On the application of Two-Photon Absorption for Laser Fault Injection attacks

Pushing the physical boundaries of Laser-based Fault Injection
Bodo Selmke, Maximilian Pollanka, Andreas Duensing, Emanuele Strieder, Hayden Wen, Michael Mittermair, Reinhard Kienberger, Georg Sigl, September 18, 2022
Introduction

Laser Fault Injection (LFI)

- Laser-systems are the most precise method for fault injection
  - High temporal precision (pulse lengths of a few nano-seconds allow targeting individual clock cycles)
  - High spatial precision (spot-sizes of approx. 1 µm)
  - High repeatability (diode-lasers offer pulse repetition rates of in the MHz-range)
  - Multi-beam fault injections (attacking redundant implementations)
Introduction

Limitations and challenges in LFI

Device access

- Backside (silicon substrate) access required
- Fault injection from frontside hardly possible due to reflection from the metal layers
- However, in practice backside not always easily accessible (e.g. BGA package)
Introduction

Limitations and challenges in LFI

Device preparation

- Package removal required
- Thinning of silicon substrate may be required to reduce device stress and loss of energy
  - Requires specialized equipment
  - Time consuming
  - Bears risk of cracking the die
  - Might be detected by countermeasures
Introduction

Limitations and challenges in LFI

Spot size physically limited

- $d_{\text{spot}} \propto \lambda \cdot f/d$
- Wavelength fixed in the near infrared range for sufficient penetration depth
- Ratio of focus distance to objective diameter $f/d$ limited due to practical reasons
- Typically, for 1064 nm lasers, spot sizes down to 1 $\mu$m achievable
- However feature sizes of modern technology nodes still decreasing...
  - On a 90 nm technology node, precise control over single bit faults feasible
  - Not at 10 nm...
Introduction

Pushing the physical boundaries of LFI

Can laser-based fault injection be further improved?

- Better precision?
- Lower requirements for device preparation?
- Harder to detect?
Introduction

Pushing the physical boundaries of LFI

Can laser-based fault injection be further improved?

- Better precision?
- Lower requirements for device preparation?
- Harder to detect?

... actually yes!
Laser silicon interaction

Single Photon Absorption (SPA)

- Energy [eV]
- CB
- VB
- Electron: λ < 1110 nm
- Hole

Two-Photon Absorption (TPA)

- Energy [eV]
- CB
- VB
- Electron
- Hole
- Virtual Intermediate State

Bandgap at room temperature ≈ 1.12 eV

Electron hole pair is generated

Not possible for λ > 1110 nm

Absorption coefficient [cm⁻¹]
- no backside LFI
- SPA LFI
- TPA LFI

Beam waist
- SPA response
- TPA response

Penetration depth [m]

Trade-off problem

Solution: Two Photon Absorption (TPA-LFI)
Laser silicon interaction

Single Photon Absorption (SPA)

- Bandgap at room temperature $\approx 1.12 \text{ eV}$

---

A trade-off problem is addressed.

Solution: Two Photon Absorption (TPA-LFI)
Laser silicon interaction

Single Photon Absorption (SPA)

- Bandgap at room temperature $\approx 1.12$ eV
- $E_{ph} \geq 1.12$ eV ($\lambda \leq 1110$ nm) excitation of electron from VB into CB
- Electron hole pair is generated
Laser silicon interaction

Single Photon Absorption (SPA)

- Bandgap at room temperature \( \approx 1.12 \text{ eV} \)
- \( E_{ph} \geq 1.12 \text{ eV} (\lambda \leq 1110 \text{ nm}) \) excitation of electron from VB into CB
- Electron hole pair is generated
- Not possible for \( \lambda > 1110 \text{ nm} \)
Laser silicon interaction

Single Photon Absorption (SPA)

- Bandgap at room temperature $\approx 1.12 \text{ eV}$
- $E_{ph} \geq 1.12 \text{ eV} (\lambda \leq 1110 \text{ nm})$ excitation of electron from VB into CB
- Electron hole pair is generated
- Not possible for $\lambda > 1110 \text{ nm}$

- Trade-off problem
- Solution: Two Photon Absorption

TPA-LFI | BS, MP, AD, ES, HW, MM, RK, GS | September 18, 2022 | PUBLIC

© Fraunhofer
Laser silicon interaction

Two-Photon Absorption (TPA)

Energy [eV]

CB
VB
Hole
Electron

< 1110nm
< 2220nm

a) Two-Photon Absorption (TPA)
   
   Virtual Intermediate State

b) Single-Photon Absorption (SPA)
   
   Virtual State

# Two-Photon Absorption (TPA)

- First photon: elevates electron from VB into virtual intermediate state
- Second photon: elevates electron further into CB
- Electron hole pair is formed
- Lifetime virtual intermediate state: \( \Delta t \geq \frac{\hbar}{4\pi \Delta E} \) (silicon: \( \sim 10^{-15} \) s)

- Low probability increased by high peak laser intensities

TPA-LFI | BS, MP, AD, ES, HW, MM, RK, GS | September 18, 2022 | PUBLIC
© Fraunhofer
Laser silicon interaction

Two-Photon Absorption (TPA)

\[ E_{ph,1} + E_{ph,2} \geq 1.12 \text{ eV} \]
\[ \rightarrow \text{ simultaneous absorption of two photons} \]

- First photon: elevates electron from VB into virtual intermediate state
- Second photon: elevates electron further into CB
- Electron hole pair is formed
- Lifetime virtual intermediate state: \[ \Delta t \geq \frac{\hbar}{4\pi \Delta E} \] (silicon: \[ \sim 10^{-15} \text{ s} \])
- Low probability increased by high peak laser intensities → increasing amount of photons

TPA-LFI | BS, MP, AD, ES, HW, MM, RK, GS | September 18, 2022 | PUBLIC

© Fraunhofer
Laser silicon interaction

Two-Photon Absorption (TPA)

- $E_{ph,1} + E_{ph,2} \geq 1.12 \text{ eV}$
  - $\rightarrow$ simultaneous absorption of two photons
- **first photon**: elevates electron from VB into virtual intermediate state
- **second photon**: elevates electron further into CB
- Electron hole pair is formed

$\lambda < 2220 \text{ nm}$
Laser silicon interaction

Two-Photon Absorption (TPA)

- \[ E_{ph,1} + E_{ph,2} \geq 1.12 \text{ eV} \]
  \( \rightarrow \) simultaneous absorption of two photons

- **first photon**: elevates electron from VB into virtual intermediate state

- **second photon**: elevates electron further into CB

- Electron hole pair is formed

- Lifetime virtual intermediate state: \( \Delta t \geq \frac{h}{4\pi \Delta E} \)
  (silicon: \( \sim 10^{-15} \text{ s} \))

\[ \begin{align*}
\text{CB} & \quad \text{VB} \\
\downarrow & \quad \downarrow \\
\text{Hole} & \quad \text{Electron}
\end{align*} \]
Laser silicon interaction

Two-Photon Absorption (TPA)

- $E_{ph,1} + E_{ph,2} \geq 1.12 \text{ eV}$
  - simultaneous absorption of two photons

- **first photon**: elevates electron from VB into virtual intermediate state

- **second photon**: elevates electron further into CB

- Electron hole pair is formed

- Lifetime virtual intermediate state: $\Delta t \geq \frac{h}{4\pi \Delta E}$
  (silicon: $\sim 10^{-15} \text{ s}$)

- Low probability increased by high peak laser intensities
  → increasing amount of photons
Laser silicon interaction

Theoretical background: SPA vs TPA

SPA

- Linear relation (Beer's law)
  \[ \frac{dI(z)}{dz} = -\alpha \lambda I(z) \]
  - Absorption rate proportional to \( I(z) \)

\[ I(z) = I_0 e^{-\alpha \lambda z} \]
  - Exponential decay of intensity

TPA

- Nonlinear relation
  \[ \frac{dI(z)}{dz} = -\beta I(z)^2 \]
  - Absorption rate proportional to \( I(z)^2 \)

\[ I(z) = I_0 (1 + I_0 \beta z) \]
  - Intensity dependence of \( z \)
Laser silicon interaction

Theoretical background: SPA vs TPA

**SPA**
- \[ I < 1 \times 10^6 \, \text{W cm}^{-2} \]
  \[ \rightarrow \text{linear relation (Beer’s law)} \]
- \[ \frac{dl(z)}{dz} = -\alpha \lambda I(z) \]
- Absorption rate prop. to \( I(z) \)

**TPA**
- \[ I > 1 \times 10^6 \, \text{W cm}^{-2} \]
  \[ \rightarrow \text{nonlinear relation} \]
- \[ \frac{dl(z)}{dz} = -\beta I(z)^2 \]
- Absorption rate prop. to \( I(z)^2 \)
- Intensity dependence of \( z \)
Laser silicon interaction

Theoretical background: SPA vs TPA

**SPA**
- \( I < 1 \times 10^6 \text{ W cm}^{-2} \)
  \( \rightarrow \) linear relation (Beer’s law)
- \( \frac{dl(z)}{dz} = -\alpha \lambda I(z) \)
- Absorption rate prop. to \( I(z) \)
- \( I(z) = I_0 e^{-\alpha \lambda z} \)
  - Exp. decay of intensity

**TPA**
- \( I > 1 \times 10^6 \text{ W cm}^{-2} \)
  \( \rightarrow \) nonlinear relation
- \( \frac{dl(z)}{dz} = -\beta I(z)^2 \)
- Absorption rate prop. to \( I(z)^2 \)
- \( I(z) = I_0 + I_0 \beta z \)
  - Intensity dependence of \( z \)
Laser silicon interaction

Theoretical background: SPA vs TPA

**SPA**
- \( I < 1 \times 10^6 \text{ W cm}^{-2} \)
  - \( \rightarrow \) linear relation (Beer’s law)

\[
\frac{dI(z)}{dz} = -\alpha \chi I(z)
\]

- Absorption rate prop. to \( I(z) \)

\[
I(z) = I_0 e^{-\alpha \chi z}
\]

- Exp. decay of intensity

**TPA**
- \( I > 1 \times 10^6 \text{ W cm}^{-2} \)
  - \( \rightarrow \) nonlinear relation

\[
\frac{dI(z)}{dz} = -\beta I(z)^2
\]

- Absorption rate prop. to \( I(z)^2 \)
Laser silicon interaction

Theoretical background: SPA vs TPA

**SPA**

- \( I < 1 \times 10^6 \text{ W cm}^{-2} \)
  \[ \rightarrow \text{linear relation (Beer’s law)} \]

- \( \frac{dl(z)}{dz} = -\alpha \lambda I(z) \)

- Absorption rate prop. to \( I(z) \)

- \( I(z) = I_0 e^{-\alpha \lambda z} \)

- Exp. decay of intensity

**TPA**

- \( I > 1 \times 10^6 \text{ W cm}^{-2} \)
  \[ \rightarrow \text{nonlinear relation} \]

- \( \frac{dl(z)}{dz} = -\beta I(z)^2 \)

- Absorption rate prop. to \( I(z)^2 \)

- \( I(z) = \frac{I_0}{1 + I_0 \beta z} \)

- Intensity dependence of \( z \)
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

Total absorption:

\[
\frac{dl(z)}{dz} = -\alpha l(z) - \beta l(z)^2
\]

SPA \quad \text{TPA}

Electron hole pair generation rate:

\[
G(z) = \frac{dN(z)}{dt} = \alpha I(z) h \nu - \beta I(z)^2 h \nu
\]

SPA \quad \text{TPA}

High peak intensities and \( \lambda > 1110 \text{ nm} \) → SPA can be neglected

Generated electron hole pairs:

\[
N_2^P(z) = \beta^2 h \nu \int_{-\infty}^{\infty} I(z, t)^2 \, dt
\]

Nonlinear model only valid for high intensities achieved by ultrashort laser pulses
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

Total absorption:

\[
\frac{dl(z)}{dz} = -\alpha l(z) - \beta l(z)^2
\]

SPA

TPA

Electron hole pair generation rate:

\[
G(z) = \frac{dN(z)}{dt} = \frac{\alpha l(z)}{h\nu} + \frac{\beta l(z)^2}{2h\nu}
\]

SPA

TPA

High peak intensities and \(\lambda > 1110\) nm → SPA can be neglected

Generated electron hole pairs:

\[
N_2P(z) = \beta \frac{2}{h\nu} \int_{-\infty}^{\infty} I(z, t) dt
\]

Nonlinear model only valid for high intensities achieved by ultrashort laser pulses
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

**Total absorption:**

\[
\frac{dl(z)}{dz} = -\alpha l(z) - \beta l(z)^2
\]

- SPA
- TPA

**Electron hole pair generation rate:**

\[
G(z) = \frac{dN(z)}{dt} = \frac{\alpha l(z)}{h\nu} + \frac{\beta l(z)^2}{2h\nu}
\]

- SPA
- TPA

- High peak intensities and \( \lambda > 1110 \) nm → SPA can be neglected
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

**Total absorption:**

\[
\frac{dI(z)}{dz} = -\alpha I(z) - \beta I(z)^2
\]

SPA TPA

**Electron hole pair generation rate:**

\[
G(z) = \frac{dN(z)}{dt} = \frac{\alpha I(z)}{h\nu} + \frac{\beta I(z)^2}{2h\nu}
\]

SPA TPA

- High peak intensities and \( \lambda > 1110 \text{ nm} \) → SPA can be neglected

**Generated electron hole pairs:**

\[
N_{2P}(z) = \frac{\beta}{2h\nu} \int_{-\infty}^{\infty} I(z, t)^2 \, dt
\]
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

Total absorption:

$$\frac{dl(z)}{dz} = -\alpha l(z) - \beta l(z)^2$$

- SPA
- TPA

Electron hole pair generation rate:

$$G(z) = \frac{dN(z)}{dt} = \frac{\alpha l(z)}{h\nu} + \frac{\beta l(z)^2}{2h\nu}$$

- SPA
- TPA

- High peak intensities and $\lambda > 1110$ nm → SPA can be neglected

Generated electron hole pairs:

$$N_{2P}(z) = \frac{\beta}{2h\nu} \int_{-\infty}^{\infty} I(z, t)^2 dt$$

- Nonlinear model only valid for high intensities achieved by ultrashort laser pulses
Two-Photon Absorption

Application and advantages

Three major advantages of TPA in comparison to SPA:

1. Transparency of silicon within wavelength region of TPA
2. Focal width: Nonlinear response below Abbe defraction limit
3. Selective excitation referred to material depth
Two-Photon Absorption
Application and advantages

Simulation of generated charge carriers

- Focal plane set inside the DUT at $z = 70 \mu m$
- Focal parameters and power chosen equally for all three wavelengths
- Different wavelengths and pulse durations
- Pulses described by gaussian beam shape
- Generated charge carrier density $N$ dependant on wavelength and material depth $z$
Two-Photon Absorption
Application and advantages

1. Transparency

- 800 nm: High intensity losses near air-silicon interface
- 2000 nm: Perfectly located spot at target depth
- No need for substrate thinning, no risk of loss or damage due to thermal effects or thinning
Two-Photon Absorption

Application and advantages

1. Transparency

- 800 nm: High intensity losses near air-silicon interface
- 2000 nm: Perfectly located spot at target depth
Two-Photon Absorption

Application and advantages

1. Transparency

- 800 nm: High intensity losses near air-silicon interface
- 2000 nm: Perfectly located spot at target depth
- No need for substrate thinning, no risk of loss or damage due to thermal effects or thinning
Two-Photon Absorption

Application and advantages

1. Transparency ($\alpha \to 0$) ✓

2. Focal width/nonlinear response
   - 1064 nm: $N_{SPA} \sim 6N_{TPA}$
     → Charge carriers all along beam path
   - 2000 nm: $w_{TPA} = \frac{1}{\sqrt{2}} w_{SPA}$
     → Symmetric focal spot and localized excitation
Two-Photon Absorption

Application and advantages

1. Transparency ($\alpha \rightarrow 0$) ✓

2. Focal width ($w_{TPA} = \frac{1}{\sqrt{2}} w_{SPA}$) ✓

3. Precise excitation
   - 1064 nm: Broadened, uneven gaussian distribution of $N$ (FWHM $\approx 40$ µm)
   - 2000 nm: $N \sim I^2$
     → Sharp excitation, evenly gaussian distribution (FWHM $\approx 15$ µm)
Two-Photon Absorption
Application and advantages

1. Transparency ($\alpha \rightarrow 0$) ✓

2. Focal width ($w_{TPA} = \frac{1}{\sqrt{2}} w_{SPA}$) ✓

3. Precise excitation ($N \sim I^2$) ✓
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

FS: fused silica wedges
A: aperture
CM: focusing mirror
CW, S: chopper wheel, shutter
BBO: nonlinear crystal
Ge: Germanium filter
FS: fused silica plate
RO: reflective focusing objective
DUT: device under test

\[ \lambda_c = 690 \text{ nm} \]
\[ \Delta \tau = 5 \text{ fs} \]

\[ \lambda_c = 2000 \text{ nm} \]
\[ \Delta \tau = 10 \text{ fs} \]
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture
- CM: focusing mirror
- CW, S: chopper wheel, shutter

\[ \lambda_c = 690 \text{ nm} \]
\[ \Delta T = 5 \text{ fs} \]

\[ \lambda_c = 2000 \text{ nm} \]
\[ \Delta T = 10 \text{ fs} \]
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture
- CM: focusing mirror
- CW, S: chopper wheel, shutter
- BBO: nonlinear crystal
- Ge: Germanium filter
- FS: fused silica plate
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture
- CM: focusing mirror
- CW, S: chopper wheel, shutter
- BBO: nonlinear crystal
- Ge: Germanium filter
- FS: fused silica plate
- RO: reflective focusing objective

\[ \lambda_c = 690 \text{ nm} \quad \Delta \tau = 5 \text{ fs} \]

\[ \lambda_c = 2000 \text{ nm} \quad \Delta \tau = 10 \text{ fs} \]
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture
- CM: focusing mirror
- CW, S: chopper wheel, shutter
- BBO: nonlinear crystal
- Ge: Germanium filter
- FS: fused silica plate
- RO: reflective focusing objective
- DUT: device under test

\[ \lambda_c = 690 \text{ nm} \]
\[ \Delta \tau = 5 \text{ fs} \]

\[ \lambda_c = 2000 \text{ nm} \]
\[ \Delta \tau = 10 \text{ fs} \]
Experimental Setup

Two Photon Absorption – Nonlinear laser fault injection

| Parameter on DUT       | TPA       | SPA       |
|------------------------|-----------|-----------|
| Center wavelength      | 2000 nm   | 1064 nm   |
| Average Power          | 30 $\mu$W | 1 $\mu$W  |
| Single pulse energy    | 7.5 nJ    | 1 nJ      |
| Focal width            | 10 $\mu$m  | 4 $\mu$m  |
| Pulse duration         | 10 fs     | 800 ps    |
Practical experiments

1. Demonstration of general functioning and investigation of precision
   - Infineon XMC1401 (Arm Cortex M0)
   - 65 nm technology node

2. Investigation of latch-up susceptible microcontroller
   - NXP LPC11E14 (Arm Cortex M0)
   - 140 nm technology node
Practical experiments

Precision test on Infineon XMC1401

- Scanning of a part of the on-chip SRAM with fixed step size
  
  *For technical reasons differing step sizes: 350 nm (TPA) and 200 nm (SPA)*

- 20 shots per location

|          | Min. | Max. | Avg.  |
|----------|------|------|-------|
| SPA      | 5%   | 30%  | 8%    |
| TPA      | 10%  | 50%  | 15.4% |

Table: Summary of overall single-bit fault probabilities XMC chip
Practical experiments

Precision test on Infineon XMC1401

- Scanning of a part of the on-chip SRAM with fixed step size
  
  *For technical reasons differing step sizes: 350 nm (TPA) and 200 nm (SPA)*

- 20 shots per location

- TPA performs significantly better than SPA, despite larger spot size!

|       | Min. | Max. | Avg. |
|-------|------|------|------|
| SPA   | 5 %  | 30 % | 8 %  |
| TPA   | 10 % | 50 % | 15.4 % |

*Table: Summary of overall single-bit fault probabilities XMC chip*
Practical experiments

Conventional 1064 nm laser system

- Experiment with the conventional 1064 nm laser setup
- Target: *NXP LPC11E14* ARM Cortex M0 microcontroller
- Laser scan and evaluation for faults in on-chip SRAM
Practical experiments

Conventional 1064 nm laser system

- Experiment with the conventional 1064 nm laser setup
- Target: NXP LPC11E14 ARM Cortex M0 microcontroller
- Laser scan and evaluation for faults in on-chip SRAM
- **No fault injection feasible**
  - Chip reacts with hard reset once SRAM area is targeted
  - Brown-out detection reacts on induced latch-up
Practical experiments

Latch-up mechanism in CMOS inverter
Practical experiments

Femtosecond 2000 nm laser system

- Testing the same chip with the femtosecond laser
- Detailed scan at locations 1 and 2
Practical experiments

Femtosecond 2000 nm laser system

- Testing the same chip with the femtosecond laser
- Detailed scan at locations 1 and 2
- **Fault injection feasible**
  - Charges localized at the relevant pn-junction for fault injection
  - Drastically reduced charge carrier density in substrate
Impact on countermeasures

- Redundancy-based countermeasures are agnostic about the fault injection technique
- Sensor-based countermeasures try to detect the fault injection itself

| Countermeasure                  | SPA | TPA |
|---------------------------------|-----|-----|
| Light detectors                 | ✗   | ✓   |
| Latch-Up sensitive design       | ✗   | ✓   |
| Bulk-builtin current sensors    | ✗   | ✗   |
| Ring Oscillators (RO)           | ✗   | ✓   |
| Backside shielding              | ✗   | ✓   |
| Thinning prevention             | ✗   | ✓   |
| Backside coating                | ✗   | ✗   |
Conclusion

- Advantages of Two Photon Absorption in comparison to regular LFI:
  - Charge carrier generation only in the focal point
  - Substrate thickness irrelevant
  - Improved spot size by approx. $1/\sqrt{2}$
- Improves circumventing certain sensor-based countermeasures
- Further research potential concerning the effectiveness on various countermeasures
Thank you for your attention
Contact Information

**Bodo Selmke**

Department Hardware Security  
Fraunhofer-Institute for  
Applied and Integrated Security

Address: Lichtenbergstraße 11  
85748 Garching (near Munich)  
Germany  
Internet: https://www.aisec.fraunhofer.de

Phone: +49 89 3229986-132  
E-Mail: bodo.selmke@aisec.fraunhofer.de

**Maximilian Pollanka**

Chair for Laser and X-Ray Physics  
TUM School of Natural Sciences  
Technical University of Munich

Address: James-Franck-Str. 1  
85748 Garching (near Munich)  
Germany  
Internet: https://www.ph.nat.tum.de/e11

Phone: +49 (89) 289 - 12865  
E-Mail: maximilian.pollanka@tum.de
Backup Slides

Application and advantages of TPA-LFI

1. Transparency:
   - low absorption coefficient $\alpha$ at $\lambda > 1110$ nm $\rightarrow$ no intensity loss
   - no need for substrate thinning
   - minimizes risk of loss or damage due to thermal effects or thinning
1. Transparency ($\alpha \rightarrow 0$) ✓

2. Focal width/nonlinear response:
   - focal spot size below the theoretical resolution limit ($w_{TPA} = \frac{w_{SPA}}{\sqrt{2}}$)
   - $\lambda < 1500 \text{ nm}$: smaller focal width via TPA compared to SPA at $\lambda = 1064 \text{ nm}$
backup slides

Application and advantages of TPA-LFI

1. Transparency ($\alpha \to 0$) ✓

2. Focal width ($w_{TPA} = \frac{w_{SPA}}{\sqrt{2}}$) ✓
Backup Slides

Fault injection mechanism in CMOS inverter