State Considered Harmful: A Discussion Of Stateless Computing And Backdoor Resistance For Calculating One Time Pads

Presented by Void

$(whoami)

- Hobbyist in hardware and general security
- Not professionally trained in anything
- isNeurotic = True
- Fan of QubesOS
  - Qubes Master Signing Key fingerprint:

    427F 11FD 0FAA 4B08 0123 F01C DDFA 1A3E 3687 9494

Context

Cheap Complexity [1]

- Universal Computing + marginal software cost + better fabrication = computers in everything
- We now generally use complex general purpose computers to emulate simple functions
- More complexity = less control of risks = more insecure
- Seriously, go watch Thoma Dullien’s presentation

Why is State Harmful?

- Reused Pads are BAD
- Breaks Information Theoretic Security(ITS)
- Increases users’ chance of getting raided

Hardware Backdoors

Relevant Backdoor Strategies

- Active tampering
  - Weaken security
    - Inject periodic signal weaken randomness
  - Denial of Service
    - Trigger fail safe systems intentionally to stop device functionality

- Data logging
  - Plaintext recovery
    - Raid user and extract data at later convenience

Backdoor Methods

- Replacement of component
- Malicious Modifications
- Embedding malicious components

Replacement

- Replace logic gate/FPGA/CPLD ICs with microcontroller
  - Very feasible as MCUs with fast and highly deterministic peripherals are on market
    - Pi Pico with its PIO peripheral
    - BeagleBone Black with its PRUs
  - If used in data path, can be used for both tampering and logging
  - If used in control path, can be used for tampering

Malicious Modification

- Dopant/transistor level trojans
  - Can be used to trigger malicious or incorrect states during run time [2]
  - POC has been done a long time ago [3]
- Design level tampers:
  - See Illinois Malicious Processor using a shadow cache to trigger malicious code execution [4]
  - Can be used for both tampering and data logging

Embedding Malicious Components

- Hardware trojans:
  - Embedding a sand grain sized microcontroller in the same chip package (black plastic blob) as a jelly bean comparator to log the output of the comparator
  - Embedding a RC oscillator feeding the input of an op amp or a internal high-impedance node of a opamp to inject signals or synchronize external noise/oscillations
  - Embedding a Programmable Metallization Cell [5] at a discrete mosfet’s gate to store if gate has last been switched on or off
  - Can be used for both tampering and data logging

Project Details

What is it?

- A device that can:
  - Generate secure and uniform random data for one time pads
  - Transfer random data securely onto physical media to use as pads
  - Encrypt/Decrypt messages using pads and user input

Threat Model

- Intended users are those who use one time pad with a need for:
  - ITS assurance in data confidentiality
  - High assurance in correctness of encryption/decryption
- Physical device/gadget should do the following:
  - Pad/Plaintext state MUST not be kept after intended wipe of state
  - Prevent leakage due to side channels
  - Prevent tampering of message
- Intended adversaries are nation state actors
- Rubberhose attacks are out of scope

Adversary Capabilities

- Interdict shipping packages with components
- Flood supply chain with counterfeit/backdoored components
- Physically raid user and confiscate device
- Advanced targeted attacks outlined in previous section
- Inflict violence on user

Project Requirements

- Mitigate outlined attacks (do not use ICs or complex chips)
- Can be verified easily without special instruments/tools
- Can be built using diverse but compatible components
- Can use components sourced from diverse sources
- Can be easily assembled/built by user without specialized tools (eg pick and place machine)

Mitigation Strategies

General Mitigation Guidelines

- REDUCE COMPLEXITY
- REDUCE RELIANCE ON PRECISION OR SPECIALIZED COMPONENTS
- Do not use integrated circuits
  - Includes analog chip like opamps and comparators
- Use a 2 layer board that can be inspected visually
- Physically build logic gates

Leakage and Sidechannels

- Mitigate side channels
  - Filter power supply/use shunt regulators
  - Use grounded shielding/enclosure to circuit
  - Use non-ceramic capacitors to avoid acoustic leakage/(injection?)
  - Use reflective/insulated enclosure to prevent thermal leakage

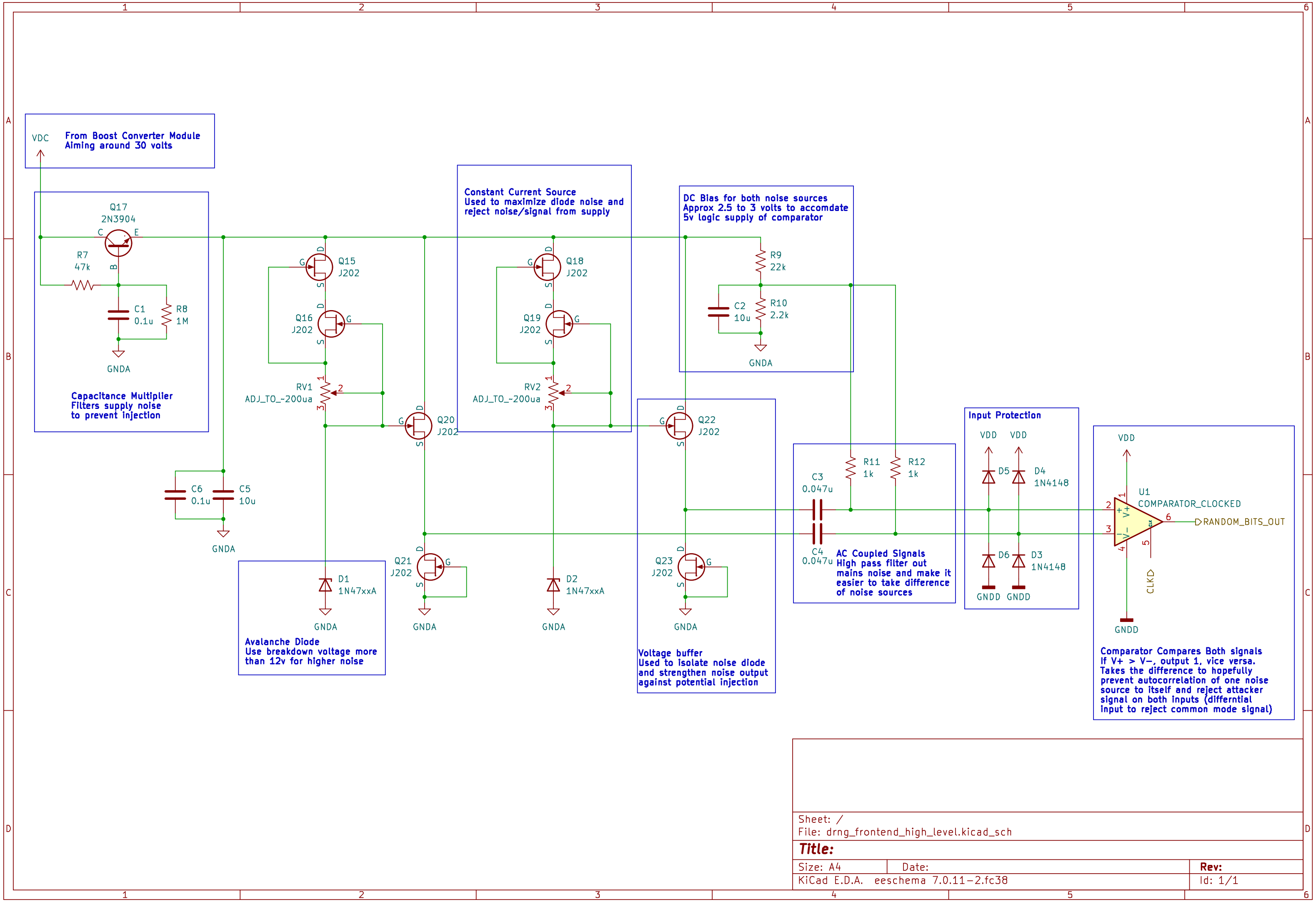
Design for Untrustworthiness

- Use side channel/injection resistant digital/analog implementations
  - Active tampering/signal injection resistant architectures
  - Schmitt trigger constructions for resistance against noise and dopant level trojans?
  - ECL logic for resistance against power analysis and current noise emissions
  - Use differential inputs for analog signals to cancel out inteference
  - Signal/source isolation through buffers/optocouplers
- Have a jig to test your individual components

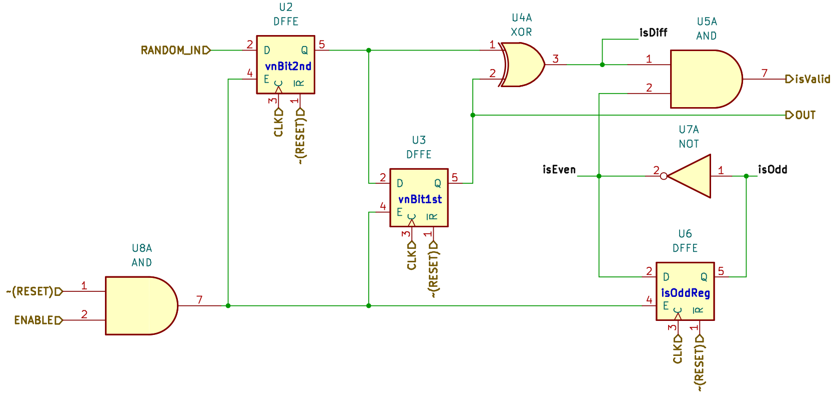
Design and Implementation

Updates:

- Implementation not completely done
- Not going with previous analog solution due to comparators being able to be backdoored
- Hardest challenges not solved yet:
  - Transfer of data onto physical pads
  - Overall device construction
  - Physical gate construction details and logic family to use



VDC
From Boost Converter Module
Aiming around 30 volts
Q17
2N3904
R7
47k
C1
0.1u
R8
1M
GNDA
Capacitance Multiplier
Filters supply noise
to prevent injection
Q15
J202
Q16
J202
RV1
ADJ_TO_~200ua
Q20
J202
C6
0.1u
C5
10u
D1
1N47xxA
Avalanche Diode
Use breakdown voltage more
than 12v for higher noise
Q21
J202
Constant Current Source
Used to maximize diode noise and
reject noise/signal from supply
Q18
J202
Q19
J202
RV2
ADJ_TO_~200ua
D2
1N47xxA
DC Bias for both noise sources
Approx 2.5 to 3 volts to accomdate
5v logic supply of comparator
R9
22k
C2
10u
R10
2.2k
Q22
J202
Q23
J202
Voltage buffer
Used to isolate noise diode
and strengthen noise output
against potential injection
C3
0.047u
C4
0.047u
R11
1k
R12
1k
AC Coupled Signals
High pass filter out
mains noise and make it
easier to take difference
of noise sources
Input Protection
VDD
D5
D4
1N4148
D6
D3
1N4148
GNDD
U1
COMPARATOR_CLOCKED
RANDOM_BITS_OUT
CLK
Comparator Compares Both signals
If V+ > V−, output 1, vice versa.
Takes the difference to hopefully
prevent autocorrelation of one noise
source to itself and reject attacker
signal on both inputs (differntial
input to reject common mode signal)
Sheet: /
File: drng_frontend_high_level.kicad_sch
Title:
Size: A4
Date:
Rev:
KiCad E.D.A. eeschema 7.0.11-2.fc38
Id: 1/1



Sheet: /

File: vn_logic.kicad_sch

Title:

Size: A4 | Date: | **Rev:**

KiCad E.D.A. eeschema 7.0.11-2.fc38 | Id: 1/1

References

1) https://www.infosecurity.us/blog/2018/6/17/cycon-2018-thomas-dulliens-security-moores-law-and-the-anomaly-of-cheap-complexity

2) https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/

3) https://eprint.iacr.org/2014/508.pdf

4) https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf

5) https://en.wikipedia.org/wiki/Programmable_metallization_cell