RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

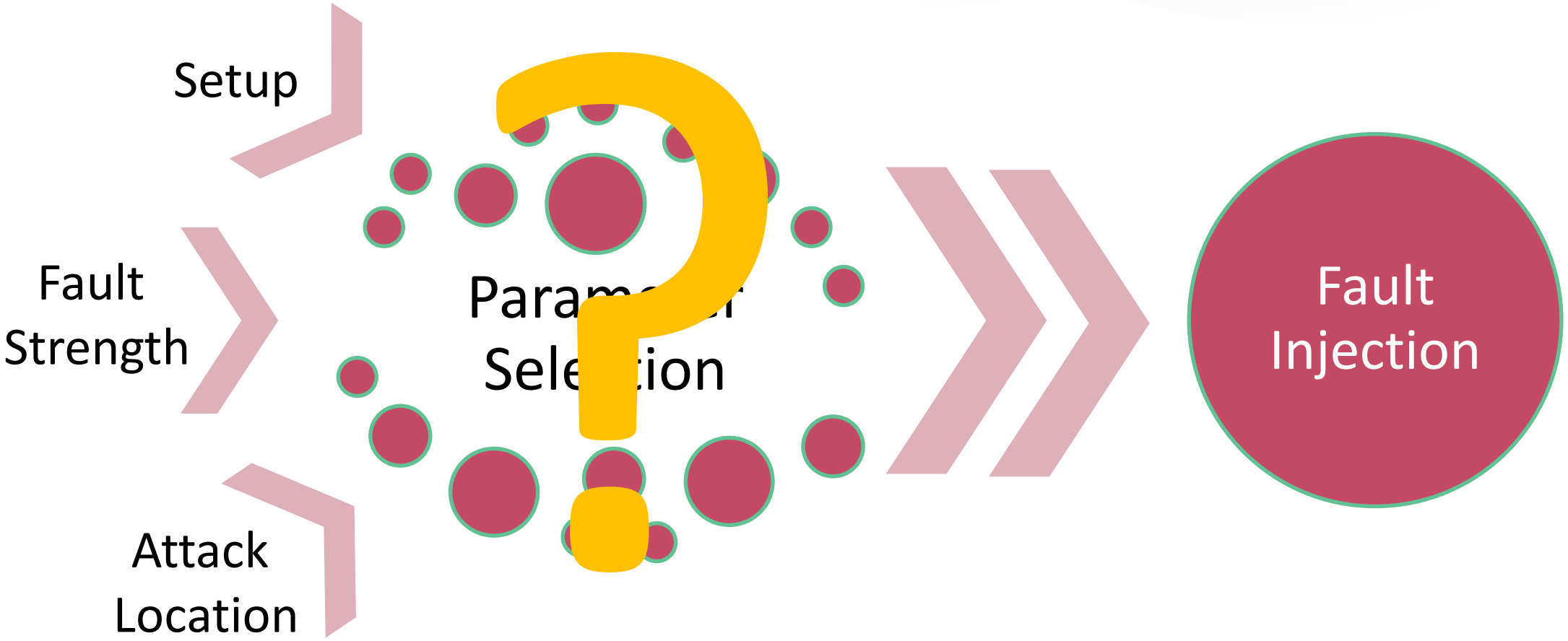
SESSION ID: CRYP-T12

A Fast Characterization Method for Semi-invasive Fault Injection Attacks

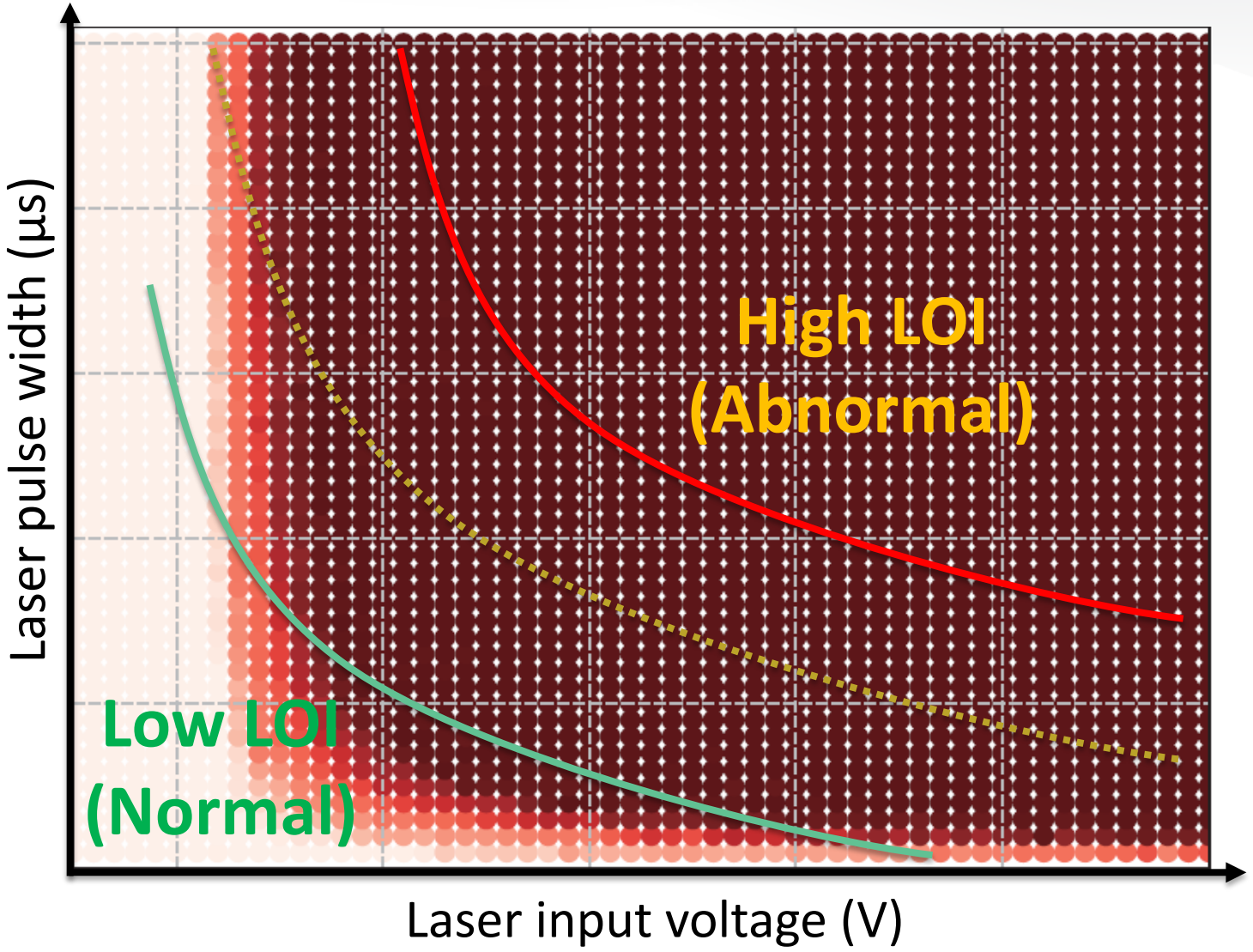
Stjepan Picek

Assistant professor
TU Delft, The Netherlands

Why Characterization?



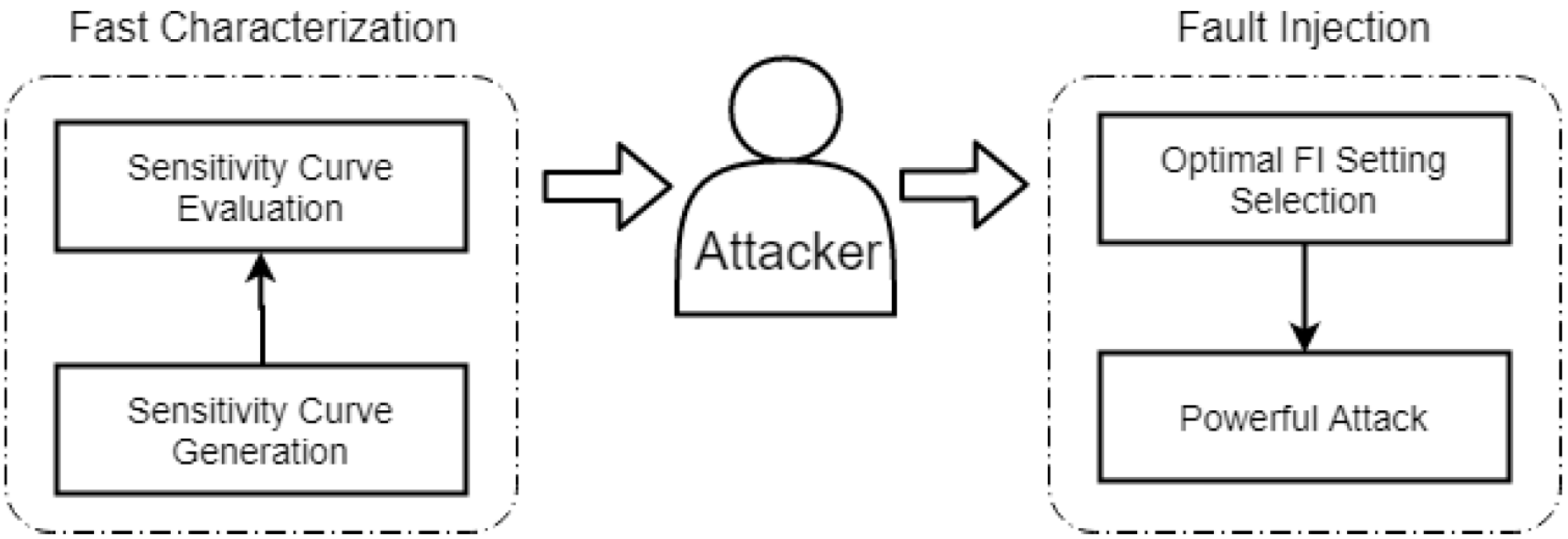
How to Characterize?



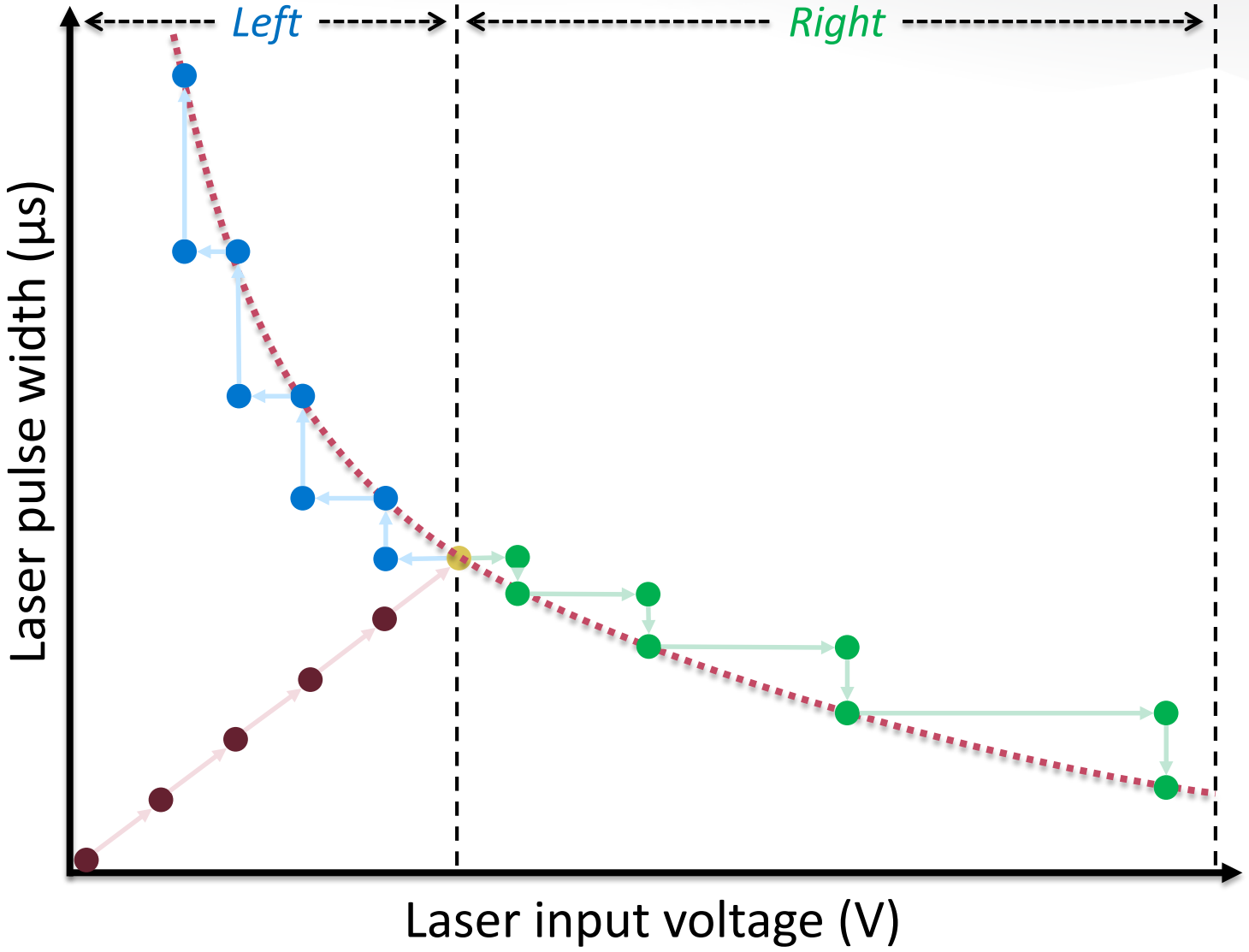
RSAConference2020

Fast Characterization Methodology

Attack Workflow



Sensitivity Curve Generation



Sensitivity curve

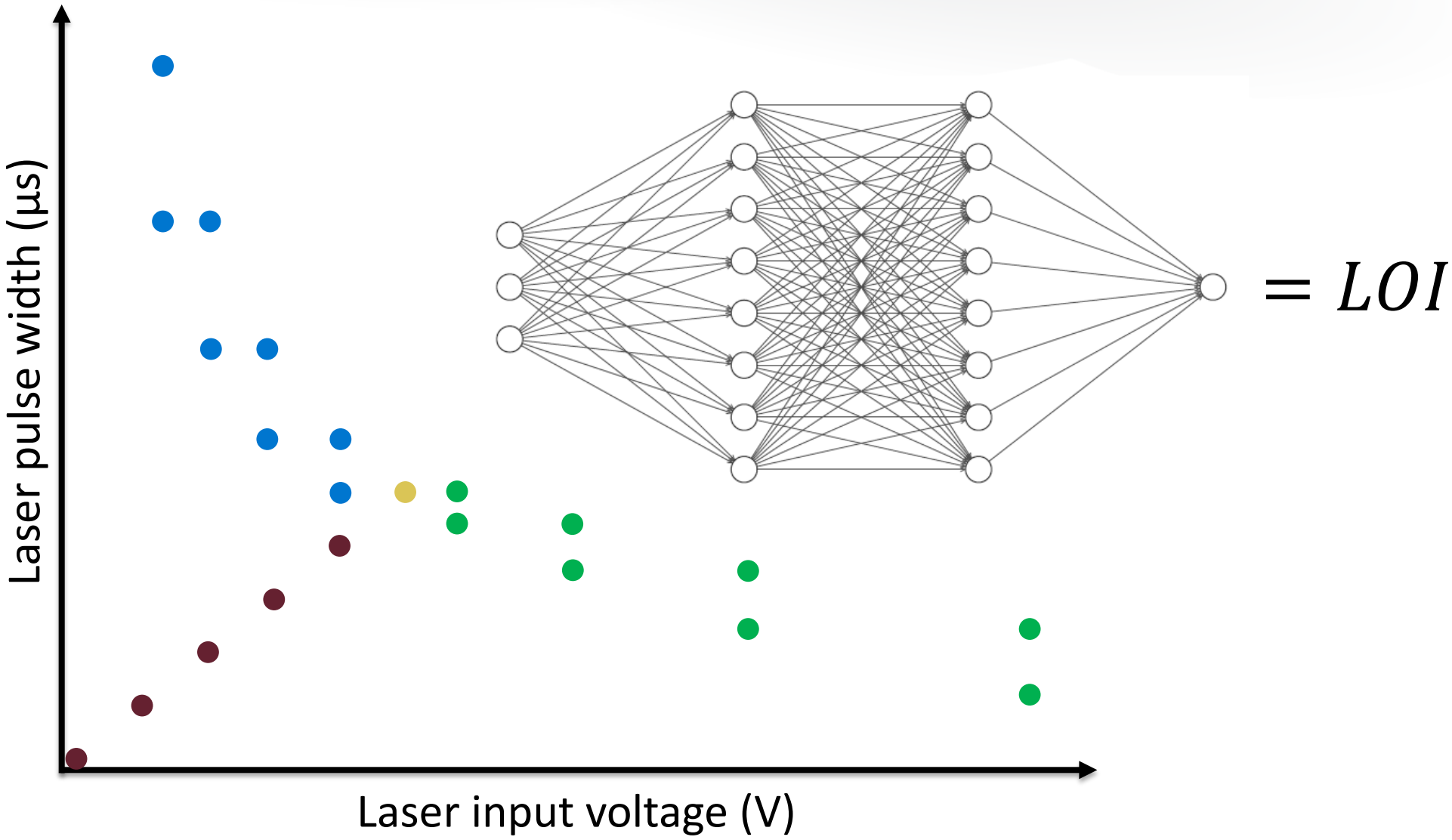
Diagonal search

Golden point

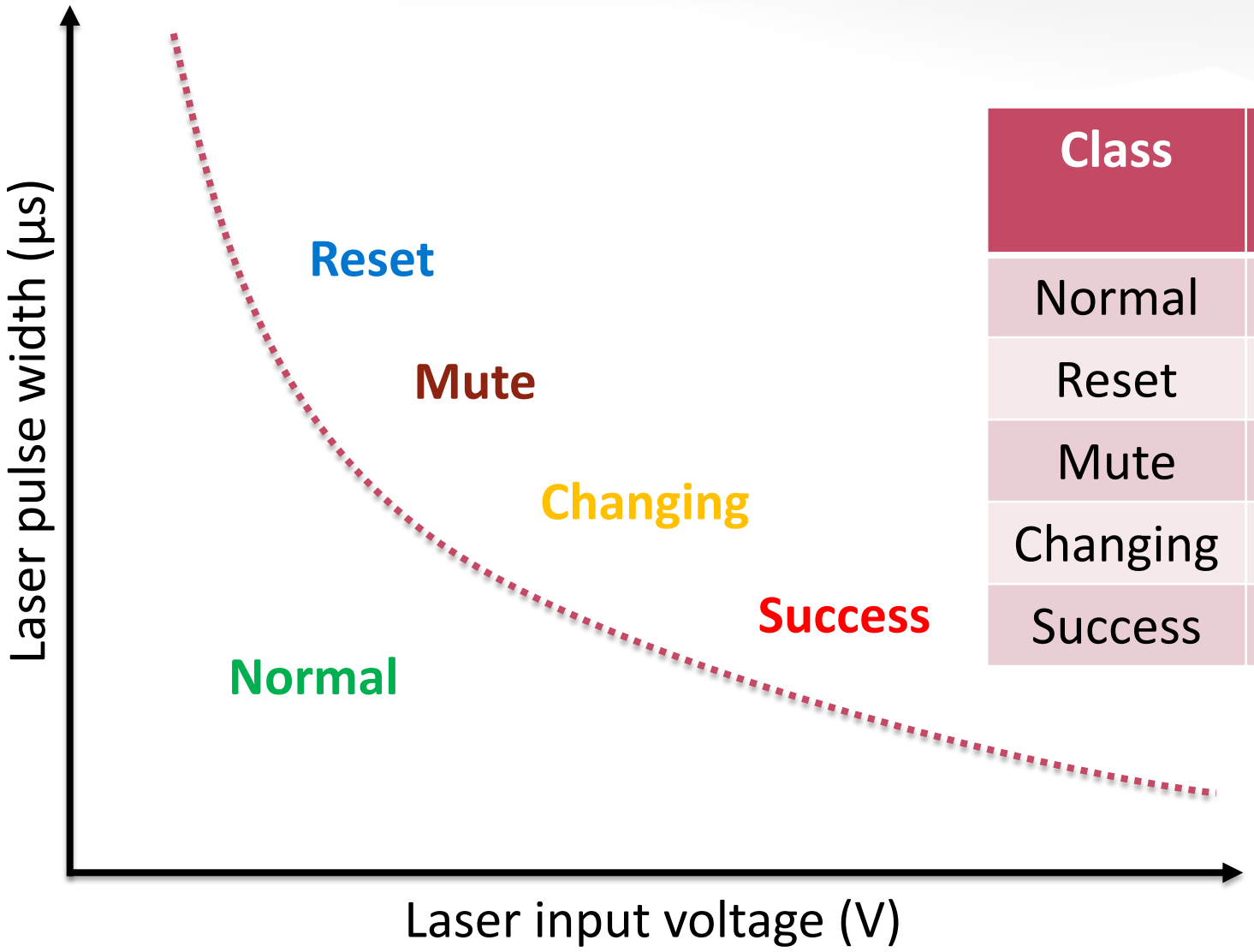
Left search

Right search

Evaluation: Predicting LOIs



Evaluation: Impact Score (IS)



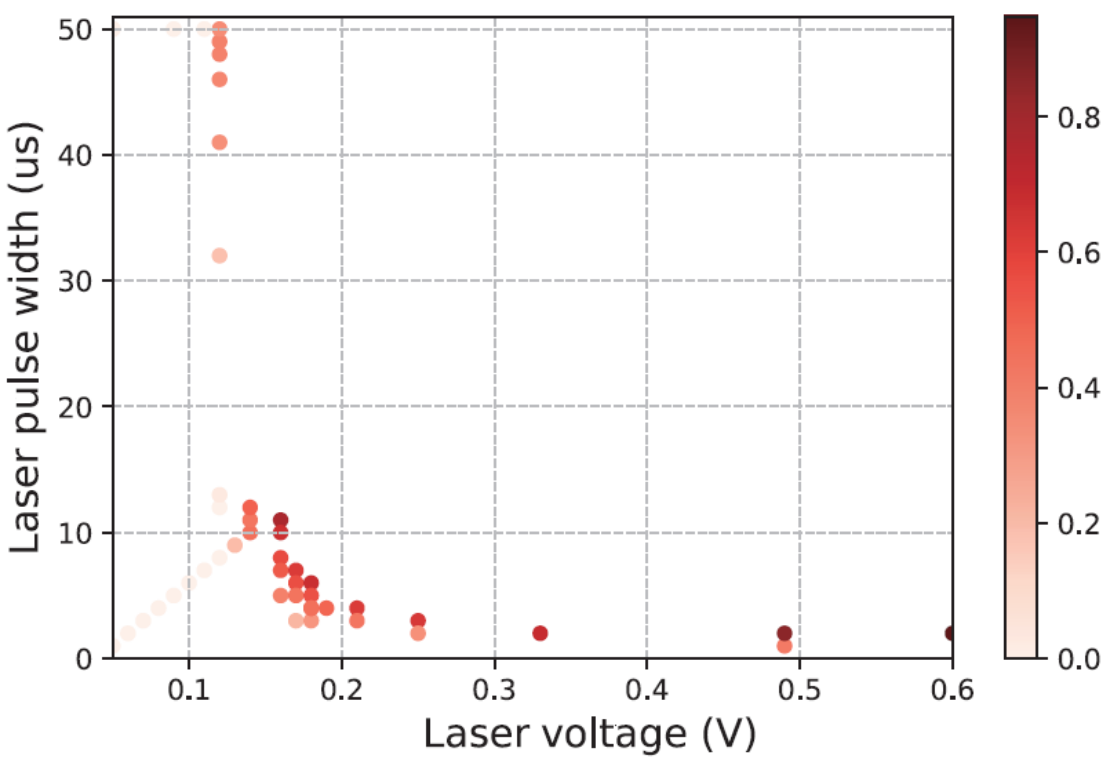
Class	Detected	Manipulated	Score
Normal			0
Reset	+		10
Mute	+	+	20
Changing		+	50
Success		++	100

RSAConference2020

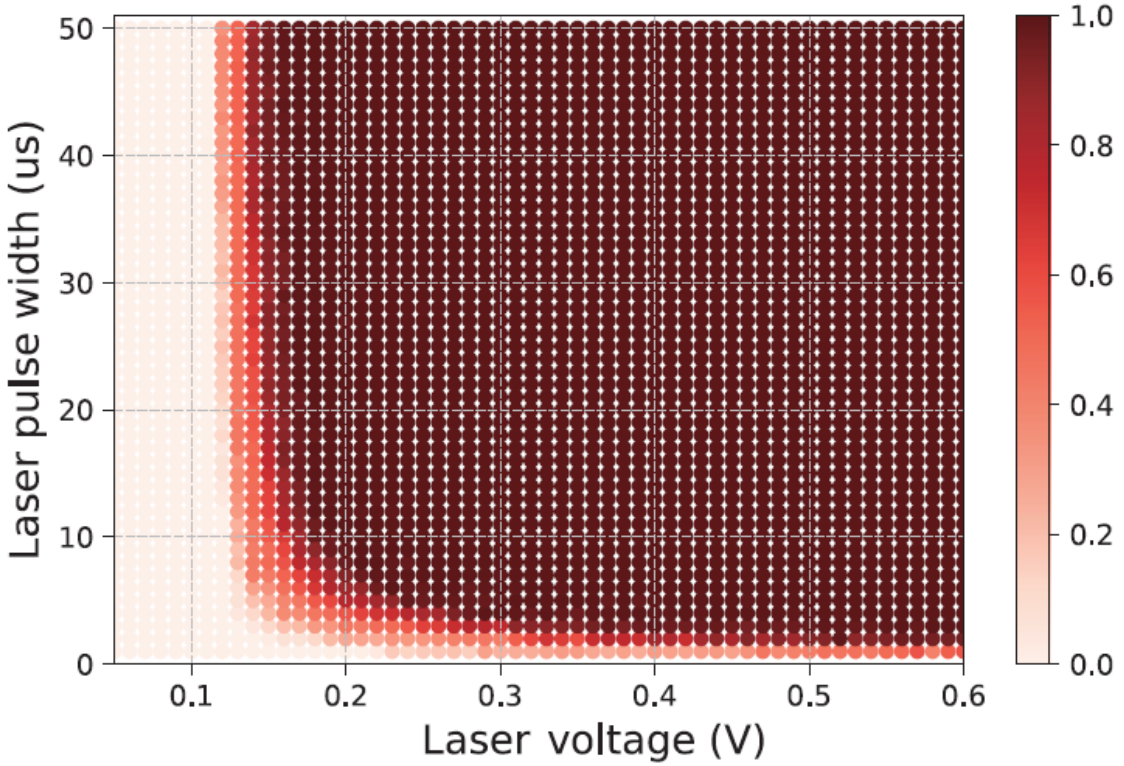
Experimental Results

Sensitivity Curve Generation

Sensitivity Curve

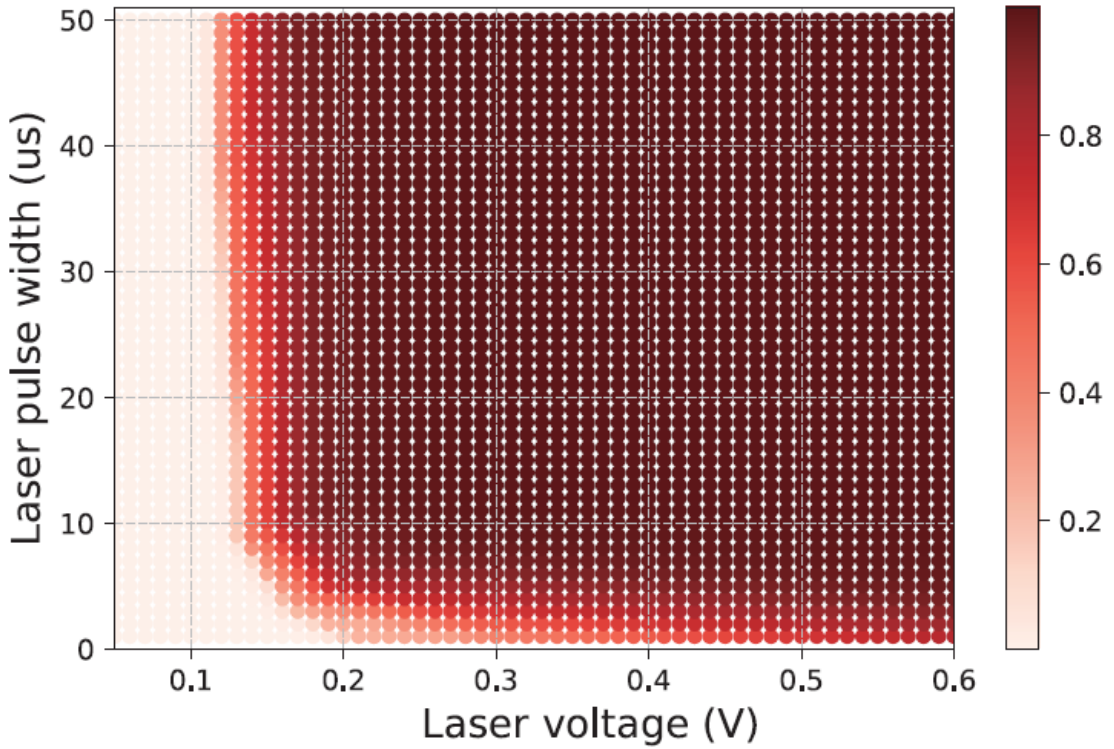


Exhaustive Scan

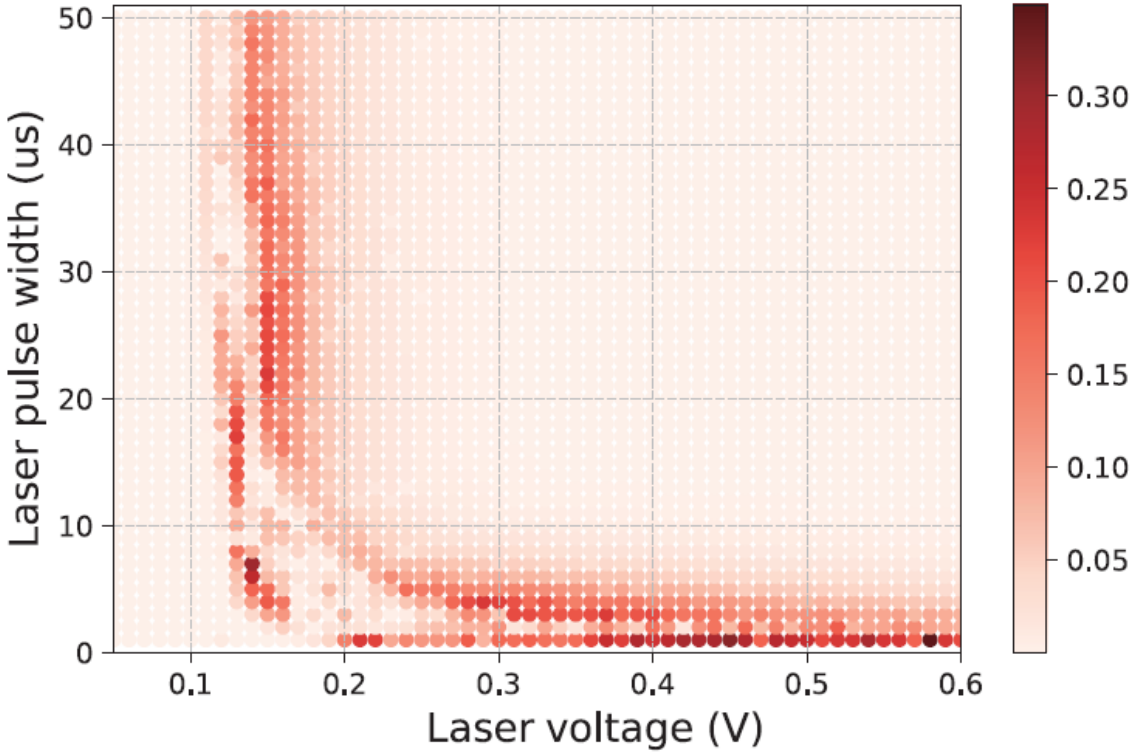


Sensitivity Curve Evaluation: Predicting LOIs

Prediction Result

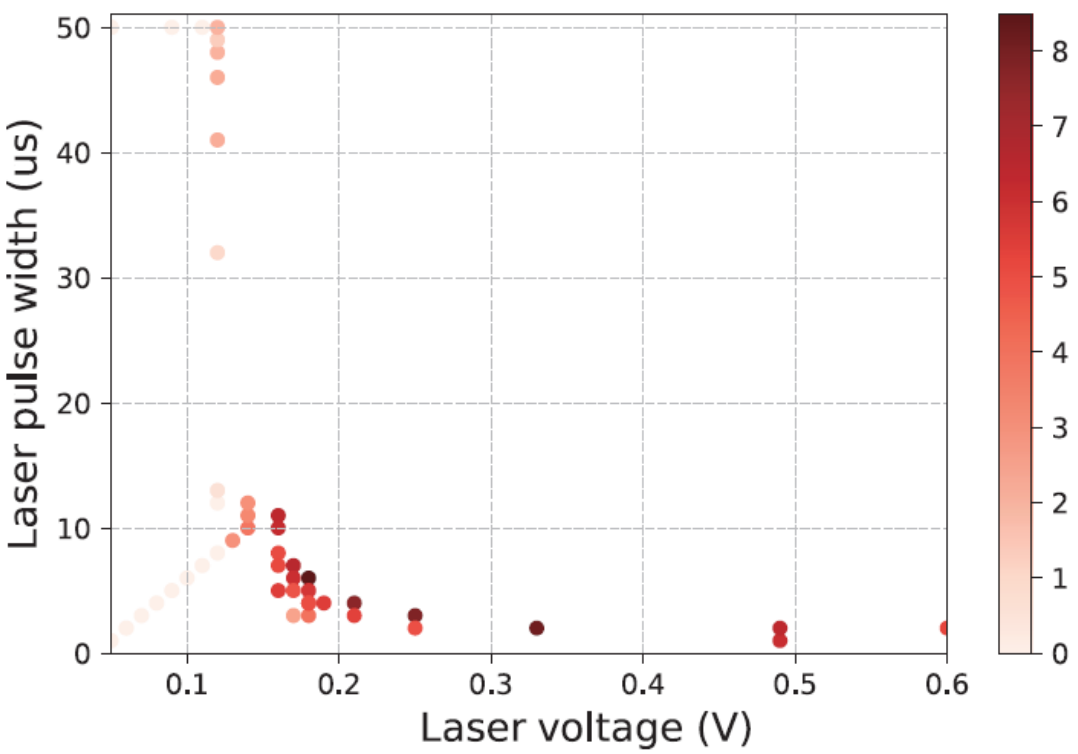


Exhaustive Scan/Prediction Error

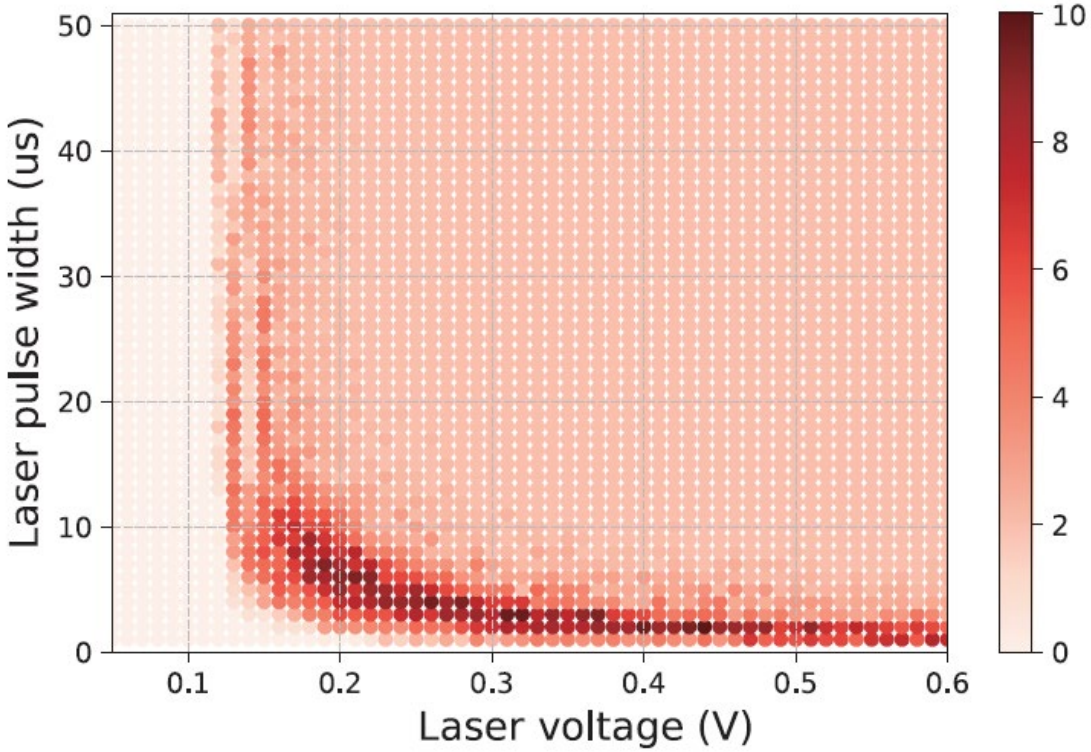


Sensitivity Curve Evaluation: Impact Score (IS)

Sensitivity Curve



Exhaustive Scan

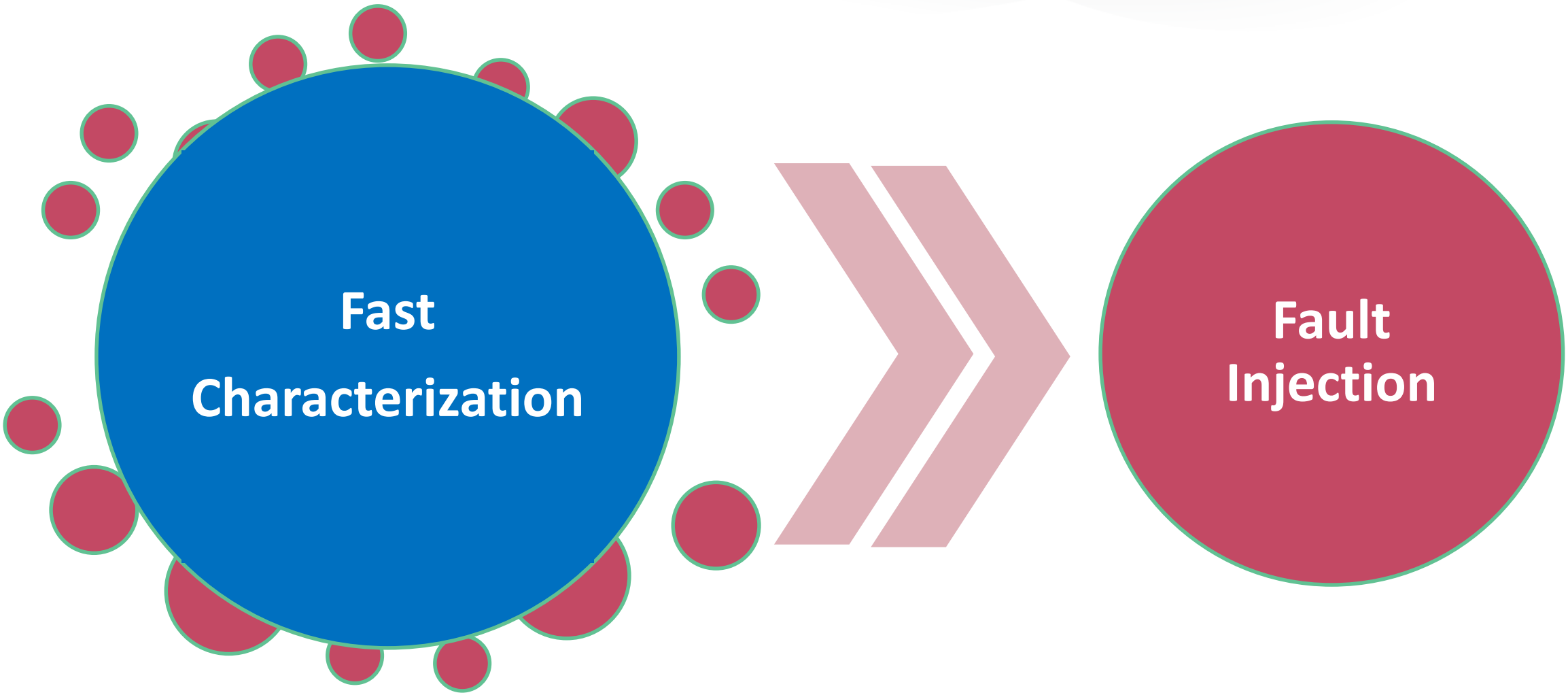


RSAConference2020

Apply It!

A stable and effective method for real evaluation

Back to Origin



Attack Strategically

Sensitivity Curve Evaluation

Optimal Parameter Selection

Sensitivity Curve Generation

Powerful Attack

RSAConference2020

Thank you!

Questions?