Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

VORONOI BASED N-DIMENSIONAL PARAMETER OPTIMIZATION FOR FAULT INJECTION ATTACKS

FDTC2023

Conference Center Prag, Czech Republic
10.09.2023

{marius.eggert|marc.stoettinger}@hs-rm.de

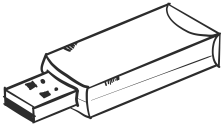
MOTIVATION

→ Evidence from digital electronic devices is becoming increasingly important in court

→ More and more devices implement various security mechanisms to protect user data

→ Security mechanisms must be bypassed to obtain data from victims or perpetrators

→ Besides software exploits, various hardware attacks exist
  - → invasive - e.g. Microprobing
  - → semi-invasive - e.g. Laser Fault Injection
  - → non-invasive - e.g. Voltage Glitching



Based on Image by rocket pixel on Freepik

PARAMETER OPTIMIZATION CHALLENGES

→ Non-invasive attacks use laboratory equipment to manipulate the target's environment

→ Semi-invasive attacks also modify equipment parameters but require package removal

→ Advanced attacks on modern hardware require multiple devices

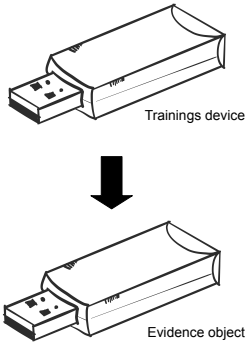
→ Professional devices further increase parameter granularity

Problem

Brute force iteration of all parameter combinations not feasible!

SPECIFIC CHALLENGES FOR LAW ENFORCEMENT

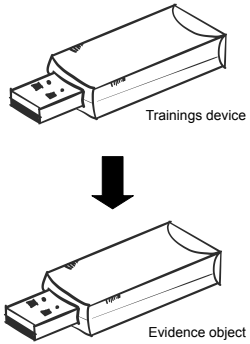
→ Data corruption and data loss are to be avoided at all cost
- → Intensive tests on comparison device
- → The attack must work across devices
- → Attack should at best be successful on the first try



Based on Image by rocket pixel on Freepik

SPECIFIC CHALLENGES FOR LAW ENFORCEMENT

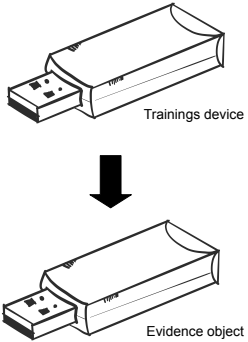
- → Data corruption and data loss are to be avoided at all cost
  - → Intensive tests on comparison device
  - → The attack must work across devices
  - → Attack should at best be successful on the first try
- → Seldom access to intellectual property of the device vendors
  - → Typically black-box scenarios
  - → Missing documentation of the device and its chips
  - → No insight about countermeasures
  - → Unknown typical operating conditions



Based on Image by rocket pixel on Freepik

SPECIFIC CHALLENGES FOR LAW ENFORCEMENT

- → Data corruption and data loss are to be avoided at all cost
  - → Intensive tests on comparison device
  - → The attack must work across devices
  - → Attack should at best be successful on the first try
- → Seldom access to intellectual property of the device vendors
  - → Typically black-box scenarios
  - → Missing documentation of the device and its chips
  - → No insight about countermeasures
  - → Unknown typical operating conditions

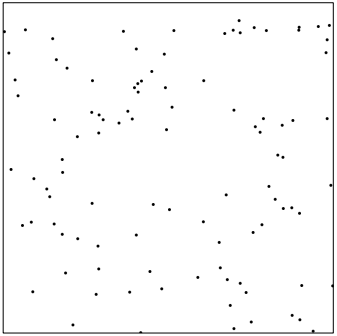


Based on Image by rocket pixel on Freepik

Challenge

We need to find the overall most reliable parameter combination across devices not only just one that worked once!

VORONOI TESSELLATION



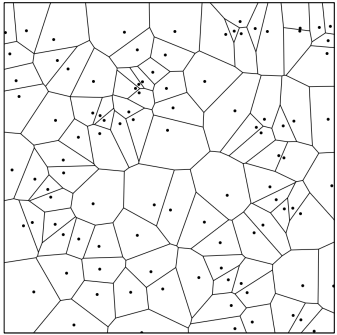
VORONOI TESSELLATION

→ Voronoi tessellation partitions a (multidimensional) space into cells

→ Each cell surrounds one input point

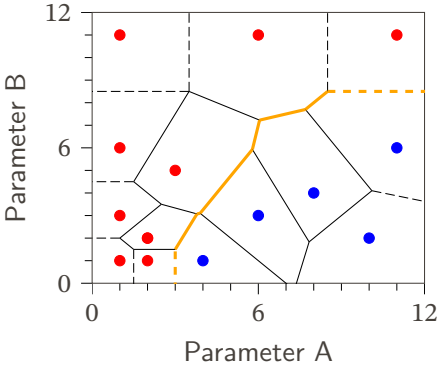
→ All coordinates that are closer to a cells point than to all other points are contained

→ Cells are separated by lines, even in high dimensions



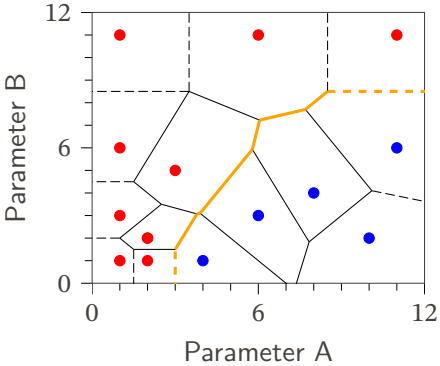
VORONOI TESSELLATION FOR POINT OF INTEREST DETERMINATION

→ Can be used for optimization during fault injection attacks
  - → Results define input points
  - → Edges define border between results
  - → Borders between result classes define polytope of interest



VORONOI TESSELLATION FOR POINT OF INTEREST DETERMINATION

- → Can be used for optimization during fault injection attacks
  - → Results define input points
  - → Edges define border between results
  - → Borders between result classes define polytope of interest
- → Result improves with each point added
- → Identifies successful parameters between classes
- → Creates a cartography of the parameter space

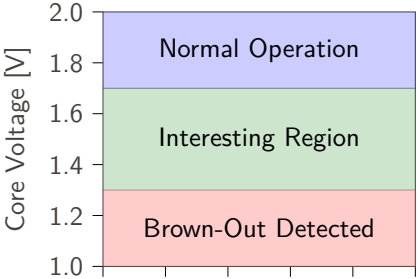


MAPPING OPTIONS

→ Failures are more time consuming

→ Some setups require long restart times

→ Tests leading to failures should be avoided



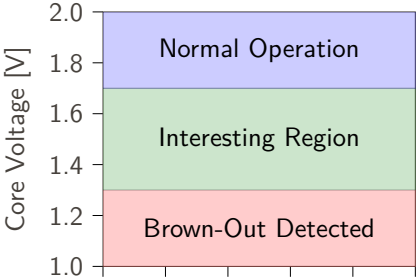
MAPPING OPTIONS

→ Failures are more time consuming

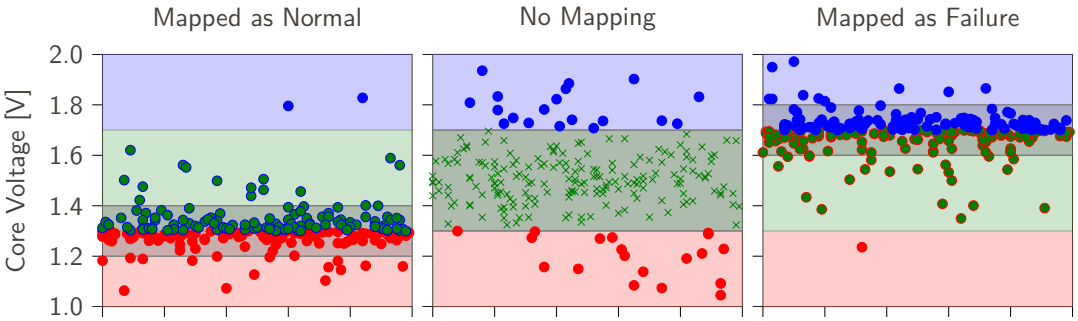
→ Some setups require long restart times

→ Tests leading to failures should be avoided

→ We can shift the polytope of interest by interpreting successful results as failures.



2D MAPPING OPTIONS VISUALIZATION

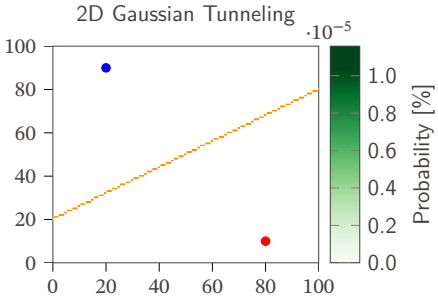


GAUSSIAN TUNNELING

→ Voronoi tessellation provides edges

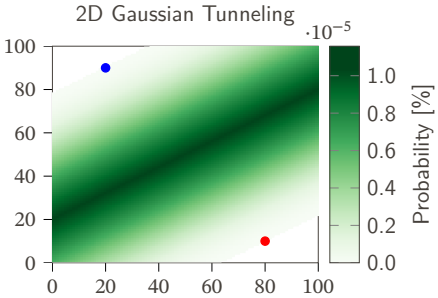
→ Edges are considered the most interesting parameter combinations

→ The global maximum can still be next to the edge

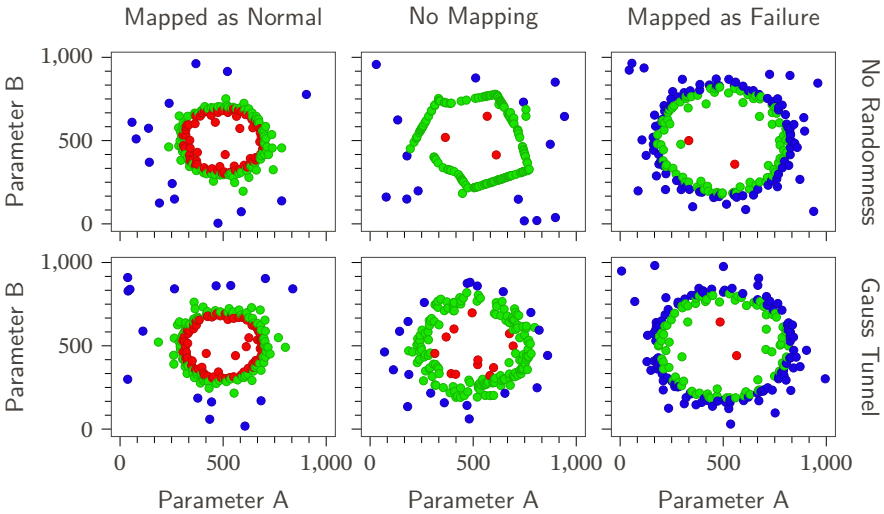


GAUSSIAN TUNNELING

- → Voronoi tessellation provides edges
- → Edges are considered the most interesting parameter combinations
- → The global maximum can still be next to the edge
- → We can perform only one test at a time
  - → Exploration space expansion through Gaussian tunneling
  - → Speedup through randomized edge point selection



MAPPING AND TUNNELING SIMULATION



SIMULATION SETUP

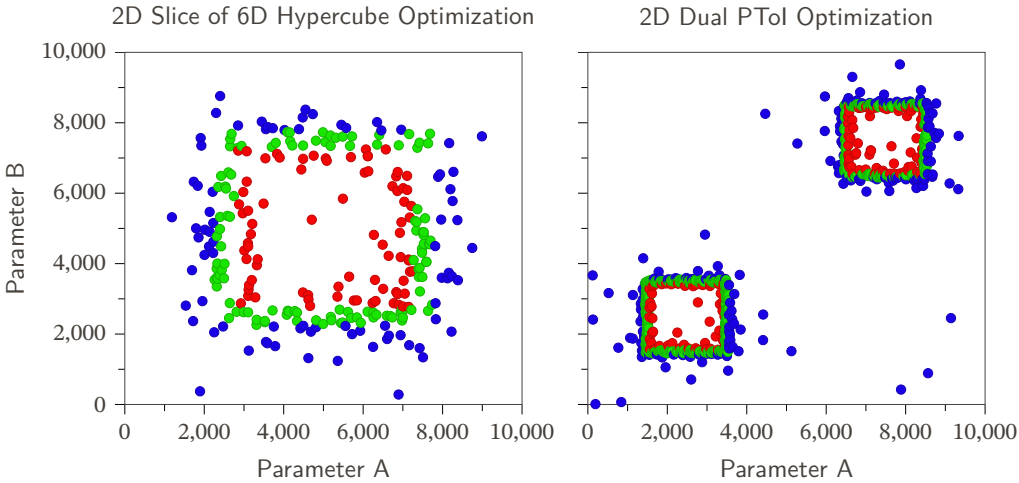
→ Simulations uses hypercubic result space

→ Each dimension is a uniformly distributed parameter
  - → 45% of the center defined as failure
  - → next 10% defined as success
  - → everything else defined as normal

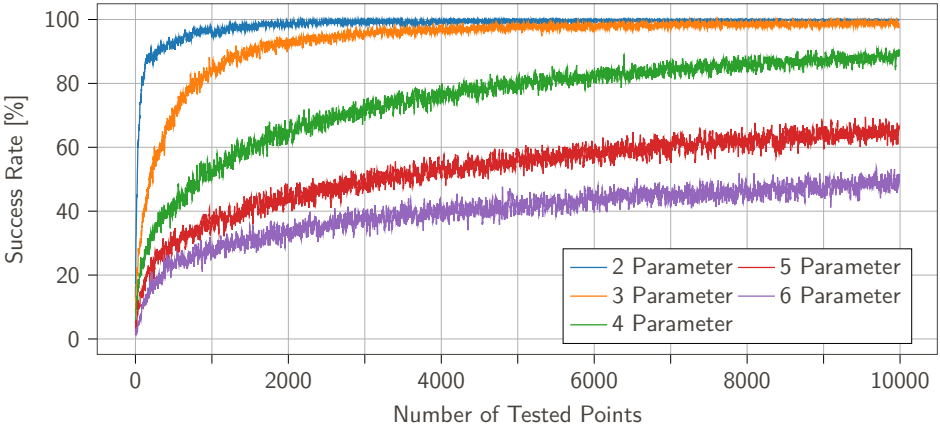
→ Pro: Constant possibility for successful outcomes per dimension

→ Con: Volumetric percentage for successes decreases per dimension
(2D: 10%, 3D: 7.5%, 4D: 5%, 5D: 3.2%, 6D: 1.9%, ...)

6D AND DUAL PTOI SIMULATION RESULTS



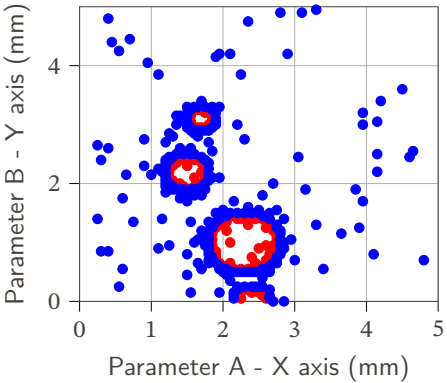
SUCCESS RATE EVALUATION



SPATIAL OPTIMIZATION EXPERIMENT SIMULATION

→ Spatial parameters seldom contain successes between failure and normal regions

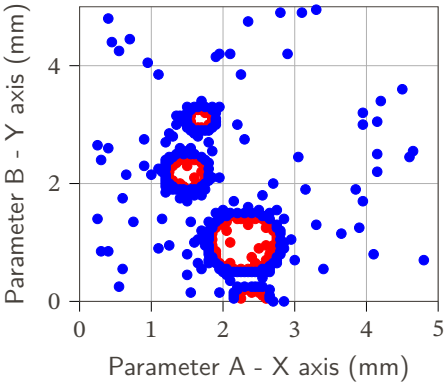
→ To evaluate spatial parameters we simulated the scenario from Rais-Ali et. al[1]



[1] I. Rais-Ali, A. Bouvet, and S. Guilley, "Quantifying the speed-up offered by genetic algorithms during fault injection cartographies," in 2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC), 2022, pp. 61–72.

SPATIAL OPTIMIZATION EXPERIMENT SIMULATION

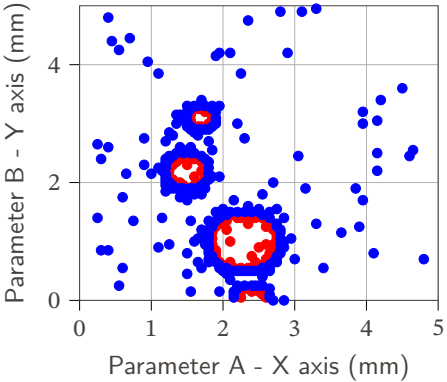
- → Spatial parameters seldom contain successes between failure and normal regions
- → To evaluate spatial parameters we simulated the scenario from Rais-Ali et. al[1]
- → Our method successfully identified all regions
- → Currently no exploration of the failure regions



[1] I. Rais-Ali, A. Bouvet, and S. Guilley, "Quantifying the speed-up offered by genetic algorithms during fault injection cartographies," in 2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC), 2022, pp. 61–72.

SPATIAL OPTIMIZATION EXPERIMENT SIMULATION

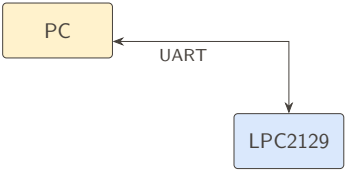
- → Spatial parameters seldom contain successes between failure and normal regions
- → To evaluate spatial parameters we simulated the scenario from Rais-Ali et. al[1]
- → Our method successfully identified all regions
- → Currently no exploration of the failure regions
- → Idea: Test edges between failures after a certain point limit



[1] I. Rais-Ali, A. Bouvet, and S. Guilley, "Quantifying the speed-up offered by genetic algorithms during fault injection cartographies," in 2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC), 2022, pp. 61–72.

EXPERIMENTAL RESULTS

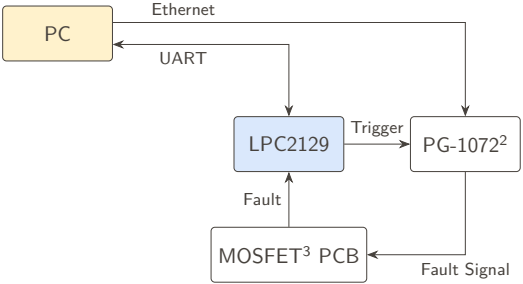
→ Target: LPC2129[1]
  → Implements simple counting loop
  → Commands and results sent over UART
  → GPIO indicates operation start



[1] https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc2000-arm7:MC_71580#/

EXPERIMENTAL RESULTS

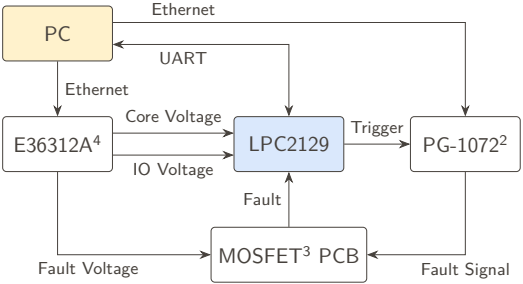
- → Target: LPC2129[1]
  - → Implements simple counting loop
  - → Commands and results sent over UART
  - → GPIO indicates operation start
- → Attack: Voltage glitching
  - → Adjustable core, I/O and fault voltage
  - → Variable fault width and delay
  - → Counting errors are interpreted as success



[1] https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc2000-arm7:MC_71580#/
[2] https://www.activetechnologies.it/pulse_rider_pg-1072_pg1074_revb/
[3] https://www.infineon.com/cms/en/product/power/mosfet/n-channel/irf7807z/

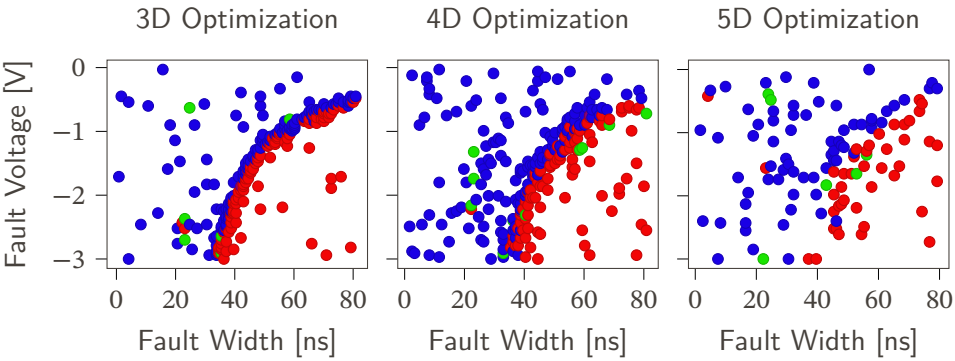
EXPERIMENTAL RESULTS

- → Target: LPC2129[1]
  - → Implements simple counting loop
  - → Commands and results sent over UART
  - → GPIO indicates operation start
- → Attack: Voltage glitching
  - → Adjustable core, I/O and fault voltage
  - → Variable fault width and delay
  - → Counting errors are interpreted as success



[1] https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc2000-arm7:MC_71580#/
[2] https://www.activetechnologies.it/pulse_rider_pg-1072_pg1074_revb/
[3] https://www.infineon.com/cms/en/product/power/mosfet/n-channel/irf7807z/
[4] https://www.keysight.com/de/de/support/E36312A/80w-triple-output-power-supply-6v-5a-2x-25v-1a.html

EXPERIMENTAL RESULTS



3D: Fault Voltage, Fault Width, Fault Delay
4D: Fault Voltage, Fault Width, Fault Delay, Core Voltage
5D: Fault Voltage, Fault Width, Fault Delay, Core Voltage, I/O Voltage

CONTRIBUTIONS & DISCUSSION

→ Contribution
- → Novel semi-deterministic method for identifying polytopes of interest
- → Effectiveness demonstrated with simulations and experiments
- → No restriction of parameters required
- → Can handle arbitrary result shapes

CONTRIBUTIONS & DISCUSSION

- → Contribution
  - → Novel semi-deterministic method for identifying polytopes of interest
  - → Effectiveness demonstrated with simulations and experiments
  - → No restriction of parameters required
  - → Can handle arbitrary result shapes
- → Discussion
  - → Focus on the border region, thus only outlines are identified
  - → For multiple interesting regions a random point selection is required
  - → High computation time for large number of input points in higher dimensions

FUTURE WORK

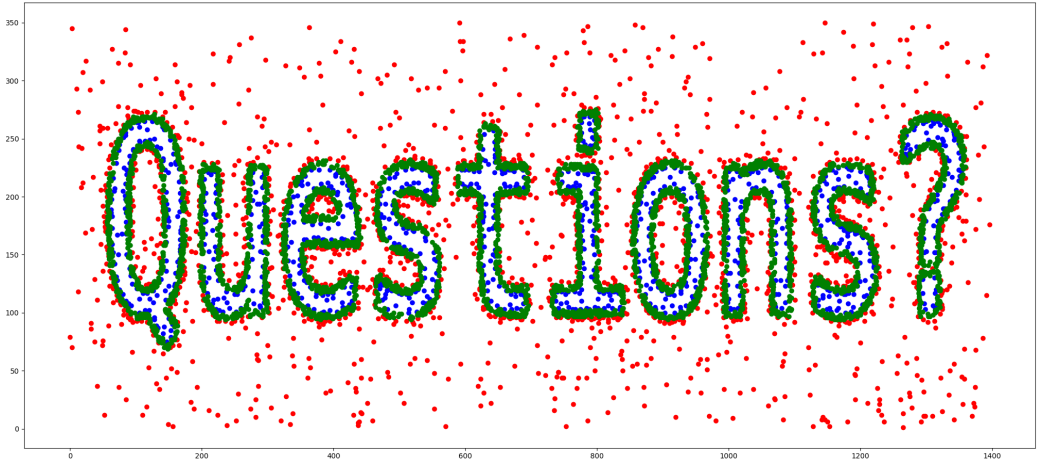
→ Calculation speed-up in higher dimensions

→ Likelihood evaluation for single successful parameter combinations

→ Combination with heuristic approaches

→ Restricting point selection to account parameter adjustment times

THANK YOU!


Questions?
350
300
250
200
150
100
50
0
0
200
400
600
800
1000
1200
1400