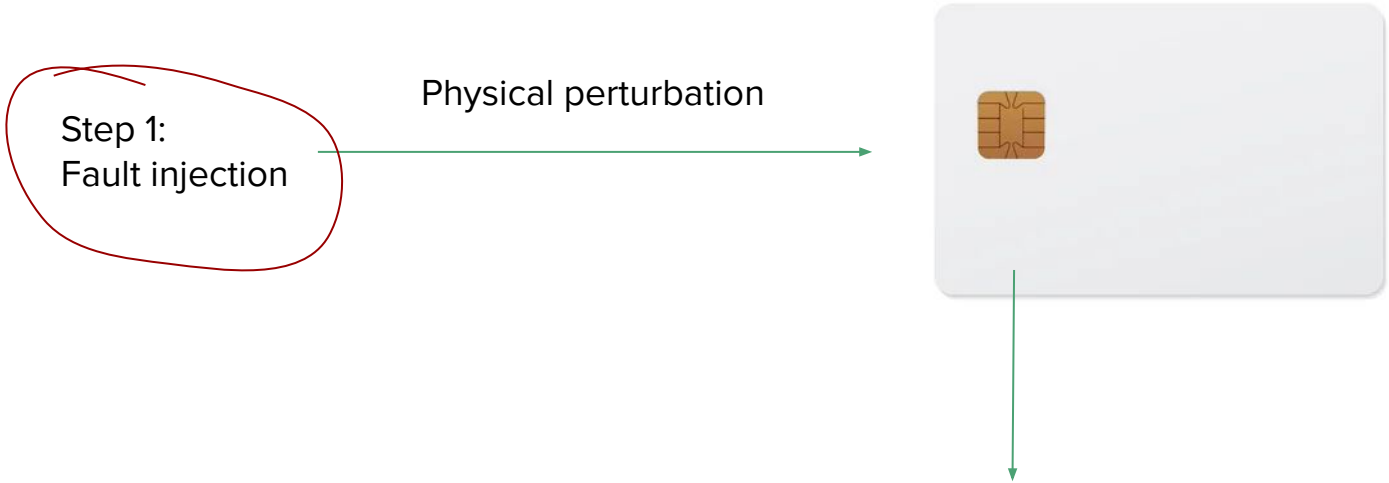
The More You Know: Improving Laser Fault Injection with Prior Knowledge

Marina Krček, Thomas Ordas, Daniele Fronte, Stjepan Picek

FDTC 2022

TU Delft
Radboud Universiteit
life.augmented

Fault Injection (FI) attacks

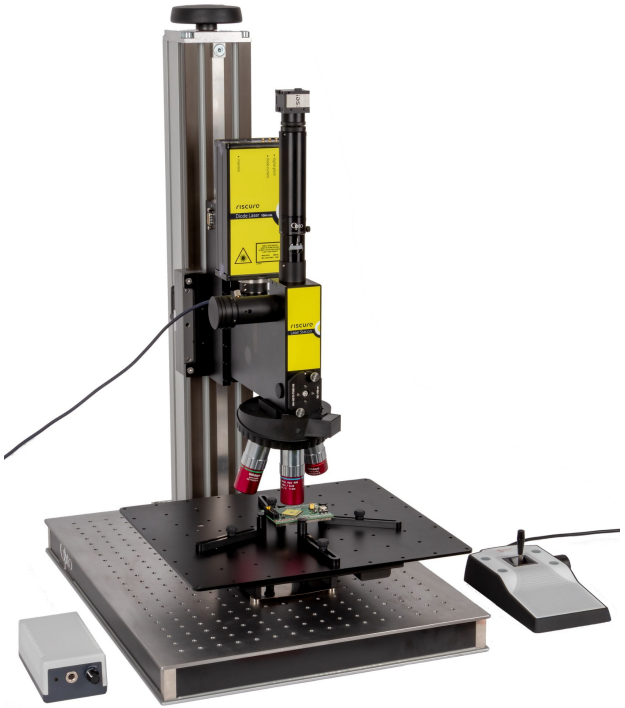


Laser Fault Injection (LFI)

Parameters

Location on the device: x, y

Laser pulse width, delay and intensity



LFI: 529 days with ≈ 0.15 seconds per point (parameter combination)

EMFI*: exhaustive search 29 203 years to conduct with ≈ 0.16 seconds per point (parameter combination)

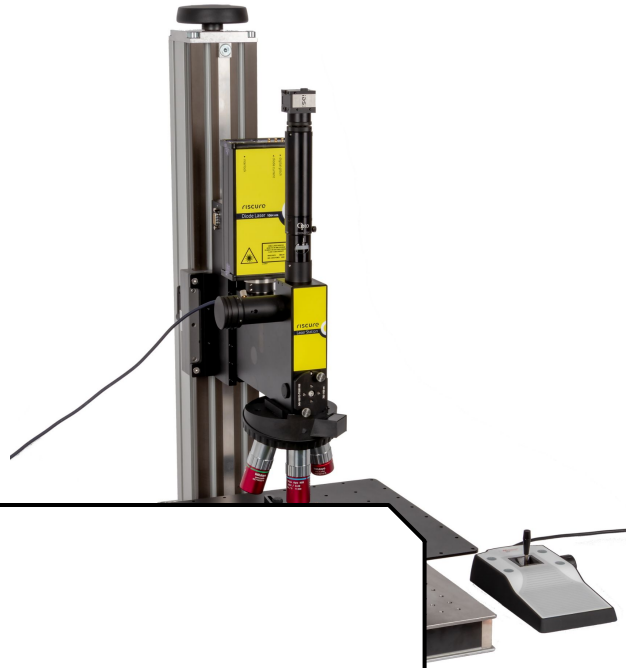
* Maldini, Antun, et al. "Genetic algorithm-based electromagnetic fault injection." *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2018.

Laser Fault Injection (LFI)

Parameters

Location on the device: x, y

Laser pulse width, delay and intensity



LFI: 529 days with ≈ 0.15 seconds per point (parameter combination)

EM
se

Issue! Large search space

* Maldini, Antun, et al. "Genetic algorithm-based electromagnetic fault injection." *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2018.

Algorithms for FI parameter search

Grid search and Random search

Evolutionary approach - memetic algorithms

Reinforcement learning

Hyperparameter tuning - Successive Halving Algorithm

- Carpi, Rafael Boix, et al. "Glitch it if you can: parameter search strategies for successful fault injection." *International Conference on Smart Card Research and Advanced Applications*. Springer, Cham, 2013.
- Maldini, Antun, et al. "Genetic algorithm-based electromagnetic fault injection." *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2018.
- Krček, Marina, Daniele Fronte, and Stjepan Picek. "On the Importance of Initial Solutions Selection in Fault Injection." *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE, 2021.
- Moradi, Mehrdad, et al. "Exploring fault parameter space using reinforcement learning-based fault injection." *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2020.
- Werner, Vincent, Laurent Maingault, and Marie-Laure Potet. "Fast Calibration of Fault Injection Equipment with Hyperparameter Optimization Techniques." *International Conference on Smart Card Research and Advanced Applications*. Springer, Cham, 2021.

Algorithms for FI parameter search

Grid search and Random search

Evolutionary approach - memetic algorithms

Reinforcement learning

Hyperparameter tuning - Successive Halving Algorithm

Issue! Any change with the FI setup or sample's behavior - the process has to be repeated anew

- Carpi, ...ranced *Applica*
- Maldin... 018.
- Krček, ...rance in *Crypto*...
- Moradi, Mehrdad, et al. "Exploring fault parameter space using reinforcement learning-based fault injection." *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2020.
- Werner, Vincent, Laurent Maingault, and Marie-Laure Potet. "Fast Calibration of Fault Injection Equipment with Hyperparameter Optimization Techniques." *International Conference on Smart Card Research and Advanced Applications*. Springer, Cham, 2021.

Proposed method

Improve performance when a change is introduced

Decision tree (DT) to learn the behavior/responses of the target

Prior knowledge

Combination with **Memetic Algorithm (MA)**

Existing algorithm

- Initial population uses the knowledge
- Other operators remain unchanged

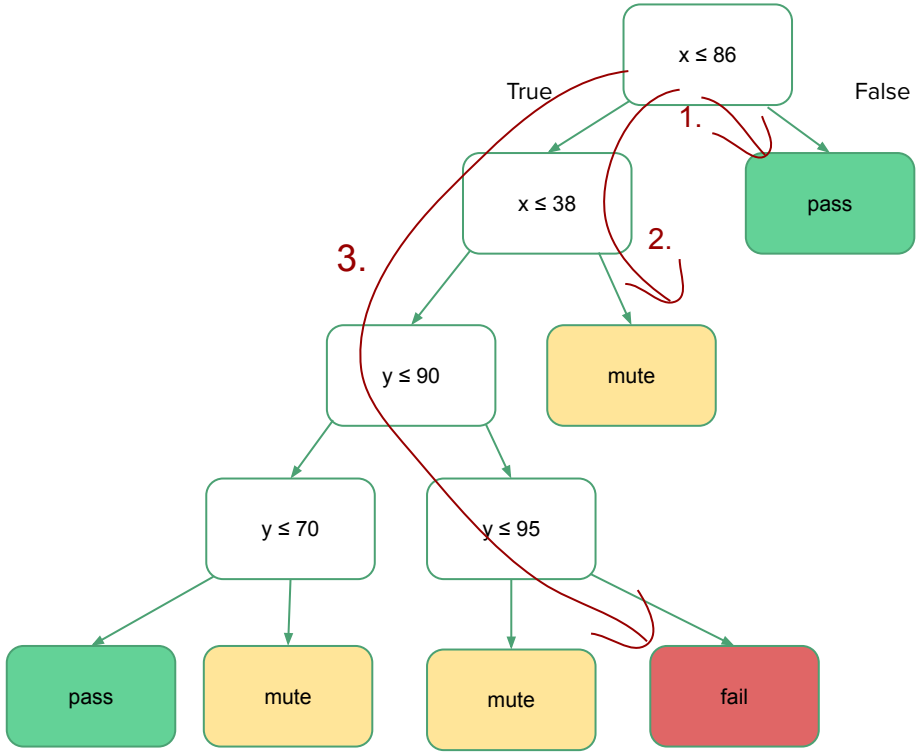
Use on **different samples of the same target**

Decision Tree (DT)

if-then rules:

1. if $x > 86$ then *pass*
2. if $x \in \langle 38, 86]$ then *mute*
3. if $x \leq 38$ *and* $y > 95$ then *fail*
4. ...

CART* algorithm



* Breiman, Leo, et al. *Classification and regression trees*. Routledge, 2017.

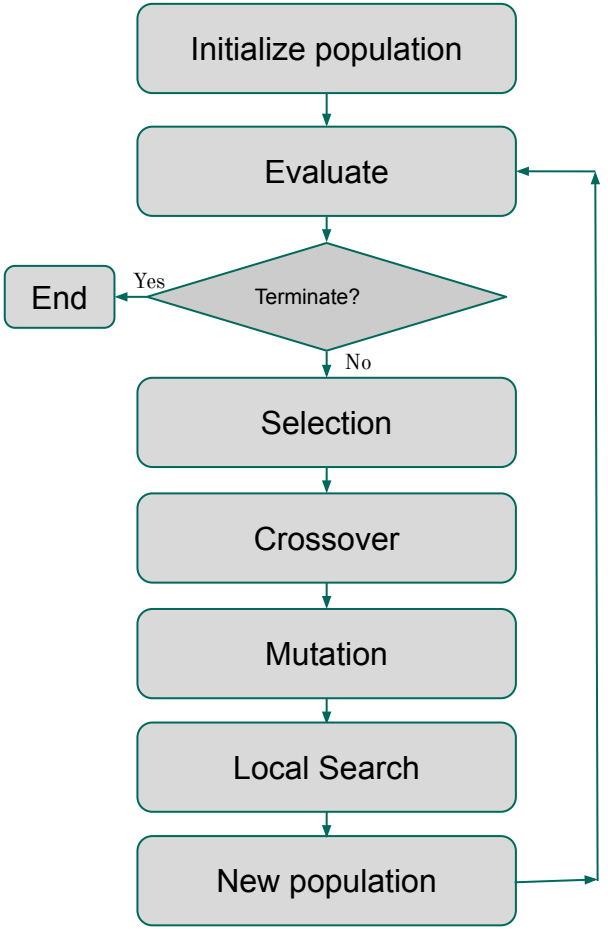
Memetic Algorithm (MA)

Solutions in the population are LFI parameters:

x, y, delay, laser pulse width and intensity

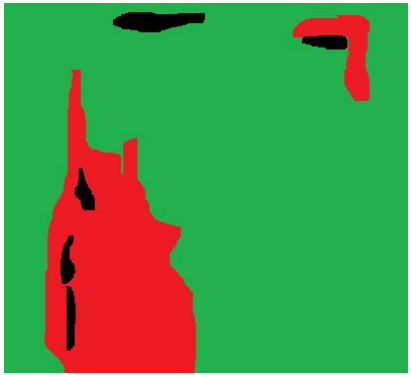
Population of size n

x_1, y_1, d_1, pw_1, i_1	f_1
x_2, y_2, d_2, pw_2, i_2	f_2
...	...
x_n, y_n, d_n, pw_n, i_n	f_n



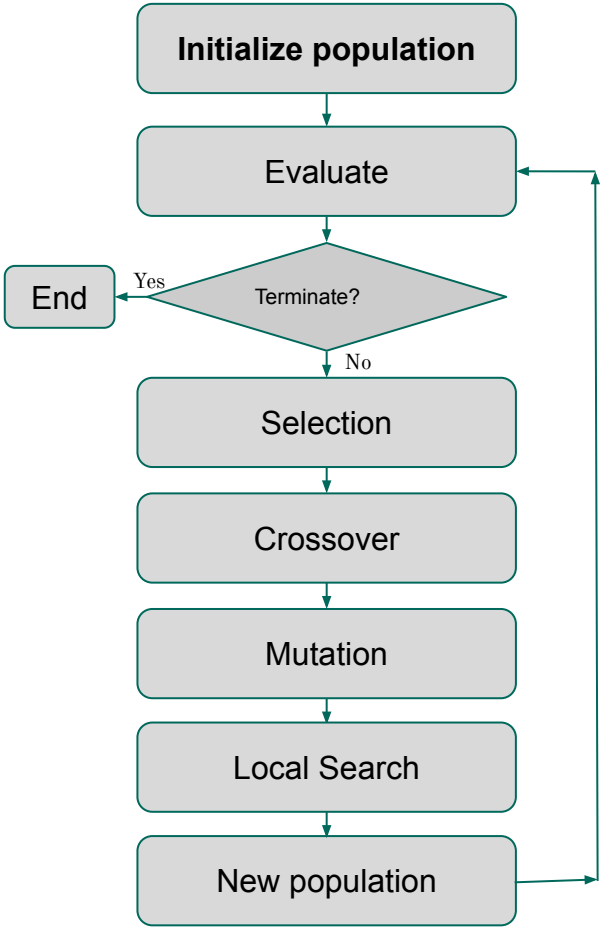
Krček, Marina, Daniele Fronte, and Stjepan Picek. "On the Importance of Initial Solutions Selection in Fault Injection." *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE, 2021.

Combining DT rules with MA



Rules for *fail*

1. $x \in \langle x_1, x_2] \; and \; y \in \langle y_1, y_2]$
2. $i \in \langle i_1, i_{max}]$
3. ...



Device under test

Target: STMicroelectronics product - confidential, 40nm technology

Test program: loading a data word from the non-volatile memory (NVM) into a register

Fault classes: *fail*, *mute*, *pass*, *changing*

Limited bounds for parameters:

305 017 650 possible parameter combinations

exhaustive would take ≃ 529 days where one laser shot takes ≃ 0.15 seconds

Experimental Setup

Different samples of the same target - IC1, IC2, IC3

- Changes in the focus: IC3 > IC1 > IC2
- FGS: 3.7 times more *fails* with IC3 then IC1
- RS: 2.7 times more *fails* with IC3 then IC1
- Both have more than IC2 with the worst focus

Fast Grid Search (FGS)	IC1	IC2	IC3
Tested parameters	12 350	12 350	12 350
fail	9 (0.07%)	0 (0%)	33 (0.27%)

Random Search (RS)	IC1	IC2	IC3
Tested parameters	5 920	5 920	5 920
fail	7 (0.12%)	3 (0.05%)	19 (0.32%)

Training data on IC1

880 DT models with different hyperparameters

On both datasets separately

Select the models based on the F1-score

	MA with random init. (10 runs)	Random Search (1 run)
Tested combinations	6 150.5	50 000
fail	366.5 (6.12%)	58 (0.12%)
changing	548.6 (8.92%)	451 (0.9%)
mute	182.6 (2.89%)	226 (0.45%)
pass	5 052.8 (82.08%)	49 265 (98.53%)

More examples for *fail* class!

Experiments on IC2

MA with random initialization: similar to IC1 results (more than FGS and RS results)

MA with DT found more fails: ≃ 61 % (64%, 55%, 52%, 72%) more

	RS	MA with random init.	MA with DT F1: 0.1776 MA data	MA with DT F1: 0.0999 MA data	MA with DT F1: 0.1999 RS data	MA with DT F1: 0.1756 RS data
Tested combinations	5920	6389.6	5059.3	5284.2	5581.3	5507.9
fail	3 (0.05%)	304.7 (5.03%)	848.4 (16.86%)	676.5 (12.48%)	633 (11.38%)	**1072.7 (19.39%)**
changing	27 (0.46%)	250 (3.88%)	234.6 (4.61%)	216.9 (4.11%)	160.2 (2.89%)	198.7 (3.6%)
mute	12 (0.2%)	147.9 (2.28%)	37.3 (0.74%)	81.7 (1.53%)	16 (0.29%)	33 (0.58%)
pass	5878 (99.29%)	5687 (88.82%)	3939 (77.79%)	4309.1 (81.51%)	4772.1 (85.44%)	4203.5 (76.43%)

Experiments on IC3

Two orders of magnitude more *fails* compared to RS

	RS	MA with DT F1: 0.1776 MA data	MA with DT F1: 0.0833 MA data	MA with DT F1: 0.1756 RS data
Tested combinations	5920	5262.7	5495.1	5554.5
fail	19 (0.32%)	1662.8 (31.53%)	**2688.8 (48.85%)**	2325.7 (41.83%)
changing	66 (1.11%)	221.9 (4.23%)	210.1 (3.81%)	153.4 (2.76%)
mute	99 (1.67%)	126 (2.37%)	74.1 (1.35%)	101.5 (1.82%)
pass	5736 (96.89%)	3252 (61.86%)	2522.1 (45.98%)	2973.9 (53.58%)

Highest F1-score did not lead to the best overall results

Rules from MA data were more specific and resulted in more *fails* in initial population

Conclusions and future work

DT rules improve the MA for FI parameter search on different samples of the same target

Number of *fail* responses found:

- Two orders of magnitude more than random search
- Up to 60% more than memetic algorithm with random initialization

Future work

- Extend the idea to manage other transferability cases, e.g., different bench or target