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

- $d_{\text{spot}} \propto \lambda \frac{f}{d}$
- 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 $\text{nm}$ technology node, precise control over single bit faults feasible
  - Not at 10 $\text{nm}$...
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]

Single-Photon Absorption (SPA)

Electron

Hole

λ < 1110nm

1.12 eV

Electron hole pair is generated

Not possible for λ > 1110 nm
Laser silicon interaction

Single Photon Absorption (SPA)

- Bandgap at room temperature $\approx 1.12$ eV
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
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
- Not possible for $\lambda > 1110$ nm

![Diagram showing single-photon absorption (SPA) with energy levels and absorption coefficient vs. wavelength.]

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

- Not possible for $\lambda > 1110$ nm

Trade-off problem

Solution:

Two Photon Absorption
Laser silicon interaction

**Two-Photon Absorption (TPA)**

- **Single-Photon Absorption (SPA)**

  - **Energy [eV]**
  - **CB**
  - **VB**
  - **+**
  - **-**
  - **< 1110nm**
  - **Hole**
  - **Electron**
  - **0**
  - **1.12**

- **Two-Photon Absorption (TPA)**

  - **Energy [eV]**
  - **CB**
  - **VB**
  - **+**
  - **-**
  - **< 2220nm**
  - **Hole**
  - **Electron**
  - **Virtual**
  - **Intermediate State**
  - **0**
  - **1.12**

**Explanation:**

- **First photon:** Elevates electron from VB into a virtual intermediate state.
- **Second photon:** Elevates electron further into CB.
- **Electron hole pair is formed.**

**Lifetime virtual intermediate state:**

\[ \Delta t \geq \frac{\hbar^4}{4 \pi \Delta E} \] (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 | 7 |

© 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

\[ \text{Virtual Intermediate State} \]

\[ \lambda < 2220 \text{nm} \]

\[ \text{Hole} \]

\[ \text{Electron} \]

\[ \text{CB} \]

\[ \text{VB} \]
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

\( \lambda < 2220 \text{nm} \)
**Laser silicon interaction**

**Two-Photon Absorption (TPA)**

- $E_{ph,1} + E_{ph,2} \geq 1.12$ 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: $\sim 10^{-15}$ s)

TPA-LFI | BS, MP, AD, ES, HW, MM, RK, GS | September 18, 2022 | 7 | PUBLIC
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: $\sim 10^{-15}$ s)
- Low probability increased by high peak laser intensities
  → increasing amount of photons
Laser silicon interaction

Theoretical background: SPA vs TPA

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

**TPA**
- $I > 1 \times 10^6 \text{ W cm}^{-2}$ → nonlinear relation
- $dI(z) \, dz = -\beta I(z)^2$
- Absorption rate prop. to $I(z)^2$
- $I(z) = I_0 \left[1 + I_0 \beta z\right]$
Laser silicon interaction

Theoretical background: SPA vs TPA

**SPA**

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

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

- Absorption rate prop. to $l(z)$

**TPA**

- $I > 1 \times 10^6 \text{ W cm}^{-2}$
  - $\rightarrow$ nonlinear relation

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

- 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 \( I(z)^2 \)
- \( I(z) = I_0 \left(1 + \beta z I_0\right)^{-1/\beta} \)
- 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 $I(z)^2$
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 \( I(z)^2 \)
  - \( I(z) = \frac{I_0}{1 + I_0 \beta z} \)
  - Intensity dependence of \( z \)
Laser silicon interaction

Theoretical background: Generation of electron hole pairs

Total absorption:

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

where \(\alpha\) is the linear absorption coefficient, \(\beta\) is the nonlinear absorption coefficient, and \(l(z)\) is the intensity of the laser beam at position \(z\).

Electron hole pair generation rate:

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

for high peak intensities and \(\lambda > 1110\) nm, \(\text{SPA can be neglected}\).

Generated electron hole pairs:

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

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

Theoretical background: Generation of electron hole pairs

Total absorption:

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

Electron hole pair generation rate:

\[
G(z) = \frac{dN(z)}{dt} = \frac{\alpha l(z)}{h\nu} + \frac{\beta l(z)^2}{2h\nu}
\]
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 \( \lambda > 1110 \text{ nm} \)
  \( \rightarrow \) SPA can be neglected
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

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

**Generated electron hole pairs:**

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

**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 \( \lambda > 1110 \text{ nm} \)
→ SPA can be neglected
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 TPA

**Generated electron hole pairs:**

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

**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 \quad TPA

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

- 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:

- Transparency of silicon within wavelength region of TPA
- Focal width: Nonlinear response below Abbe defraction limit
- 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 $z$
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 \((\alpha \rightarrow 0) \checkmark\)

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

3. Precise excitation
   - 1064 nm: Broadened, uneven gaussian distribution of \(N\) (FWHM \(\approx 40 \, \mu m\))
   - 2000 nm: \(N \sim I^2\)
     \(\rightarrow\) Sharp excitation, evenly gaussian distribution (FWHM \(\approx 15 \, \mu m\))
Two-Photon Absorption

Application and advantages

1. Transparency ($\alpha \to 0$) ✓

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

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

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

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges

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

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

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- A: aperture

![Experimental Setup Diagram]

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

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

Two Photon Absorption – Nonlinear laser fault injection

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

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

- FS: fused silica plate
- RO: reflective focusing objective
- DUT: device under test

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

![Diagram of experimental setup]

**Key components:**
- Laser source
- Aperture (A)
- Fused silica wedges (FS)
- Focusing mirror (CM)
- Chopper wheel (CW)
- Shutter (S)
- Nonlinear crystal (BBO)
- Germanium filter (Ge)
- Reflective focusing objective (RO)
- Device under test (DUT)

**Wavelengths and Durations:**
- Laser wavelength ($\lambda_c$) = 690 nm
- Duration ($\Delta\tau$) = 5 fs
- Laser wavelength ($\lambda_c$) = 2000 nm
- Duration ($\Delta\tau$) = 10 fs

**Graph:**
- Intensity vs. Wavelength
- Intensity [arb. u.]
- Wavelength [nm]

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

© Fraunhofer
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

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

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

Two Photon Absorption – Nonlinear laser fault injection

- FS: fused silica wedges
- 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

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

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

TwoPhoton Absorption – Nonlinear laser fault injection

<table>
<thead>
<tr>
<th>Parameter on DUT</th>
<th>TPA</th>
<th>SPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center wavelength</td>
<td>2000 nm</td>
<td>1064 nm</td>
</tr>
<tr>
<td>Average Power</td>
<td>30 µW</td>
<td>1 µW</td>
</tr>
<tr>
<td>Single pulse energy</td>
<td>7.5 nJ</td>
<td>1 nJ</td>
</tr>
<tr>
<td>Focal width</td>
<td>10 µm</td>
<td>4 µm</td>
</tr>
<tr>
<td>Pulse duration</td>
<td>10 fs</td>
<td>800 ps</td>
</tr>
</tbody>
</table>
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
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!

<table>
<thead>
<tr>
<th></th>
<th>Min.</th>
<th>Max.</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPA</td>
<td>5 %</td>
<td>30 %</td>
<td>8 %</td>
</tr>
<tr>
<td>TPA</td>
<td>10 %</td>
<td>50 %</td>
<td>15.4 %</td>
</tr>
</tbody>
</table>

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

![CMOS Inverter Diagram]
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

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>SPA</th>
<th>TPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Light detectors</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Latch-Up sensitive design</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Bulk-builtin current sensors</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Ring Oscillators (RO)</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Backside shielding</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Thinning prevention</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Backside coating</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
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. $\frac{1}{\sqrt{2}}$

- 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
1. Transparency:

- low absorption coefficient $\alpha$ at $\lambda > 1110 \text{ nm} \rightarrow$ no intensity loss
- no need for substrate thinning
- minimizes risk of loss or damage due to thermal effects or thinning
Application and advantages of TPA-LFI

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

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

Application and advantages of TPA-LFI

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

2. Focal width ($w_{TPA} = \frac{w_{SPA}}{\sqrt{2}}$) ✓
Fault injection mechanism in CMOS inverter