Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels

USENIX Security 2023

11th August 2022

Andreas Kogler
TU-Graz

Jonas Juffinger
TU-Graz

Lukas Giner
TU-Graz

Lukas Gerlach
CISPA

Martin Schwarzl
TU-Graz

Michael Schwarz
CISPA

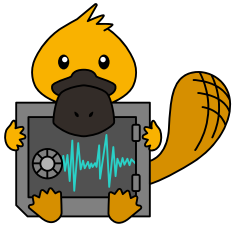
Daniel Gruss
TU-Graz

Stefan Mangard
TU-Graz

Motivation

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

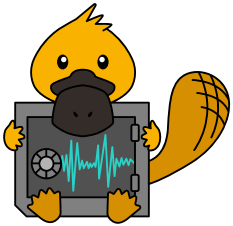
Motivation



Software-based Power Side Channels

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

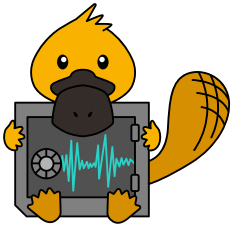


Software-based Power Side Channels

- **Specific** targets: AES

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

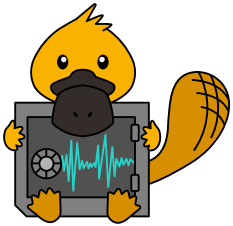


Software-based Power Side Channels

- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation

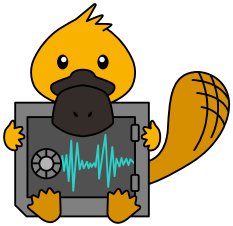


Software-based Power Side Channels

- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation



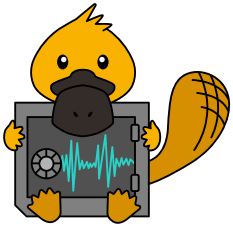
Software-based Power Side Channels

- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Transient Execution Attacks

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation



Software-based Power Side Channels

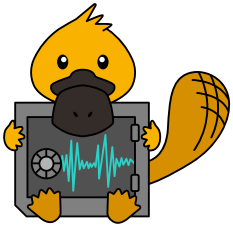
- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Transient Execution Attacks

- **Generic** targets: CPU components

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation



Software-based Power Side Channels

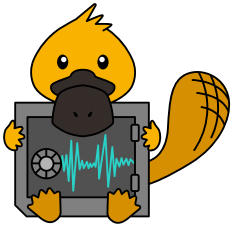
- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Transient Execution Attacks

- **Generic** targets: CPU components
- Leak arbitrary data: Cache content

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation



Software-based Power Side Channels

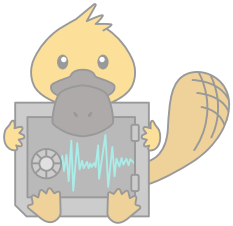
- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Transient Execution Attacks

- **Generic** targets: CPU components
- Leak arbitrary data: Cache content
- **Agnostic** to side channels

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Motivation



Software-based Power Si

- **Specific** targets: AES
- Leak edge cases: RSA, SIKE, KASLR
- **Limited** to a side channels

Execution Attacks

- **Generic** targets: CPU components
- Leak arbitrary data: Cache content
- **Agnostic** to side channels

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

High-Level Idea

Traditional Power Model Components

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Number of set bits

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Number of set bits

$\mathrm{hw}(11_2) = 2$

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Number of set bits

$\mathrm{hw}(11_2) = 2$

Hamming Distance: $\mathrm{hd}(x, y)$

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Number of set bits

$\mathrm{hw}(11_2) = 2$

Hamming Distance: $\mathrm{hd}(x, y)$

Number of different bits

Traditional Power Model Components

Hamming Weight: $\mathrm{hw}(x)$

Number of set bits

$\mathrm{hw}(11_2) = 2$

Hamming Distance: $\mathrm{hd}(x, y)$

Number of different bits

$\mathrm{hd}(11_2, 01_2) = 1$

Collide+Power - Overview

- **Collide+Power** exploits leakage between:

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Overview

- **Collide+Power** exploits leakage between:
  - **Guess $\mathcal{G}$:** Attacker-controlled data

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Overview

- **Collide+Power** exploits leakage between:
  - **Guess** $\mathcal{G}$**:** Attacker-controlled data
  - **Value** $\mathcal{V}$**:** Victim secret data

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Overview

- **Collide+Power** exploits leakage between:
  - **Guess** $\mathcal{G}$**:** Attacker-controlled data
  - **Value** $\mathcal{V}$**:** Victim secret data

Hamming distance: $\mathrm{hd}(\mathcal{G}, \mathcal{V})$

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Overview

- **Collide+Power** exploits leakage between:
  - **Guess** $\mathcal{G}$**:** Attacker-controlled data
  - **Value** $\mathcal{V}$**:** Victim secret data

💡 Hamming distance: $\mathrm{hd}(\mathcal{G}, \mathcal{V})$

$\rightarrow$ How to exploit this limited information?

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Intuition

$$\mathcal{P}(\mathcal{G}, \mathcal{V}) \approx \ldots$$

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Intuition

$$\mathcal{P}(\mathcal{G}, \mathcal{V}) \approx \mathsf{hd}(\mathcal{G}, \mathcal{V})$$

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Intuition

$$\mathcal{P}(\mathcal{G}, \mathcal{V}) \approx \mathsf{hd}(\mathcal{G}, \mathcal{V})$$

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\underbrace{\mathcal{P}(\mathcal{G}, \mathcal{V})}_{\text{model}} \approx \mathsf{hd}(\mathcal{G}, \mathcal{V})$$

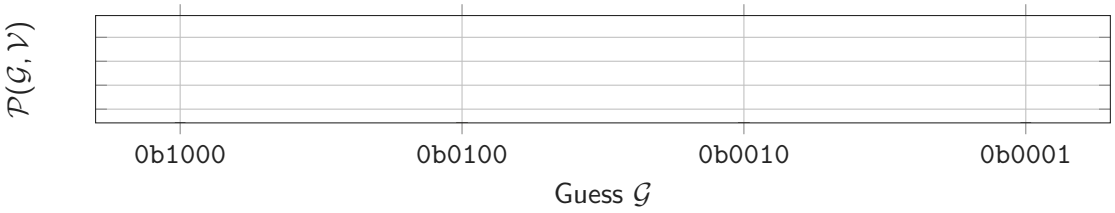
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Intuition

$$\underbrace{\mathcal{P}(\mathcal{G}, \mathcal{V})}_{\text{model}} \approx \underbrace{\mathsf{hd}(\mathcal{G}, \mathcal{V})}_{\text{signal}}$$

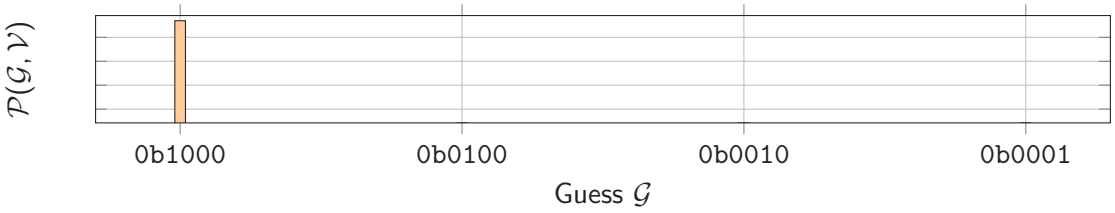
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\mathcal{P}(\mathcal{G}, 0101_2) \approx \mathsf{hd}(\mathcal{G}, 0101_2)$$



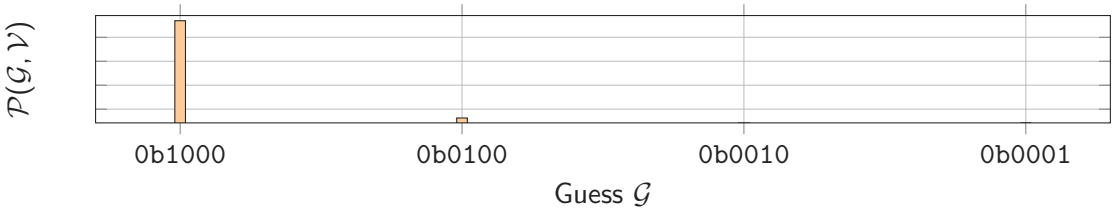
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\mathcal{P}(1000_2, 0101_2) \approx \mathsf{hd}(\mathbf{1}000_2, \mathbf{0}101_2) = 3$$



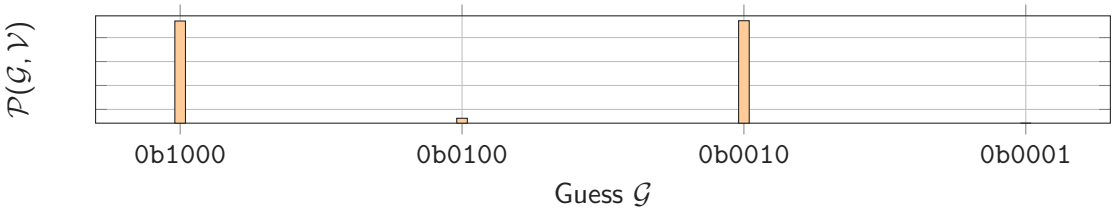
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\mathcal{P}(0100_2, 0101_2) \approx \mathsf{hd}(0\mathbf{1}00_2, 0\mathbf{1}01_2) = 1$$



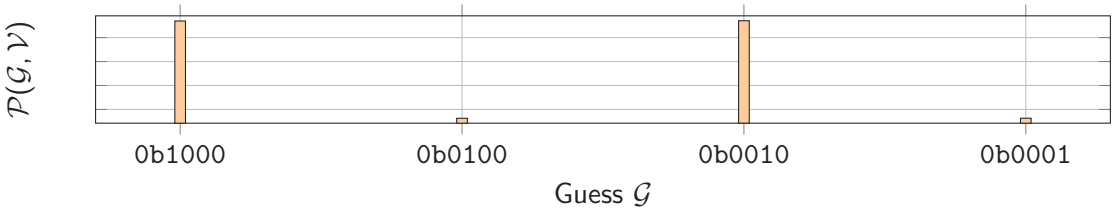
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\mathcal{P}(0010_2, 0101_2) \approx \mathsf{hd}(00\mathbf{1}0_2, 01\mathbf{0}1_2) = 3$$



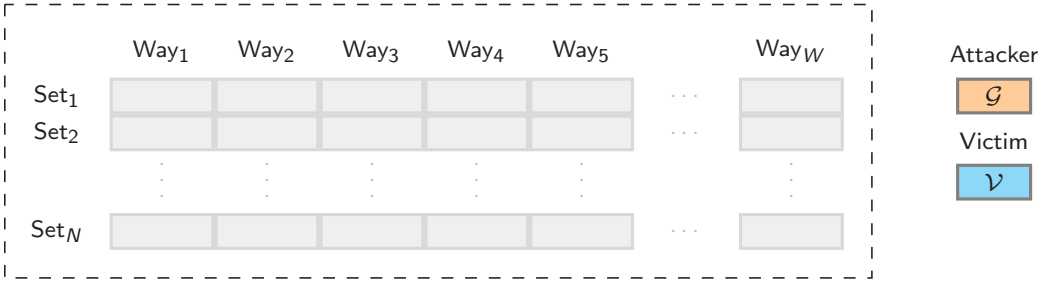
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

$$\mathcal{P}(0001_2, 0101_2) \approx \mathsf{hd}(000\mathbf{1}_2, 010\mathbf{1}_2) = 1$$



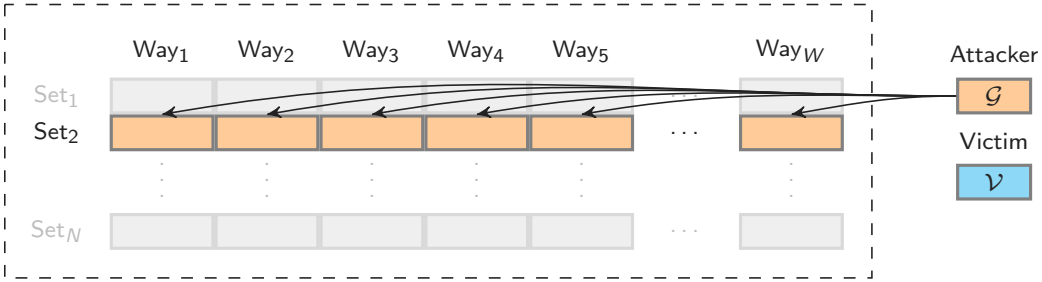
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Memory Subsystem



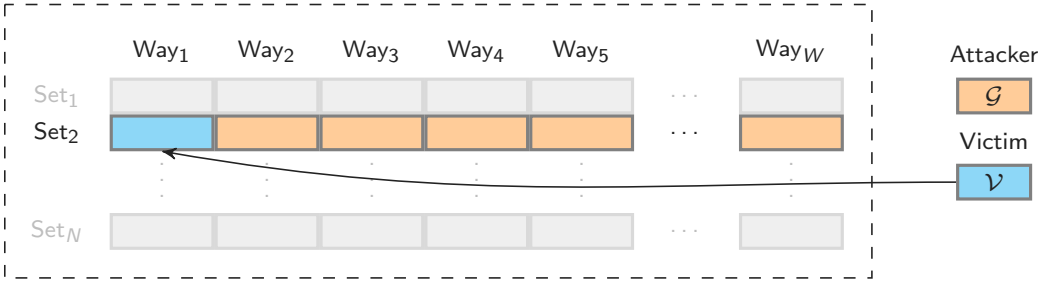
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Memory Subsystem



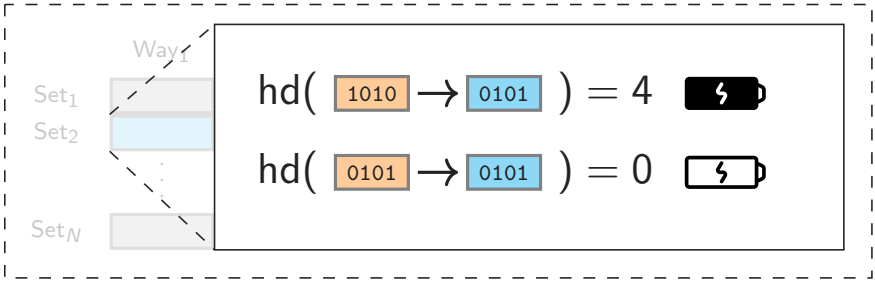
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Memory Subsystem



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Memory Subsystem



Attacker

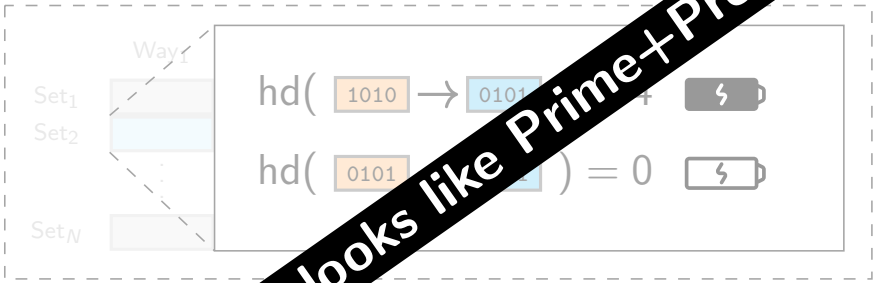
$\mathcal{G}$

Victim

$\mathcal{V}$

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Collide+Power - Memory Subsystem



This looks like Prime+Probe!

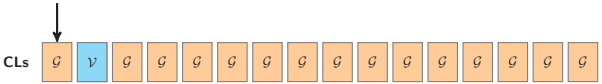
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis

Leakage Analysis - Experiment Setup

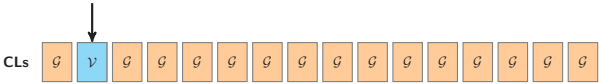
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



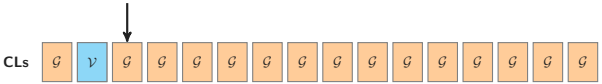
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



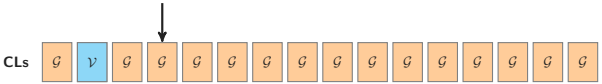
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



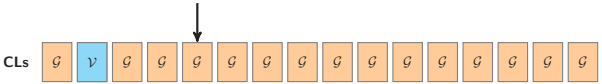
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



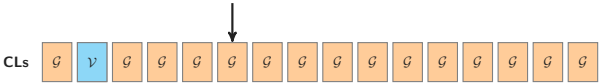
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



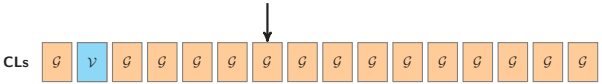
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



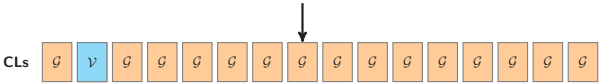
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



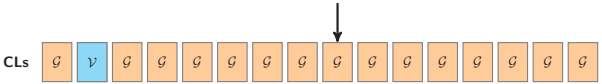
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



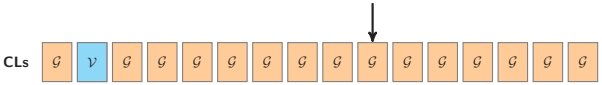
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



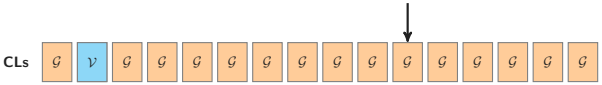
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



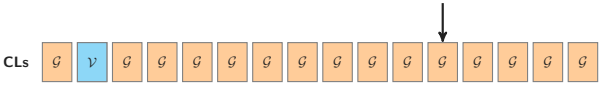
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



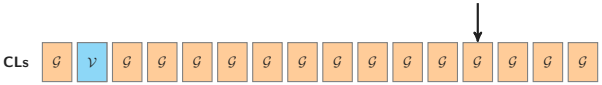
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



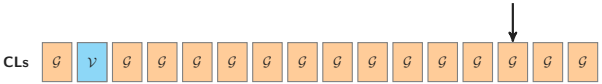
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



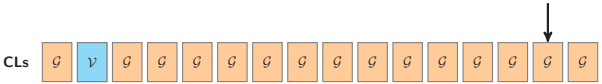
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



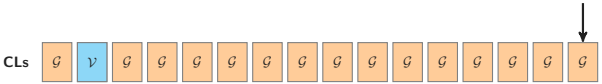
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



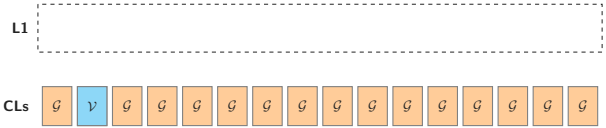
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



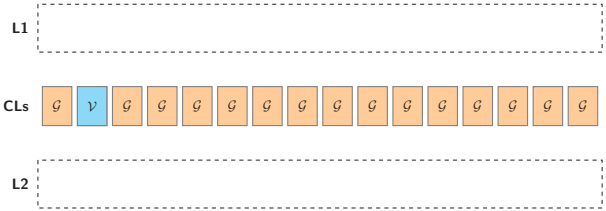
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Experiment Setup



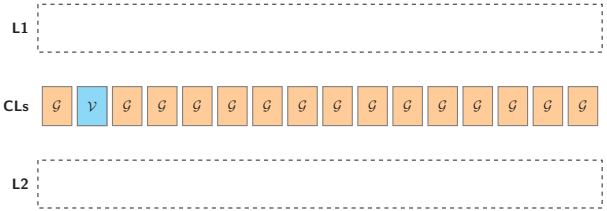
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

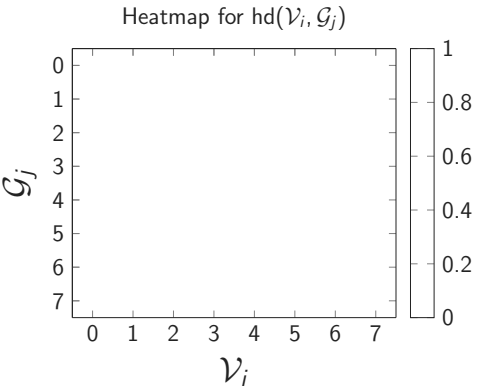
Leakage Analysis - Experiment Setup



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

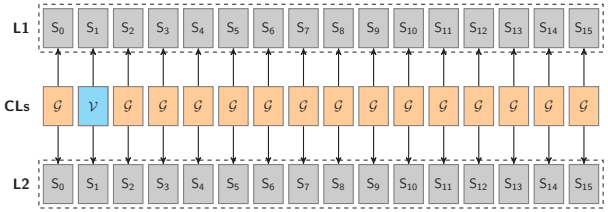
Leakage Analysis - Experiment Setup

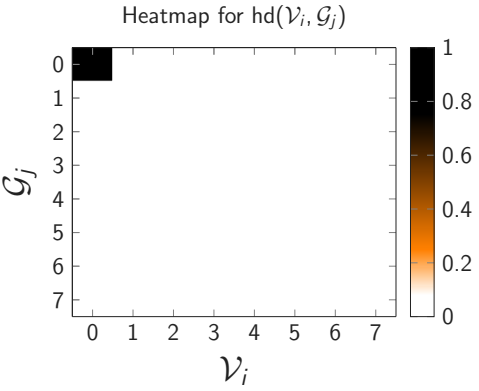




Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

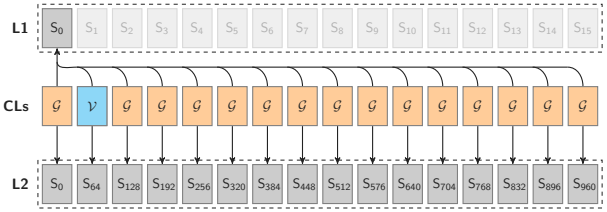
Leakage Analysis - No Eviction

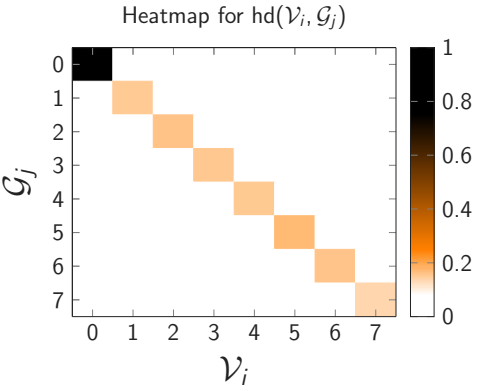




Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

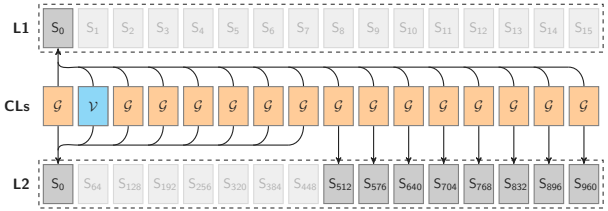
Leakage Analysis - L1 Eviction

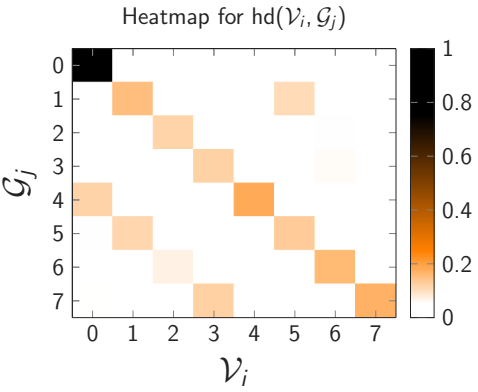




Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

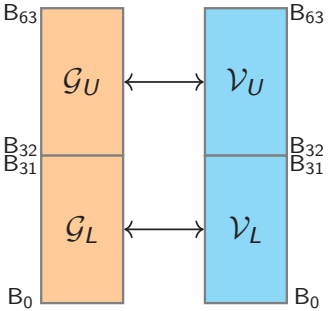
Leakage Analysis - L1+L2 Eviction





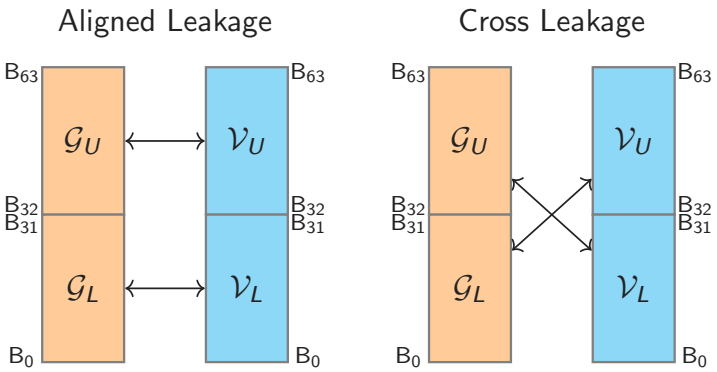
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Aligned Leakage



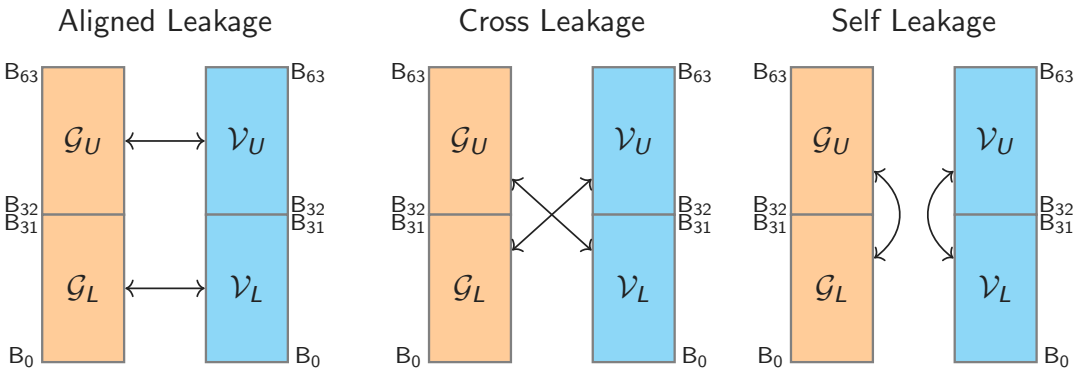
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Generalization



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Leakage Analysis - Generalization



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

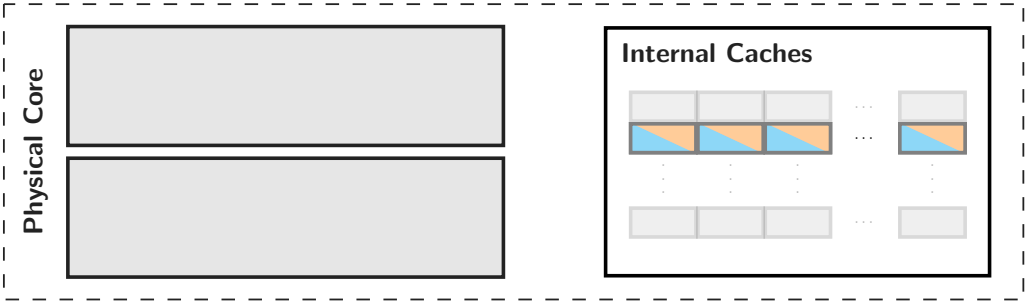
Leakage Analysis: Results

Inst.	Evict.	Effectiveness		Aligned Leakage		Cross Leakage		Self Leakage		Weights			
		$\hat{\rho}$	SNR_A	$\mathrm{hd}(v_L, g_L)$	$\mathrm{hd}(v_U, g_U)$	$\mathrm{hd}(v_L, g_U)$	$\mathrm{hd}(v_U, g_L)$	$\mathrm{hd}(v_L, v_U)$	$\mathrm{hd}(g_L, g_U)$	$\mathrm{hw}(v_L)$	$\mathrm{hw}(v_U)$	$\mathrm{hw}(g_L)$	$\mathrm{hw}(g_U)$
		$\cdot 1$	$\cdot 10^{-3}$	a_0 in μW	a_1 in μW	c_0 in μW	c_1 in μW	s_0 in μW	s_1 in μW		w_1 in μW	w_2 in μW	w_3 in μW
Load	None	0.311	72.004	544.5	4.2	1.1	0.5	0.0			0.0	362.6	0.0
	L1	0.907	7.873	598.3	278.8	0.0	0.0				0.0	6124.4	2696.9
	L1+L2	0.822	5.632	339.3	141.7	106.6			0.0		0.0	3750.7	1435.0
Prefetch	None	0.003	0.000	0.0				0.0	0.0	0.0	0.0	1.7	2.8
	L1	0.370	11.365	136			0.1	0.0	0.0	0.0	0.0	454.1	455.5
	L1+L2	0.300	5.29			40.9	43.0	0.0	0.0	0.0	0.0	334.0	332.5
Store	None	0.003	0.00		0.0	0.0	3.1	0.0	0.0	0.0	0.0	7.0	0.0
	L1	0.241	3.876	63.3	74.5	4.9	9.6	0.0	0.0	0.0	0.0	204.6	303.2
	L1+L2	0.450	6.457	133.7	169.0	84.7	86.2	0.0	0.0	0.0	0.0	347.1	1130.5

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

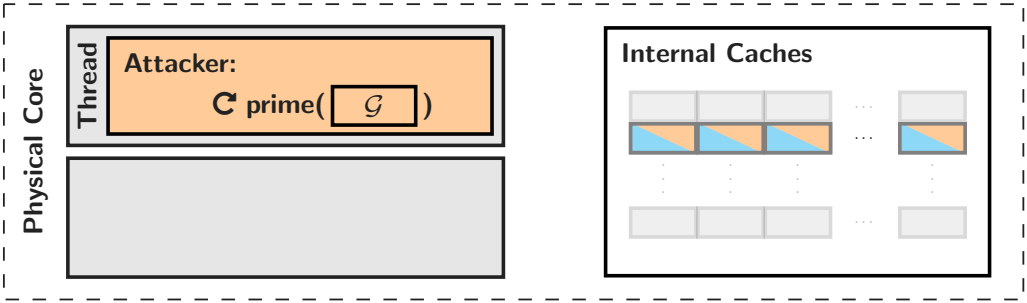
Generic Attacks

MDS-style Attack



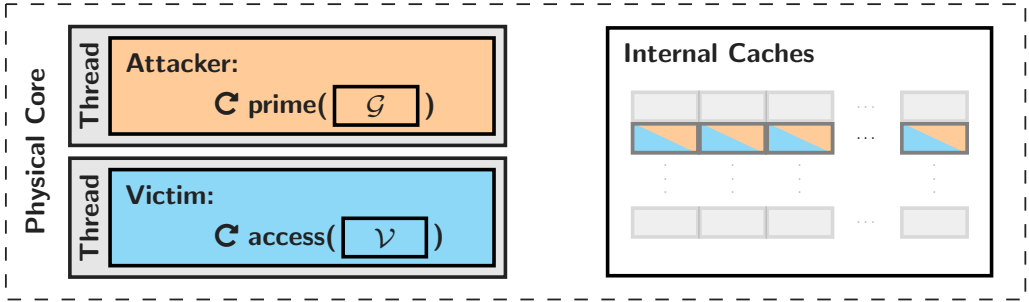
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

MDS-style Attack



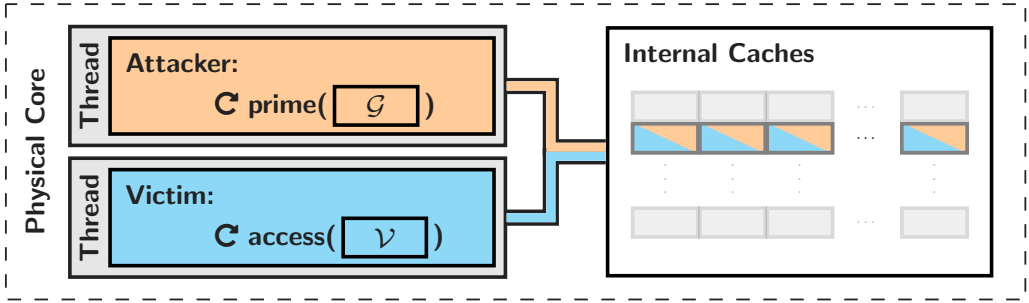
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

MDS-style Attack



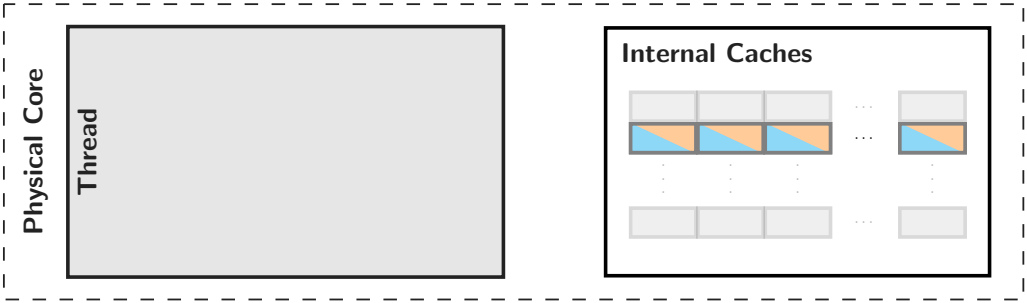
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

MDS-style Attack



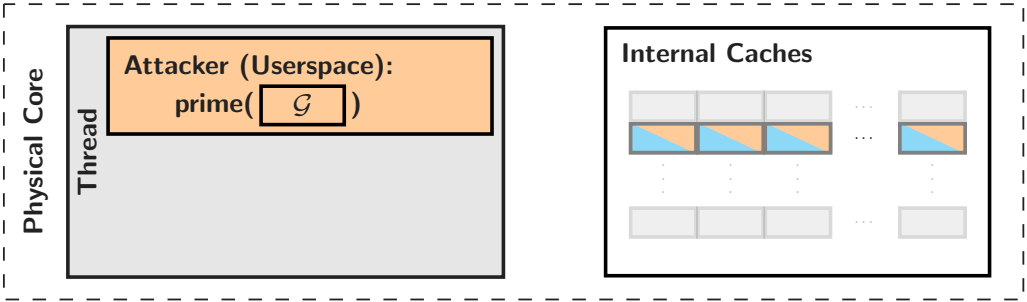
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Meltdown-style Attack



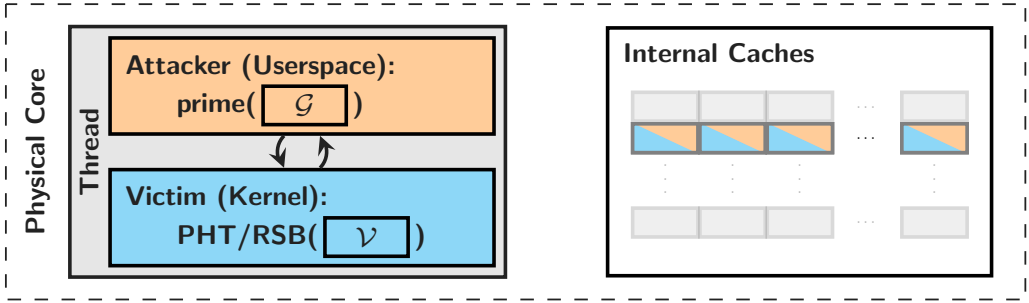
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Meltdown-style Attack



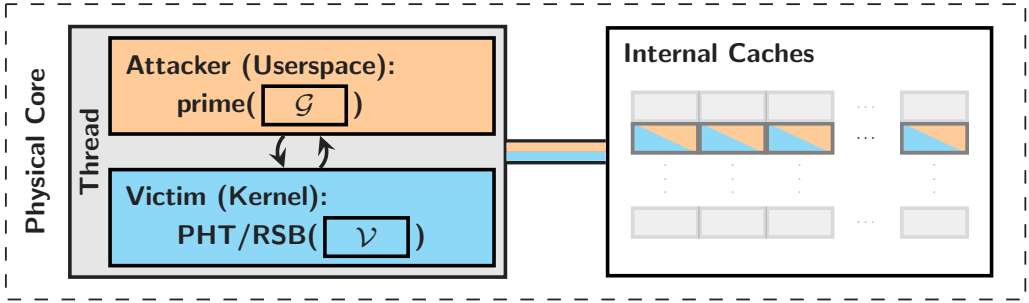
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Meltdown-style Attack



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Meltdown-style Attack



Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

This must be slow?

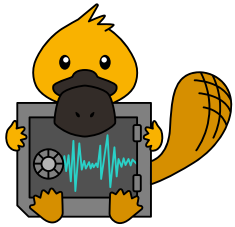
NO!

It is EXTREMELY slow![1]

[1] With the current state-of-the-art.

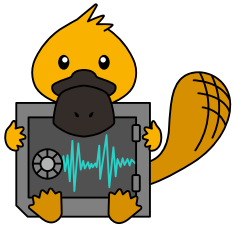
Software-based Power Side Channels

Software-based Power Side Channels



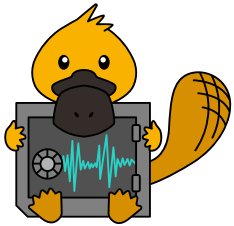
- Direct power measurements

Software-based Power Side Channels



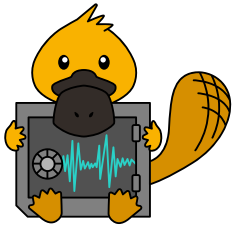
- Direct power measurements
- Unpriviledged Interface

Software-based Power Side Channels



- Direct power measurements
- ~~Unpriviledged Interface~~

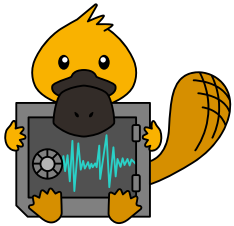
Software-based Power Side Channels



- Direct power measurements
- ~~Unpriviledged Interface~~

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Software-based Power Side Channels

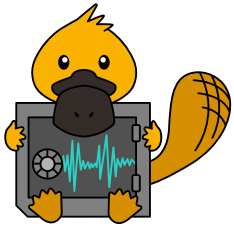


- Direct power measurements
- ~~Unpriviledged Interface~~

- Indirect power measurements

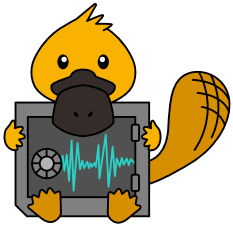
Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Software-based Power Side Channels

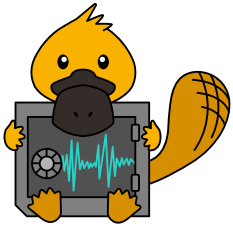


- Direct power measurements
- ~~Unpriviledged Interface~~

- Indirect power measurements
- Higher consumption $\rightarrow$ more throttling

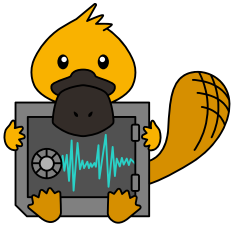


- **MDS-style:**
  4.82 bit/h



- **MDS-style:**
  4.82 bit/h
- **Meltdown-style (RSB):**
  0.84 bit/h

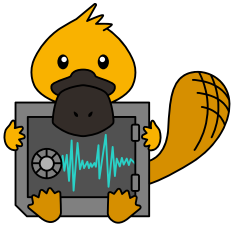
Software-based Power Side Channels



- **MDS-style:**
  4.82 bit/h
- **Meltdown-style (RSB):**
  0.84 bit/h

- **MDS-style:**
  0.065 to 0.68 bit/h

Software-based Power Side Channels



- **MDS-style:**
  4.82 bit/h
- **Meltdown-style (RSB):**
  0.84 bit/h

- **MDS-style:**
  0.065 to 0.68 bit/h
- **Meltdown-style estimate (PHT):**
  99.95 days/bit to 2.86 years/bit

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique
  - **Agnostic** to the power related signal

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique
  - **Agnostic** to the power related signal
  - **Hard** to prevent

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique
  - **Agnostic** to the power related signal
  - **Hard** to prevent
- **Passed** artifact evaluation

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique
  - **Agnostic** to the power related signal
  - **Hard** to prevent
- **Passed** artifact evaluation

- For **more** details:
  - Prefetcher effects
  - Differential measurement
  - Even more evaluation ...

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at

Final Remarks & Takeaways

- Collide+Power: `https://collidepower.com`
  - **Generic** arbitrary data leakage technique
  - **Agnostic** to the power related signal
  - **Hard** to prevent
- **Passed** artifact evaluation

- For **more** details:
  - Prefetch[illegible]ets
  - Diff[illegible] measurement
  - [illegible]more evaluation ...

Read the Paper

Andreas Kogler 0xhilbert andreas.kogler@iaik.tugraz.at