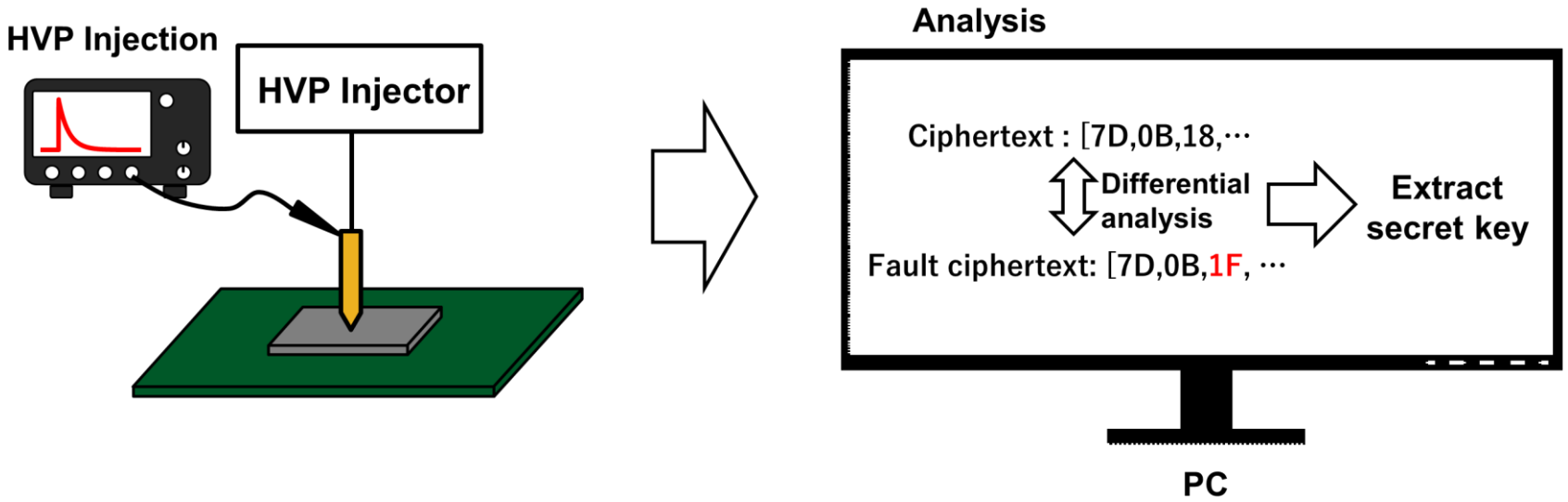
Fault injection attacks exploiting high voltage pulsing over Si-substrate backside of IC chips

Yusuke Hayashi, Rikuu Hasegawa, Takuya Wadatsumi,
Kazuki Monta, Takuji Miki, Makoto Nagata

Kobe University

Fault Injection

- Use physical attack to extract a private key



- Method
  - ✓ Clock Glitch
  - ✓ Voltage Glitch
  - ✓ EM(electromagnetic)
  - ✓ Laser
  - ✓ **HVP (High Voltage Pulse)**

Threat of attack methods

- Threat levels according to attack methods

Method	Injection location		De-packaging	Equipment Cost	Fault spot size
	Frontside	Backside			
Clock glitch			No	Low	Global
Voltage glitch			No	Low	Global
EM pulse	Yes	Yes	No	Low	Global
Laser beam	No	Yes	Yes	High	Local
HVP	**Yes**	**Yes**	**Yes**	**Low**	**Local**

- Fault analysis
  - ✓ DFA (Differential Fault Analysis)
  - ✓ LFA (Linear Fault Analysis)
  - ✓ IFA (Ineffective Fault Analysis)

- **Fault analysis requires highly localized Fault Injection**

Attack capability in Si backside HVP

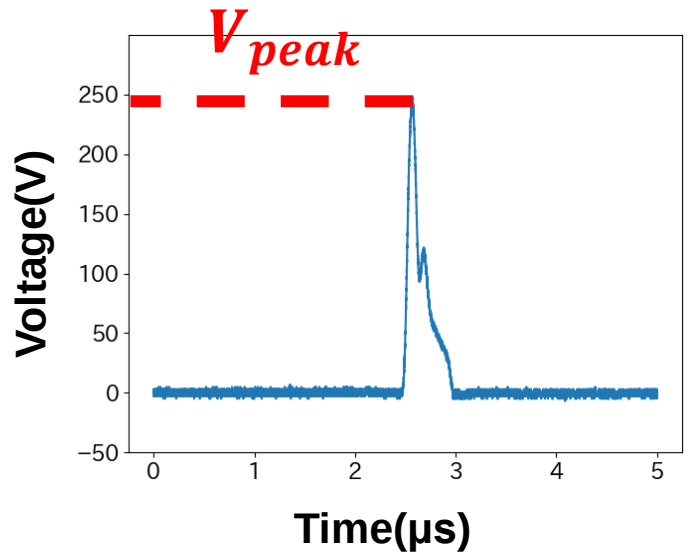
- The threat of Si backside HVP (Simulation and measurement)
  - ✓ Si backside HVP can induce faults among highly localized
  - ✓ Thinner Si-substrate thicknesses increase the threat

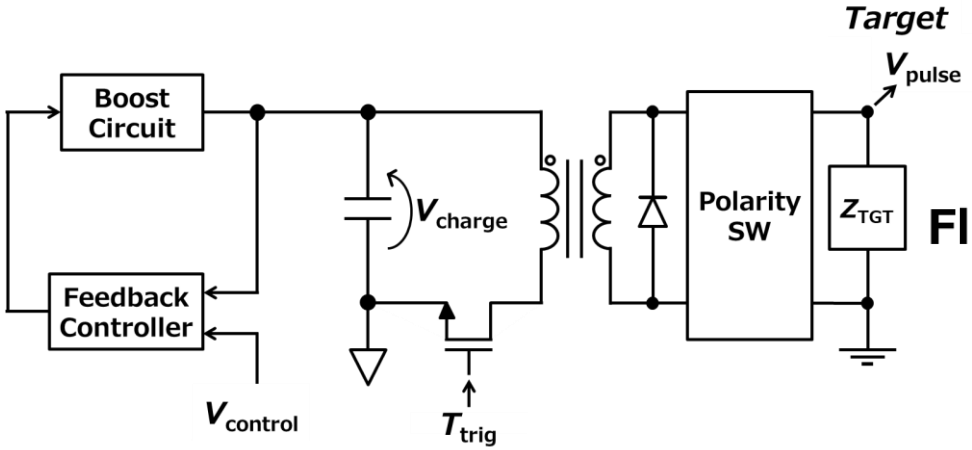
- DFA on AES using Si backside HVP
  - ✓ Fault injection in the 9th round of AES
  - ✓ Possible to derive secret keys by DFA

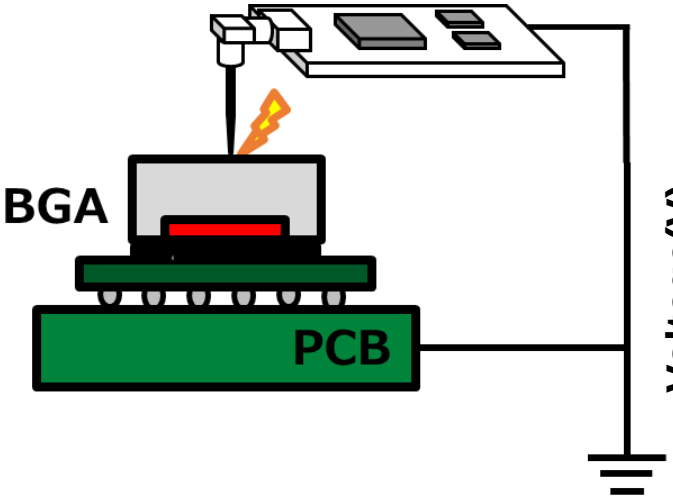
- **Si backside HVP is a threat as Fault Injection attack**

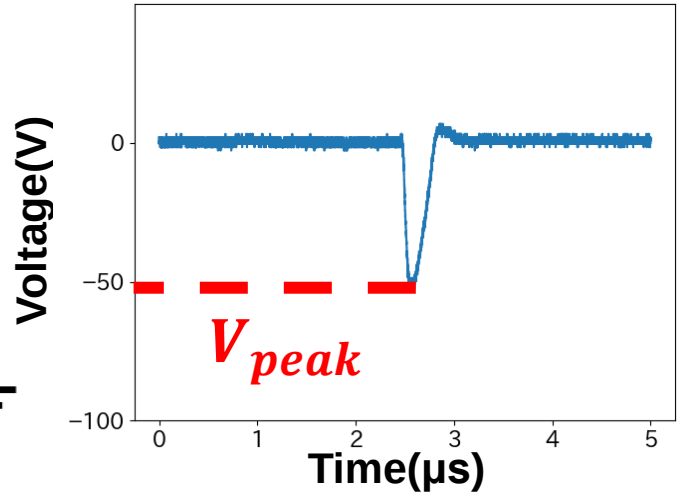
Si backside HVP

- A needle contact with the Si-substrate on the backside of a flip-chip IC
- V_{peak} can be controlled by $V_{control}$



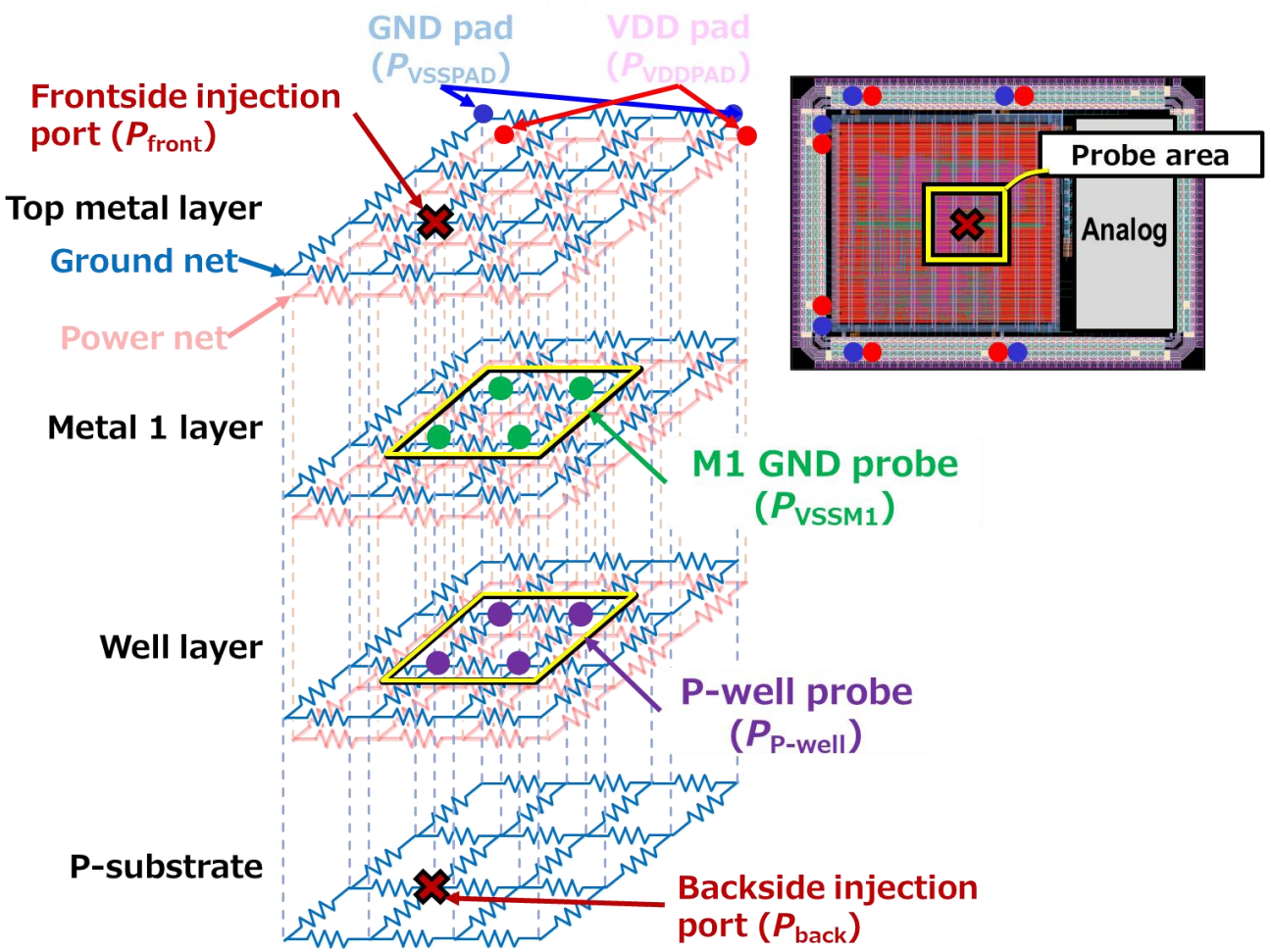




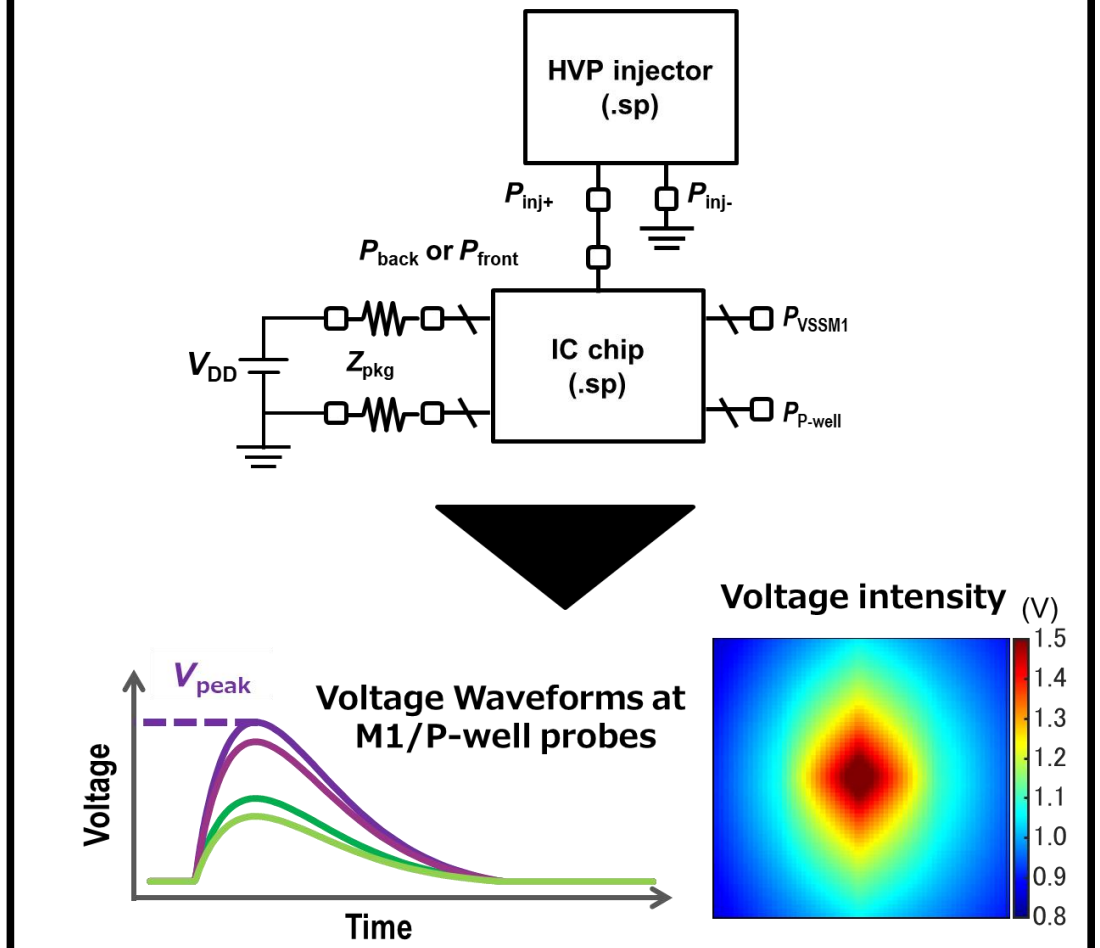


Simulation Evaluation

①Chip model

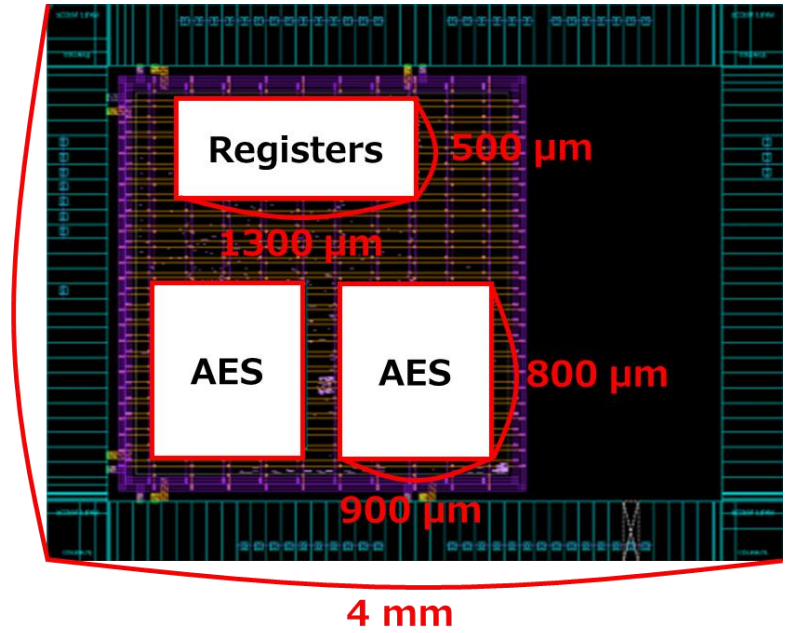


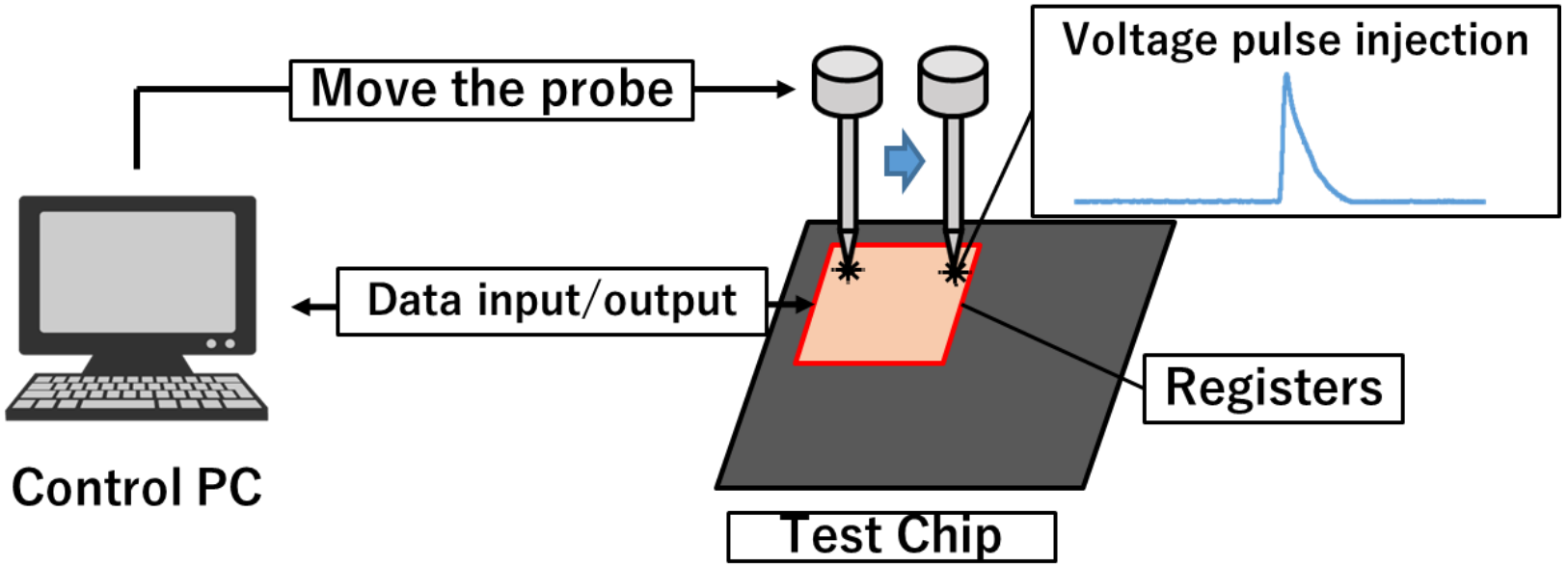
②SPICE simulation

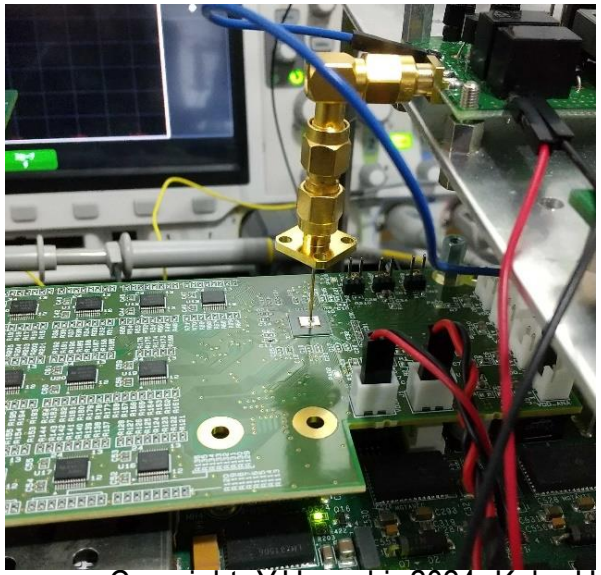


Measurement of HVP ability

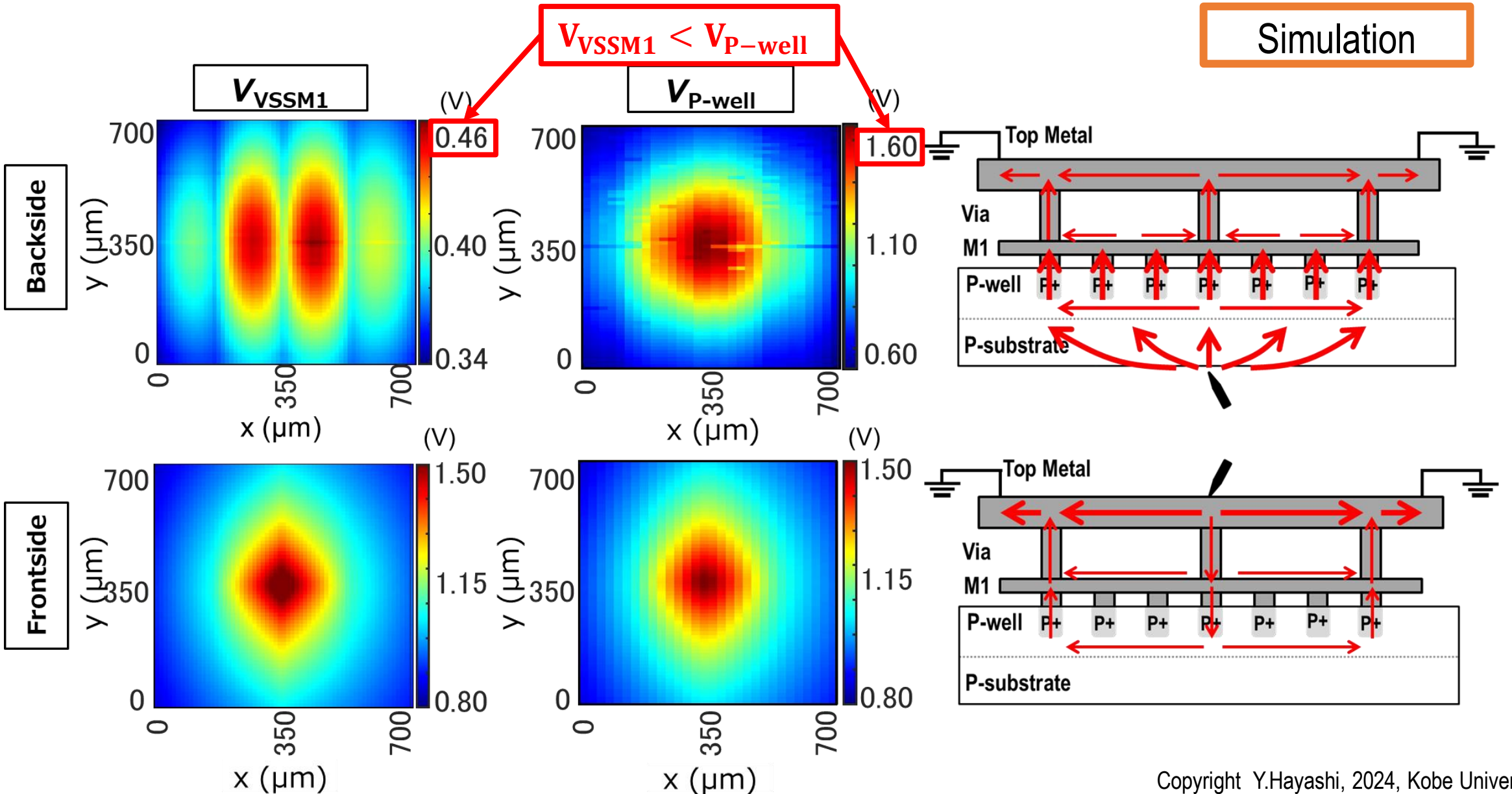
- Si backside HVP is injected in the area of FFs
- All FFs are initially set ("111...1“) or reset ("000...0")







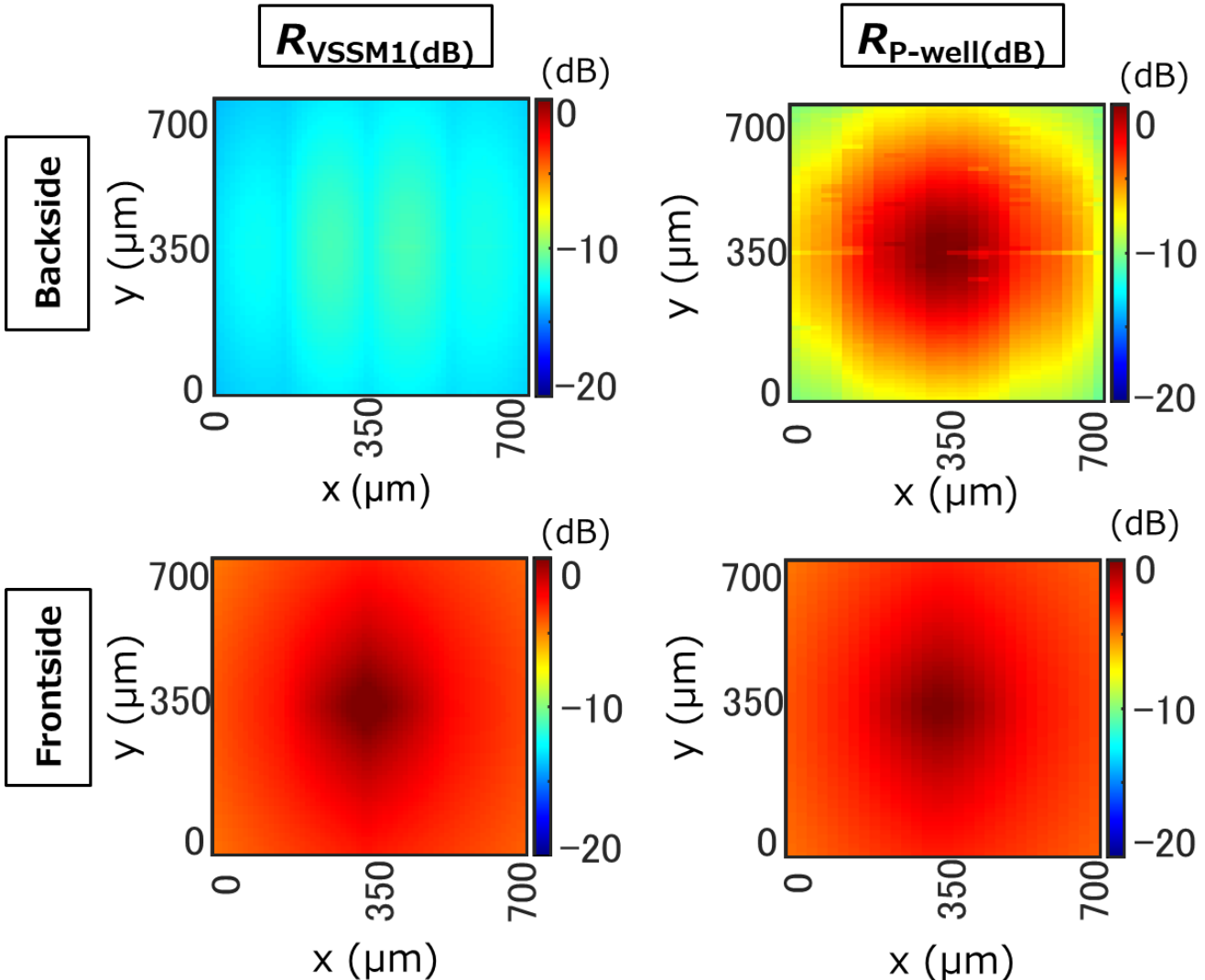
Voltage intensity from the frontside and backside

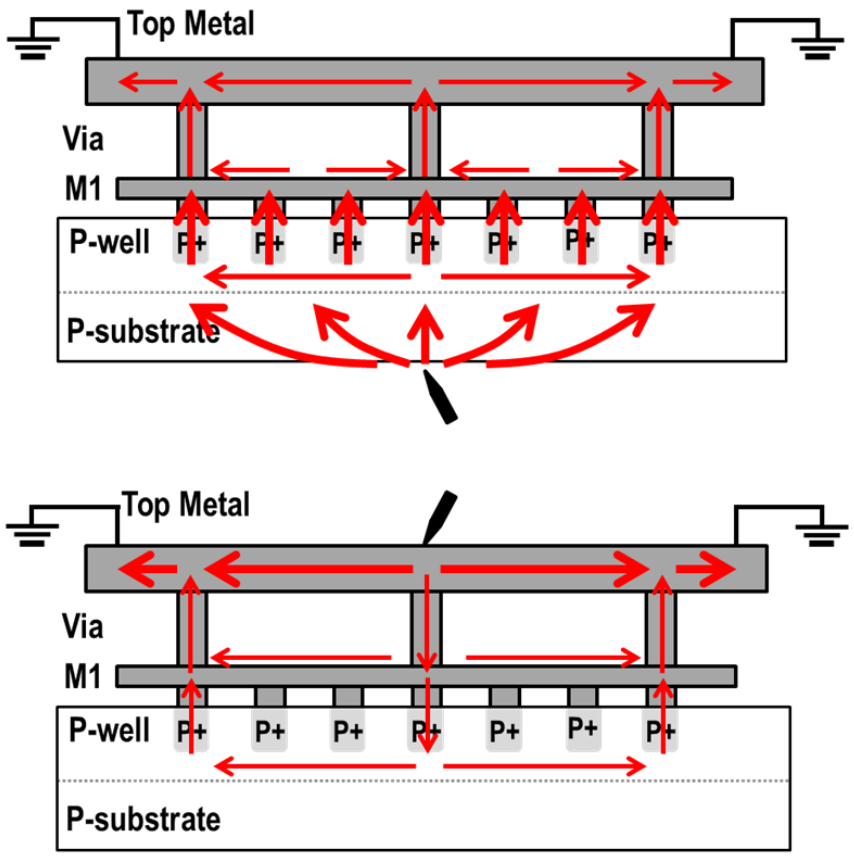


Localization from the frontside and backside

$$R_{VSSM1}(dB) = 20log_{10}\frac{V_{VSSM1}(V)}{Max(V_{P-well}(V))} \quad R_{P-well}(dB) = 20log_{10}\frac{V_{P-well}(V)}{Max(V_{P-well}(V))}$$

Simulation

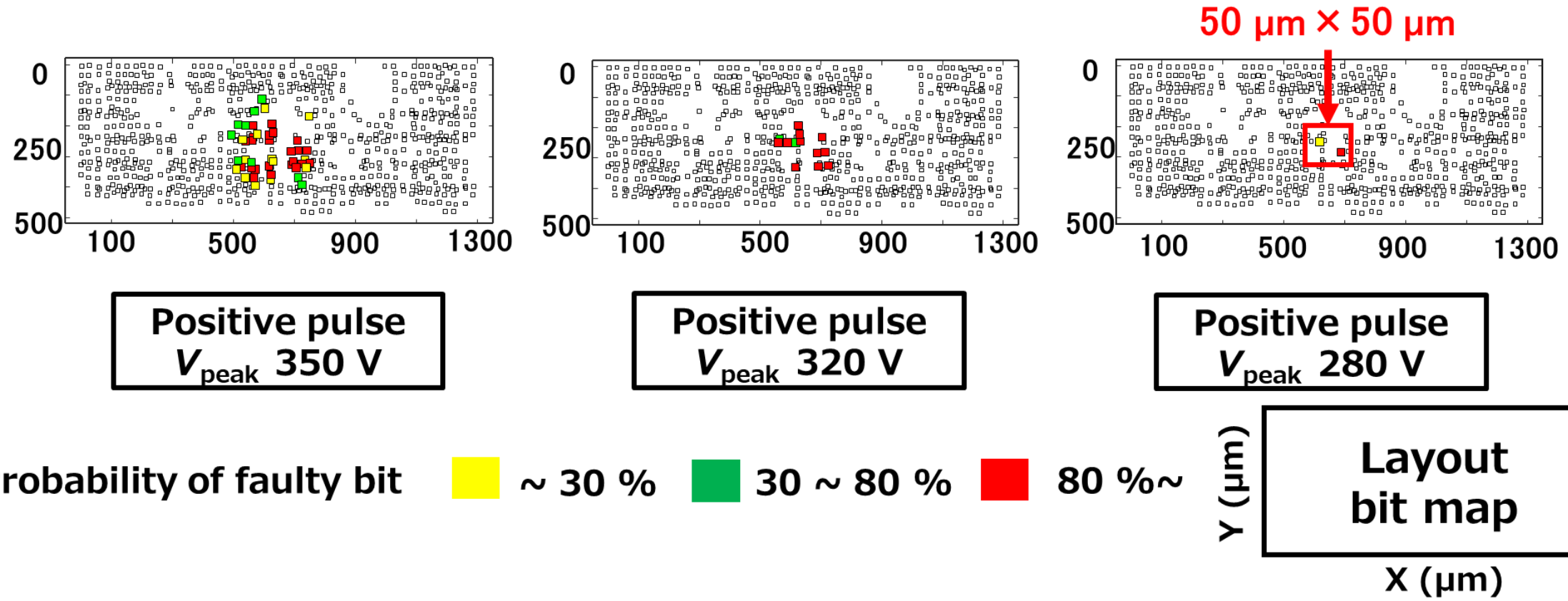




Controllability of localization by V_{peak}

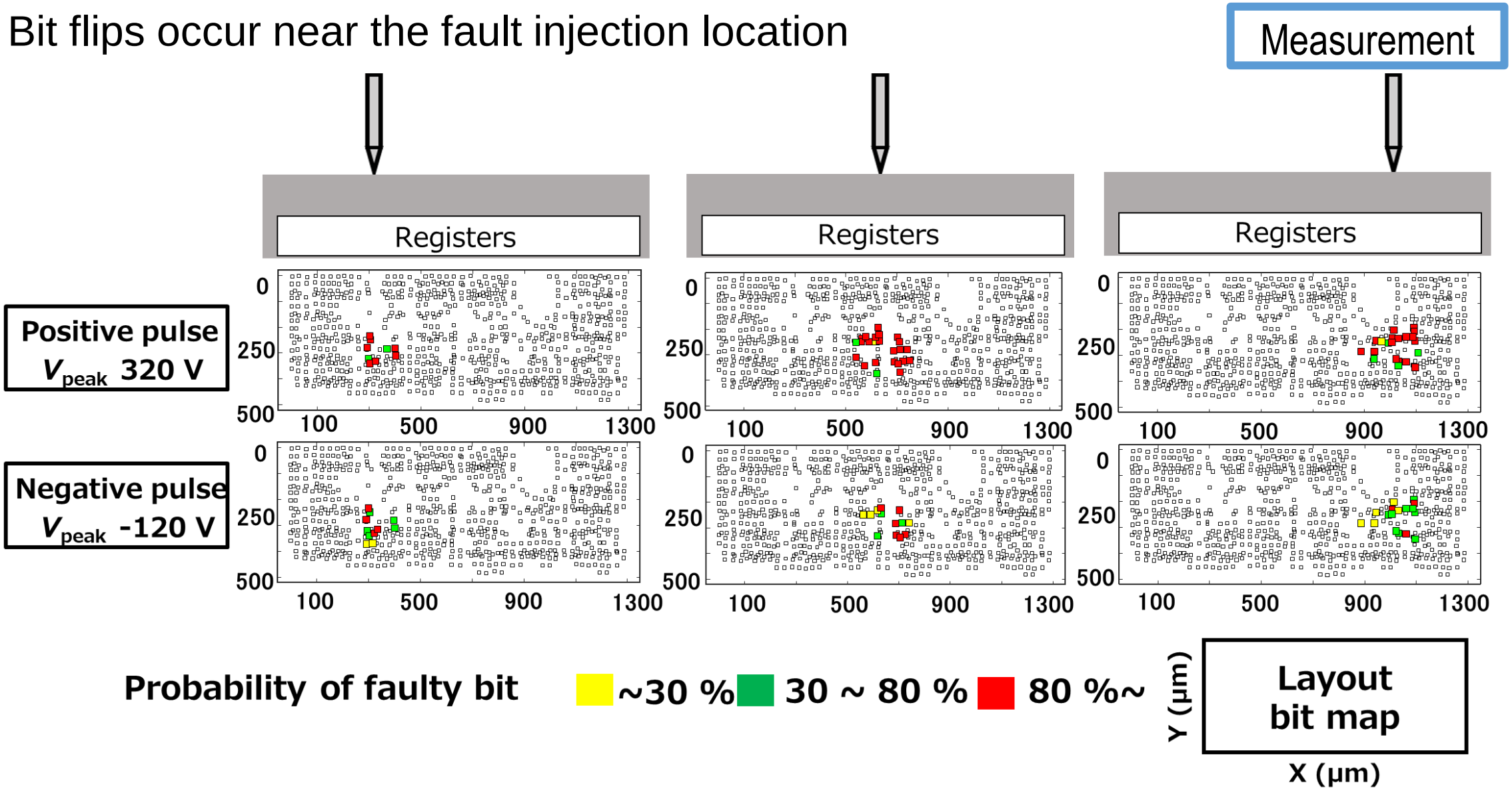
- The area of impact can be controlled by V_{peak}

Measurement



Controllability of Fault Injection Location

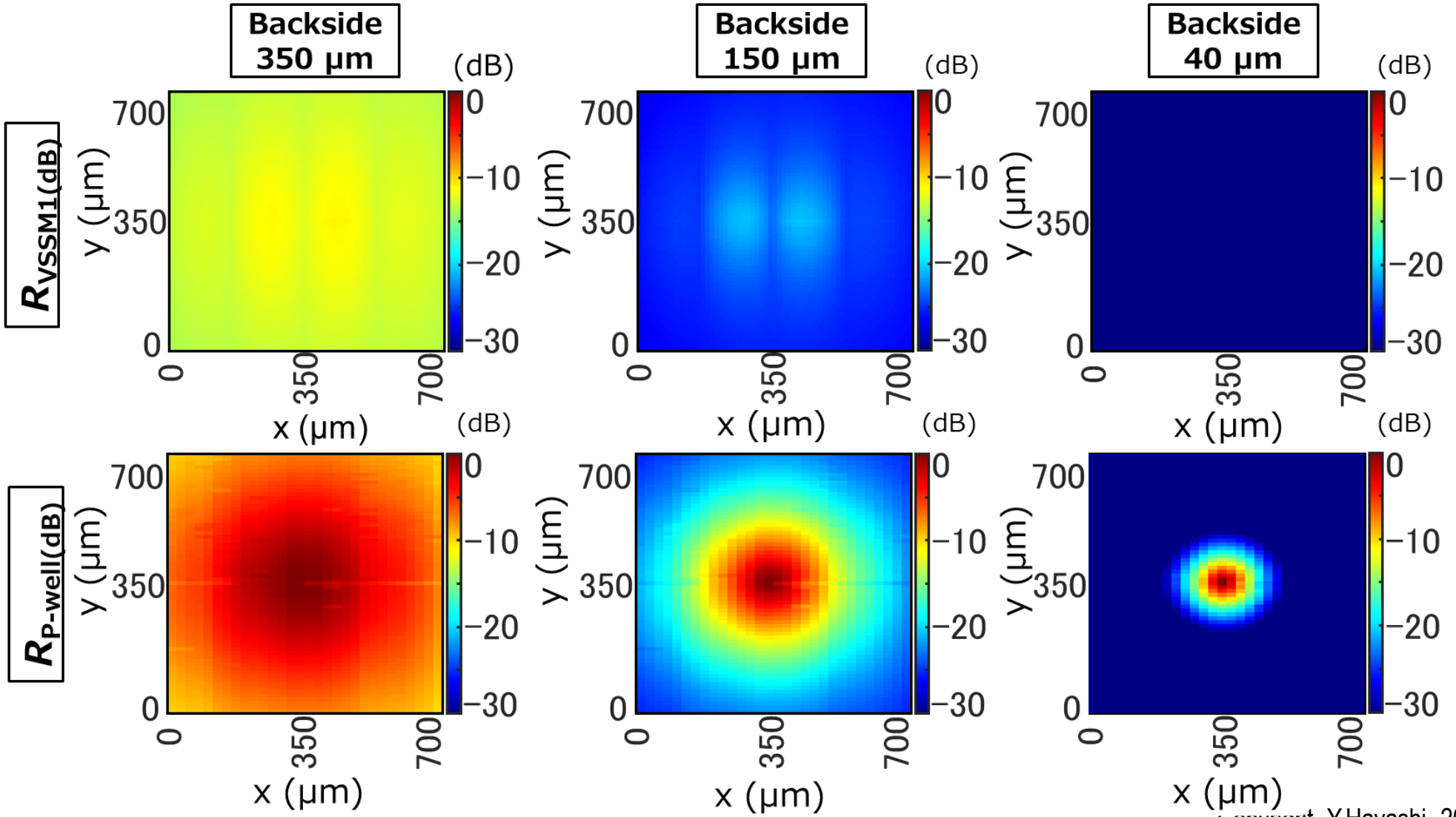
- Bit flips occur near the fault injection location



Localization by Si-substrate thickness

- Thinner Si-substrate thicknesses are more localized

Simulation

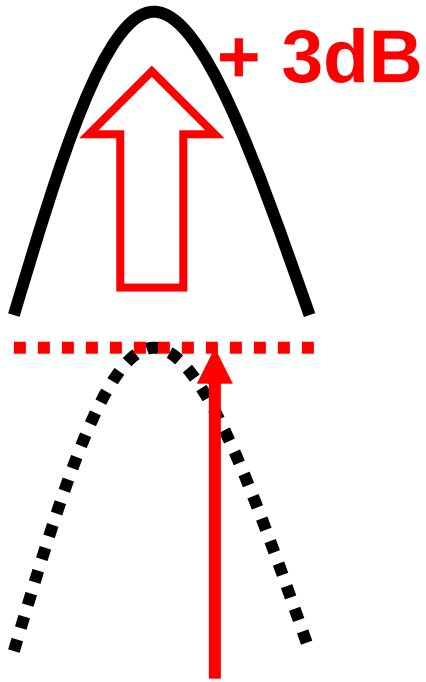


Attackability vs. Si-substrate thickness

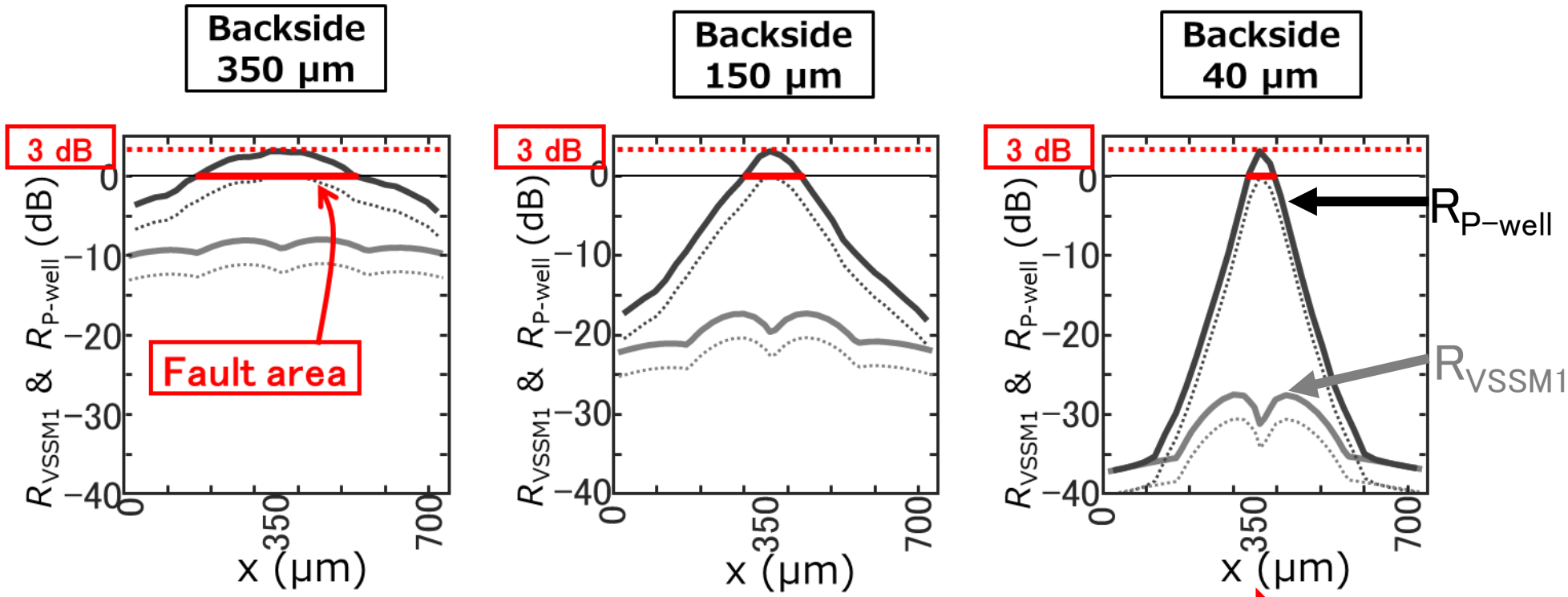
- The localization of faults increases as the Si-substrate becomes thinner

Simulation

  - ✓ It facilitates fault analysis such as DFA



Minimum voltage to cause fault



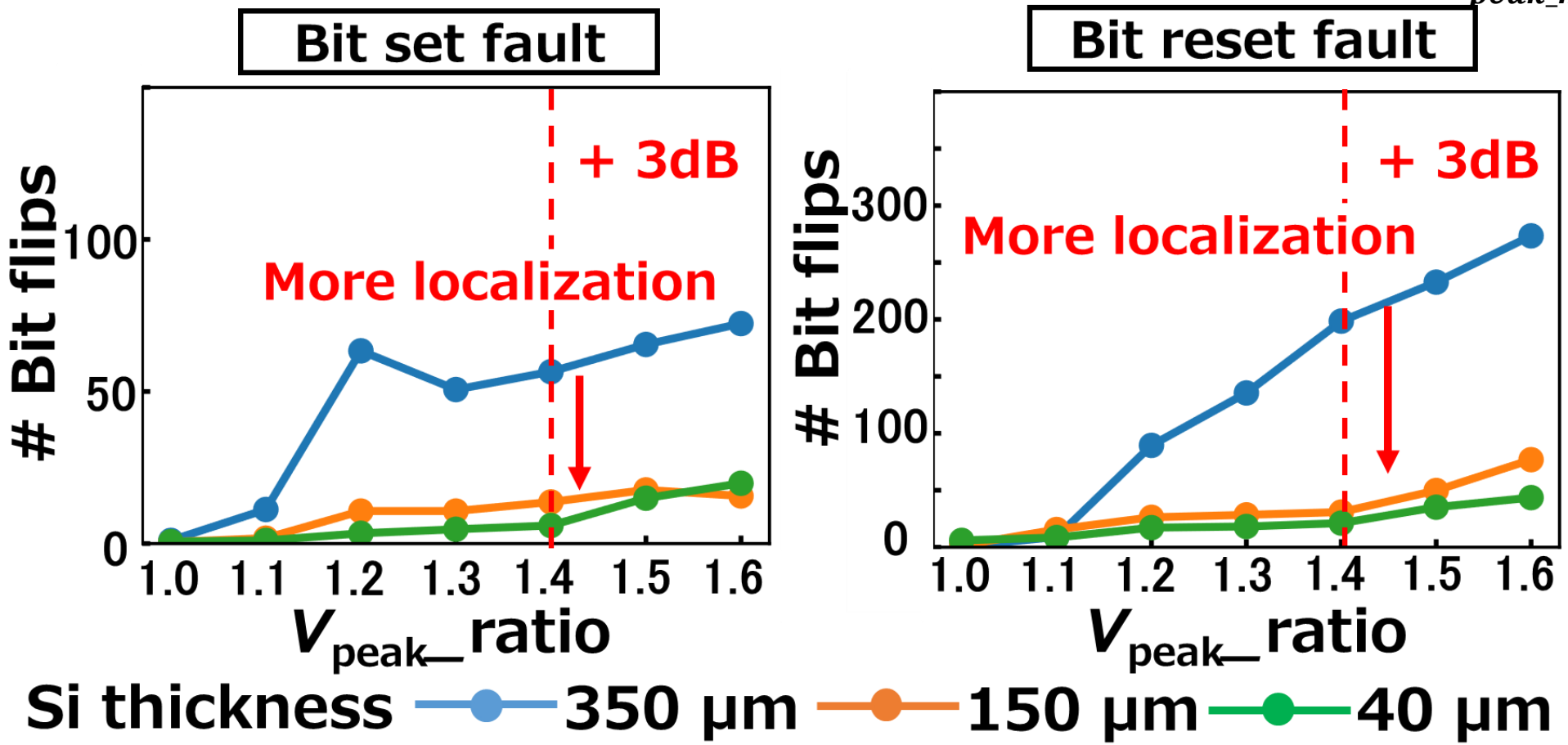
Fault area is more localized as Si-substrate get thinned

Attackability vs. Si-substrate thickness

- Thinner Si-substrate thicknesses are less sensibility

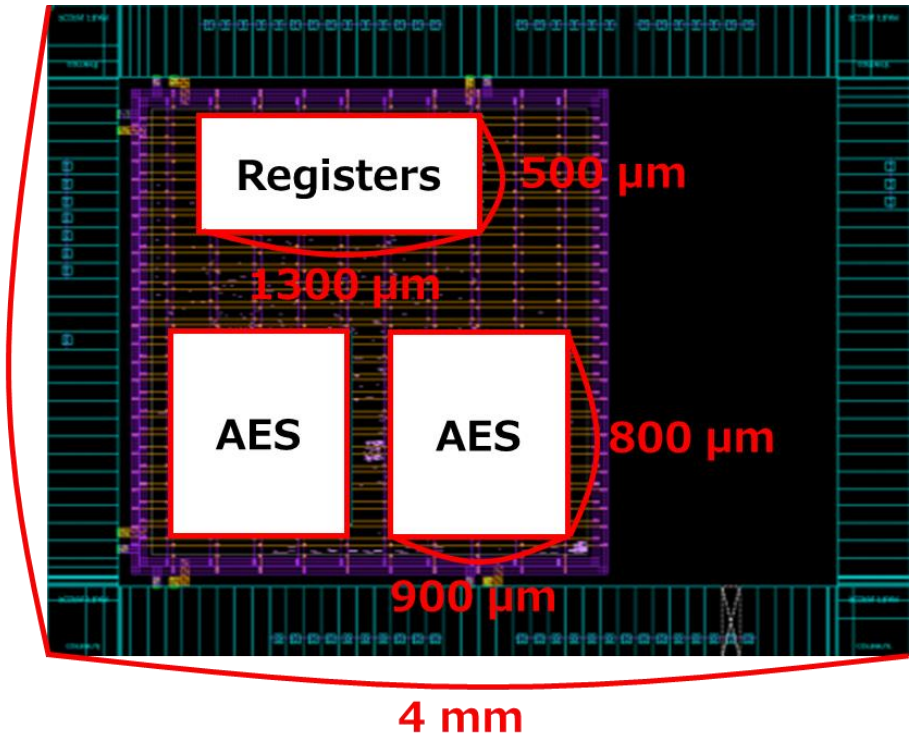
Measurement

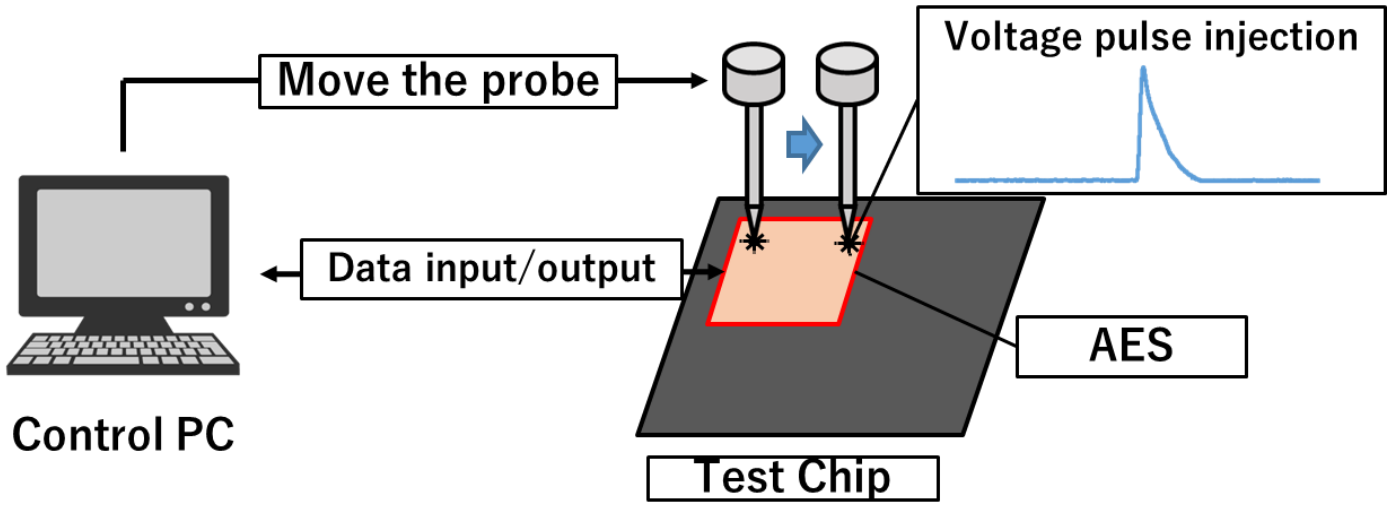
$$V_{peak\_ratio} = \frac{V_{peak}}{V_{peak\_min\_fault}}$$



DFA on AES using Si backside HVP

- HVP is injected in the 9th round of AES operation
- AES
  - ✓ The operation frequency: 10MHz
- The faulty ciphertexts are analyzed to extract a secret key

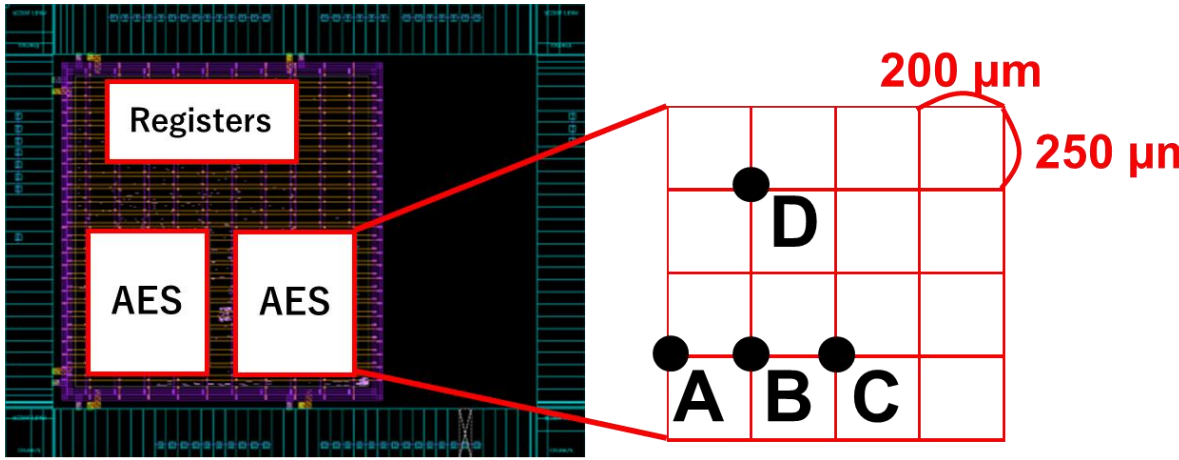




DFA on AES using Si backside HVP

- 4 byte fault ciphertext can be obtained at 4 points

- **Possible to derive secret keys by DFA**
  - ✓ **Positive pulse : 320V**
  - ✓ **Negative pulse : -120V**



A

C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}

B

C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}

C

C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}

D

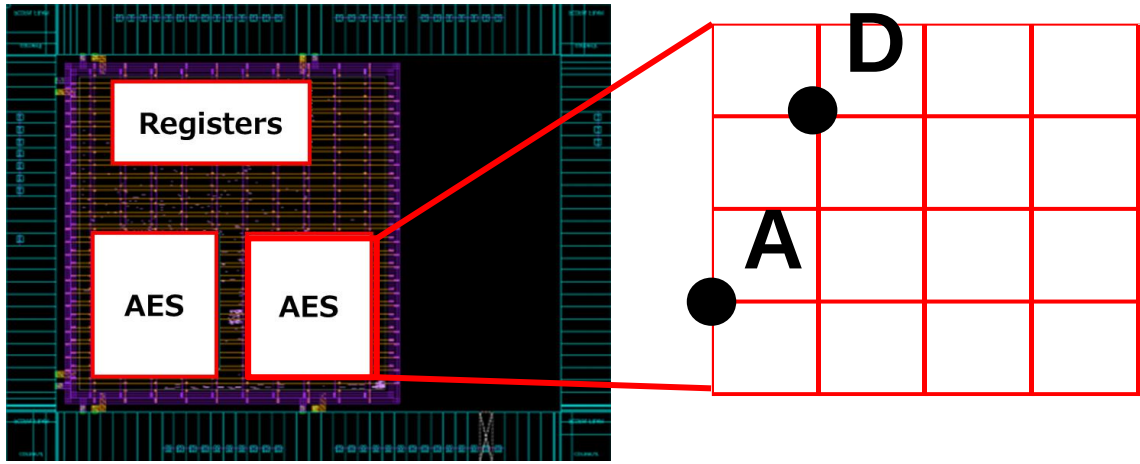
C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}

Output of faulty ciphertext

Faulty byte

Faulty bytes by V_{peak}

- V_{peak} : 320V→370V
  - ✓ Fault occurs in 8 bytes at point A
  - ✓ Fault occurs in 5 bytes at point D



A

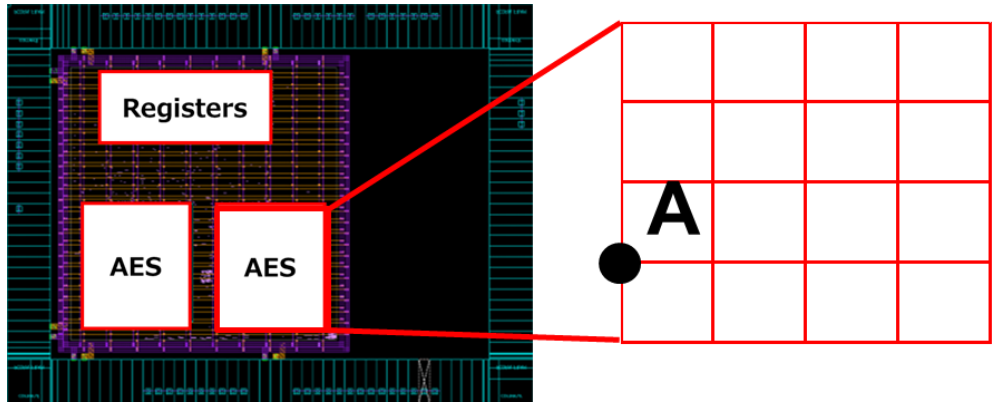
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}
C_4	C_8	C_{12}	C_{16}

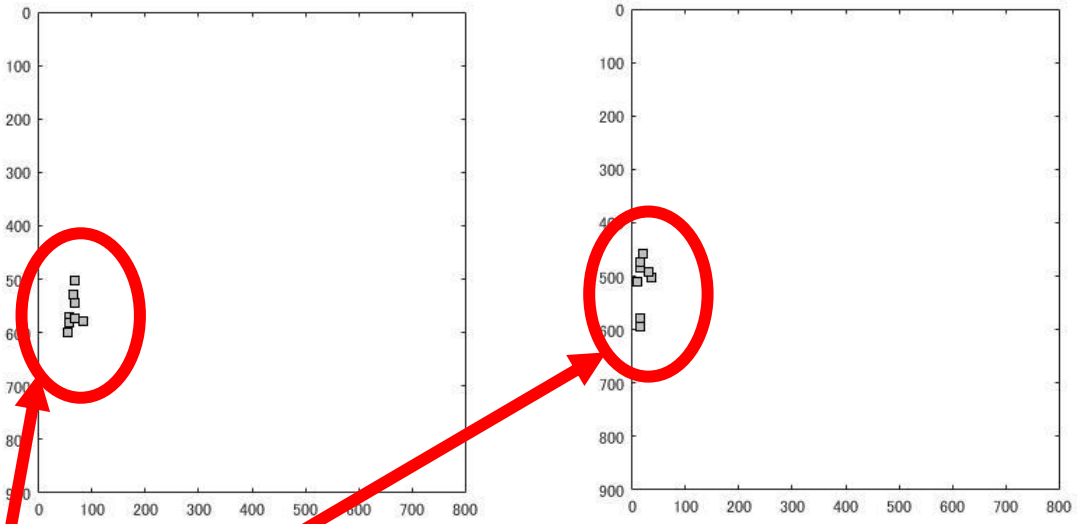
D

C_0	C_4	C_8	C_{12}
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}

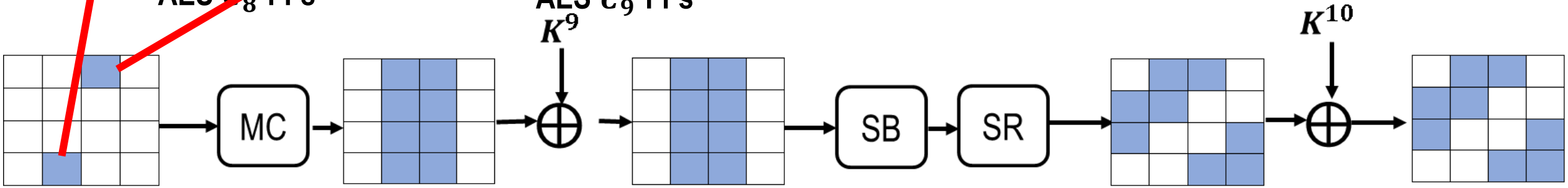
Faulty ciphertext at point A

- Possible to attack 2 bytes at the same time





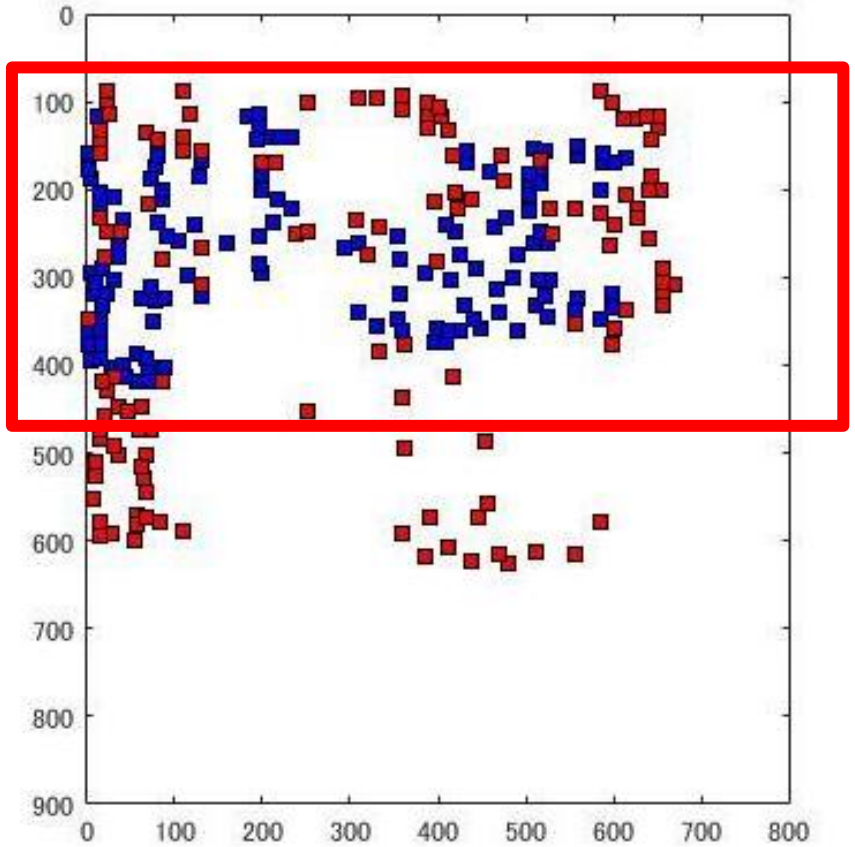
C_1	C_5	C_9	C_{13}
C_2	C_6	C_{10}	C_{14}
C_3	C_7	C_{11}	C_{15}
C_4	C_8	C_{12}	C_{16}

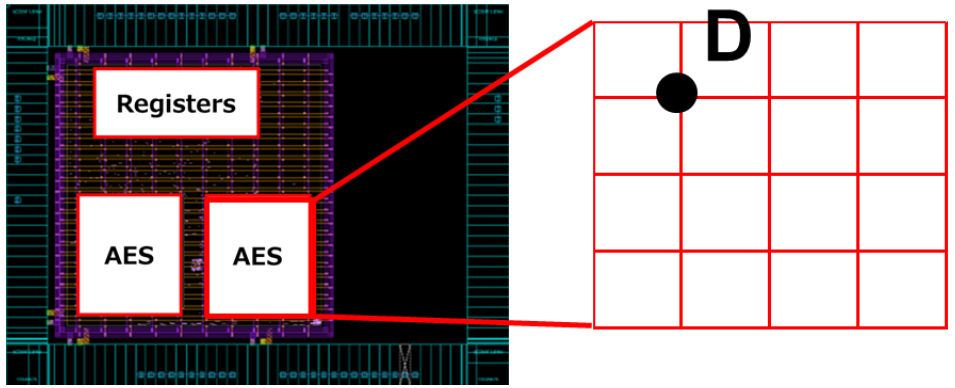


Fault propagation process

Faulty ciphertext at point D

- Difficult to obtain analyzable fault ciphertext





The FFs storing the round key

The FFs storing the round output data

Future works

- Understanding the principle of bit-flip is necessary
  - ✓ The principle of bit flipping with HVP with positive is examined
    - T. Wadatsumi *et al*., "Chip-Backside Vulnerability to Intentional Electromagnetic Interference in Integrated Circuits," in *IEEE Transactions on Electromagnetic Compatibility*, doi: 10.1109/TEMC.2024.3440919.
  - ✓ Understanding of the principles for HVP with negative pulses is also necessary.
- Methods to counter HVP will also be devised

Conclusion

- Ability of Si backside HVP to precisely target local circuits
  - ✓ It can control the location and area of fault
  - ✓ Thinner Si-substrate thicknesses are more localized.
    - – It could be a serious threat as IC chips become thinner
- DFA on AES using Si backside HVP injection
  - ✓ It is possible to derive secret keys by DFA

This work has been supported by JSPS KAKENHI Grant No. JP22H04999 and by SECOM Science and Technology Foundation

