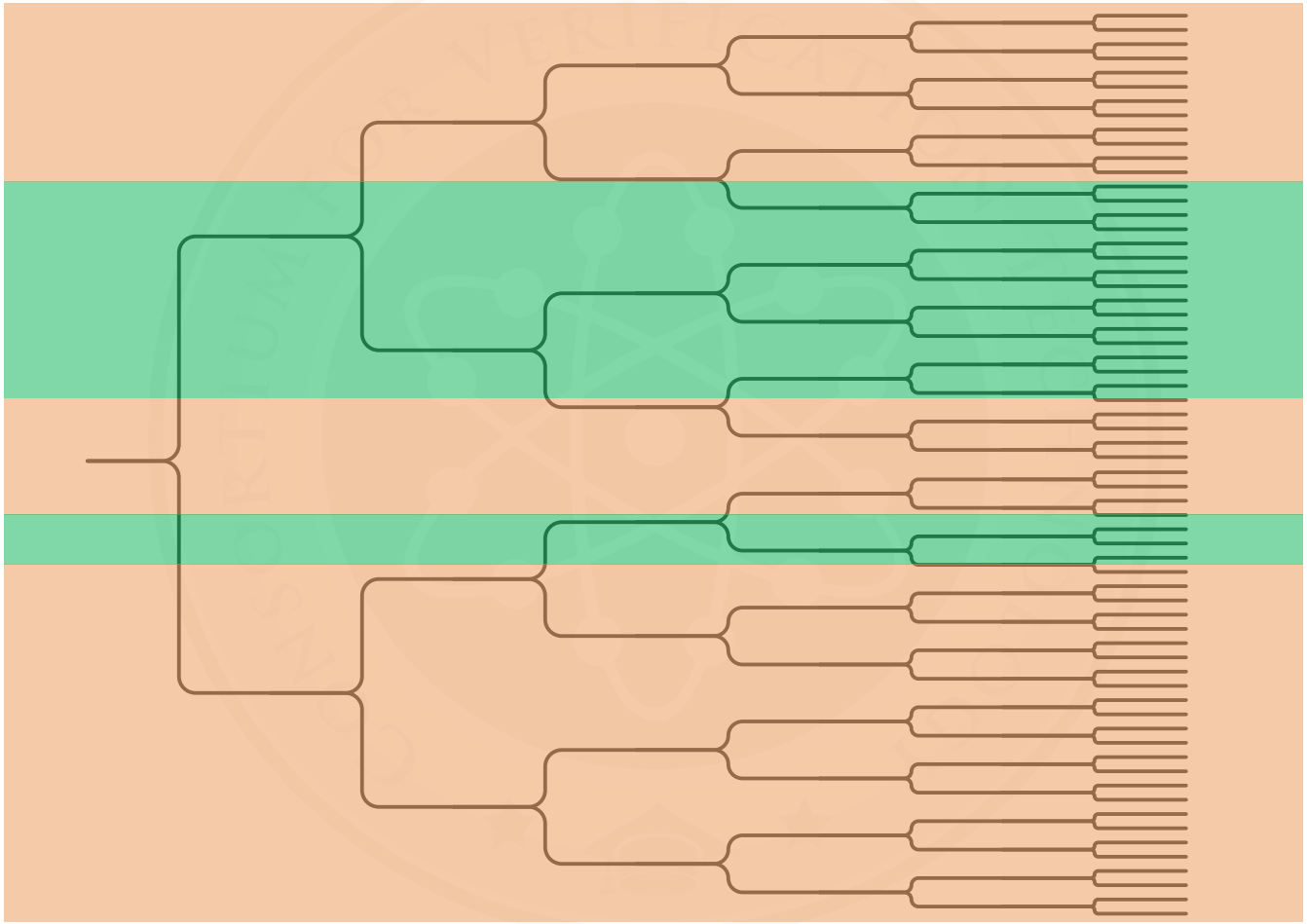


Basic Operation of SAR ADC (4-bit)

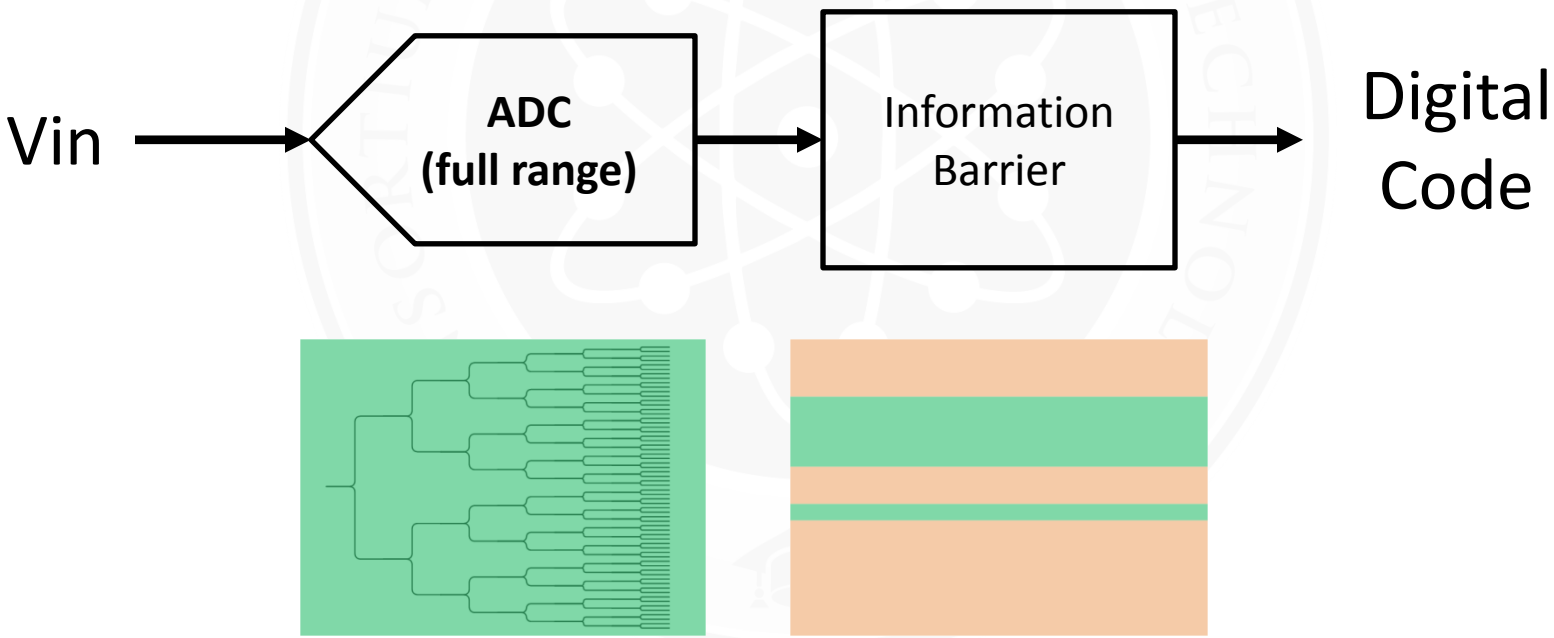
Decision 4/4



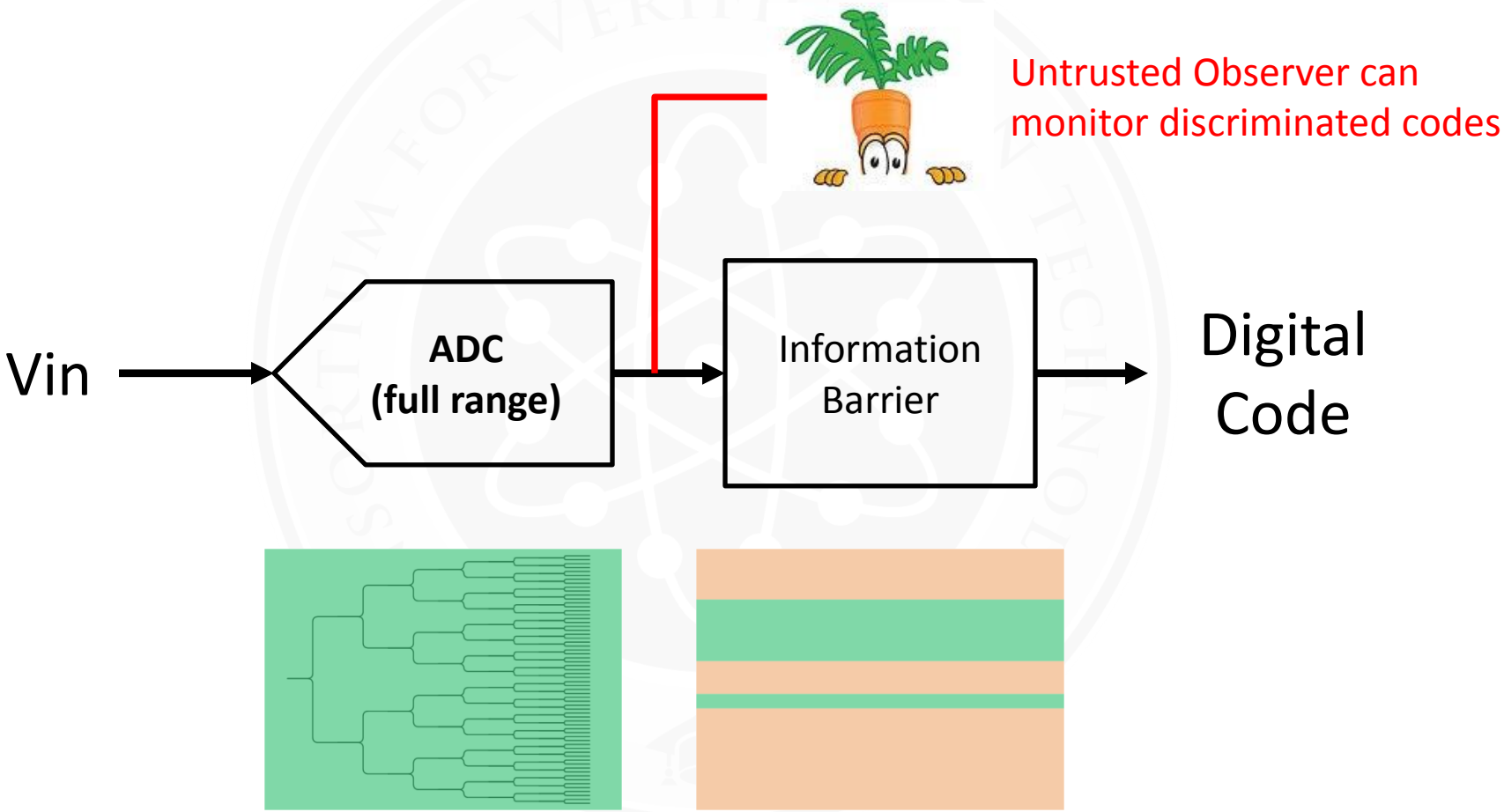
Problem: Only measure specific amplitudes



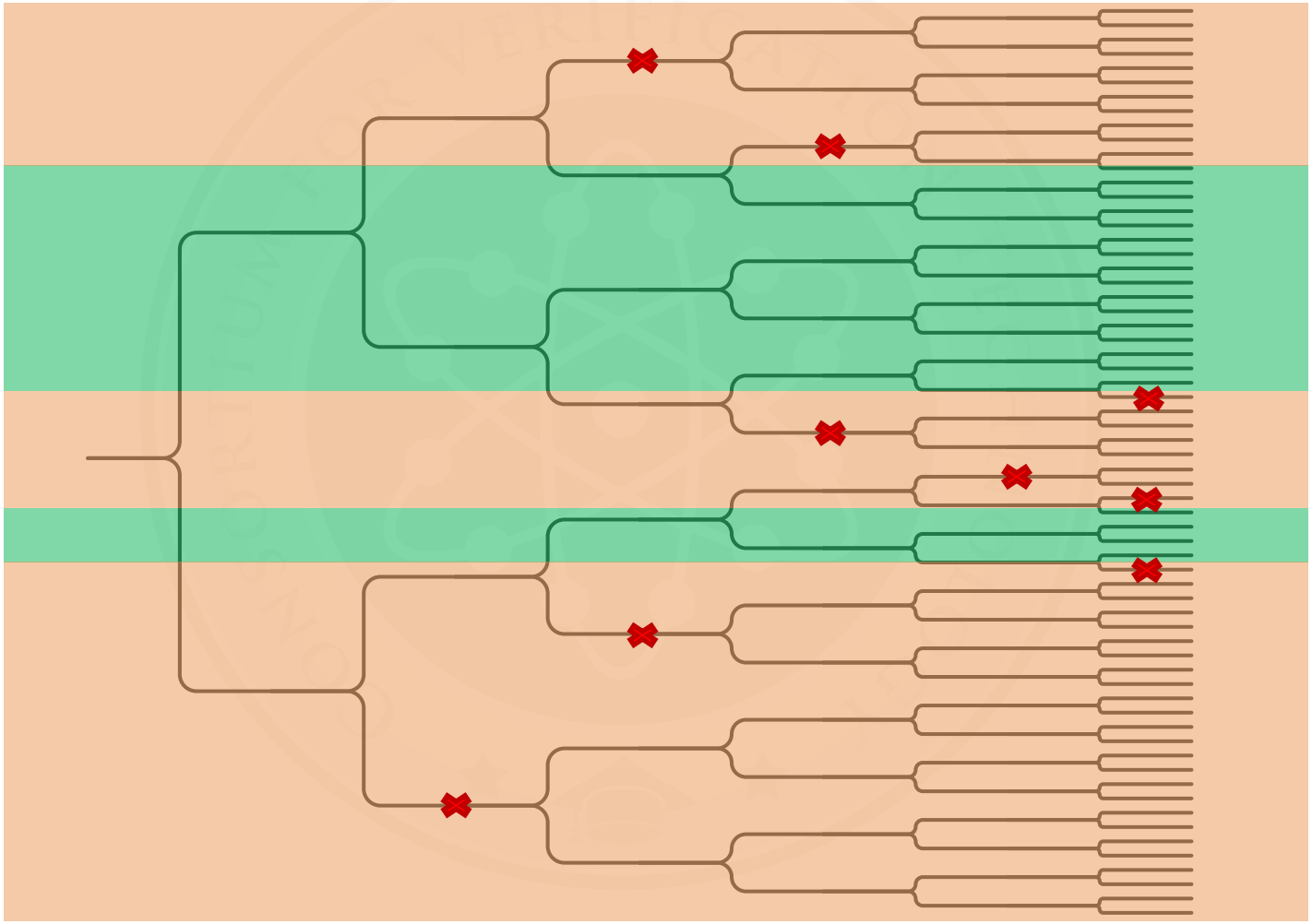
Question: Why not use a full-range ADC, and only report desired amplitudes?



Answer: Discriminated codes can still be obtained



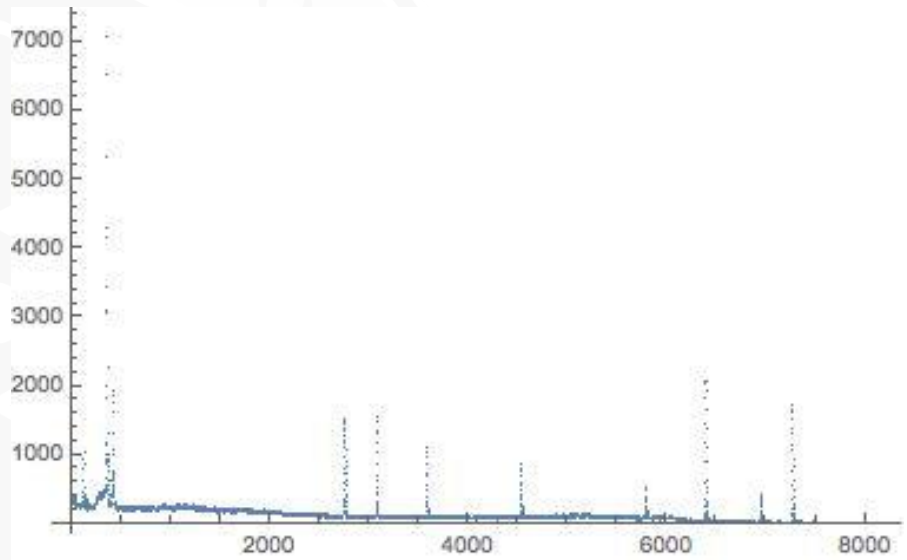
Question: Why not stop ADC when entering an excluded zone, an Interruptible SAR?



Interruptible SAR

Simulate the SAR process

- Set up allowable amplitude ranges to measure
- As amplitude becomes better resolved, if not in allowable amplitude range, terminate process
- Spread event over the known energy interval



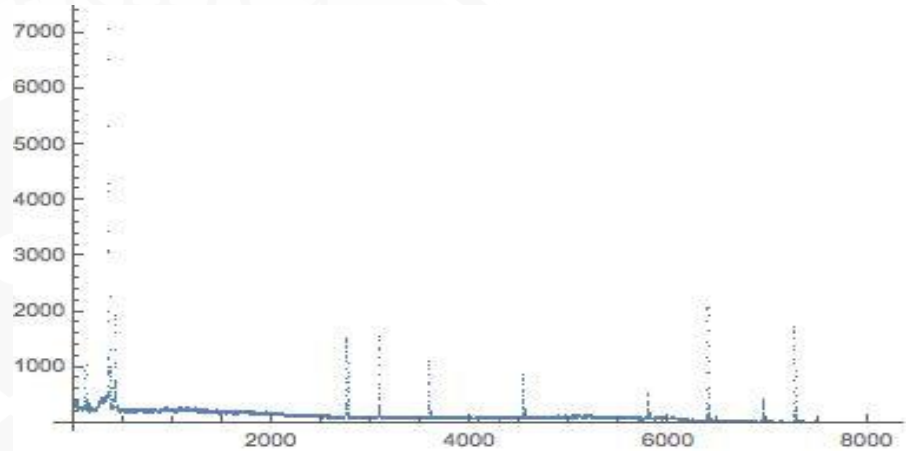
Expect high throughput gains since most events can be quickly discarded

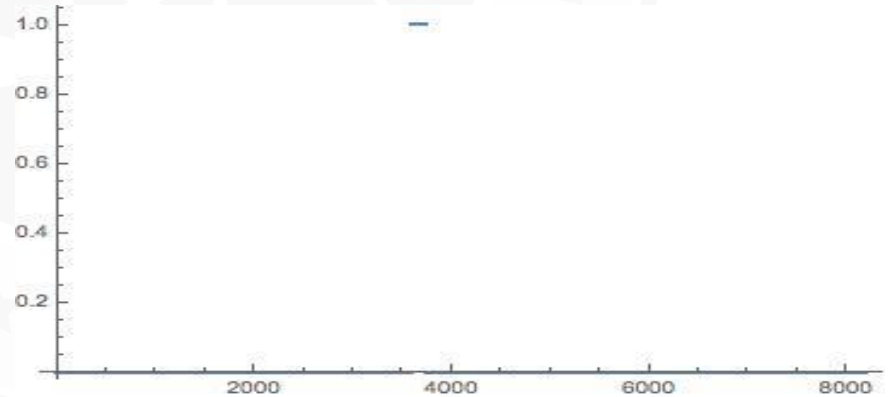
Conserves events. Area and spectral shape are meaningful.

Input Spectrum and Allowable Measurement Windows

Test case:

- Measured spectrum from combined Cs-137, Co-60, Na-22, Bi-207 calibration sources.
- But only Cs-137 allowable.

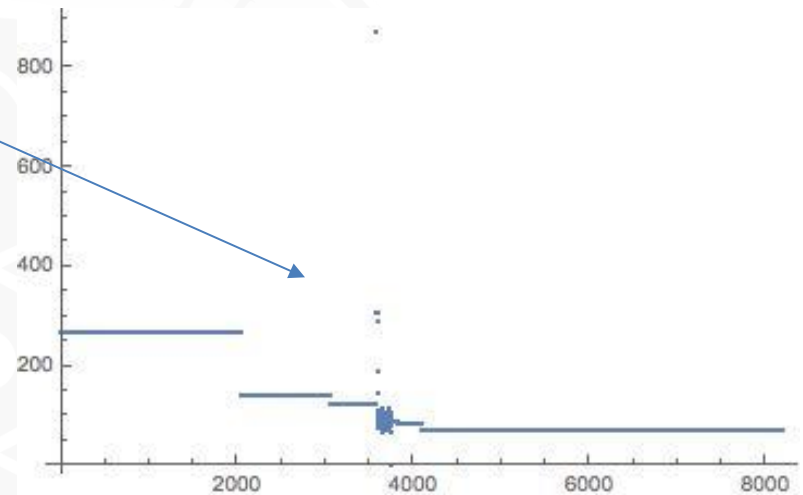


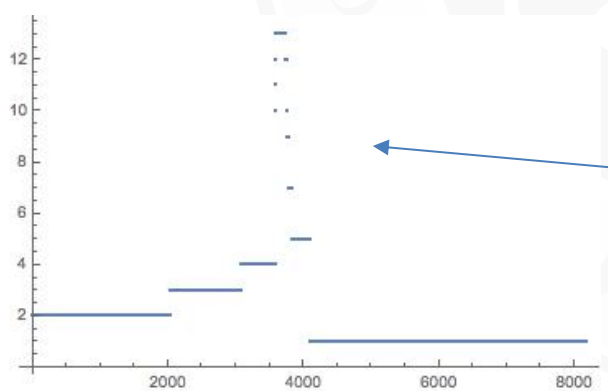


Try 13-bit interruptible SAR ADC

Output Spectrum and Throughput Efficiency

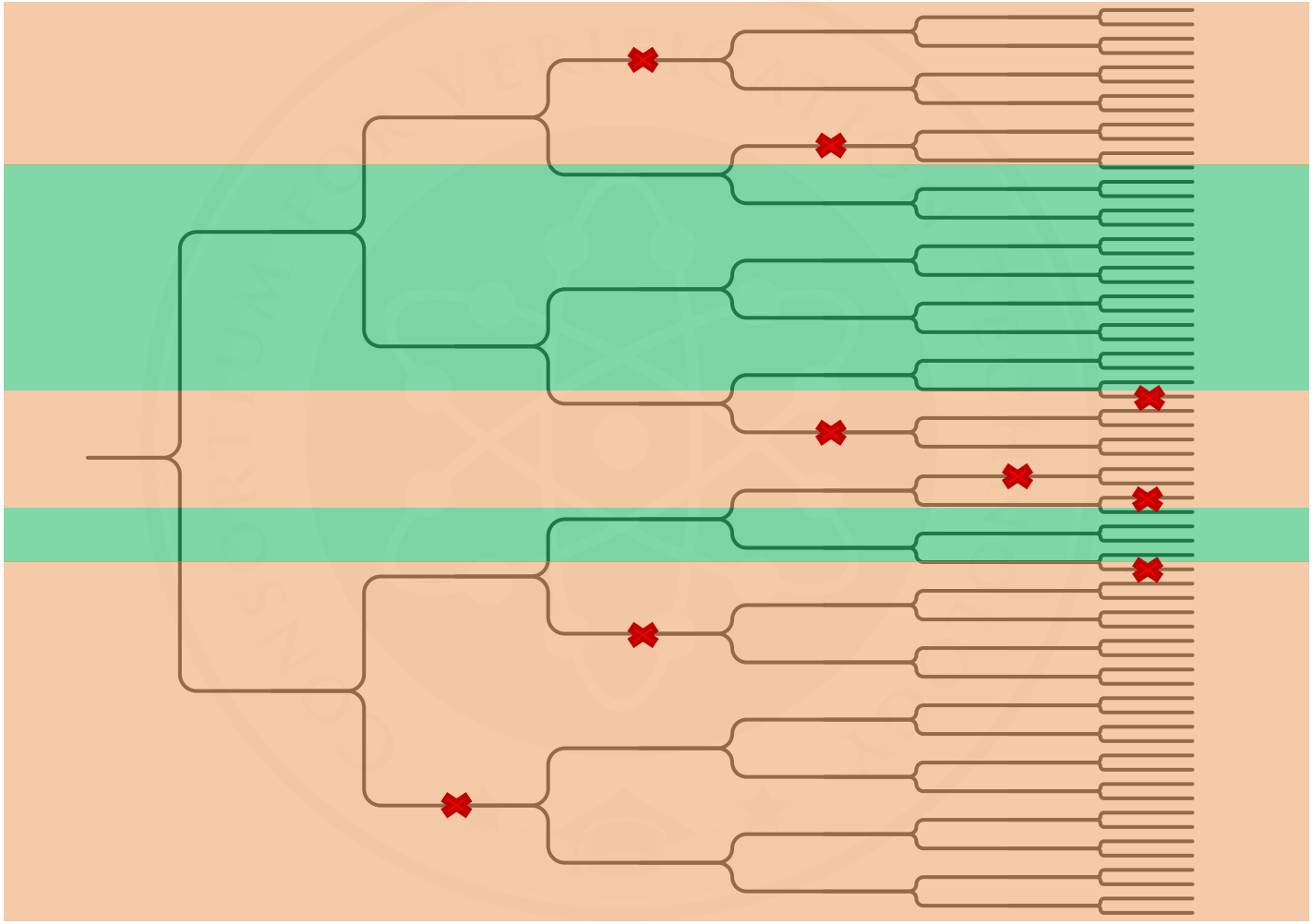
- Output spectrum preserves allowable energy information, spectral shape.
- Other spectral information appears as background
- Counts are preserved.





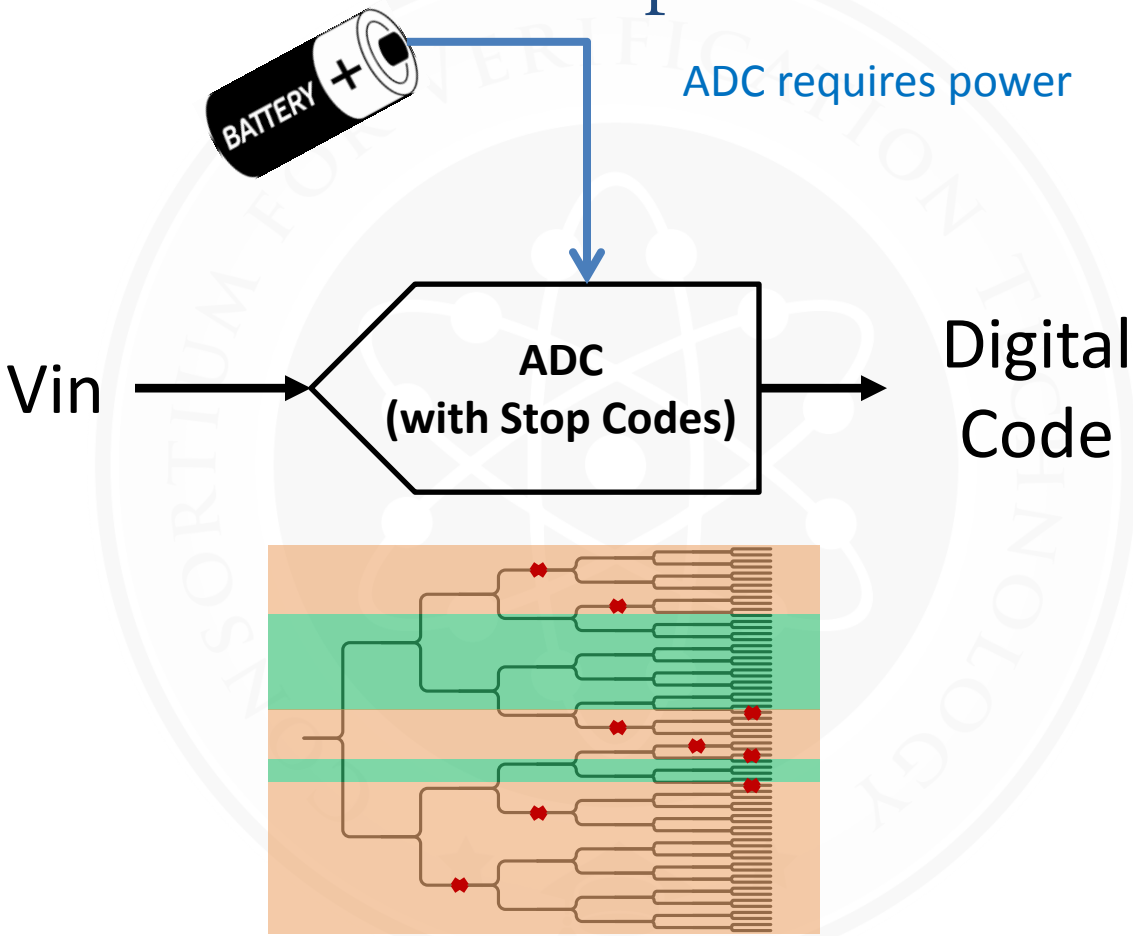
- Process steps as a function of amplitude
- Time saved is 6x.
- Fraction of pulses in allowable energy range is 1.2%

Question: Why not use an Interruptible SAR?



Question: Why not use an Interruptible SAR?

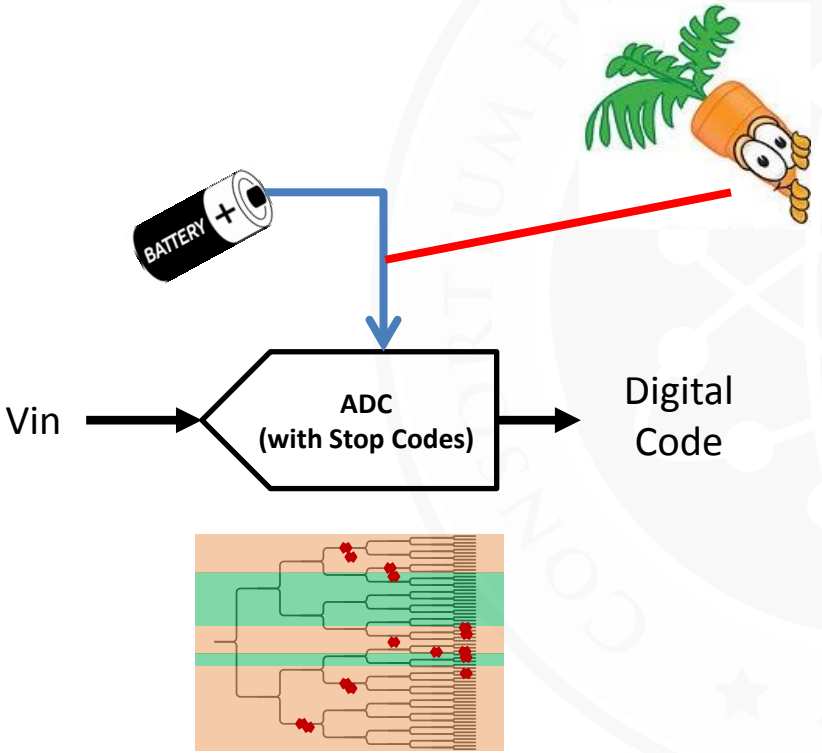
Answer part 1:

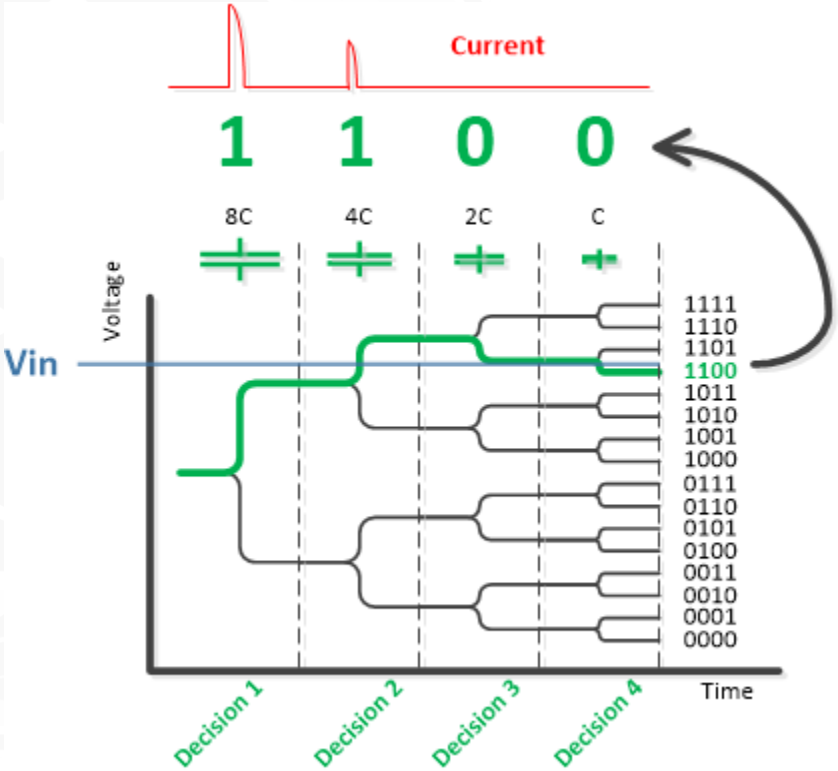


Question: Why not use an Interruptible SAR?

Answer part 2:

- Untrusted Observer can monitor current draw (which is proportional to digital code)
- *Approximate* amplitudes in exclusion zones can be determined with partial codes

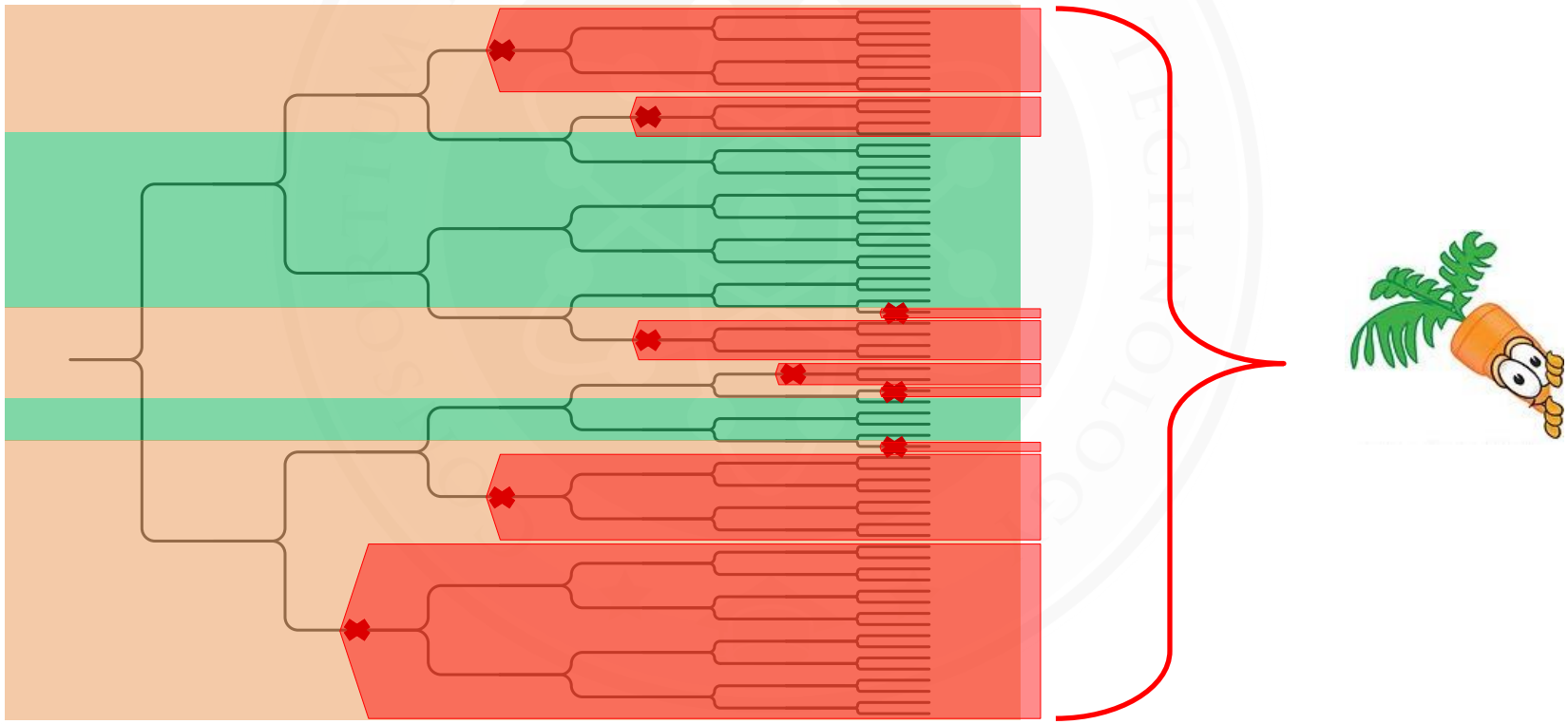




Question: Why not use an Interruptible SAR?

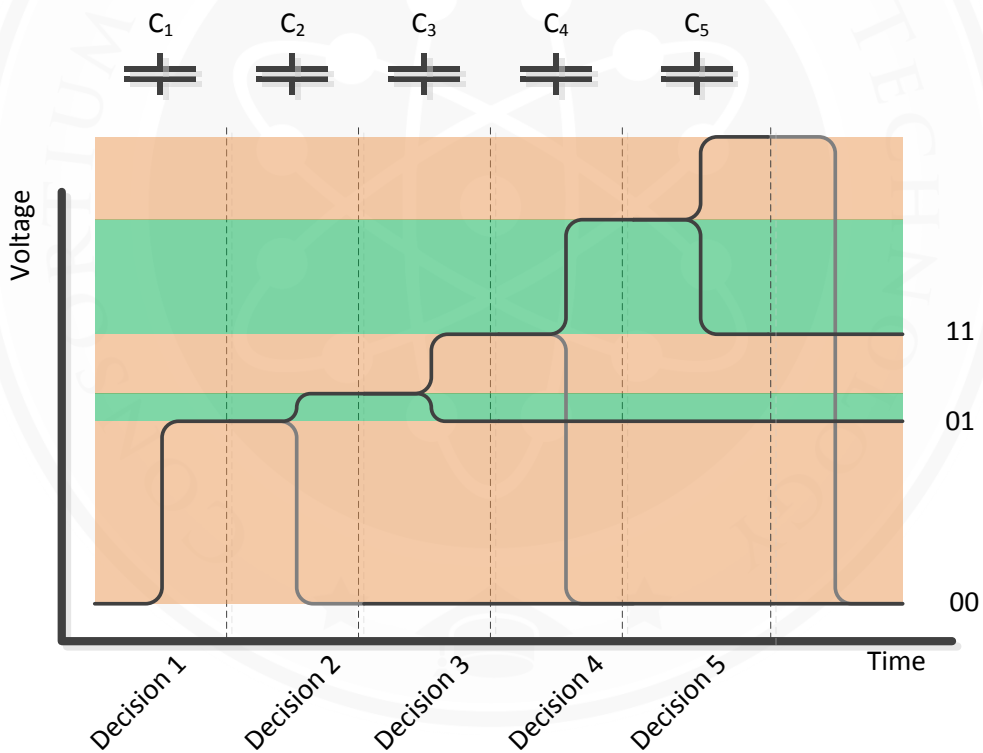
Answer part 2 (visual):

- Untrusted Observer can determine the range of the excluded code, ie: know the code is within one of the dark red decision regions
- Result is a 'lower resolution' code of all values in an exclusion zone.



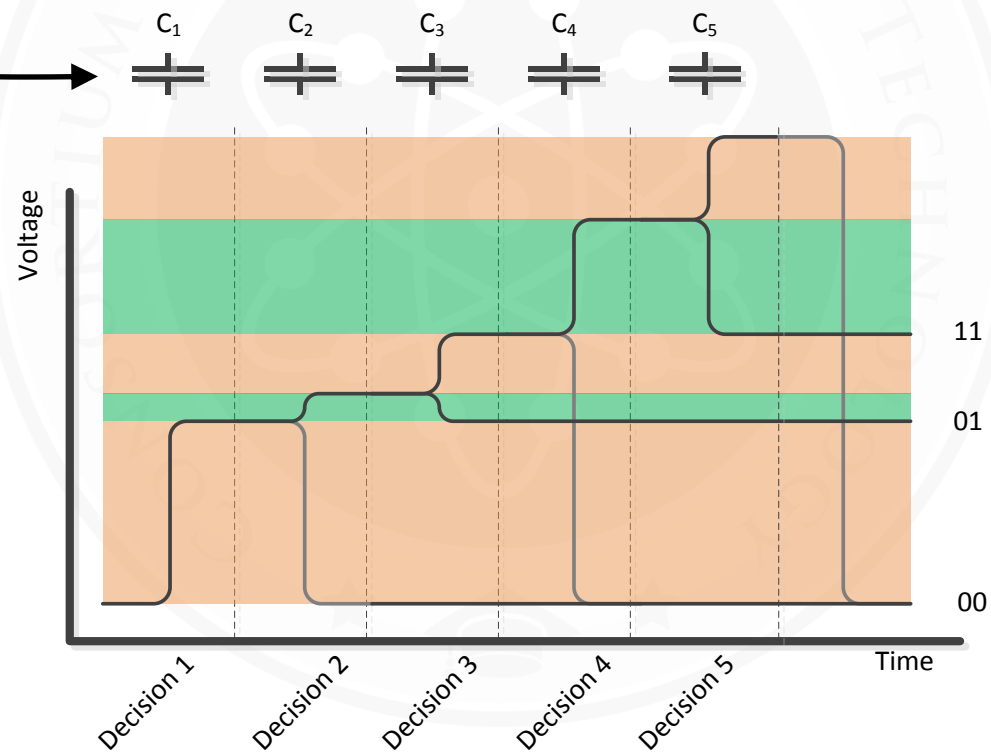
Partial Solution:

1. Make capacitors configurable (non-binary weighted)
2. Only allow codes at window edges
   - Thus not physically possible to have codes in an exclusion zone
3. Only have increasing codes & run all codes regardless of decision
   - Thus current draw is the same for each ADC conversion



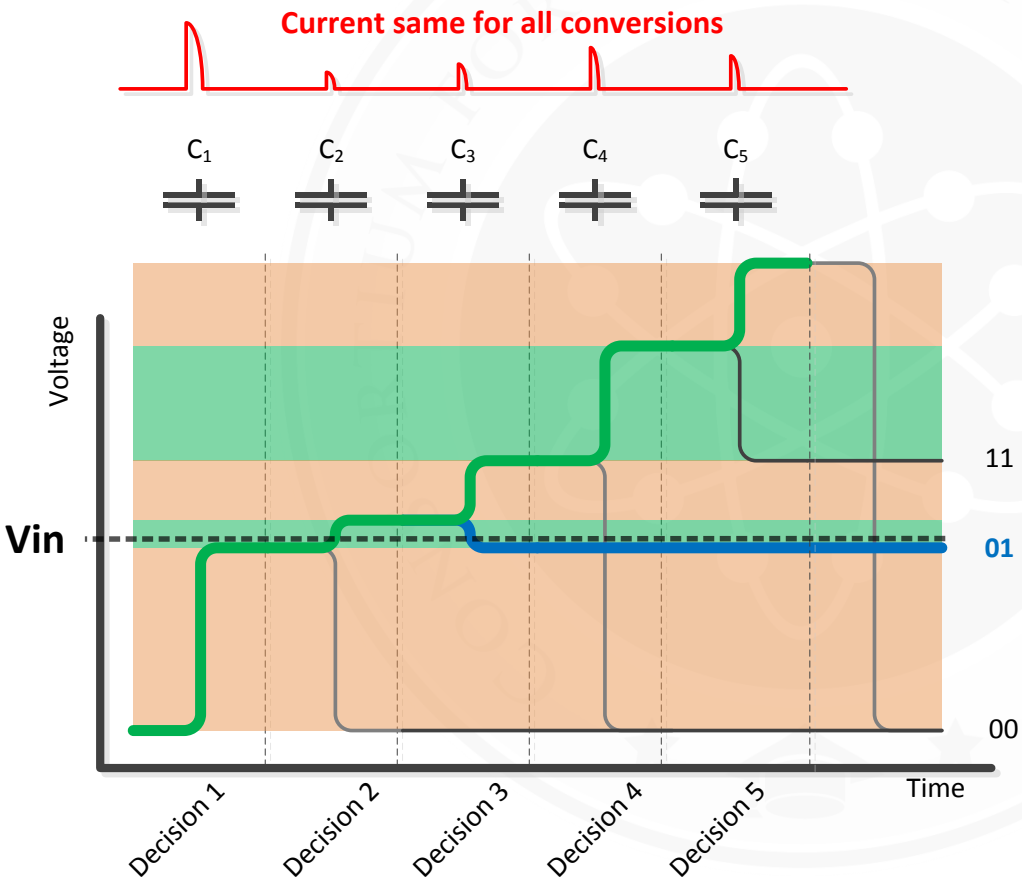
Partial Solution

1. Make capacitors configurable (non-binary weighted)
2. Only allow codes at window edges
   - Thus not possible to have codes in an exclusion zone
3. Only have increasing codes & run all codes regardless of decision
   - Thus current draw is the same for each ADC conversion



Partial Solution

3. Only have increasing codes & run all codes regardless of decision
   - Thus current draw is the same for each ADC conversion

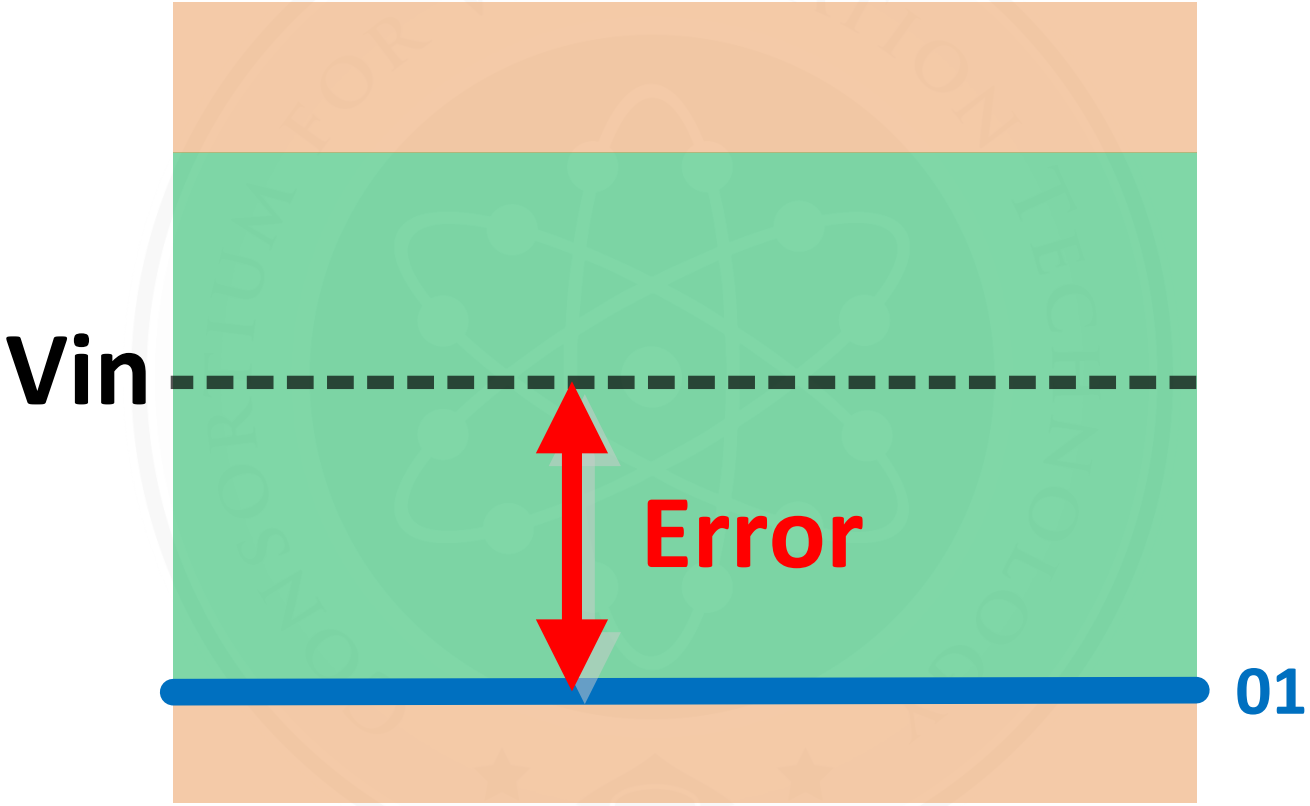


ADC cycles through all codes (green line), even after a decision is made (blue line)

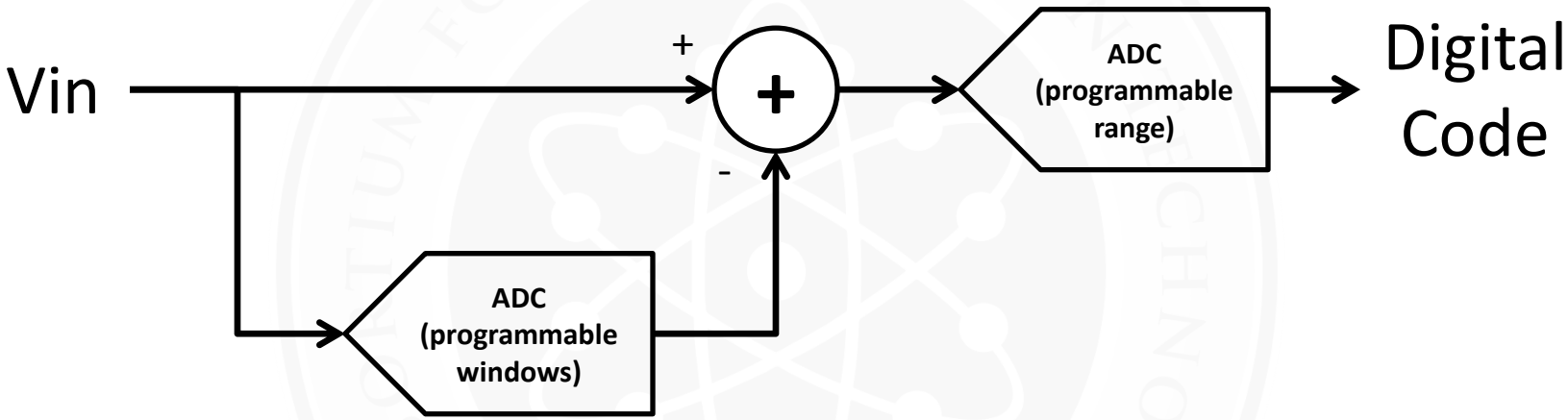
Untrusted observer sees same ADC current (red line) regardless of ADC decision

Cost: Throughput, all comparisons are made (no early exit)

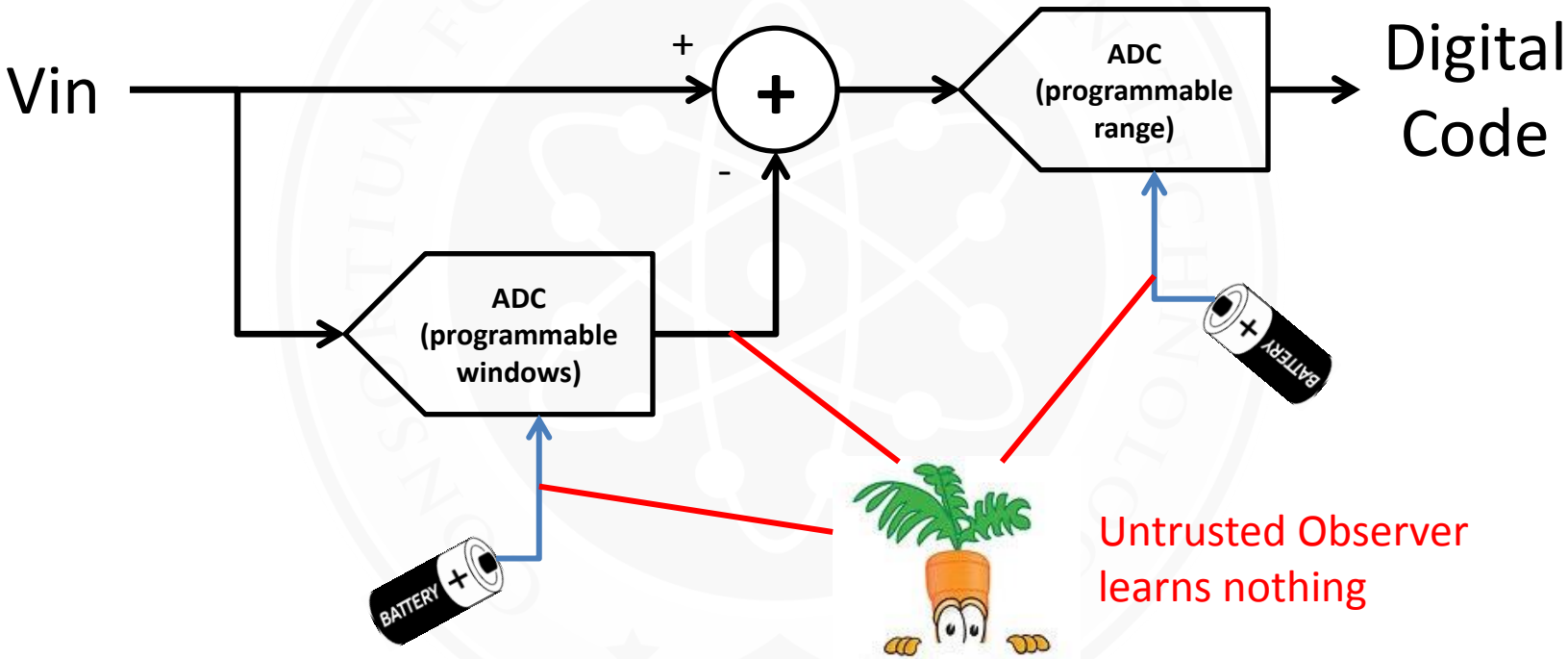
Problems with Partial Solution: Huge Error



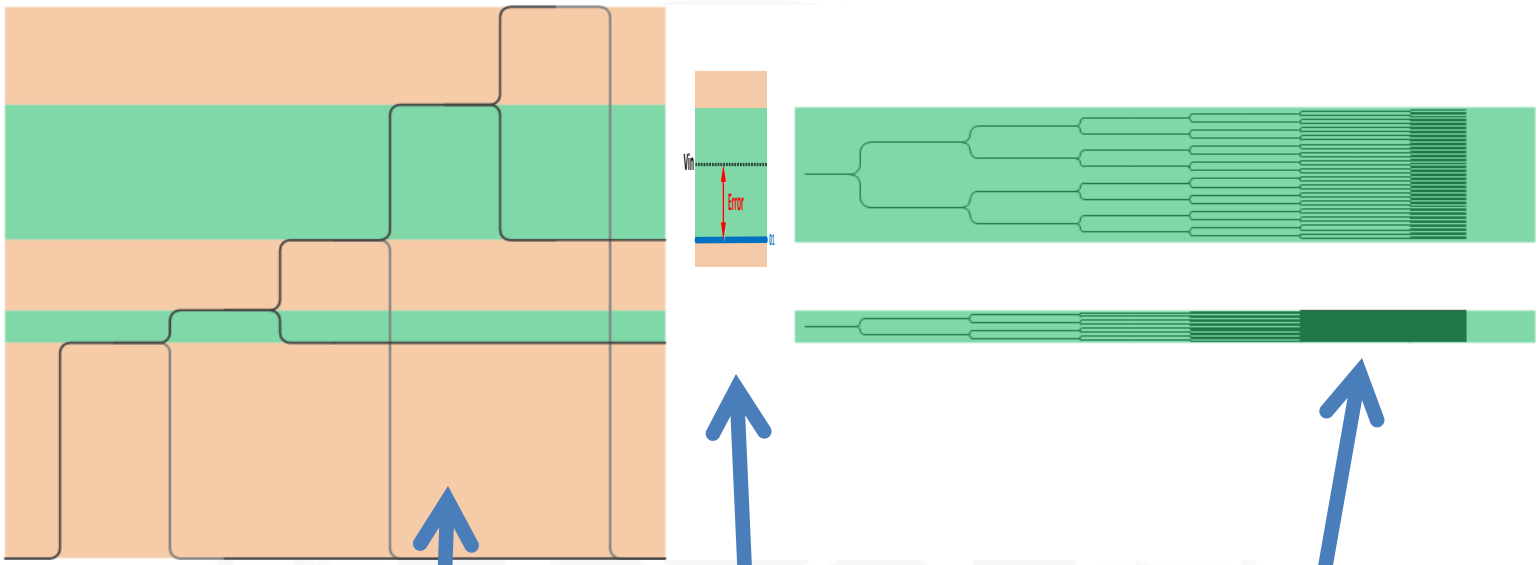
Solution: Send the error to a second stage ADC, set its measurement range to the window size

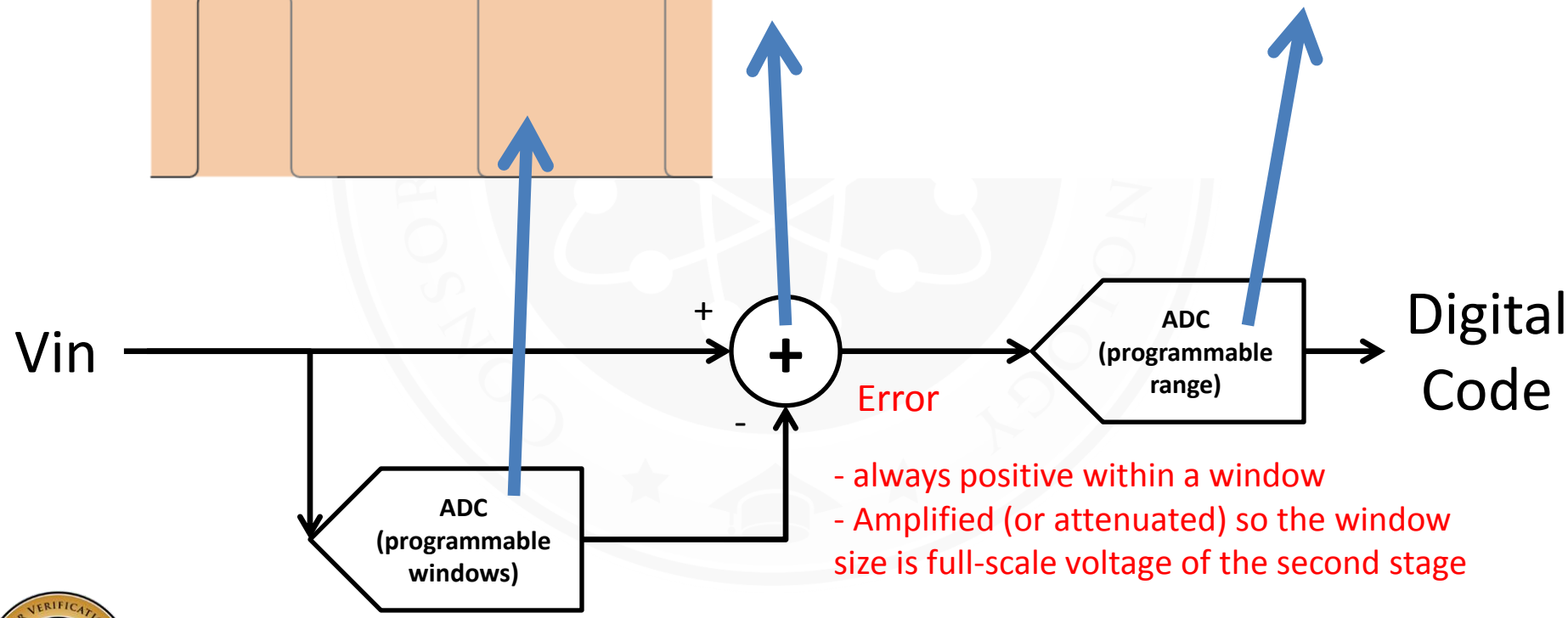


Solution is robust against side attacks from an untrusted observer



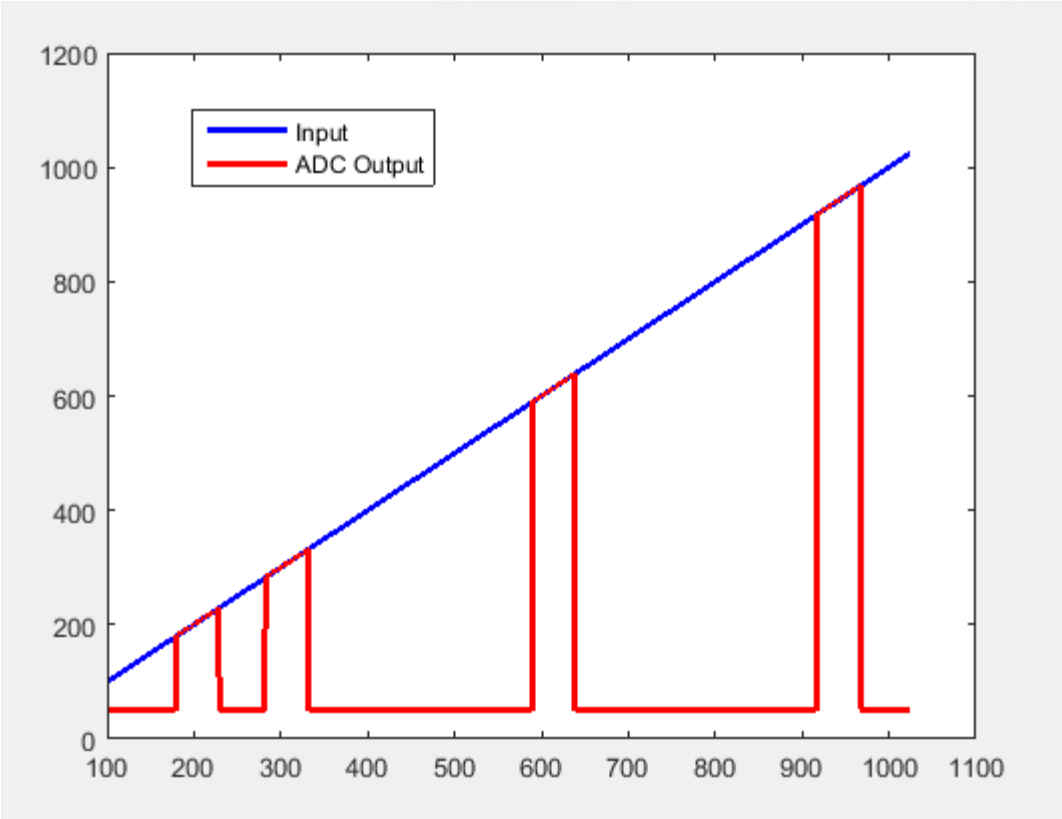
Final decision tree (a visual)





- always positive within a window
- Amplified (or attenuated) so the window size is full-scale voltage of the second stage

Simulation Results

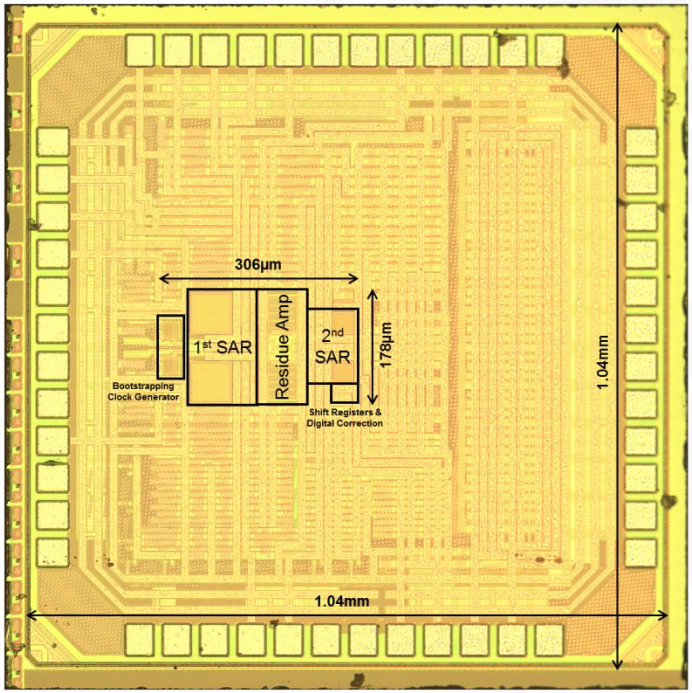


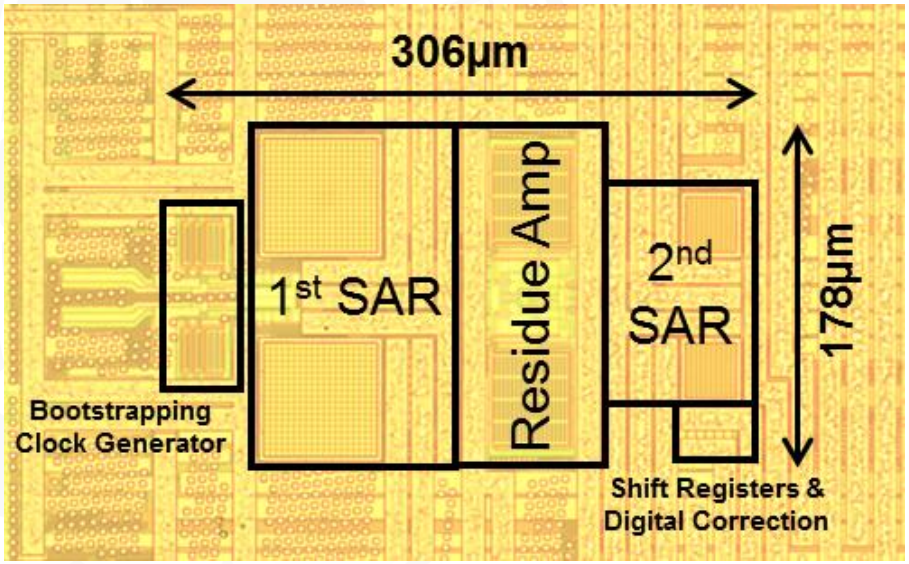
Number, location, and size of windows are programmable

ADC physically can't measure input ranges outside a window

Similar two-stage SAR ADC architecture

- ☺ This is state-of-the art, presented at ISSCC 2015 [Yon Lim, Michael P. Flynn]
- ☹ This design uses binary weights (decisions),
- ☺ We can modify design for programmable decision regions





Questions?