Cold Boot Attack

Lucas S., Alex J., Mike S. und
Benjamin B.

Gliederung

1. Grundidee
    1. Grundlagen
    2. Konzept
2. Versuchsaufbau
3. Durchführung
4. Erwartungen
5. Ergebnisse
6. Schwierigkeiten

Grundidee

- Experiment basiert auf einem Experiment aus Princeton
- Sensible Daten zur Laufzeit im RAM gehalten
- RAM ist flüchtiger Speicher (ohne Strom entladen)
- Tatsächlich: RAM verliert exponentiell Daten über Zeit (üblich 1-30 Sekunden)
- Theorie: Das Entladen kann signifikant verzögert werden durch hohen Abfall der Temperatur

Konzept

- Kühlung in laufendem Betrieb
  - Durch Kältespray auf ca. -40°C
- RAM unmittelbar danach entfernen
- Kühl halten durch Lagerung in flüssigem Stickstoff (zwischen -196°C und -210°C)
- Auslesen sensibler Daten
- Fehlerkorrektur

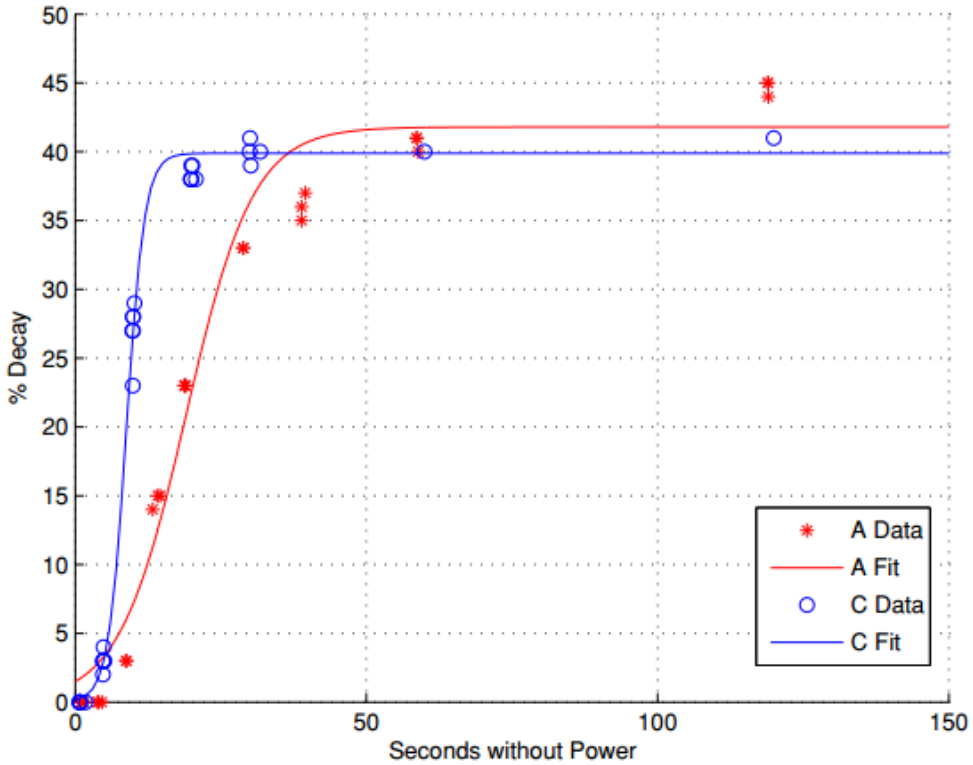
Versuchsaufbau

- Hardware
  - Desktop-PC:
    - 1024 MB DDR1-Speicher
    - Xubuntu 16.04 32-Bit
  - USB-Stick bootfähig mit RAM-Dumper
  - Kältespray (-40°C und rückstandsfrei)
  - Flüssiger Stickstoff (Danke an Herrn Misch aus der Physik)
  - Laptop mit Ubuntu 16.04
    - RAM-Dump auslesen mit dd
    - Suche nach kritischen Daten durch ein Python-Skript (selbst entwickelt)

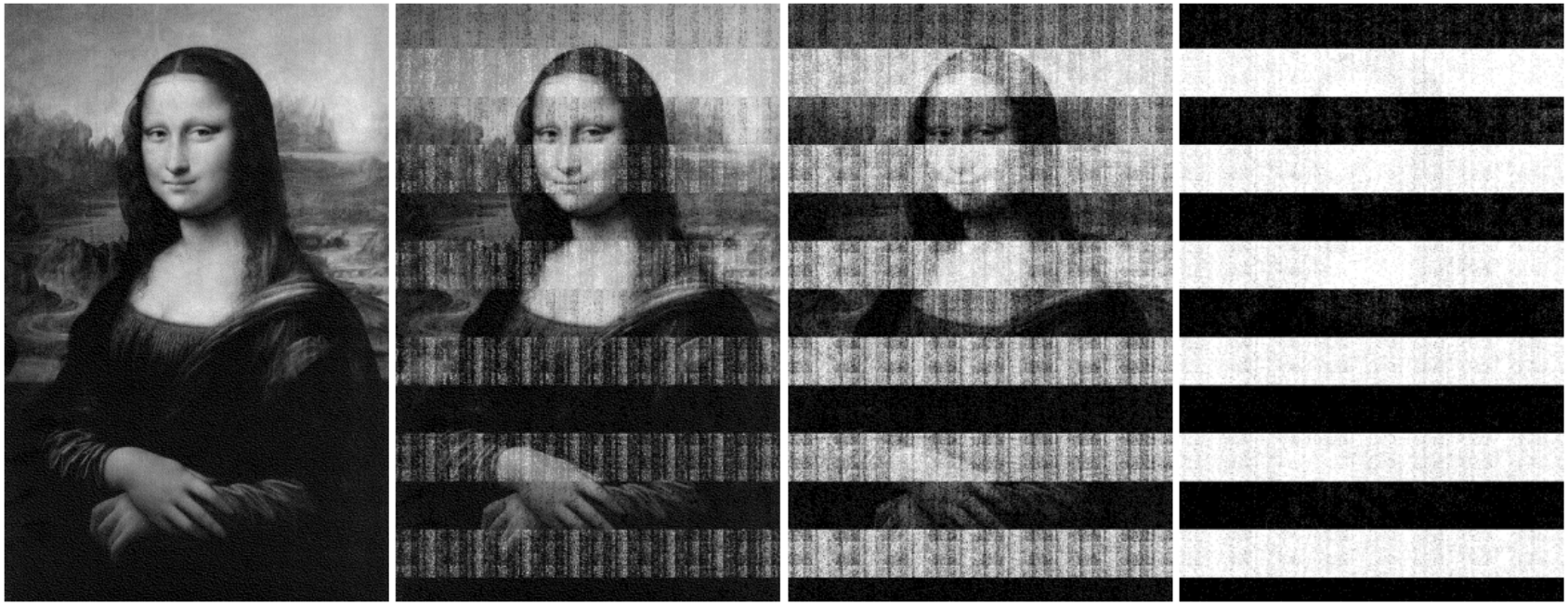
Durchführung

- Im Betrieb Bild in den Speicher laden (4-mal aus Redundanzgründen)
- Speicher durch Kältespray großflächig kühlen
- Strom entfernen
- RAM ausbauen und in den flüssigen Stickstoff überführen
- Warten…
- Arbeitsspeicher in Rechner einbauen
- Booten mit RAM-Dump
- Speicher-Stick durch anderen Rechner auslesen
- Daten auswerten

Erwartungen



Erwartungen



Ergebnisse

Ohne Kühlung

Original Reset 2s 4s 6s

Ergebnisse

Mit Kältespray

Original 5s 10s 30s

Ergebnisse

Mit Stickstoff gekühlt

Original

ca. 5min

ca. 10min

Schwierigkeiten

- Daten in den RAM schreiben
- RAM auslesen
- Einige Rechner flushen beim booten den RAM
- Große Objekte werden verteilt im RAM abgelegt
- ECC-Speicher funktioniert nicht