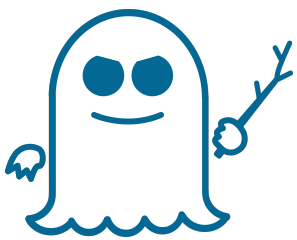
Sicherheitslücken in der x86 / amd64 - Architektur

Marcell Haritopoulos

Matthias Paulitsch

Michael Sismanovic

13. Februar 2019



Inhaltsverzeichnis

1 Einführung
- Grundinformationen
- Geschichtliche Entwicklung
- Speicherverwaltung
- Prozessor Modi

2 Spectre
- Grundinformationen
- Out of Order Execution
- Spectre Angriffe
- Versionen und Gegenvorkehrungen

3 Meltdown
- Grundinformationen
- Vorgehensweise
- Unterschied zu Spectre
- Gegenvorkehrungen / „Fixes“

4 Weiterführende Literatur

Einführung

1 Einführung
- Grundinformationen
- Geschichtliche Entwicklung
- Speicherverwaltung
- Prozessor Modi

2 Spectre

3 Meltdown

4 Weiterführende Literatur

Grundinformationen

Grundinformationen

Was ist x86?

x86 ist eine ISA

Grundinformationen

Was ist x86?

x86 ist eine ISA

Was ist ISA?

ISA steht für (Instruction Set Architecture)
z.B: POP, PUSH, ADD, JUMP ...

Grundinformationen

Was ist x86?

x86 ist eine ISA

Was ist ISA?

ISA steht für (Instruction Set Architecture)
z.B: POP, PUSH, ADD, JUMP ...

Woher kommt der Name x86

Die Modellnummern der ersten Intel-Prozessoren endeten fast alle mit 86 (80**86**, 802**86**, 803**86**, 804**86**, 805**86**)

Geschichte

Geschichte

- 1978 - erste x86-Prozessoren erschienen mit nur 16 Bits (8086 und 8088)

Geschichte

- 1978 - erste x86-Prozessoren erschienen mit nur 16 Bits (8086 und 8088)
- 1985 wurde auf 32 Bit aufgerüstet (80386)

Geschichte

- 1978 - erste x86-Prozessoren erschienen mit nur 16 Bits (8086 und 8088)
- 1985 wurde auf 32 Bit aufgerüstet (80386)
- 1999 wurde bekanntgegeben, dass AMD x86 auf 64 Bit aufrüsten will.
  Intel hingegen entschied sich dafür, eine neue Prozessorarchitektur zu entwickeln (Itanium-Architektur IA-64)

Virtual Memory

Virtual Memory

Begriffserklärung:

Virtueller Arbeitsspeicher ermöglicht es jedem einzelnen Prozess, so zu agieren, als stünde ihm der gesamte Arbeitsspeicher allein zur Verfügung. Dadurch bekommt jedes Programm seinen eigenen Adressraum und wird von allen anderen Prozessen isoliert.

Virtual Memory

Begriffserklärung:

Virtueller Arbeitsspeicher ermöglicht es jedem einzelnen Prozess, so zu agieren, als stünde ihm der gesamte Arbeitsspeicher allein zur Verfügung. Dadurch bekommt jedes Programm seinen eigenen Adressraum und wird von allen anderen Prozessen isoliert.

Wieso brauchen wir Virtual Memory?

Verhindert, dass Programme auf den selben physikalischen Speicher (unkontrolliert) zugreifen.
Programme können sich also nicht gegenseitig beeinflussen oder Daten klauen.

Paging

Paging

Begriffserklärung:

Paging ist eine Methode zur virtuellen Adressierung. Der physische Speicher wird in 4k Page Frames aufgeteilt und in den virtuellen Speicher reingehängt. Durch gleiche Page-Größen wird Fragmentierung verhindert.

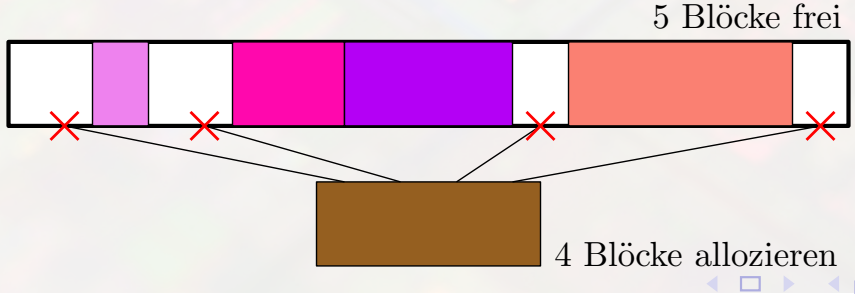
Paging

Begriffserklärung:

Paging ist eine Methode zur virtuellen Adressierung. Der physische Speicher wird in 4k Page Frames aufgeteilt und in den virtuellen Speicher reingehängt. Durch gleiche Page-Größen wird Fragmentierung verhindert.

Was ist Memory Fragmentation?

Lücken in der Belegung von Speicherblöcken.
Durch Allozieren und Freigeben von Speicher können nicht zusammenhängende Lücken entstehen.



Prozessor Modi

Prozessor Modi

Real Mode:

Jeder x86 Prozessor startet im Real Mode. Im Real Mode stehen weder der Erweiterter Speicher noch der Virtuelle Adressraum zur Verfügung. Der Real Mode ist sehr unsicher, deshalb wird meistens beim Starten des Betriebssystems in den Protected Mode gewechselt.

Prozessor Modi

Real Mode:

Jeder x86 Prozessor startet im Real Mode. Im Real Mode stehen weder der Erweiterter Speicher noch der Virtuelle Adressraum zur Verfügung. Der Real Mode ist sehr unsicher, deshalb wird meistens beim Starten des Betriebssystems in den Protected Mode gewechselt.

Protected Mode:

Der Protected Mode erlaubt das Setzen von Zugriffsberechtigungen (Lesen / Schreiben / Ausführen) durch die Protection Rings. Die Protection Rings sind hierarchische Sicherheitsstufen. Es gibt 4 Ringe, angefangen mit Ring 0, der die meisten Privilegien hat und Ring 3, der die wenigsten Privilegien hat.

Spectre

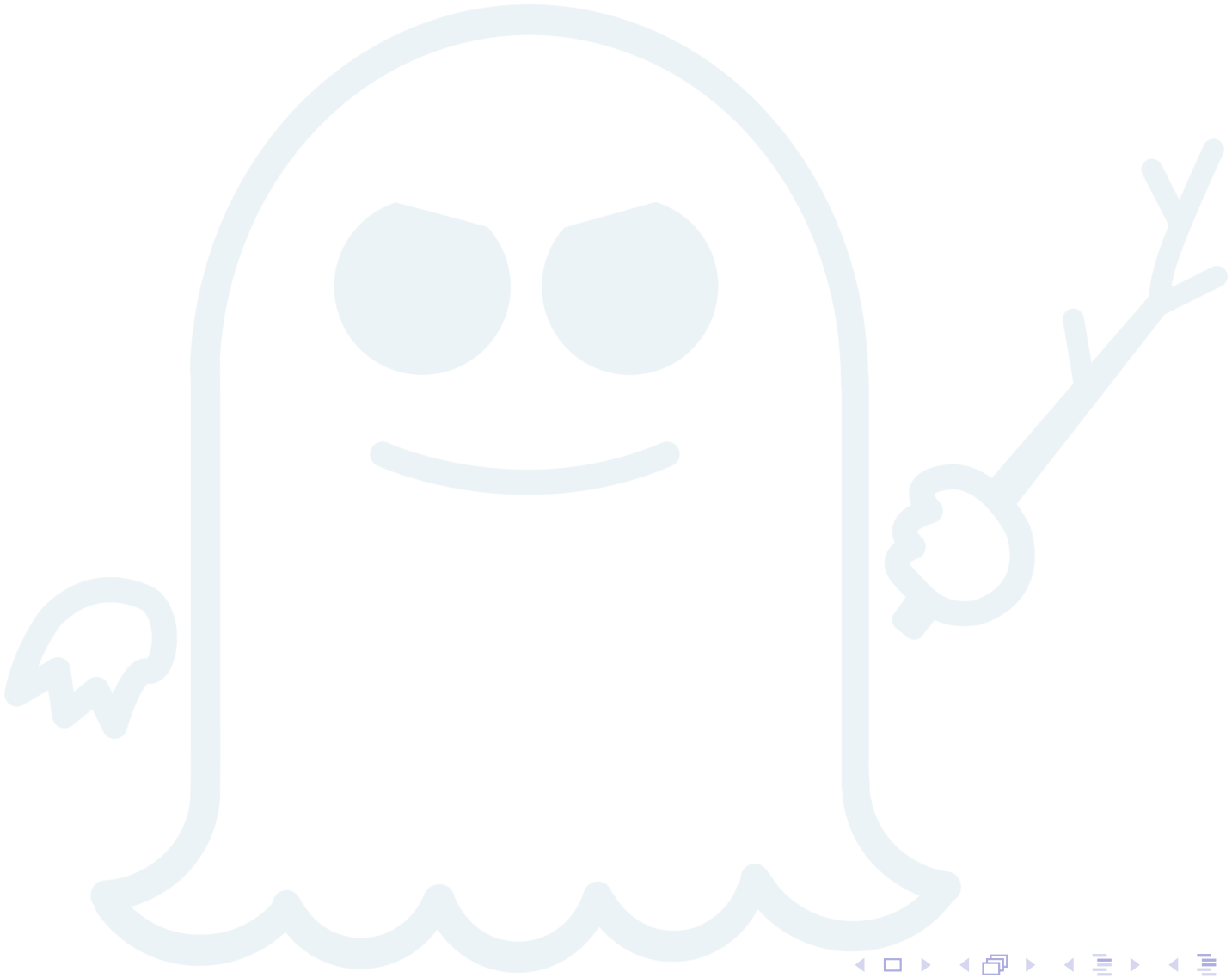
1 Einführung

2 Spectre
- Grundinformationen
- Out of Order Execution
- Spectre Angriffe
- Versionen und Gegenvorkehrungen

3 Meltdown

4 Weiterführende Literatur

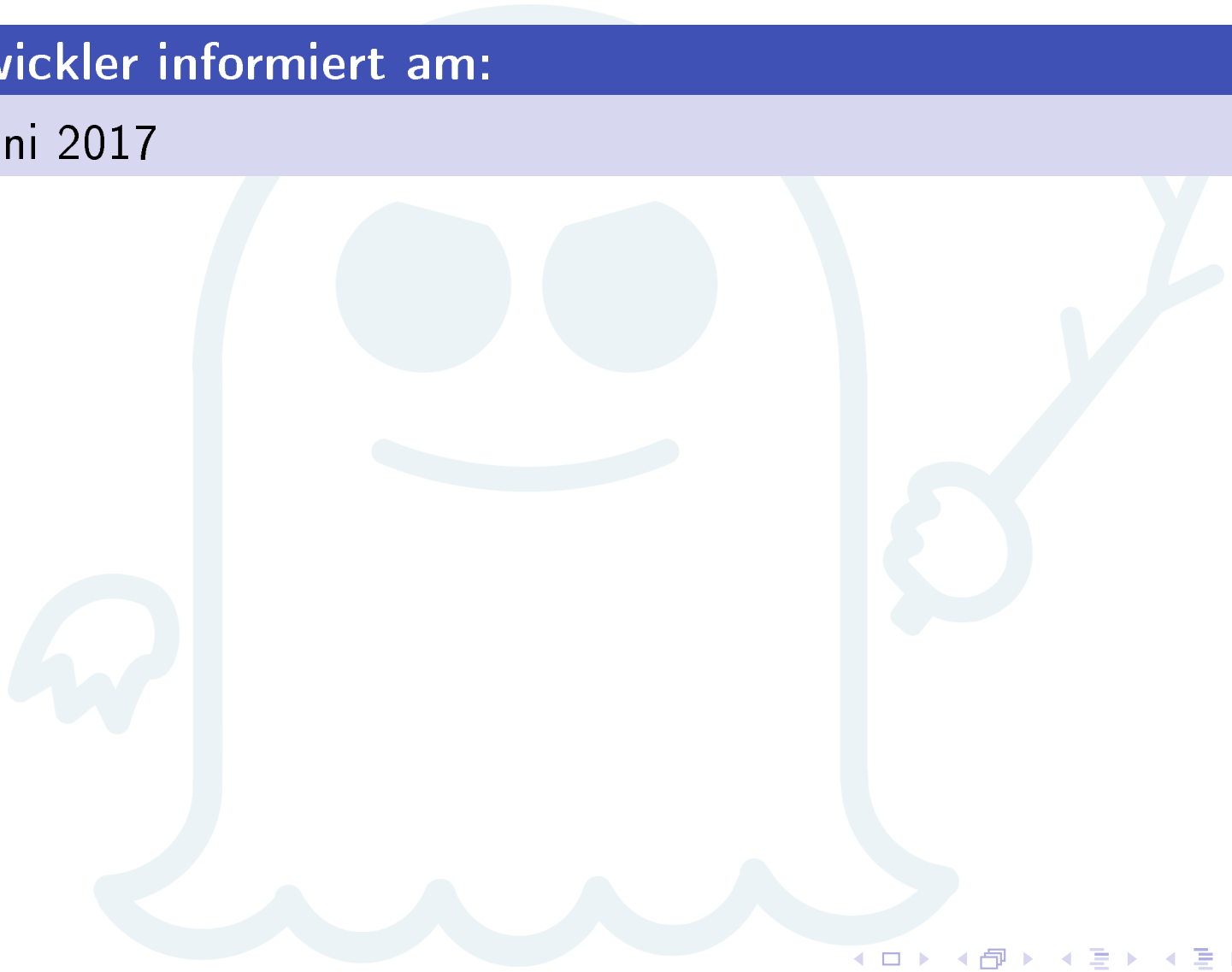
Spectre Grundinformationen



Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017



Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Google Project Zero	Jann Horn

Entdeckt von:

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Entdeckt von:

Google Project Zero	Jann Horn
Independent	Paul Kocher

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Entdeckt von:

Google Project Zero	Jann Horn
Independent	Paul Kocher
University of Michigan	Daniel Genkin

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Entdeckt von:

Google Project Zero	Jann Horn
Independent	Paul Kocher
University of Michigan	Daniel Genkin
Rambus Security Division	Mike Hamburg

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

Veröffentlichung:

3. Jänner 2018

Entdeckt von:

Google Project Zero	Jann Horn
Independent	Paul Kocher
University of Michigan	Daniel Genkin
Rambus Security Division	Mike Hamburg
TU Graz	Moritz Lipp

Spectre Grundinformationen

Entwickler informiert am:

1. Juni 2017

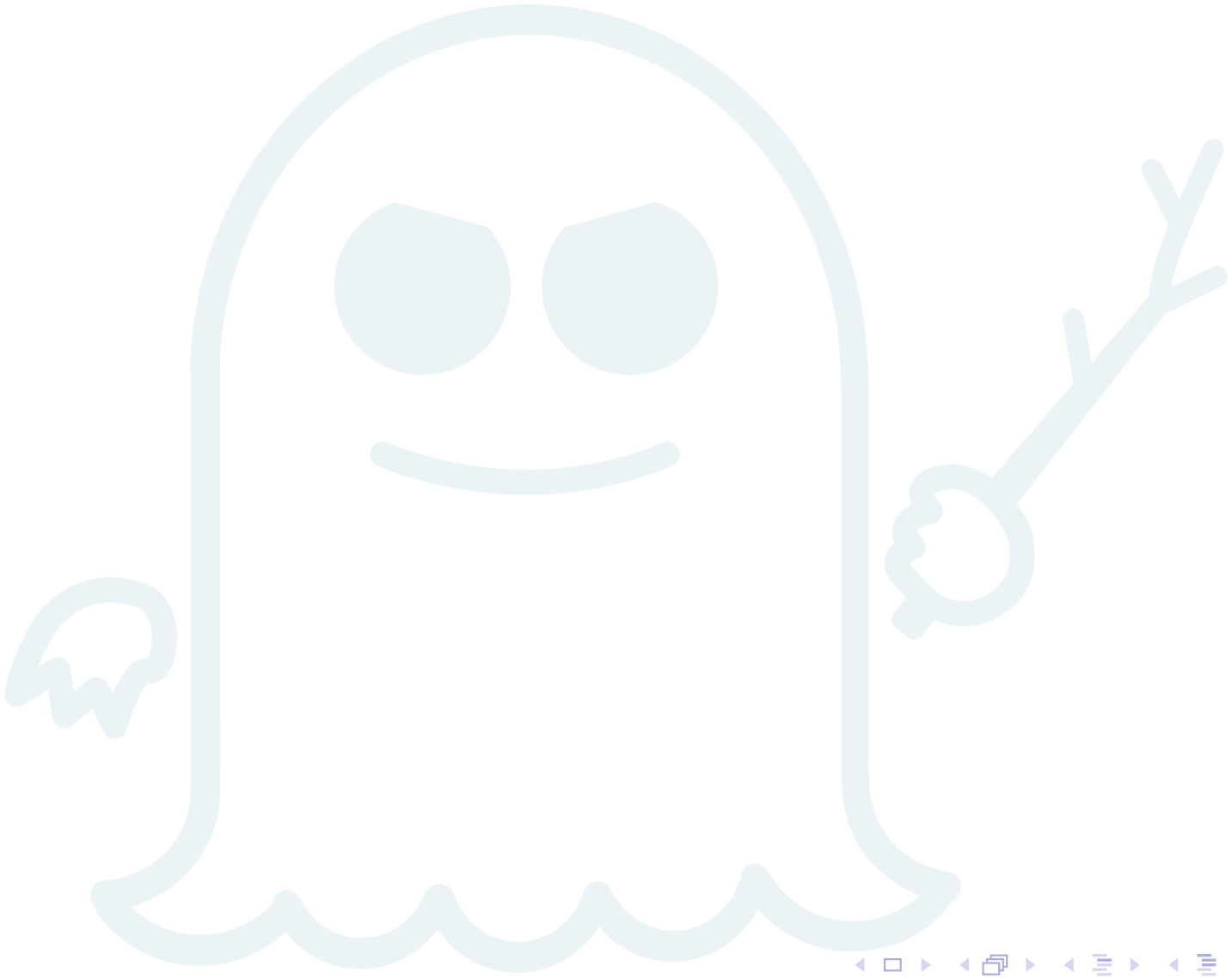
Veröffentlichung:

3. Jänner 2018

Entdeckt von:

Google Project Zero	Jann Horn
Independent	Paul Kocher
University of Michigan	Daniel Genkin
Rambus Security Division	Mike Hamburg
TU Graz	Moritz Lipp
University of Adelaide	Yuval Yarom

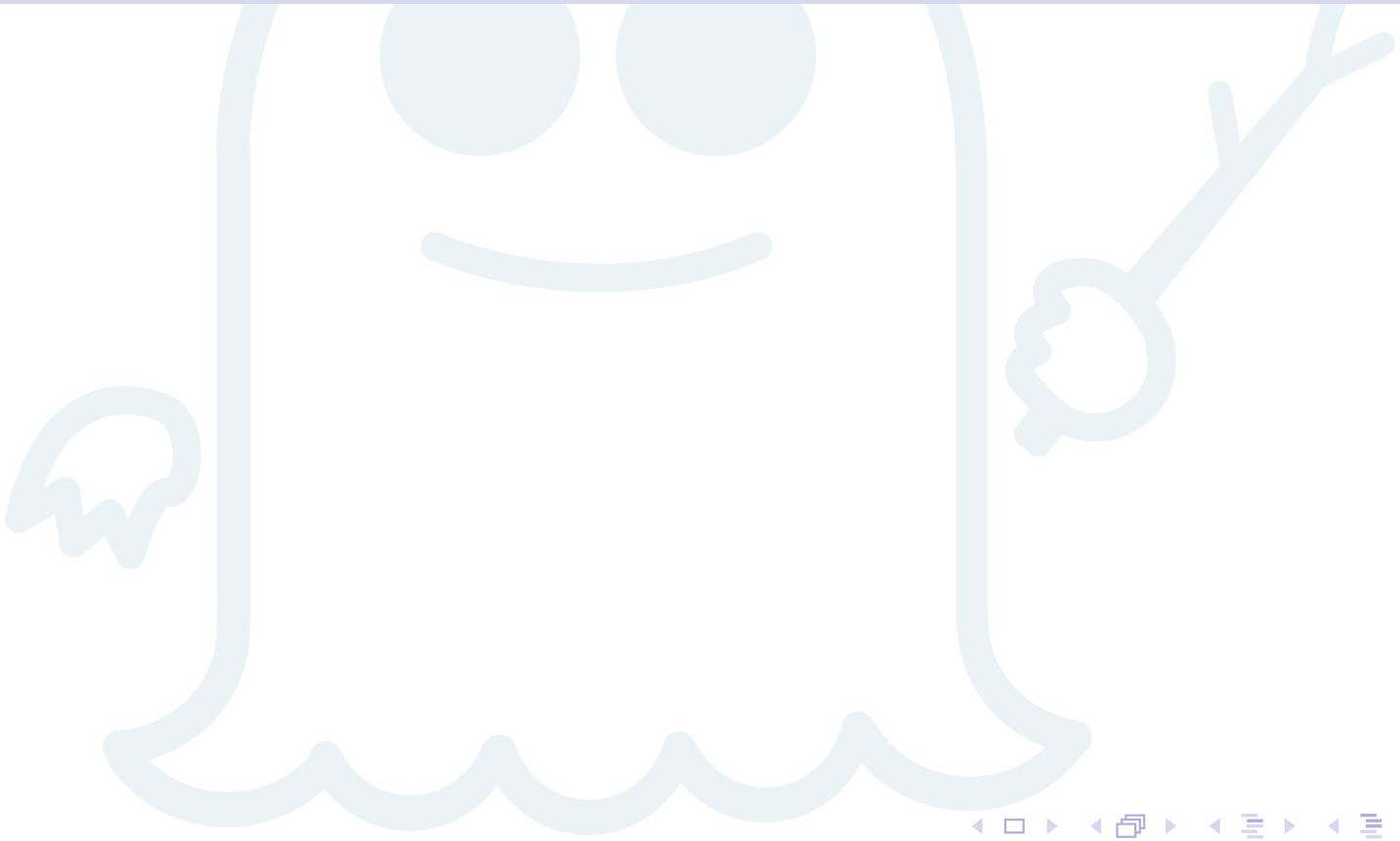
Spectre Grundinformationen



Spectre Grundinformationen

Warum heißt es Spectre?

“The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time.“



Spectre Grundinformationen

Warum heißt es Spectre?

"The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time."

Begriffserklärung:

Spectre beschreibt Angriffsszenarien, bei denen Prozesse Sicherheitslücken in Mikroprozessoren ausnutzen um Informationen des virtuellen Speichers auszulesen

Spectre Grundinformationen

Warum heißt es Spectre?

“The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time.“

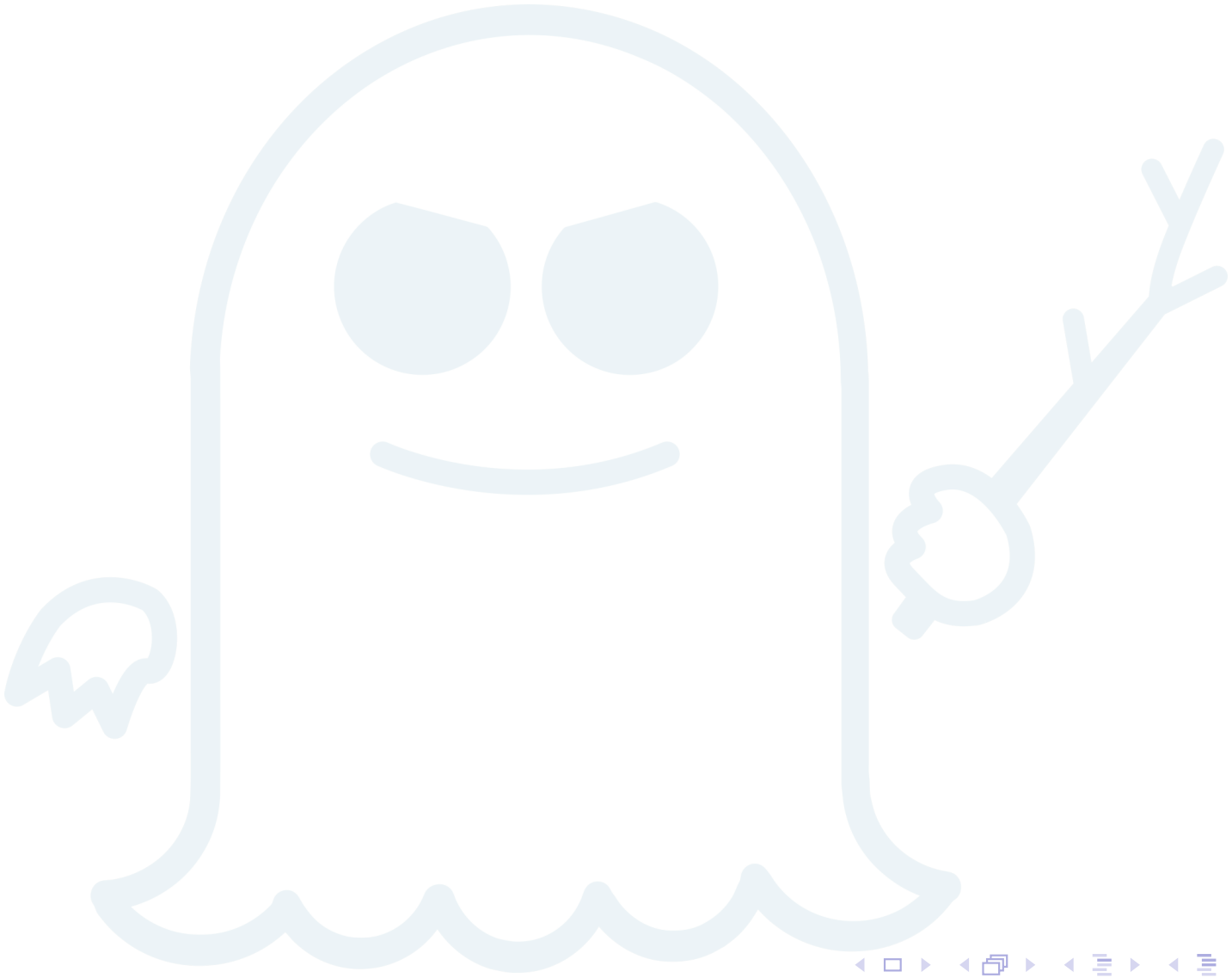
Begriffserklärung:

Spectre beschreibt Angriffsszenarien, bei denen Prozesse Sicherheitslücken in Mikroprozessoren ausnutzen um Informationen des virtuellen Speichers auszulesen

Zusätzliche Vorraussetzung

Mikroprozessor verwendet out-of-order-execution

Out of Order Execution



Out of Order Execution

Begriffserklärung:

Bezeichnet die Möglichkeit, Maschinenbefehle in den Ausführungseinheiten eines Prozessors in einer anderen Reihenfolge auszuführen, als sie im Programmcode stehen.

Out of Order Execution

Begriffserklärung:

Bezeichnet die Möglichkeit, Maschinenbefehle in den Ausführungseinheiten eines Prozessors in einer anderen Reihenfolge auszuführen, als sie im Programmcode stehen.

Vorteil

Stufen der Pipeline besser ausgelastet

Out of Order Execution

Begriffserklärung:

Bezeichnet die Möglichkeit, Maschinenbefehle in den Ausführungseinheiten eines Prozessors in einer anderen Reihenfolge auszuführen, als sie im Programmcode stehen.

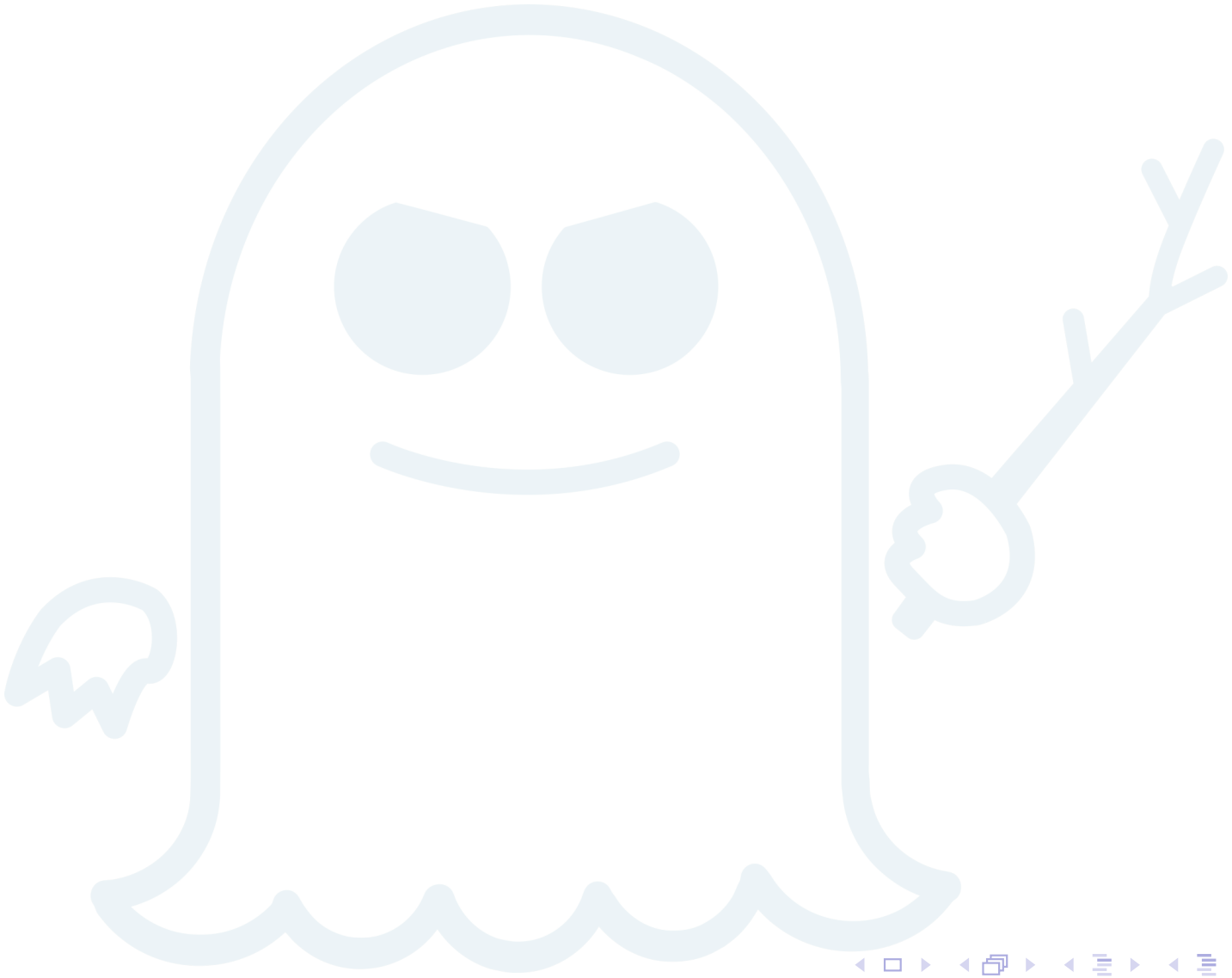
Vorteil

Stufen der Pipeline besser ausgelastet

Problematik

Nur auf von einander unabhängige Befehle anwendbar

Out of Order Execution bei Spectre



Out of Order Execution bei Spectre

Ausnützen der Out of Order Execution:

Out of Order Execution bei Spectre

Ausnützen der Out of Order Execution:

- Prozessausführung beeinflusst

Out of Order Execution bei Spectre

Ausnützen der Out of Order Execution:

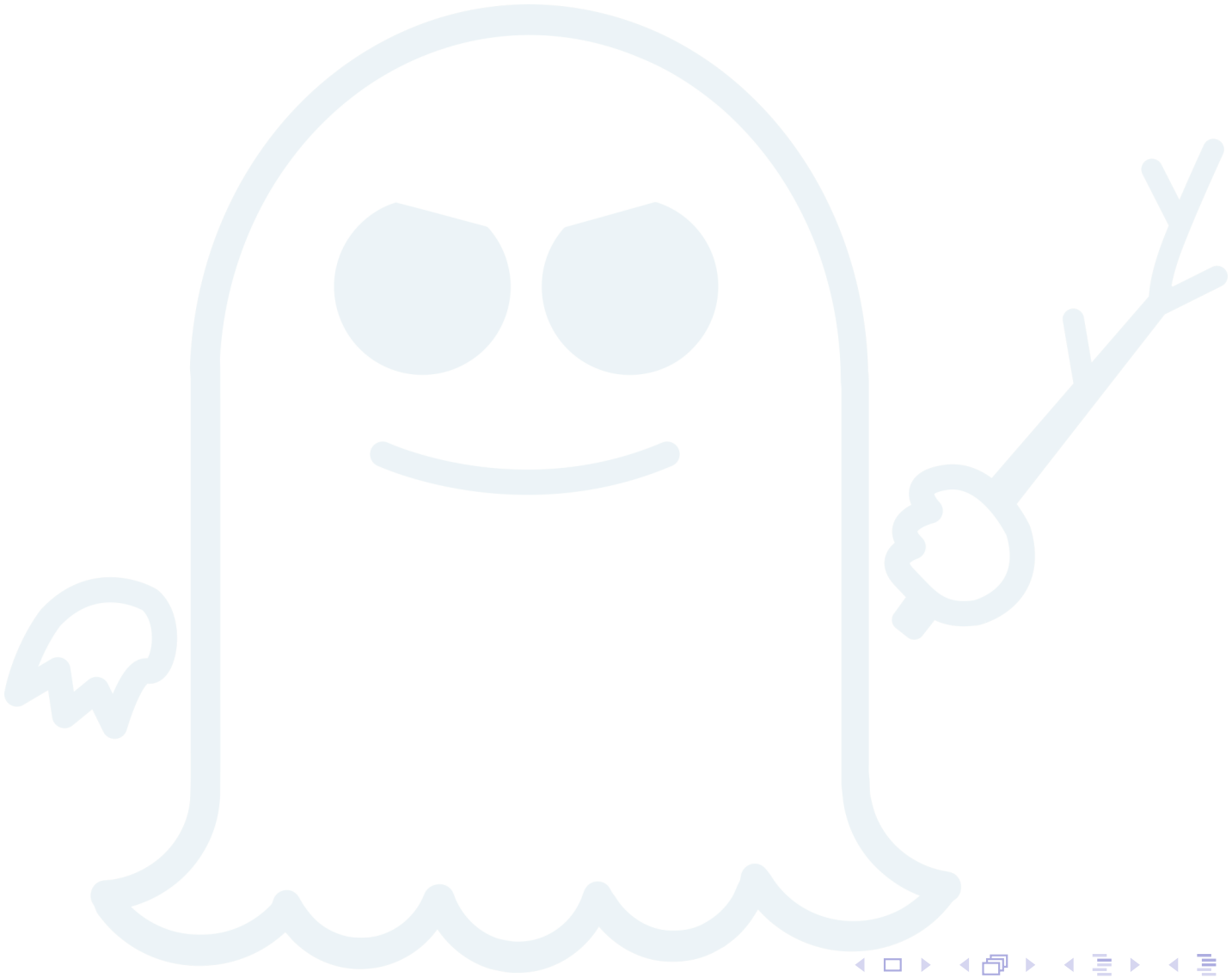
- Prozessausführung beeinflusst
- Inhalt einer Speicherzelle aus dem Adressraum ausgelesen

Out of Order Execution bei Spectre

Ausnützen der Out of Order Execution:

- Prozessausführung beeinflusst
- Inhalt einer Speicherzelle aus dem Adressraum ausgelesen
- Hinterlässt bemerkbare Spur im Cache

Speculative Execution



Speculative Execution

Begriffserklärung:

Ist eine Optimierungstechnik, bei der ein Computer System eine Tätigkeit ausführt, die im weiteren Programmablauf nicht zwingend benötigt wird. Der Prozess wird beendet, bevor überhaupt bekannt ist, ob dieser nötig war, oder nicht.

Speculative Execution

Begriffserklärung:

Ist eine Optimierungstechnik, bei der ein Computer System eine Tätigkeit ausführt, die im weiteren Programmablauf nicht zwingend benötigt wird. Der Prozess wird beendet, bevor überhaupt bekannt ist, ob dieser nötig war, oder nicht.

Ziel:

Einer Verzögerung in der Ausführung vorzubeugen

Speculative Execution

Begriffserklärung:

Ist eine Optimierungstechnik, bei der ein Computer System eine Tätigkeit ausführt, die im weiteren Programmablauf nicht zwingend benötigt wird. Der Prozess wird beendet, bevor überhaupt bekannt ist, ob dieser nötig war, oder nicht.

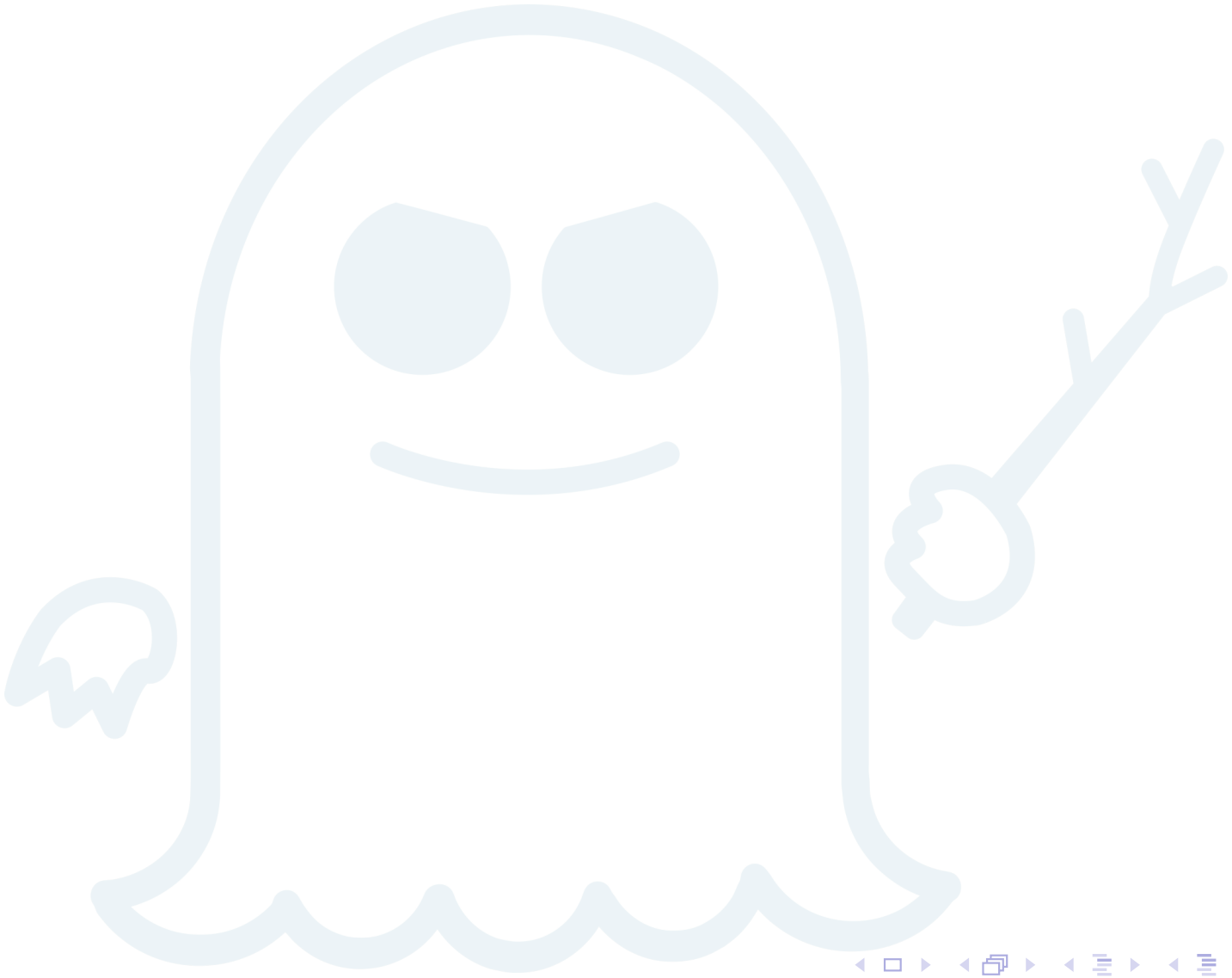
Ziel:

Einer Verzögerung in der Ausführung vorzubeugen

Ungebrauchte Ausführungen:

Änderungen werden rückgängig gemacht und die Ergebnisse werden ignoriert

Spectre Angriffe



Spectre Angriffe

Zitat:

"Speculative logic is unfaithful in how it executes, can access the victim's memory and registers, and can perform operations with measurable side effects."

Spectre Angriffe

Zitat:

“Speculative logic is unfaithful in how it executes, can access the victim’s memory and registers, and can perform operations with measurable side effects.“

Konsequenzen:

Spectre Angriffe

Zitat:

“Speculative logic is unfaithful in how it executes, can access the victim’s memory and registers, and can perform operations with measurable side effects.“

Konsequenzen:

- Spectre Angriffe Nutzen Sicherheitslücken in der Implementierung der Speculative Execution aus

Spectre Angriffe

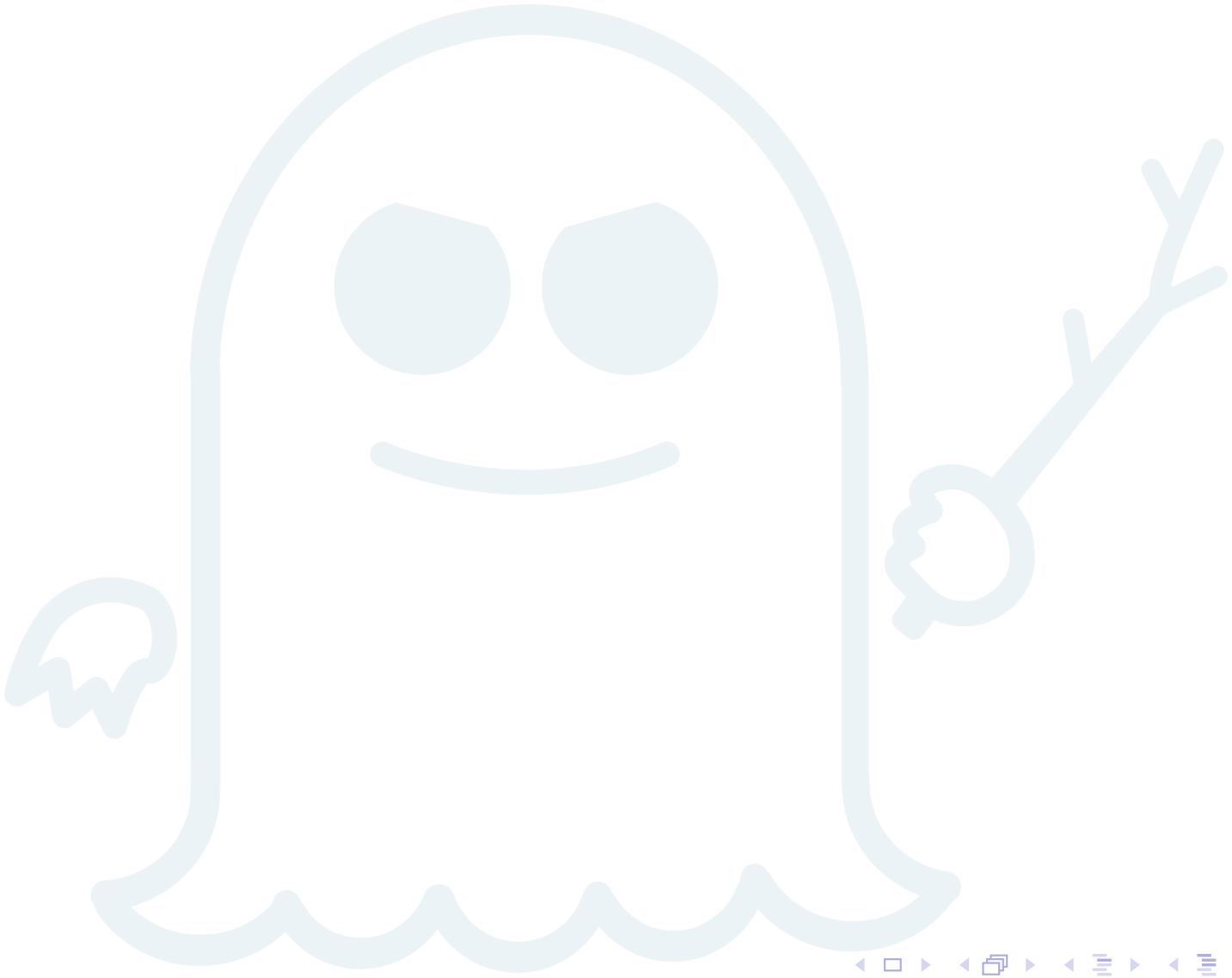
Zitat:

“Speculative logic is unfaithful in how it executes, can access the victim’s memory and registers, and can perform operations with measurable side effects.“

Konsequenzen:

- Spectre Angriffe Nutzen Sicherheitslücken in der Implementierung der Speculative Execution aus
- Zugriff auf Speicher und Register möglich

Spectre Angriffe



Spectre Angriffe

Zitat:

"Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary"

Spectre Angriffe

Zitat:

“Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim’s confidential information via a side channel to the adversary“

Konsequenzen

Spectre Angriffe

Zitat:

“Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim’s confidential information via a side channel to the adversary“

Konsequenzen

- Befehle ausgeführt,die bei einem korrekten Ablauf nicht ausgeführt werden würden

Spectre Angriffe

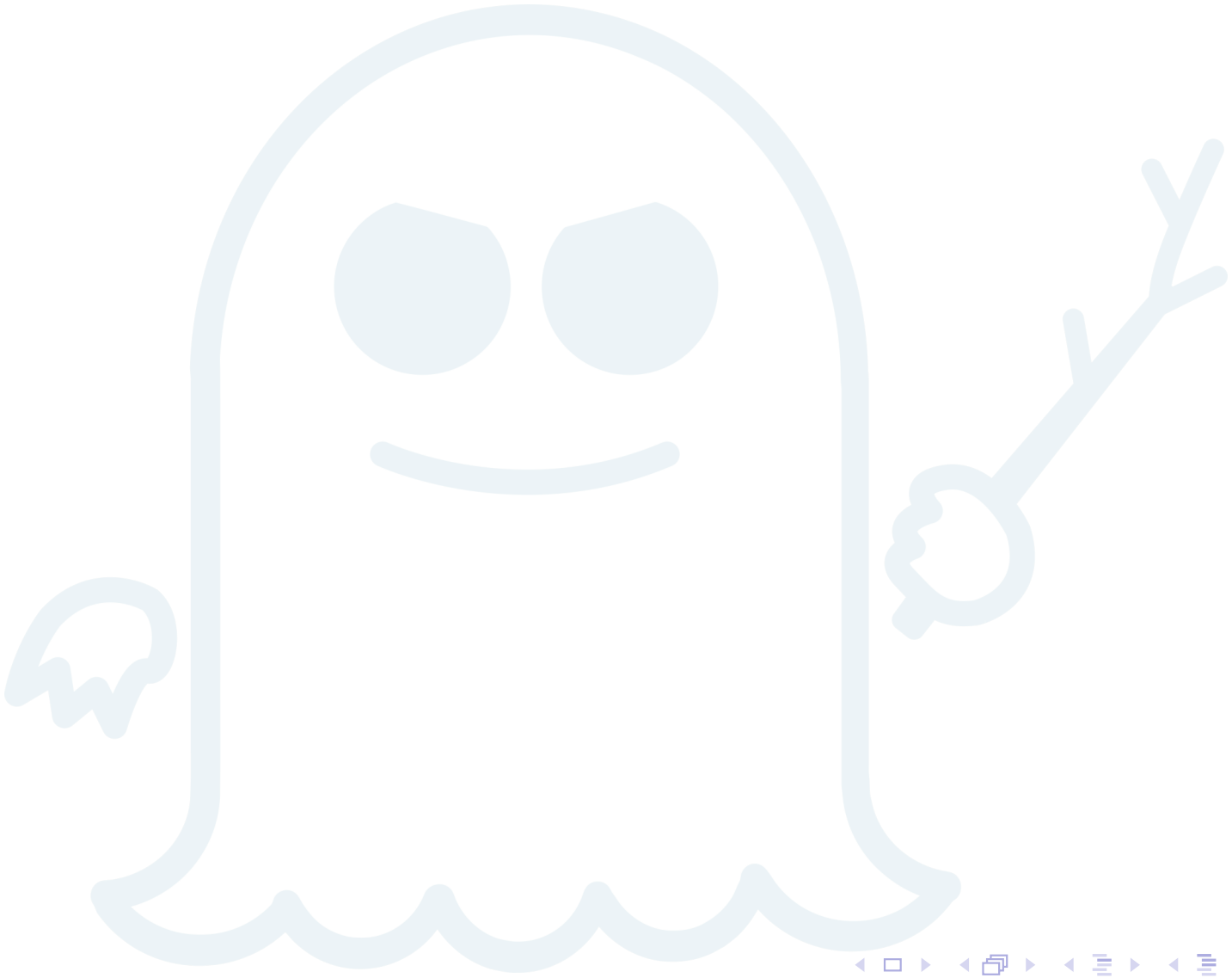
Zitat:

“Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim’s confidential information via a side channel to the adversary“

Konsequenzen

- Befehle ausgeführt,die bei einem korrekten Ablauf nicht ausgeführt werden würden
- Vertrauliche Informationen über side channel übertragen

Spectre Angriffe



Spectre Angriffe

Zitat:

"Speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing and side-channel attacks."

Spectre Angriffe

Zitat:

“Speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing and side-channel attacks.“

Konsequenzen

Spectre Angriffe

Zitat:

“Speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing and side-channel attacks.“

Konsequenzen

- Mehrere Sicherheitsvorkehrungen zu Nichte gemacht

Spectre Angriffe

Zitat:

“Speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing and side-channel attacks.“

Konsequenzen

- Mehrere Sicherheitsvorkehrungen zu Nichte gemacht
- Viele verschiedene Lücken ausnützbar

Spectre Versionen und Gegenvorkehrungen

Spectre Versionen und Gegenvorkehrungen

- Mehr als zehn verschiedene Versionen bekannt

Spectre Versionen und Gegenvorkehrungen

- Mehr als zehn verschiedene Versionen bekannt
- Einige **nur durch Hardware Änderungen behebbar**

Spectre Versionen und Gegenvorkehrungen

- Mehr als zehn verschiedene Versionen bekannt
- Einige **nur durch Hardware Änderungen behebbar**
- Mögliche Gegenvorkehrungen bewirken massive Performance Nachteile

Meltdown

1 Einführung

2 Spectre

3 Meltdown
- Grundinformationen
  - Veröffentlichung
  - Cache
  - Das Betriebssystem im virtuelle Adressraum
- Vorgehensweise
- Unterschied zu Spectre
- Gegenvorkehrungen / „Fixes“

4 Weiterführende Literatur

Meltdown - Grundinformationen

Veröffentlichung

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Meltdown - Grundinformationen
Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017
Veröffentlichung: 3. Jänner 2018

Meltdown - Grundinformationen
Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017
Veröffentlichung: 3. Jänner 2018

Entdecker:

Meltdown - Grundinformationen
Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017
Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas

Meltdown - Grundinformationen
Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017
Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas
G-Data Advanced Analytics	Anders Fogh

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas
G-Data Advanced Analytics	Anders Fogh
Google Project Zero	Jann Horn

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas
G-Data Advanced Analytics	Anders Fogh
Google Project Zero	Jann Horn
University of Michigan	Daniel Genkin

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas
G-Data Advanced Analytics	Anders Fogh
Google Project Zero	Jann Horn
University of Michigan	Daniel Genkin
University of Adelaide	Yuval Yarom

Meltdown - Grundinformationen

Veröffentlichung

Meltdown ist eine Sicherheitslücke, die hardwareseitige Zugriffsbeschränkungen „schmelzen“ lässt.

Entdeckung: 28. Juli 2017

Veröffentlichung: 3. Jänner 2018

Entdecker:

TU Graz	Moritz Lipp
	Michael Schwarz
	Daniel Gruss
	Stefan Mangard
Cyberus Technology GmbH	Thomas Prescher
	Werner Haas
G-Data Advanced Analytics	Anders Fogh
Google Project Zero	Jann Horn
University of Michigan	Daniel Genkin
University of Adelaide	Yuval Yarom
Rambus Security Division	Mike Hamburg

Meltdown - Grundinformationen
Cache

Meltdown - Grundinformationen
Cache

- Zugriff auf Arbeitsspeicher ist vergleichsweise teuer

Meltdown - Grundinformationen
Cache

- Zugriff auf Arbeitsspeicher ist vergleichsweise teuer
- Räumliche und zeitliche Lokalität trifft auf viele Programme zu

Meltdown - Grundinformationen
Cache

- Zugriff auf Arbeitsspeicher ist vergleichsweise teuer
- Räumliche und zeitliche Lokalität trifft auf viele Programme zu

Cache

Caches sind **kleine Zwischenspeicher**, die direkt im Prozessor verbaut sind. Nahegelegene Daten werden vorgeladen und abgelegt, um auf diese schneller zugreifen zu können.

Meltdown - Grundinformationen
Cache

Meltdown - Grundinformationen
Cache

- Zugriff auf gecached Daten ist wesentlich schneller

Meltdown - Grundinformationen
Cache

- Zugriff auf gecached Daten ist wesentlich schneller
- Moderne CPUs haben drei bis vier **Levels** an Caches. Je größer, desto langsamer ist der Zugriff

Meltdown - Grundinformationen
Cache

- Zugriff auf gecached Daten ist wesentlich schneller
- Moderne CPUs haben drei bis vier **Levels** an Caches. Je größer, desto langsamer ist der Zugriff

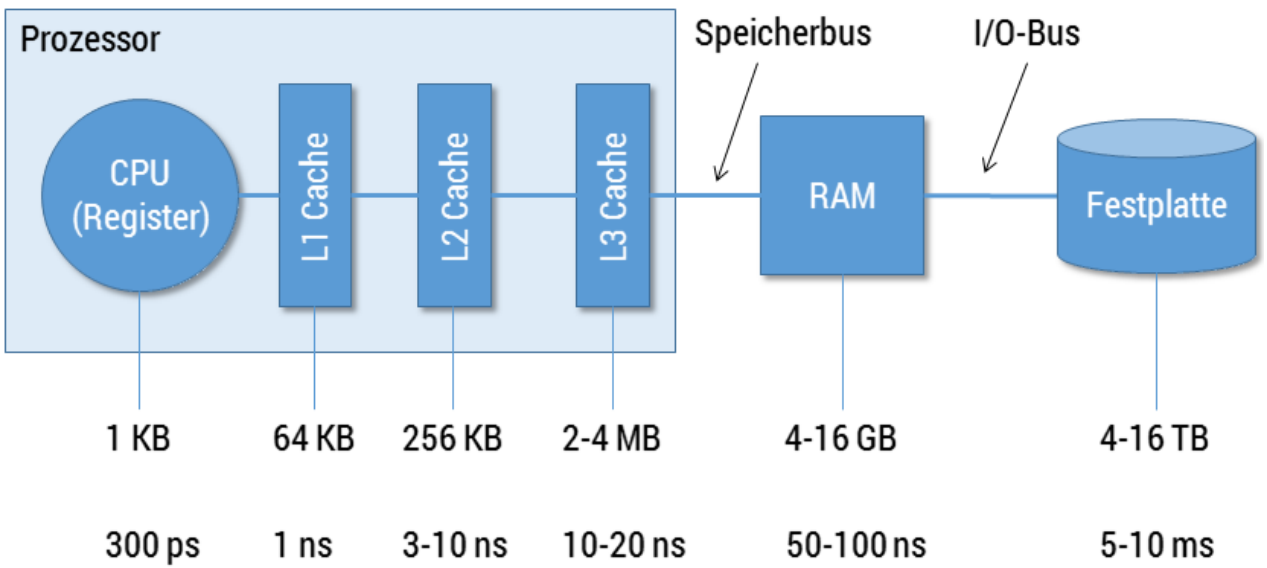


Abbildung: Speicherhierachie[1]

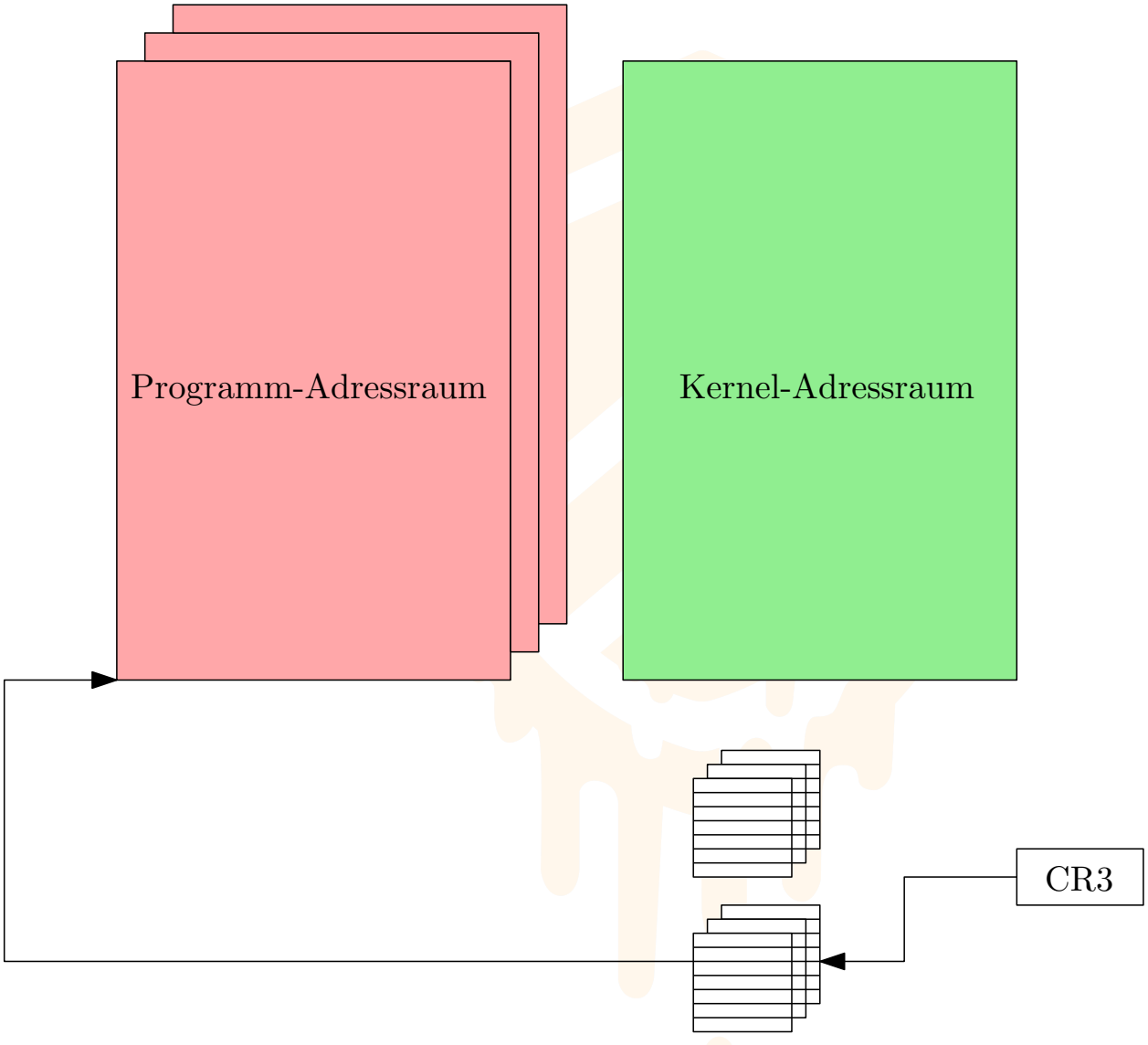
[1] Quelle: TU Chemnitz - Rechnerarchitektur und -systeme

Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum

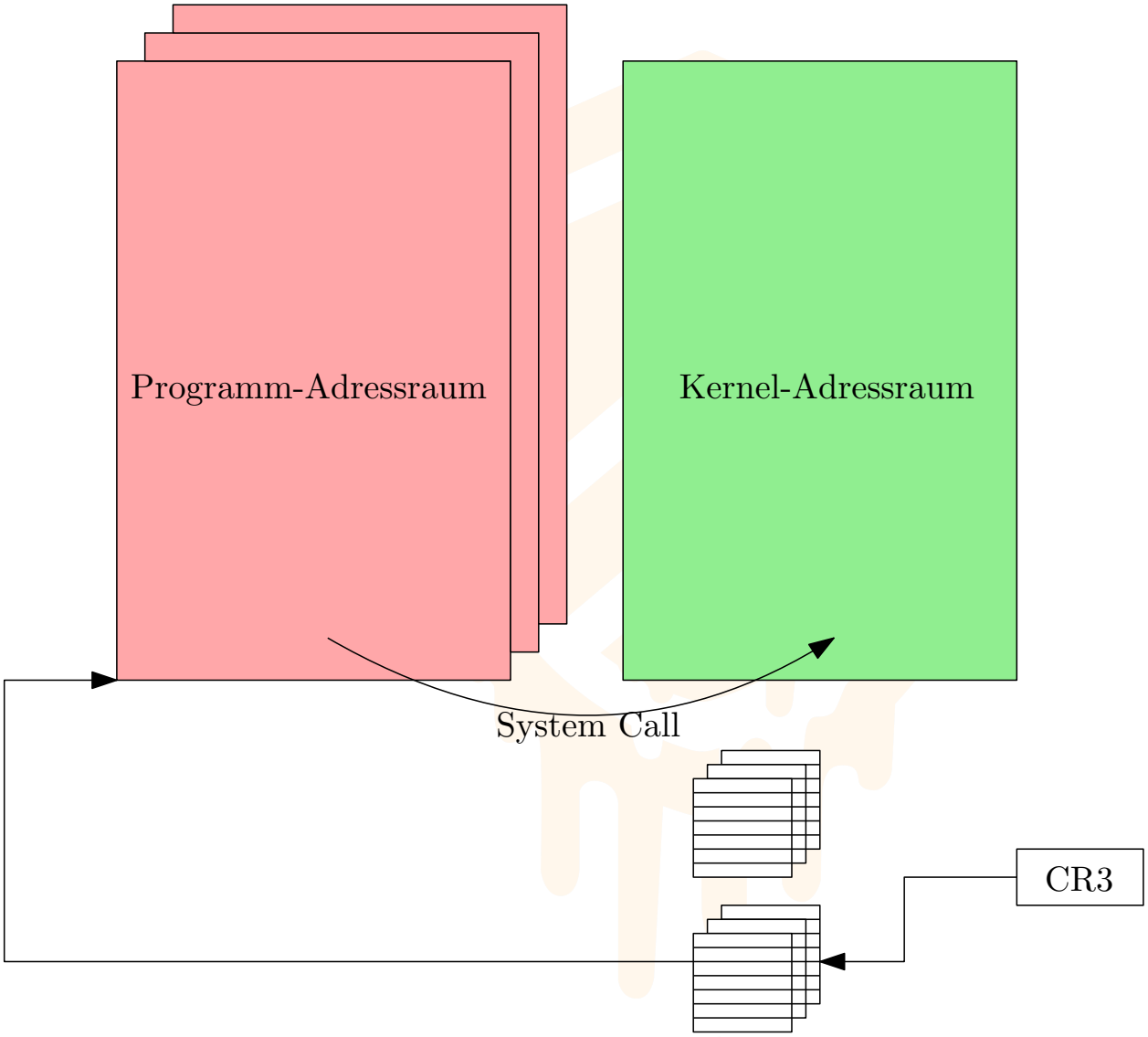
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



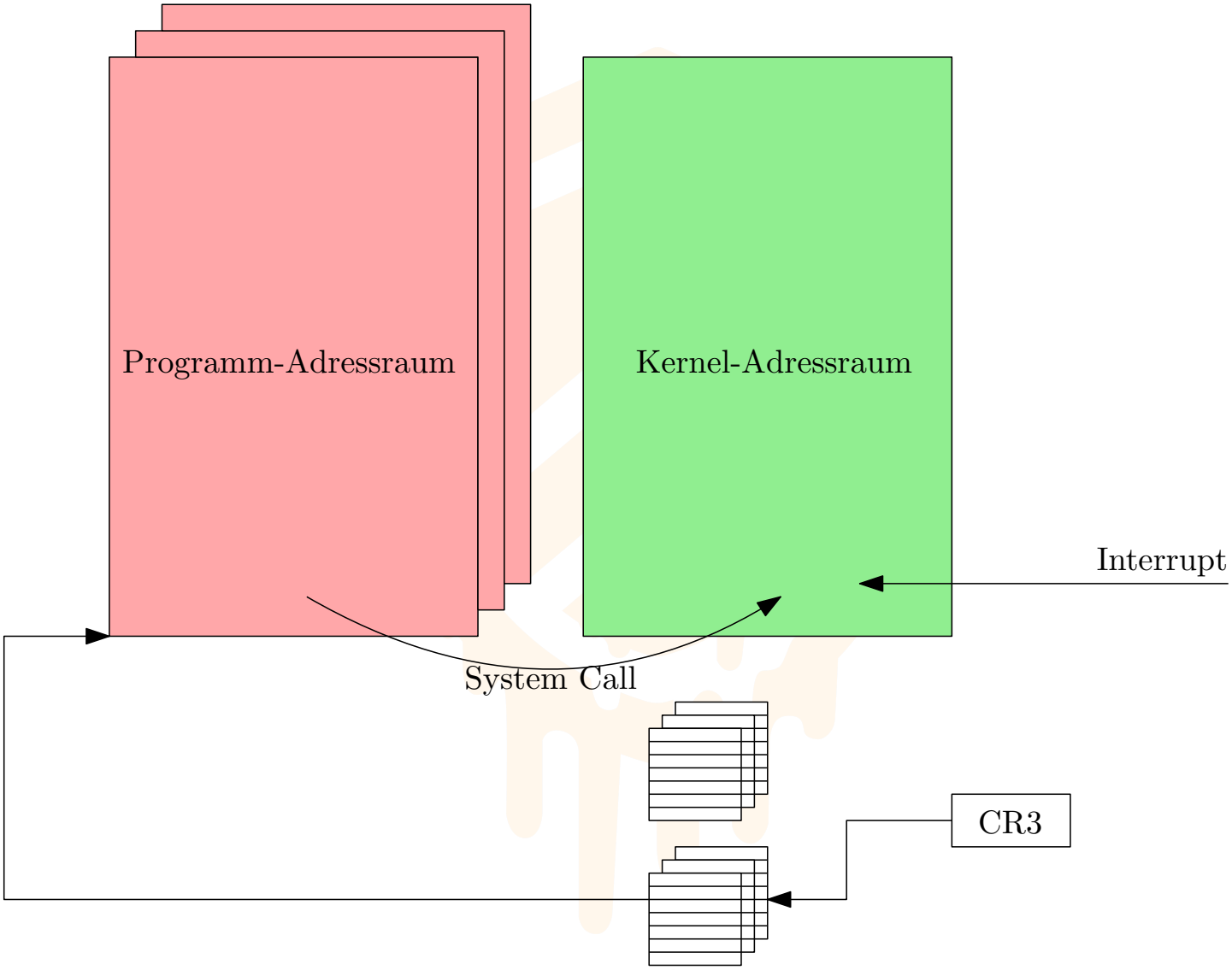
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



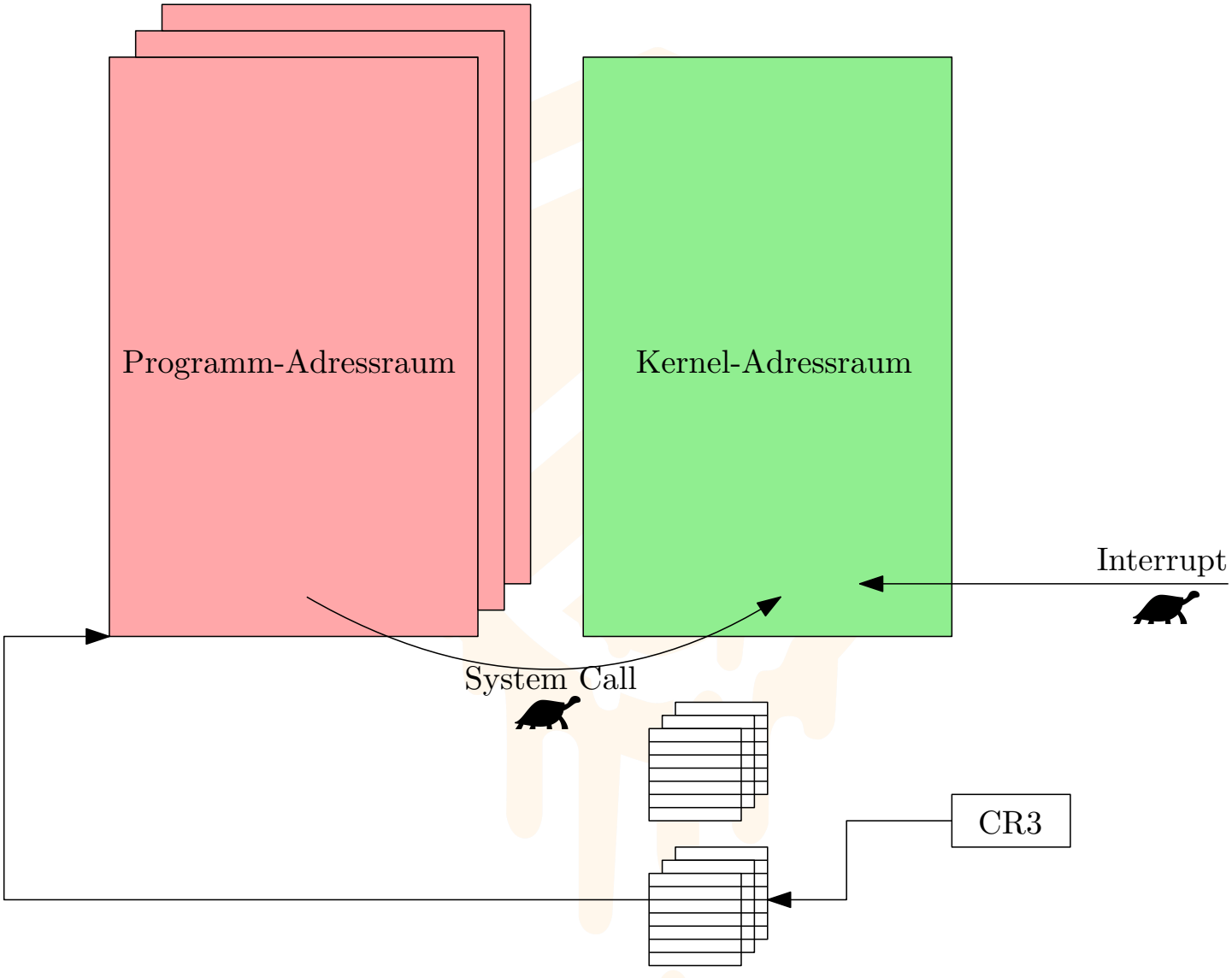
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



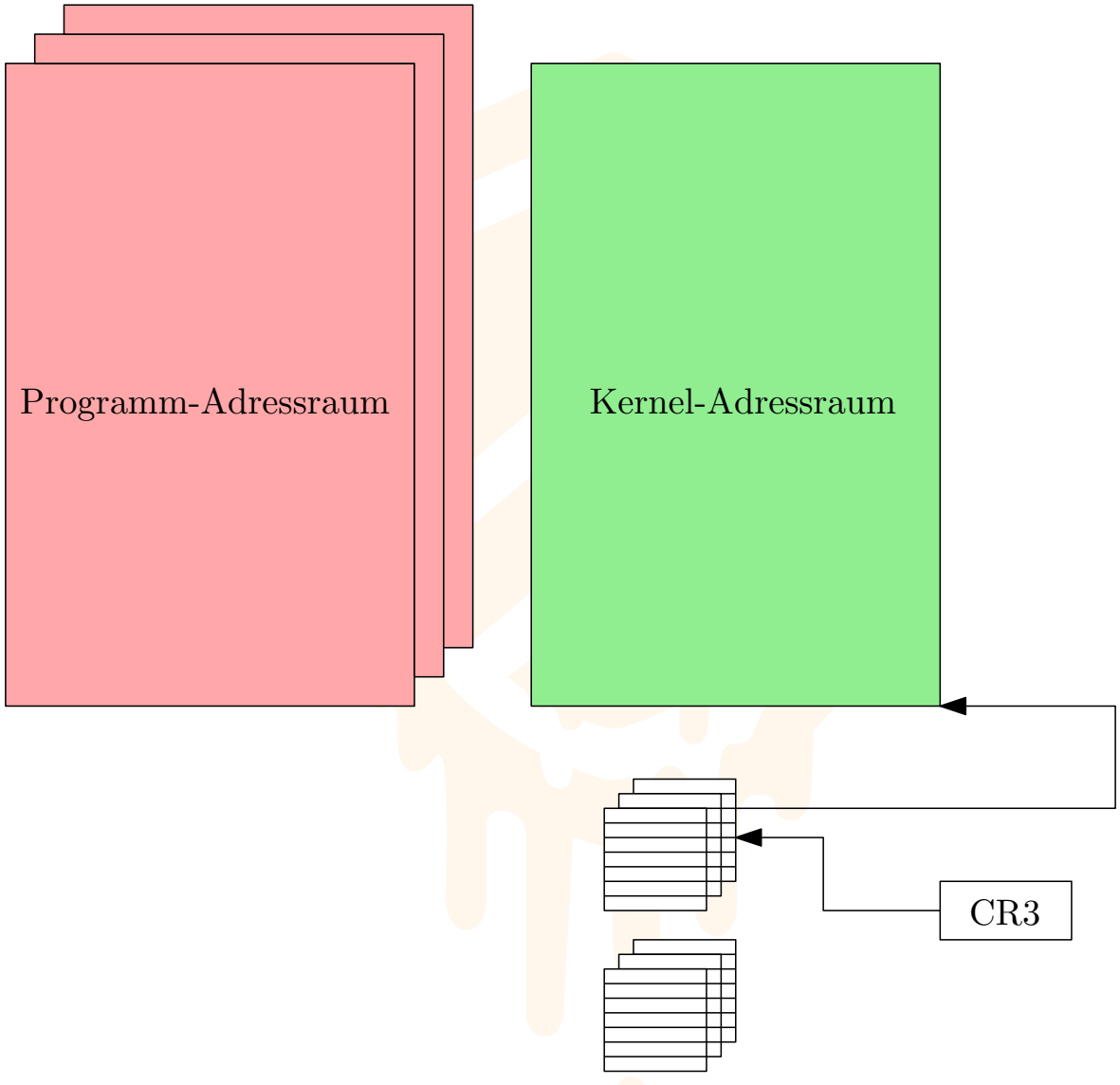
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



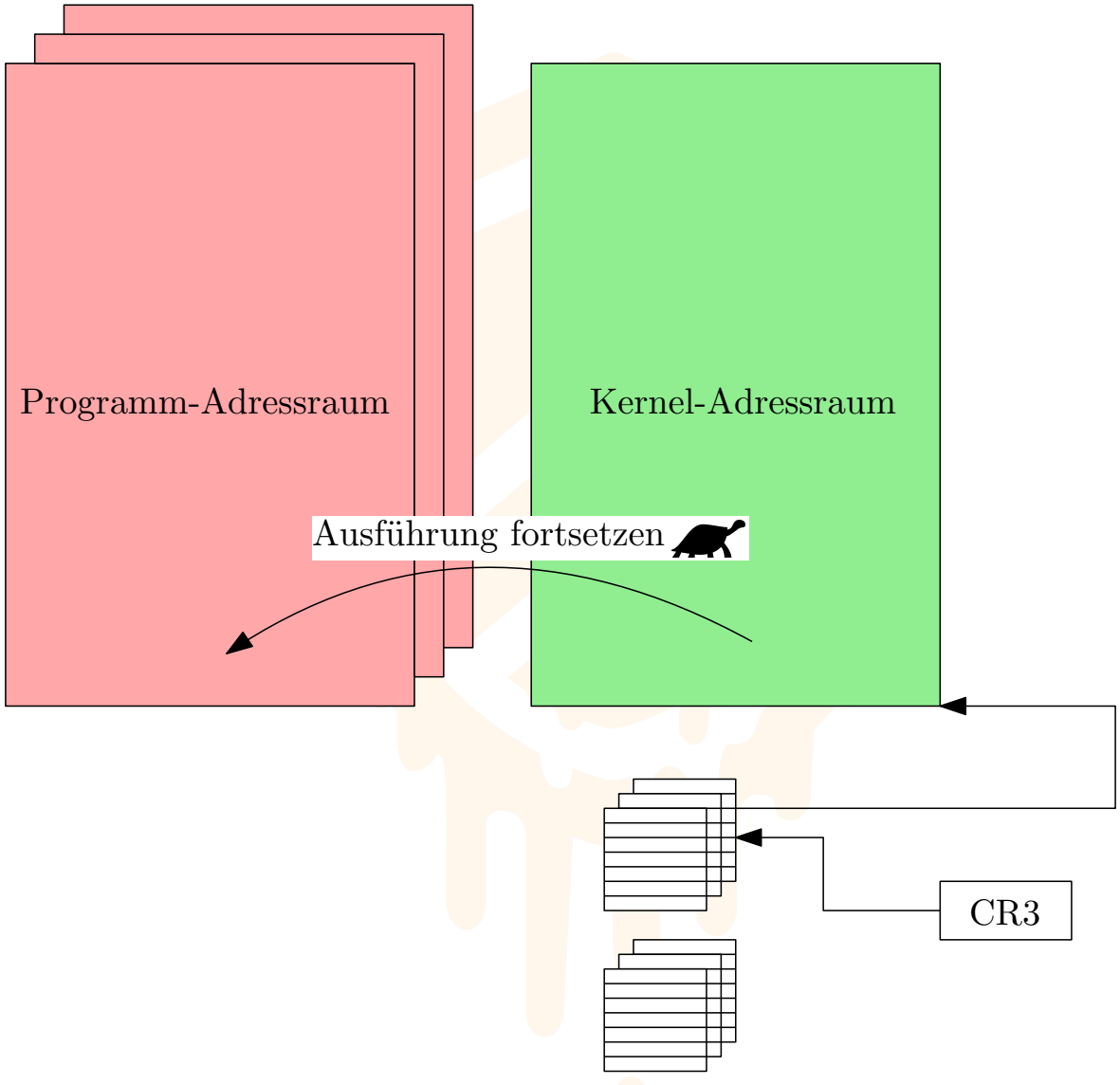
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



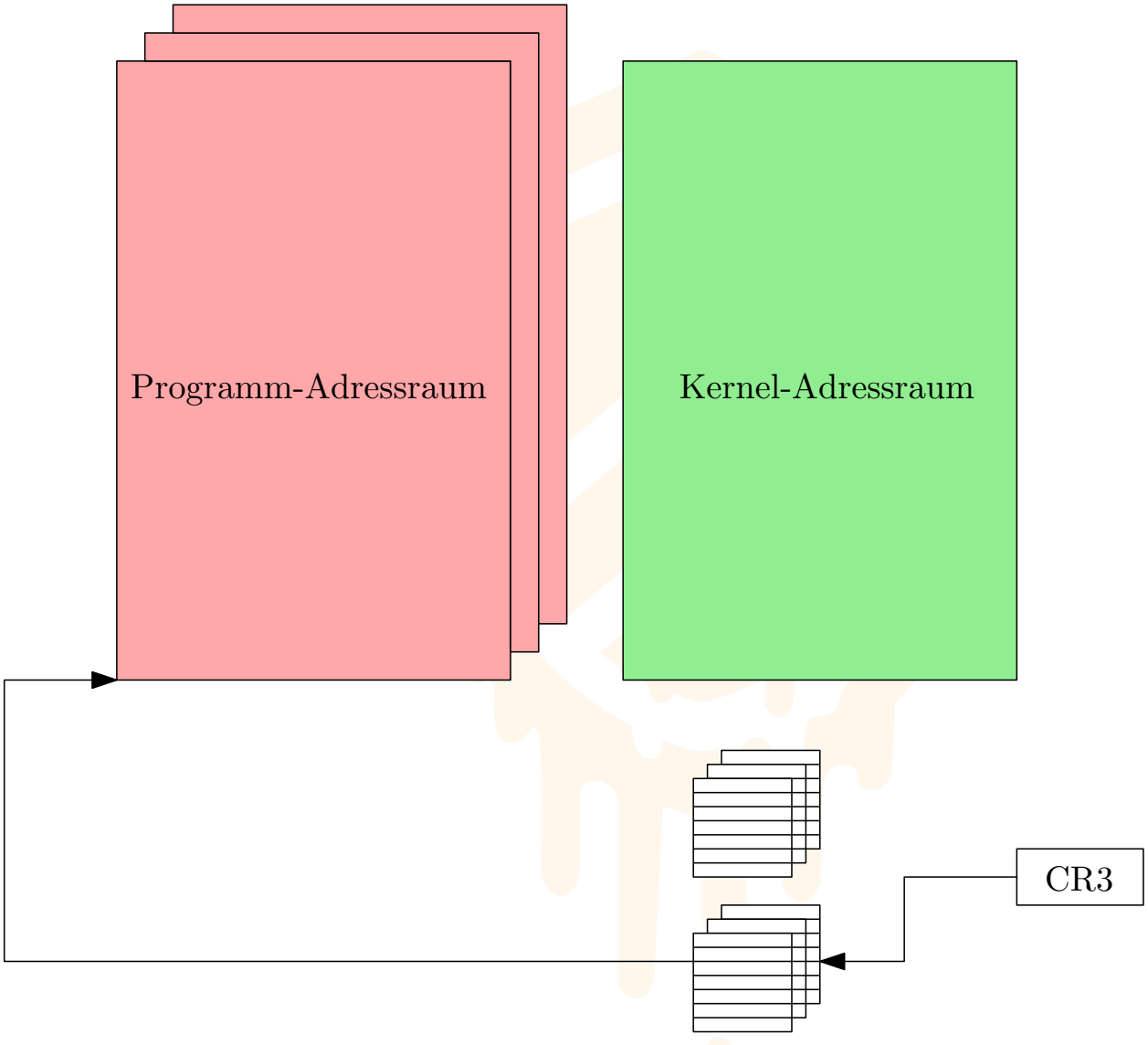
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



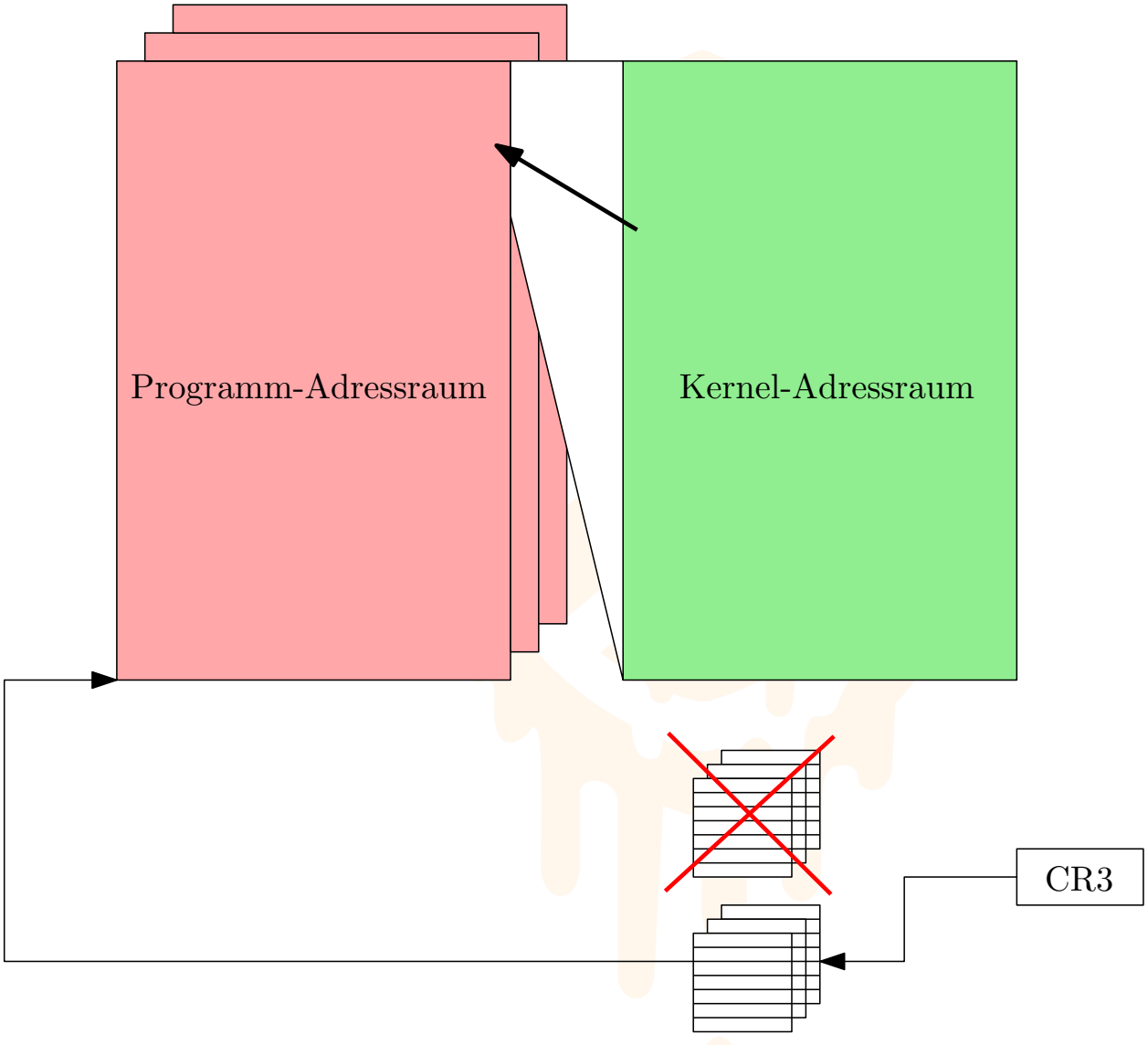
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



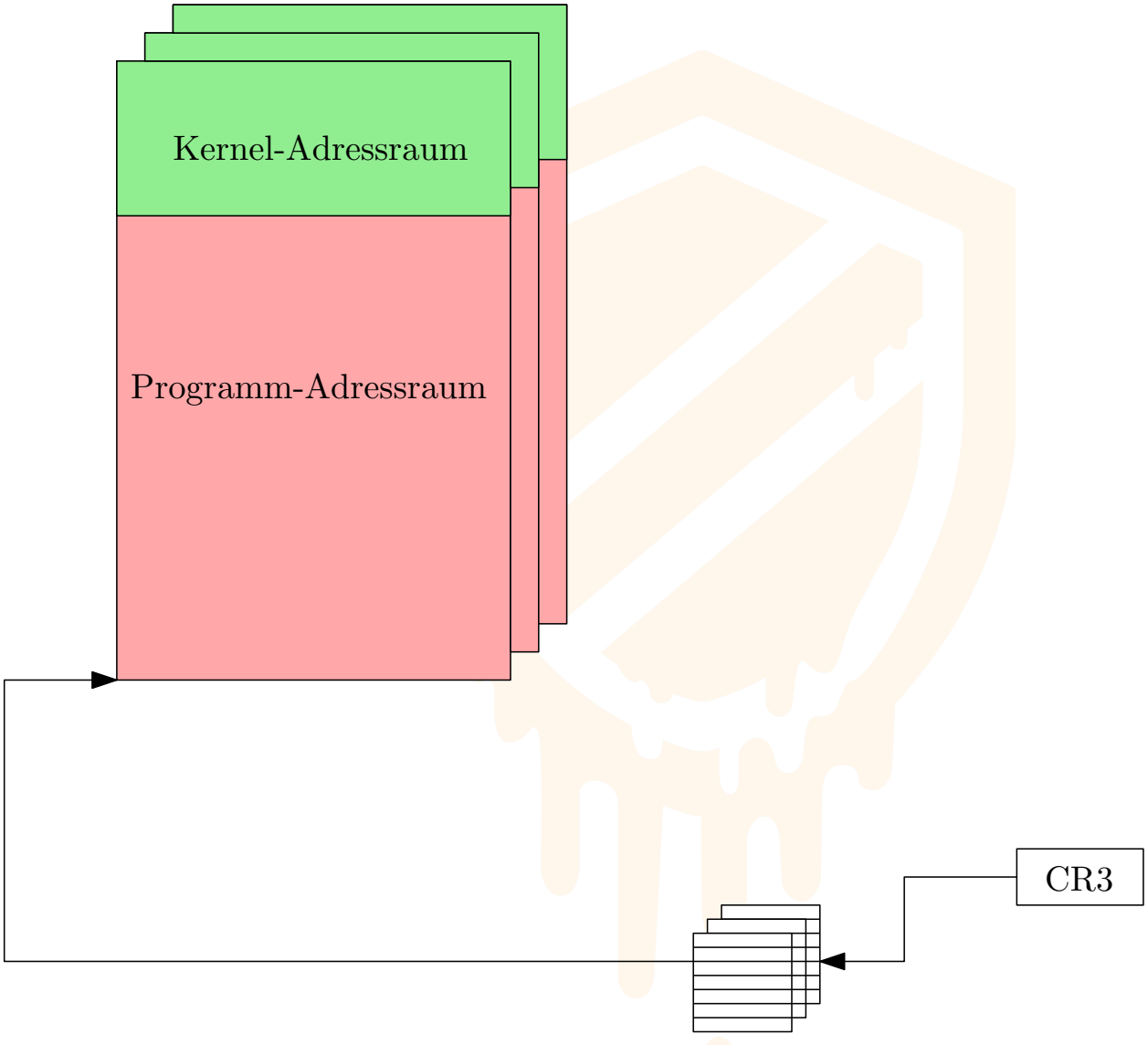
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



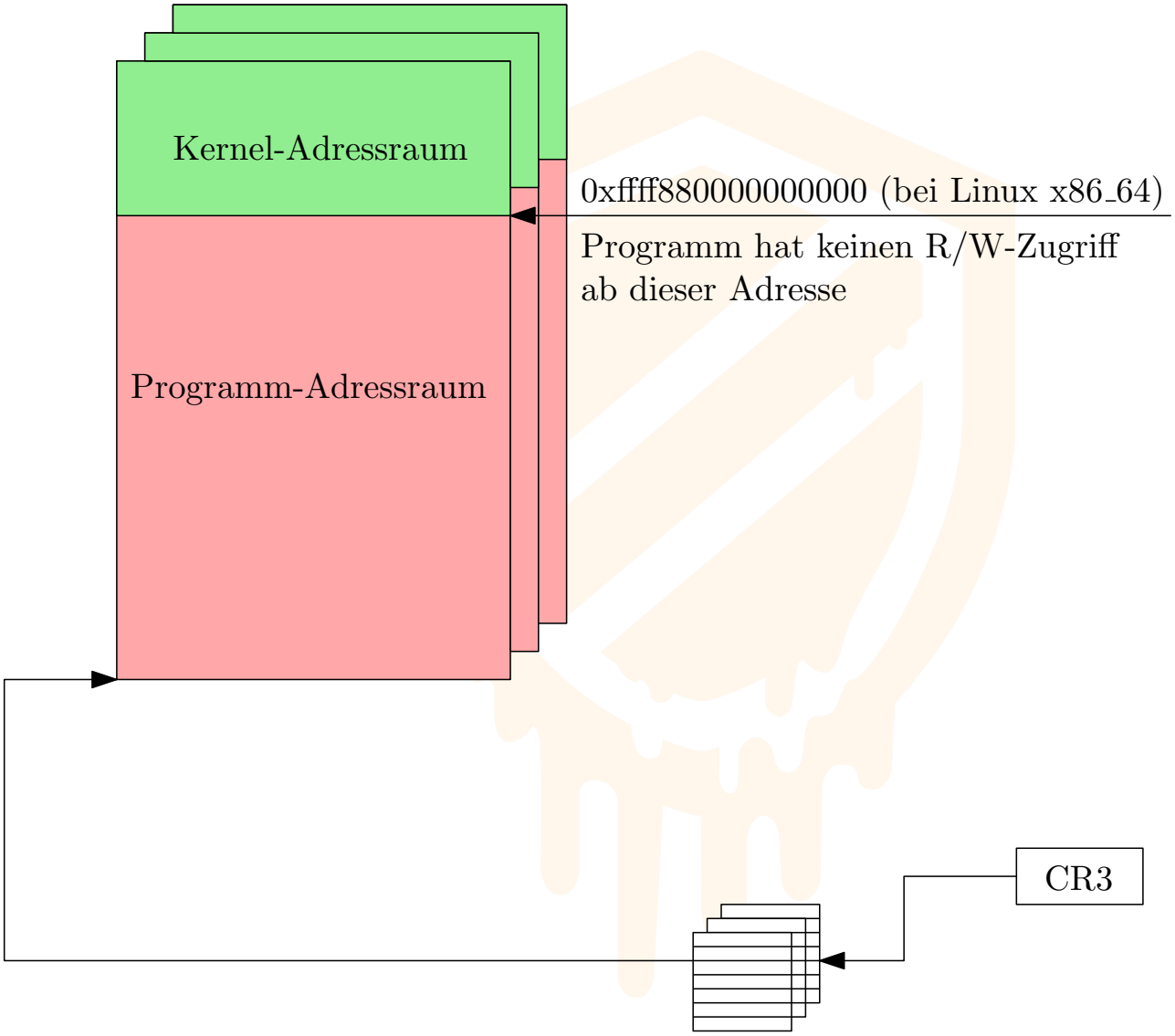
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



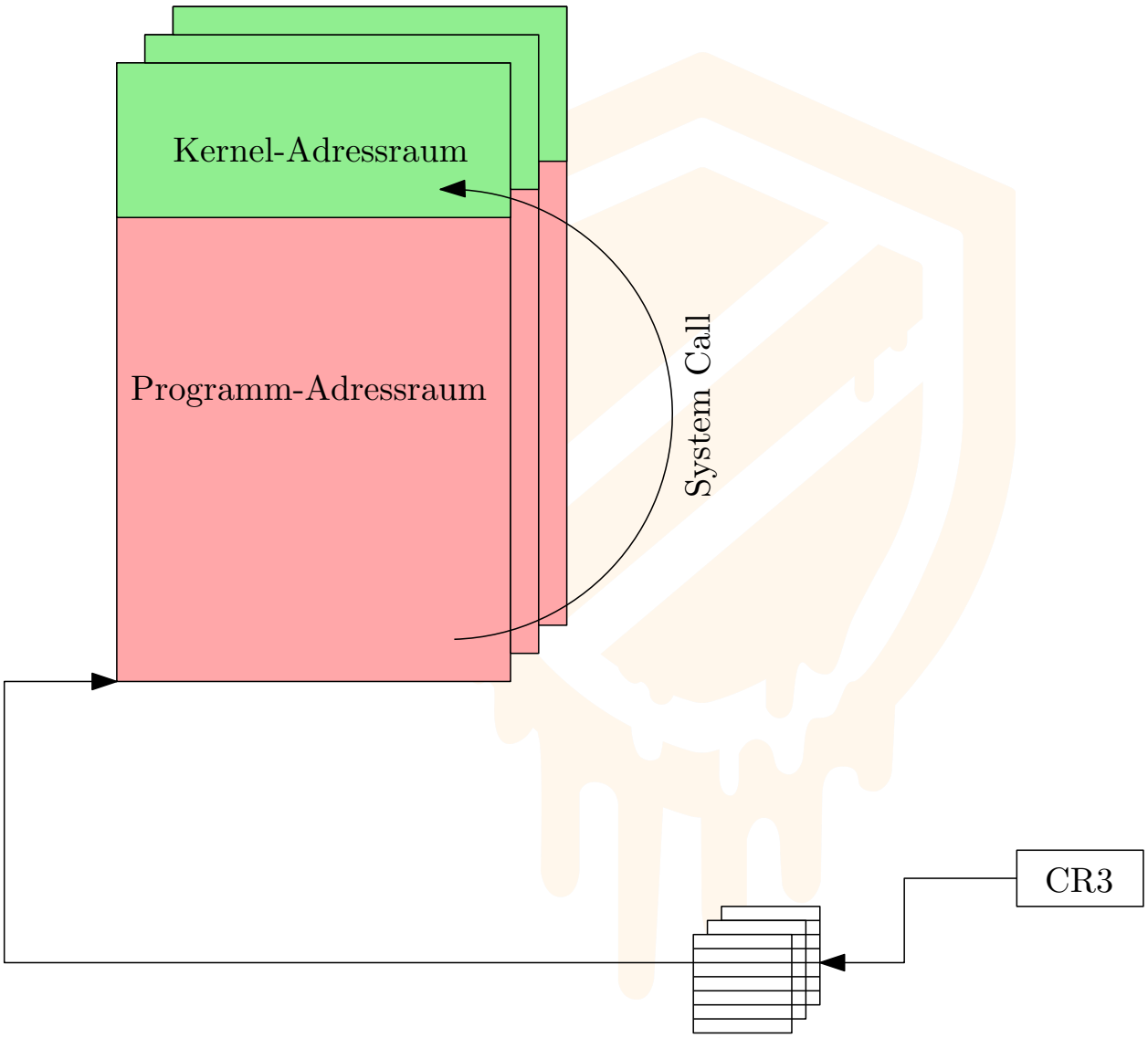
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



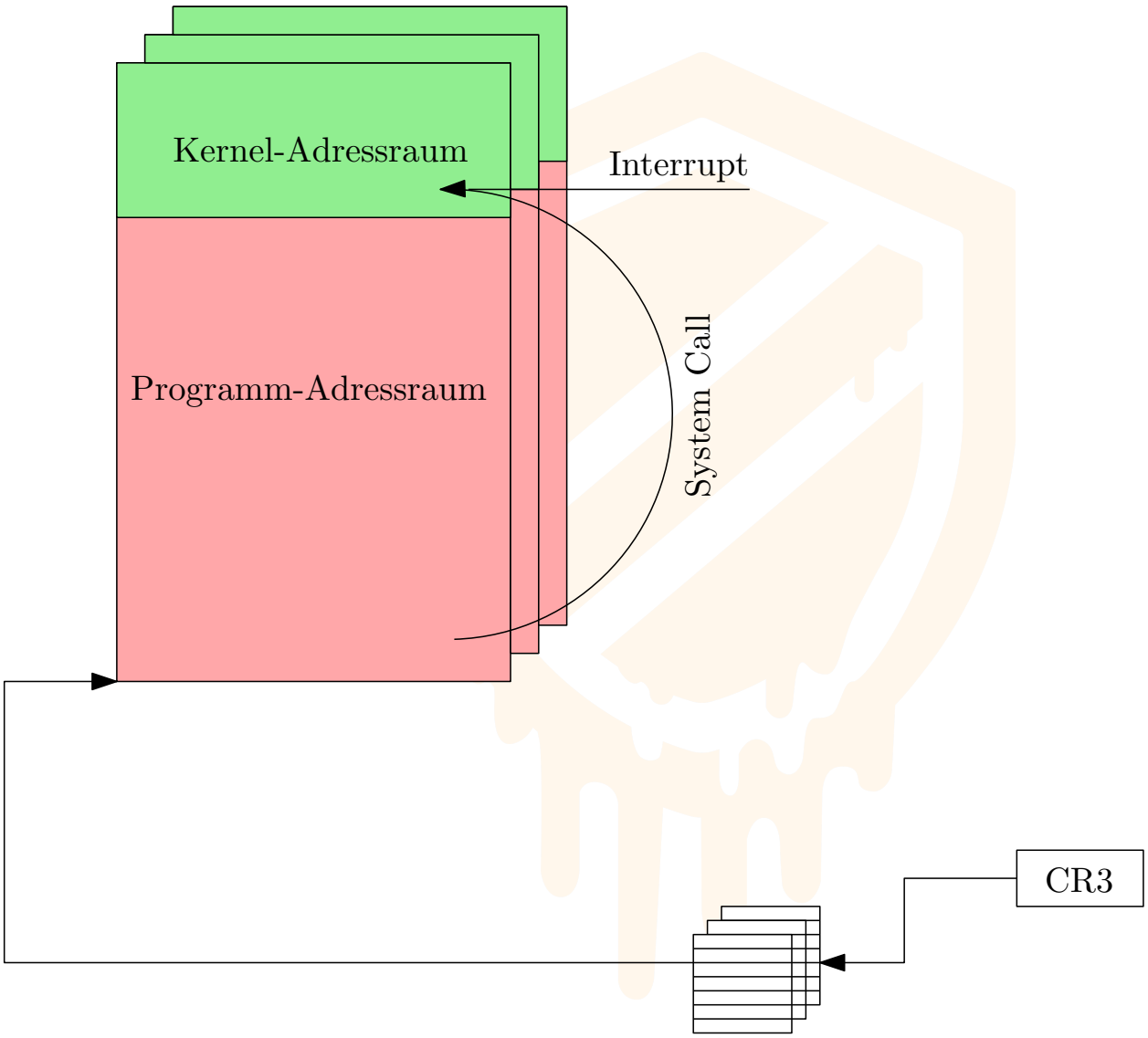
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



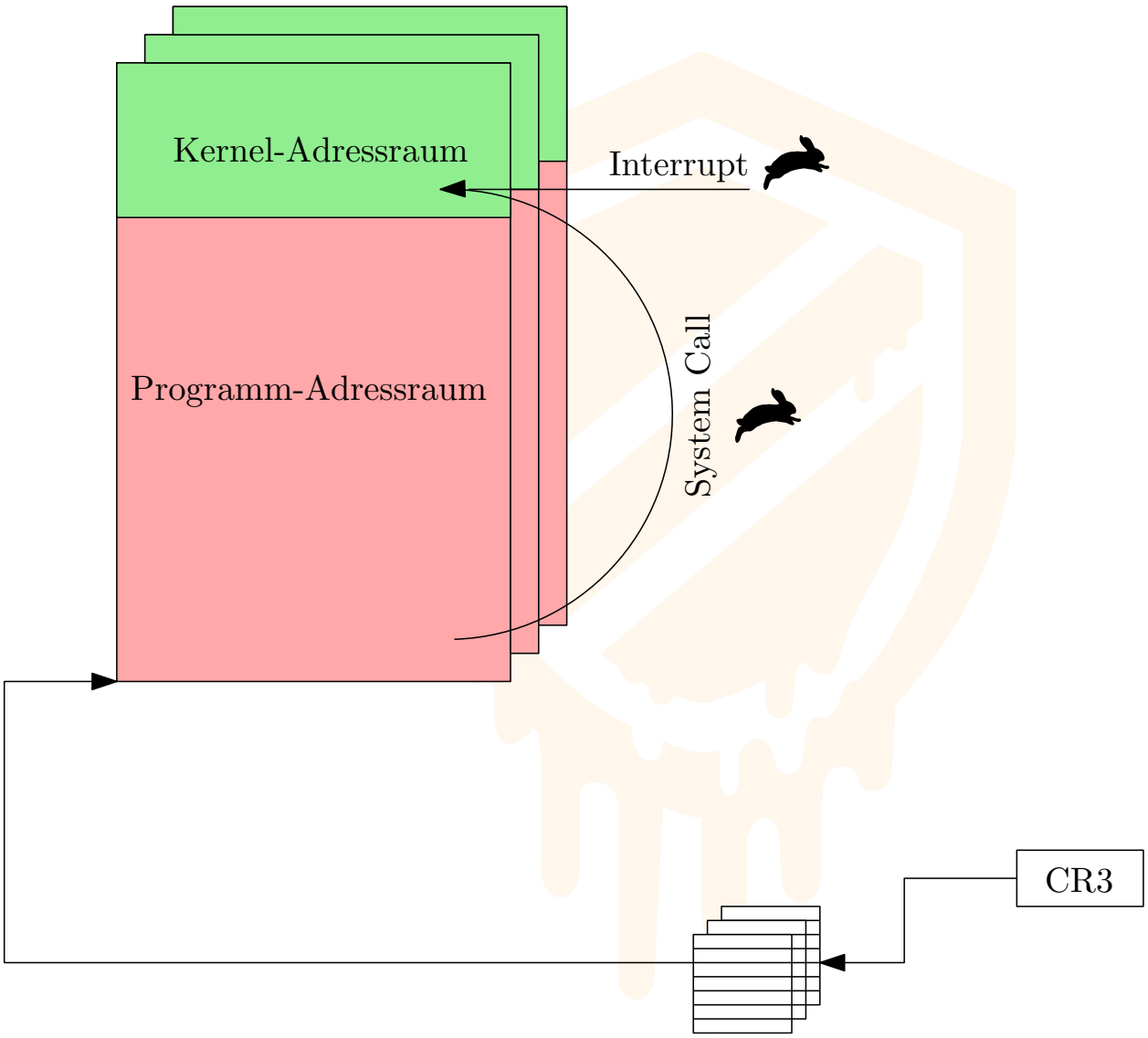
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



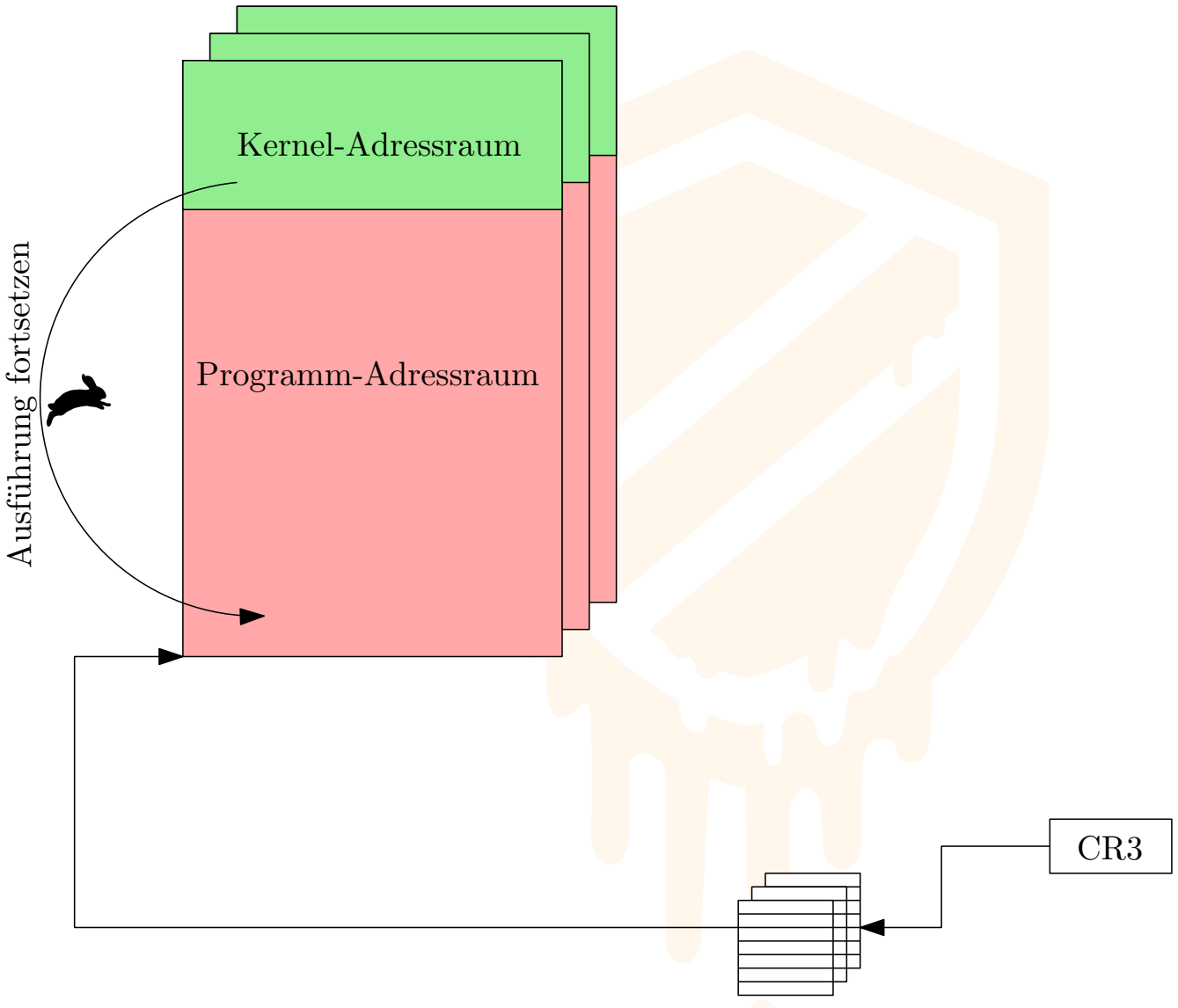
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



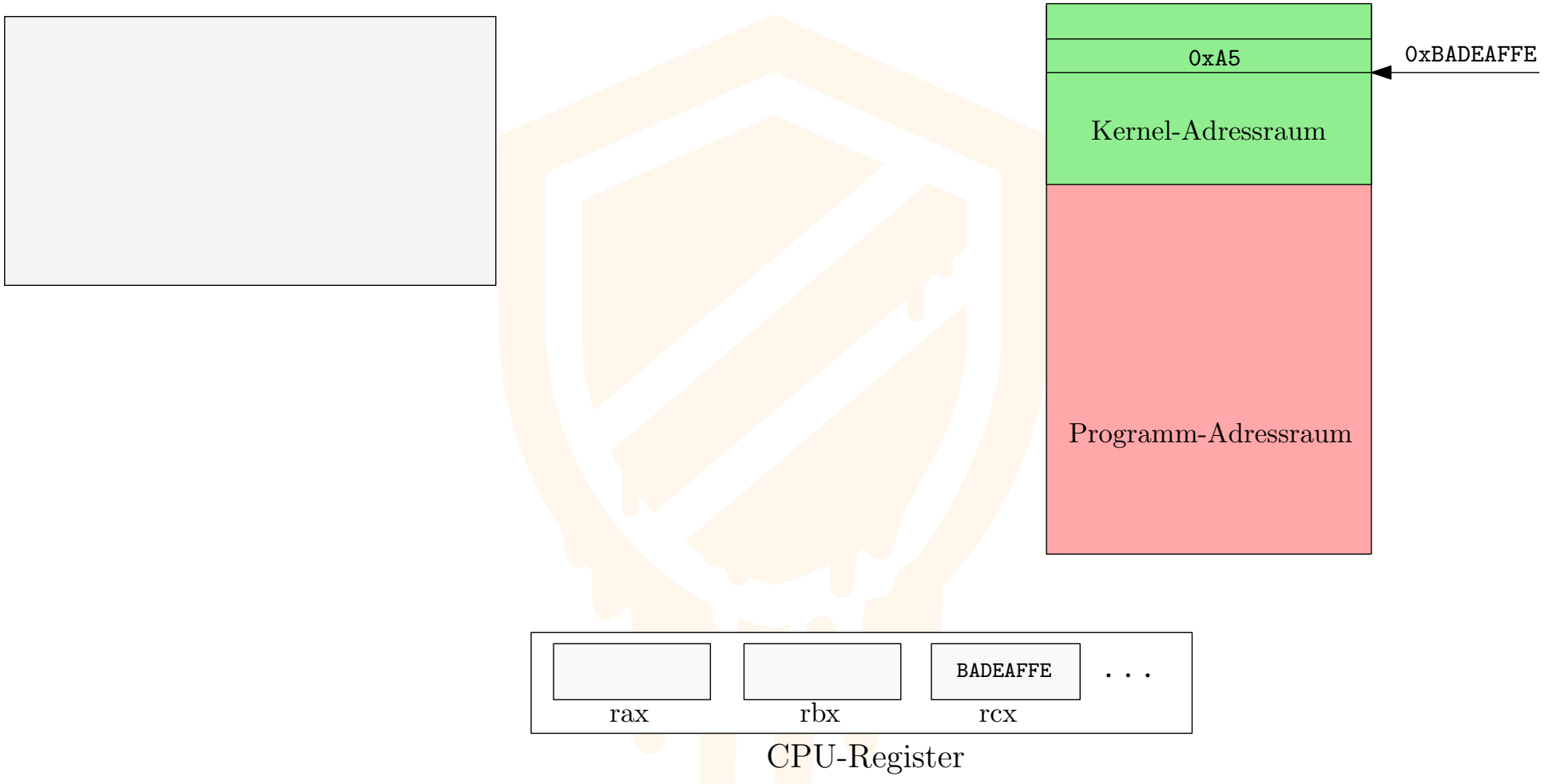
Meltdown - Grundinformationen

Das Betriebssystem im virtuelle Adressraum



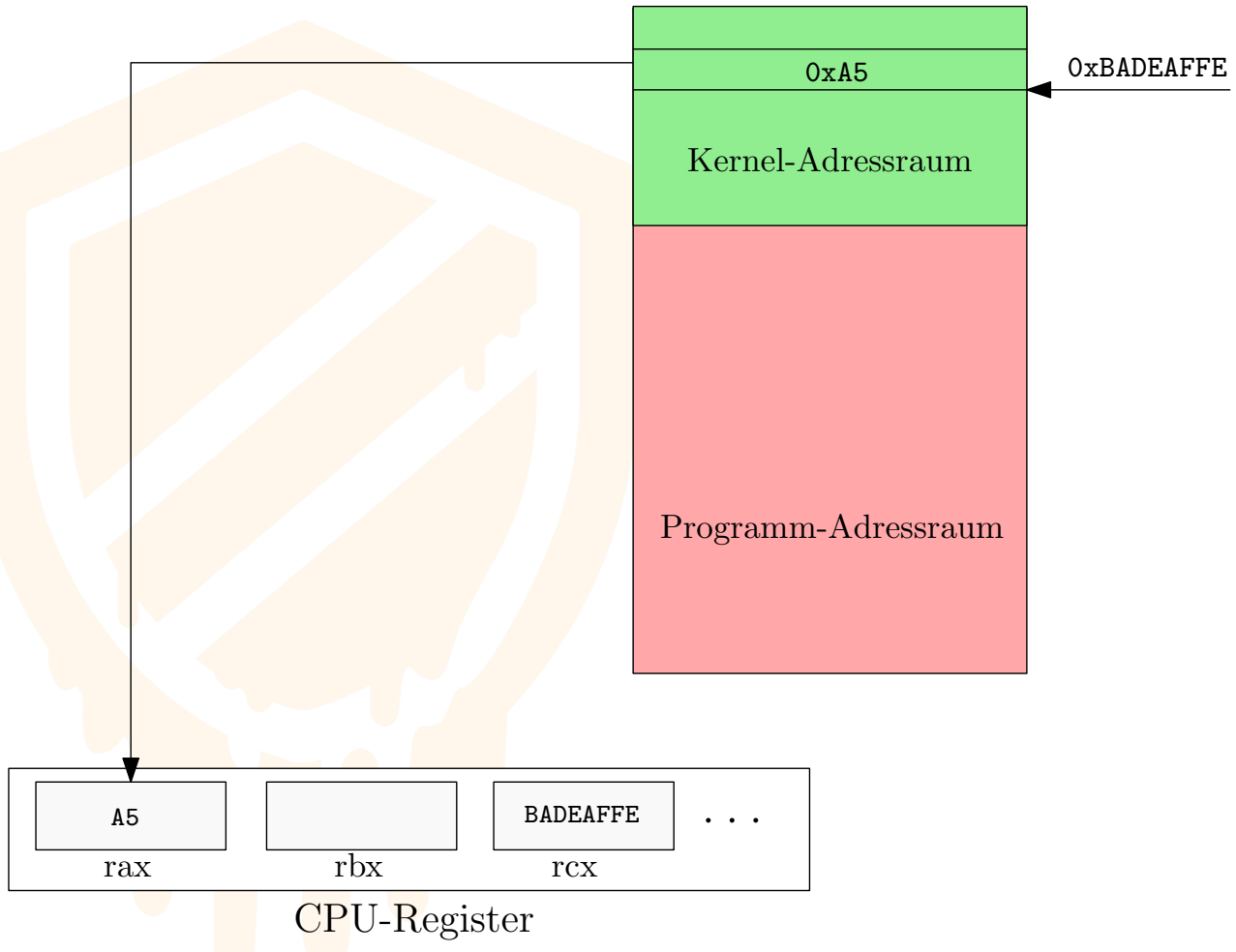
Meltdown - Vorgehensweise

Meltdown - Vorgehensweise

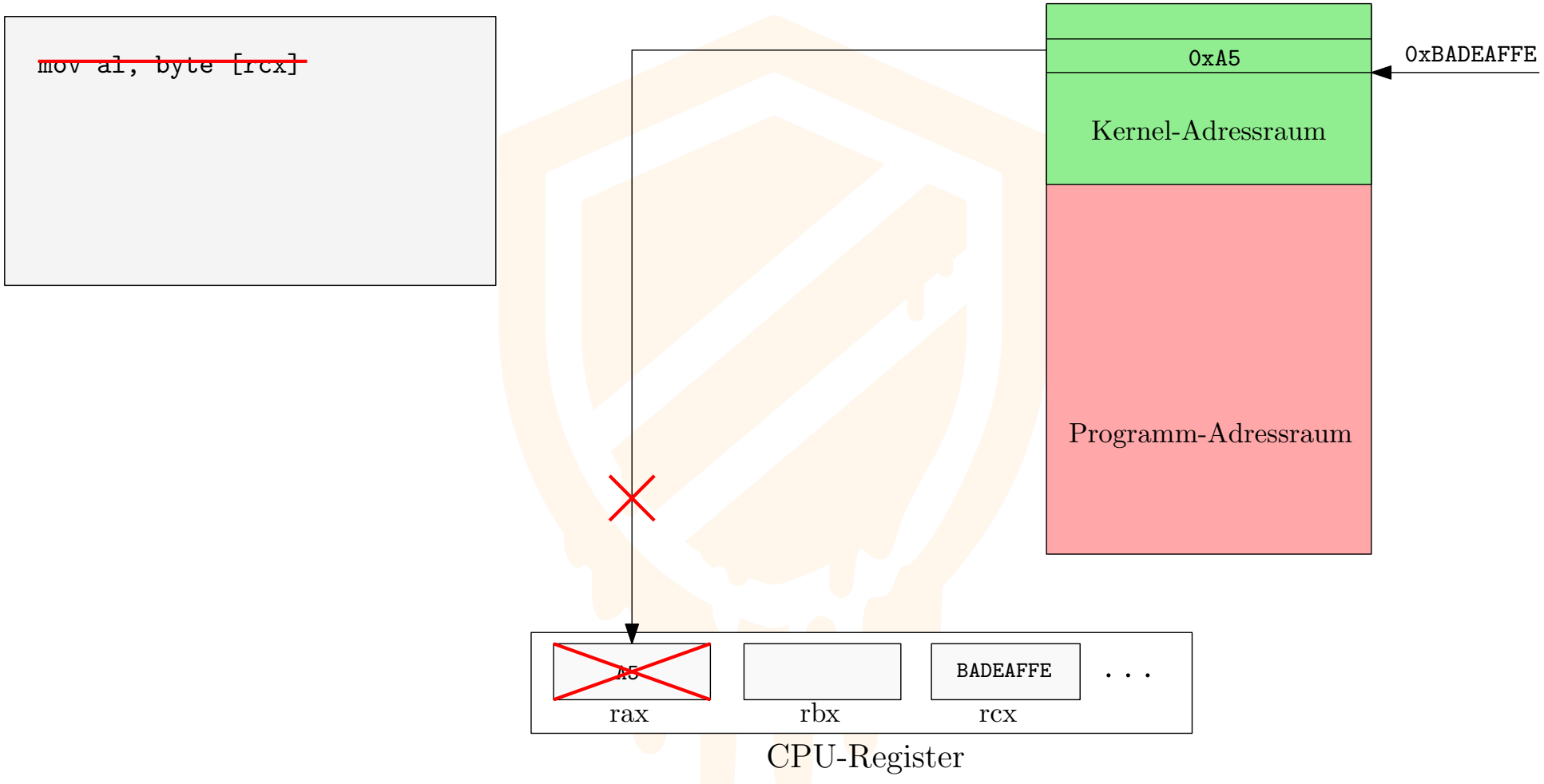


Meltdown - Vorgehensweise

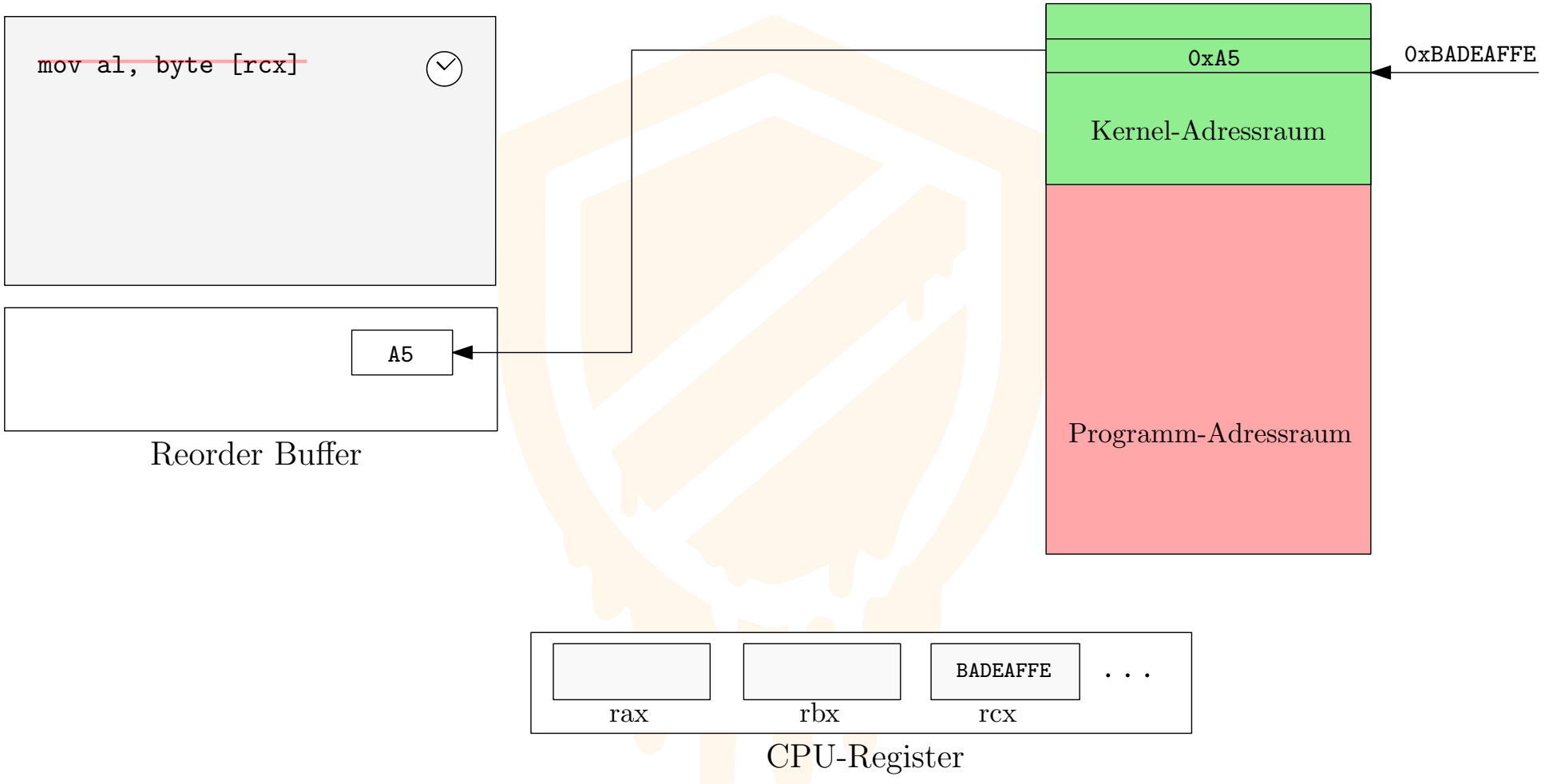
```
mov al, byte [rcx]
```



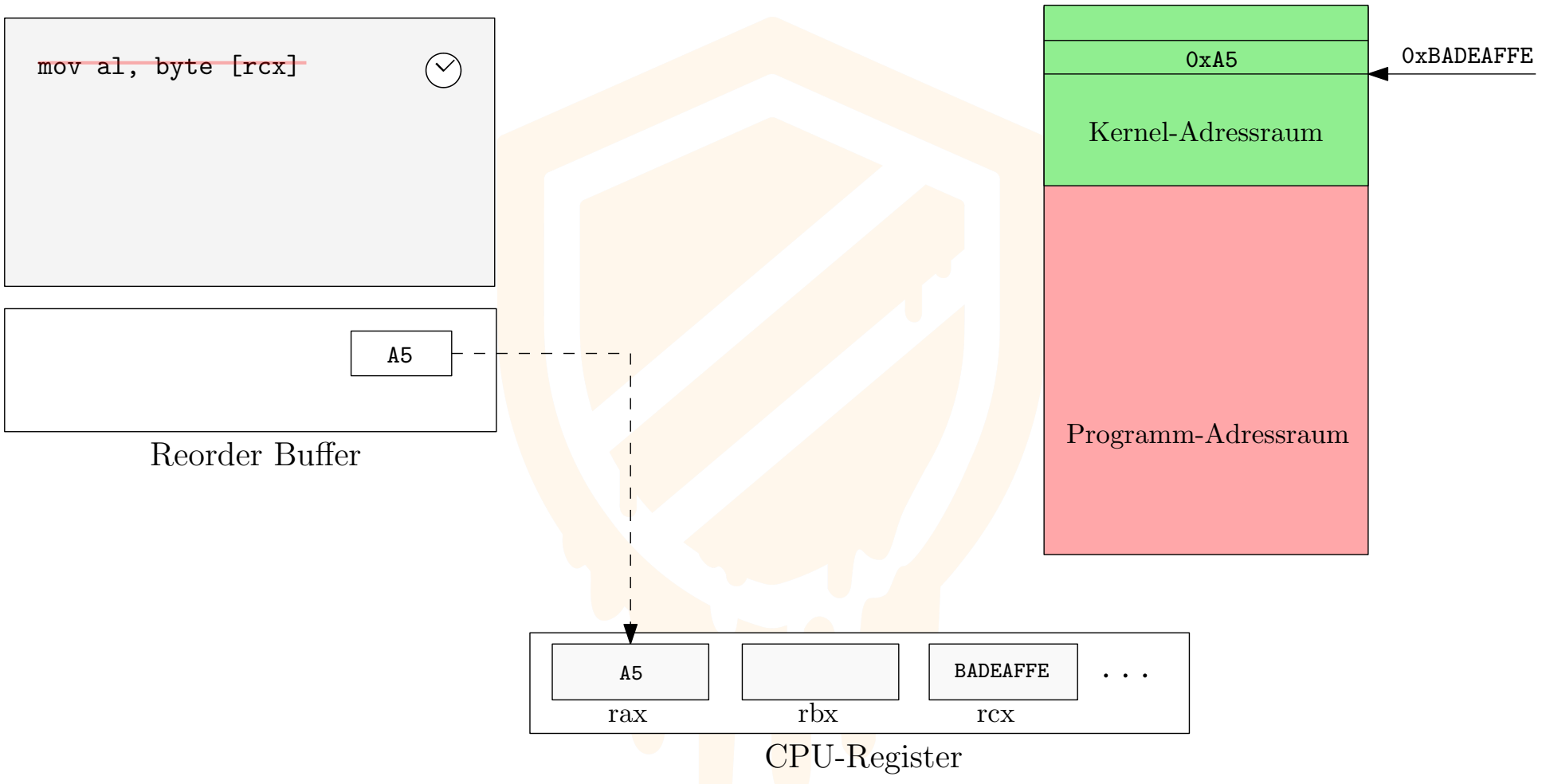
Meltdown - Vorgehensweise



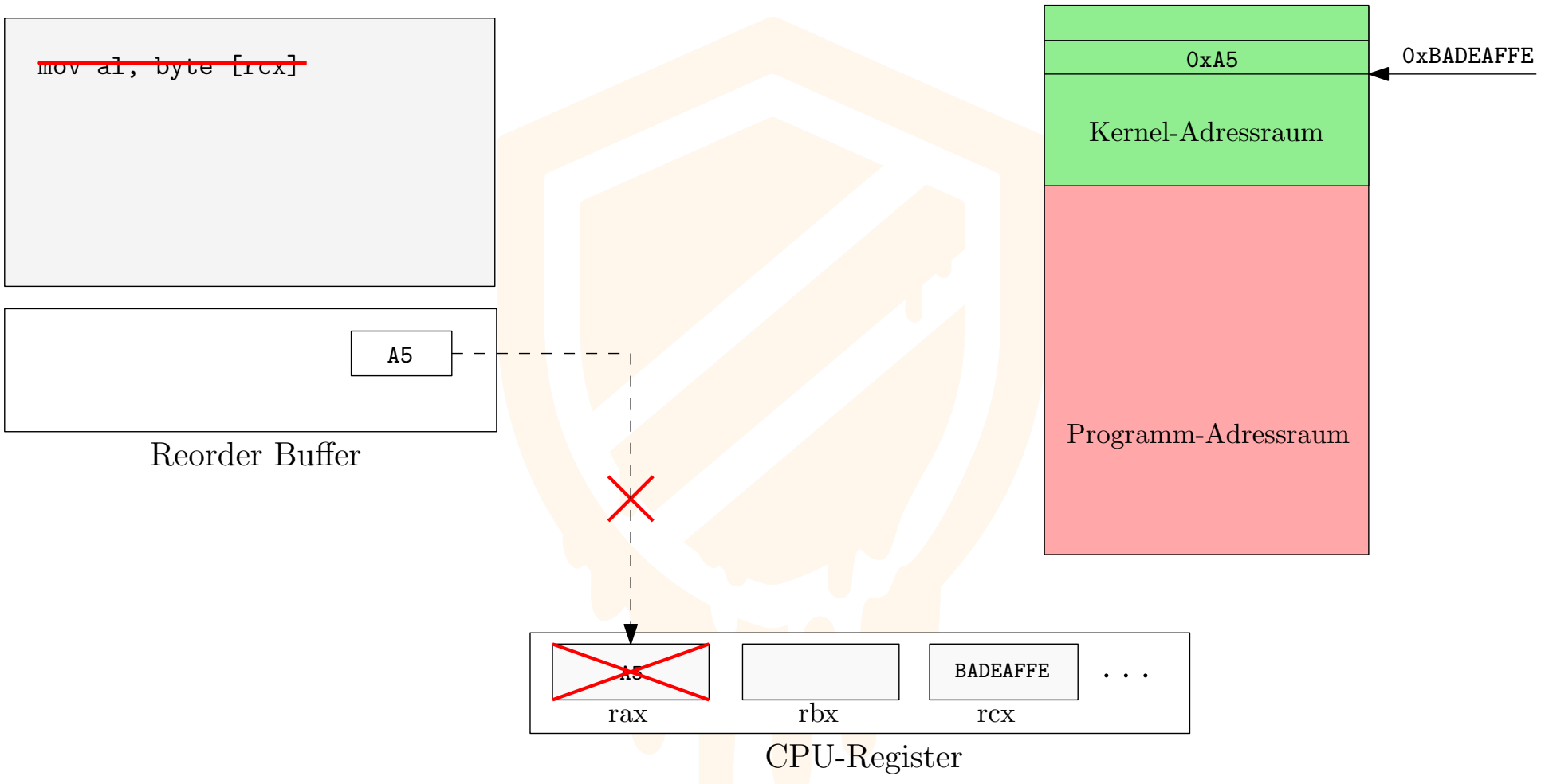
Meltdown - Vorgehensweise



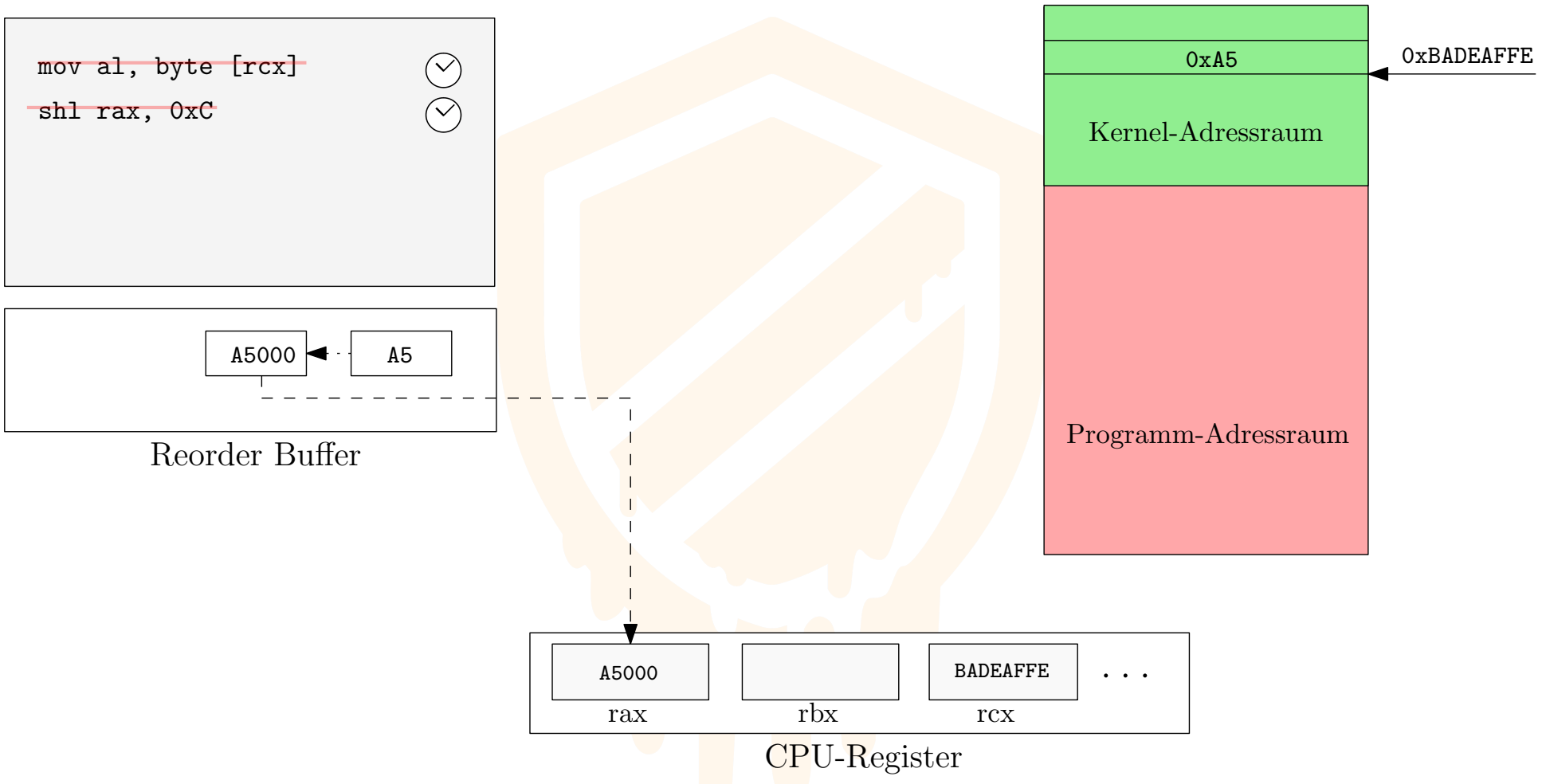
Meltdown - Vorgehensweise



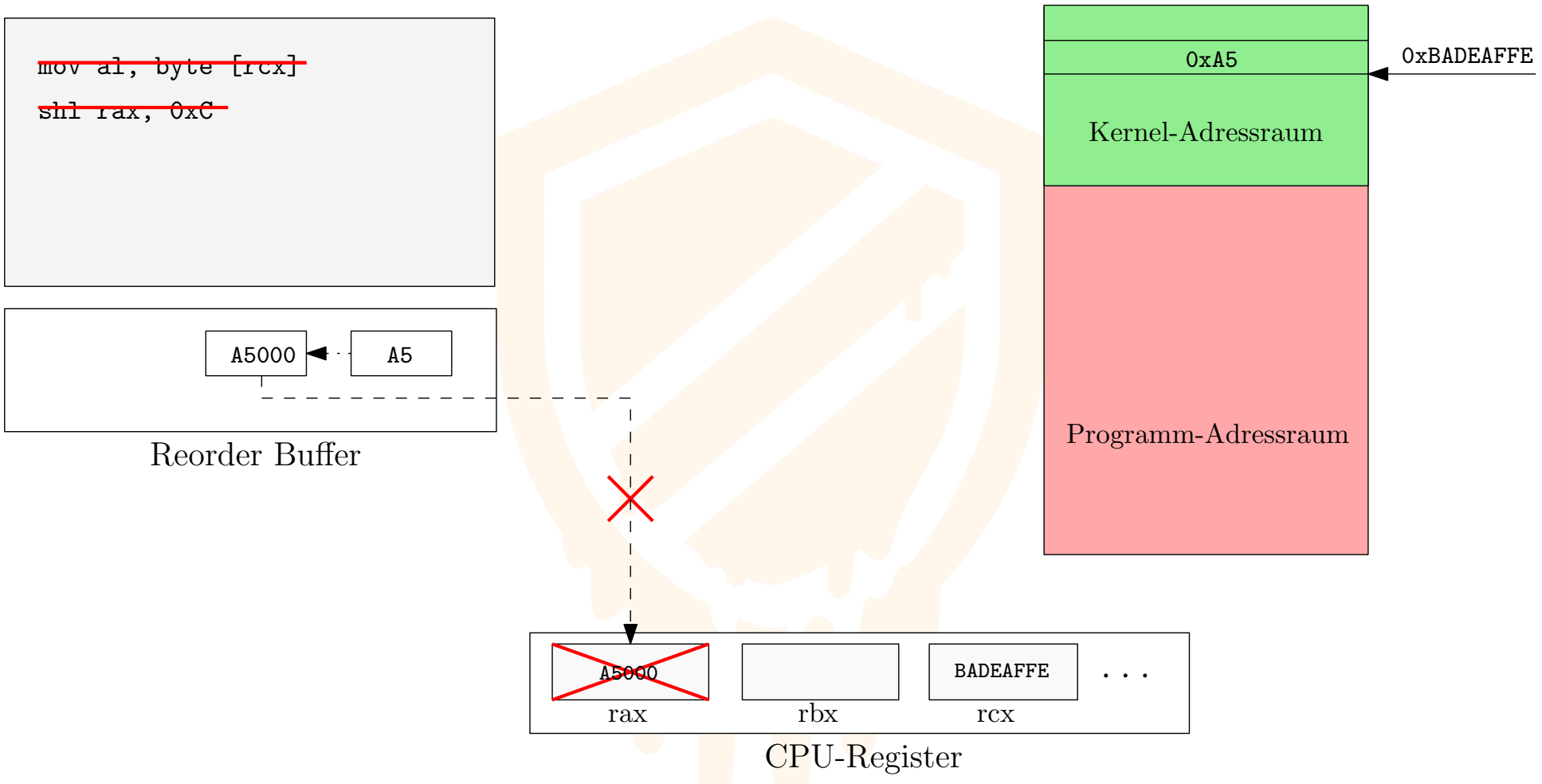
Meltdown - Vorgehensweise



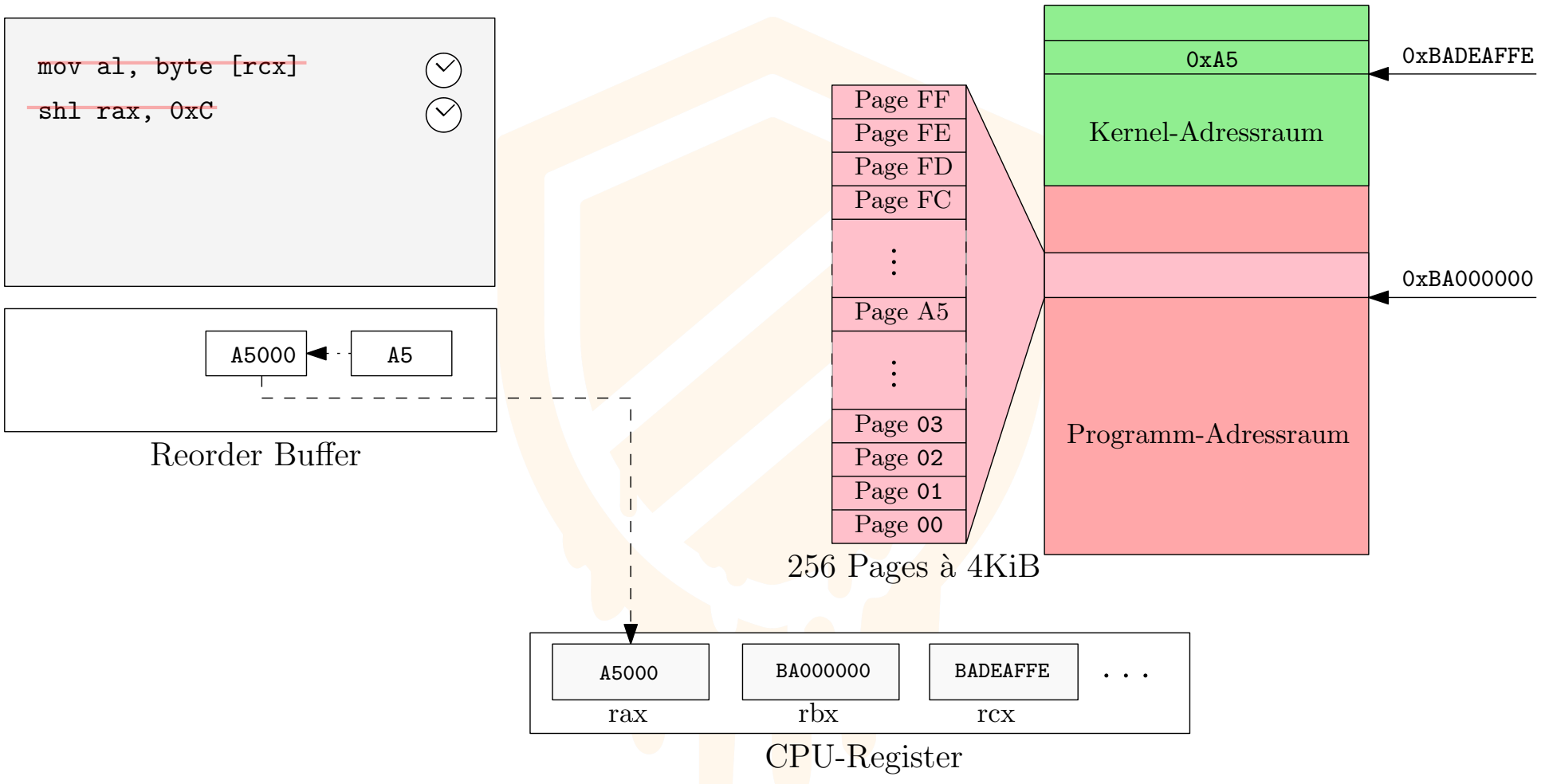
Meltdown - Vorgehensweise



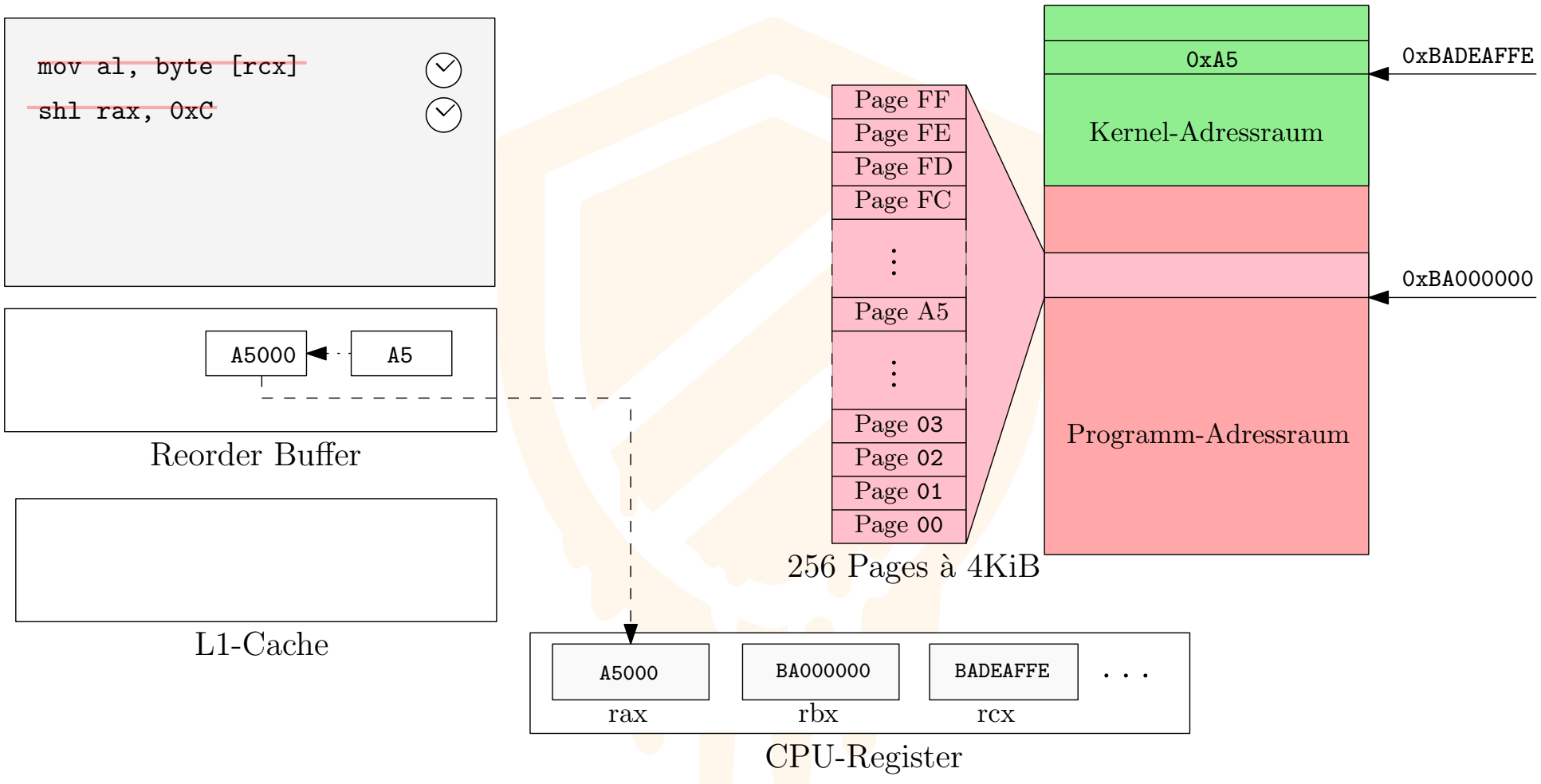
Meltdown - Vorgehensweise



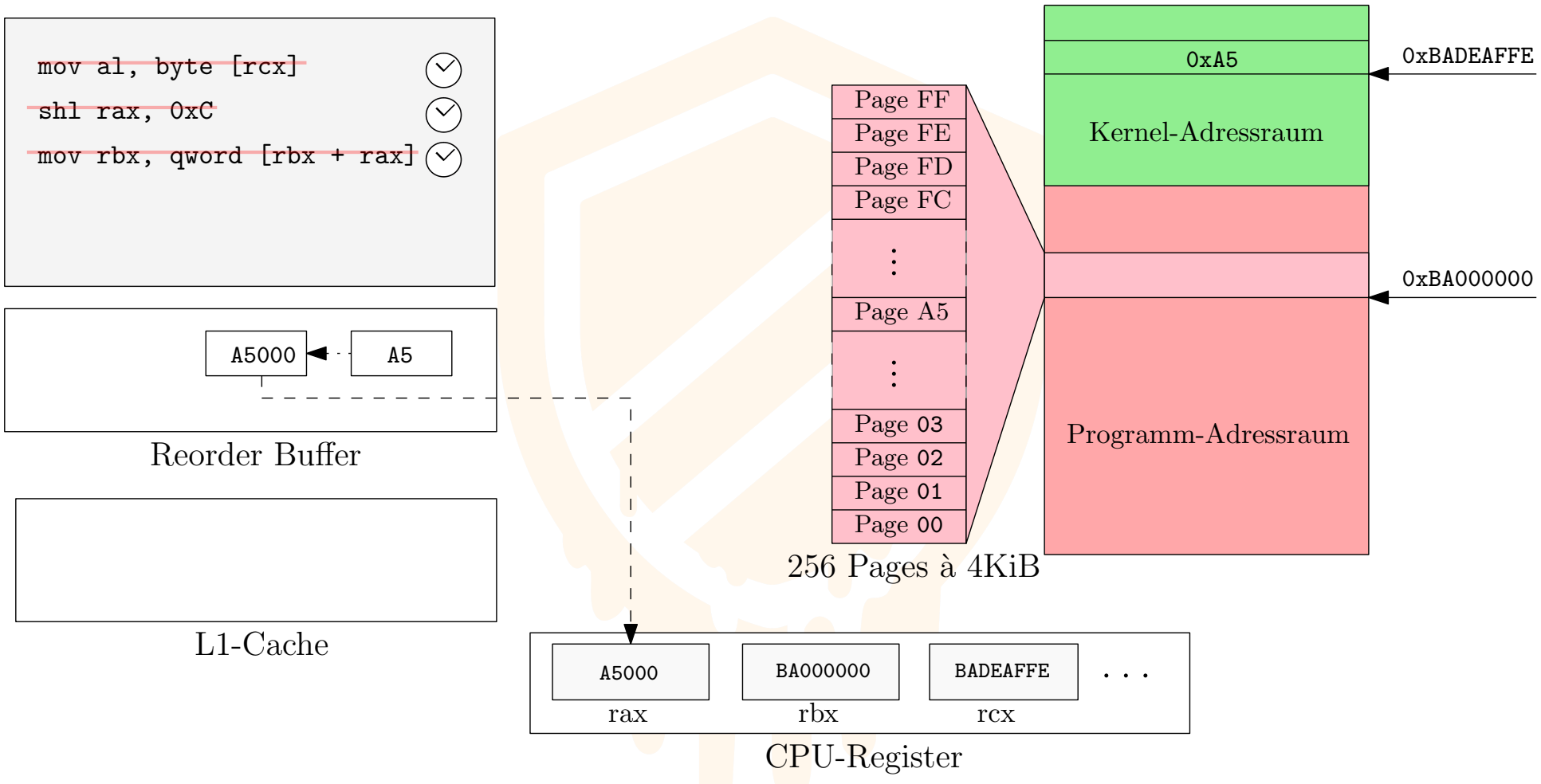
Meltdown - Vorgehensweise



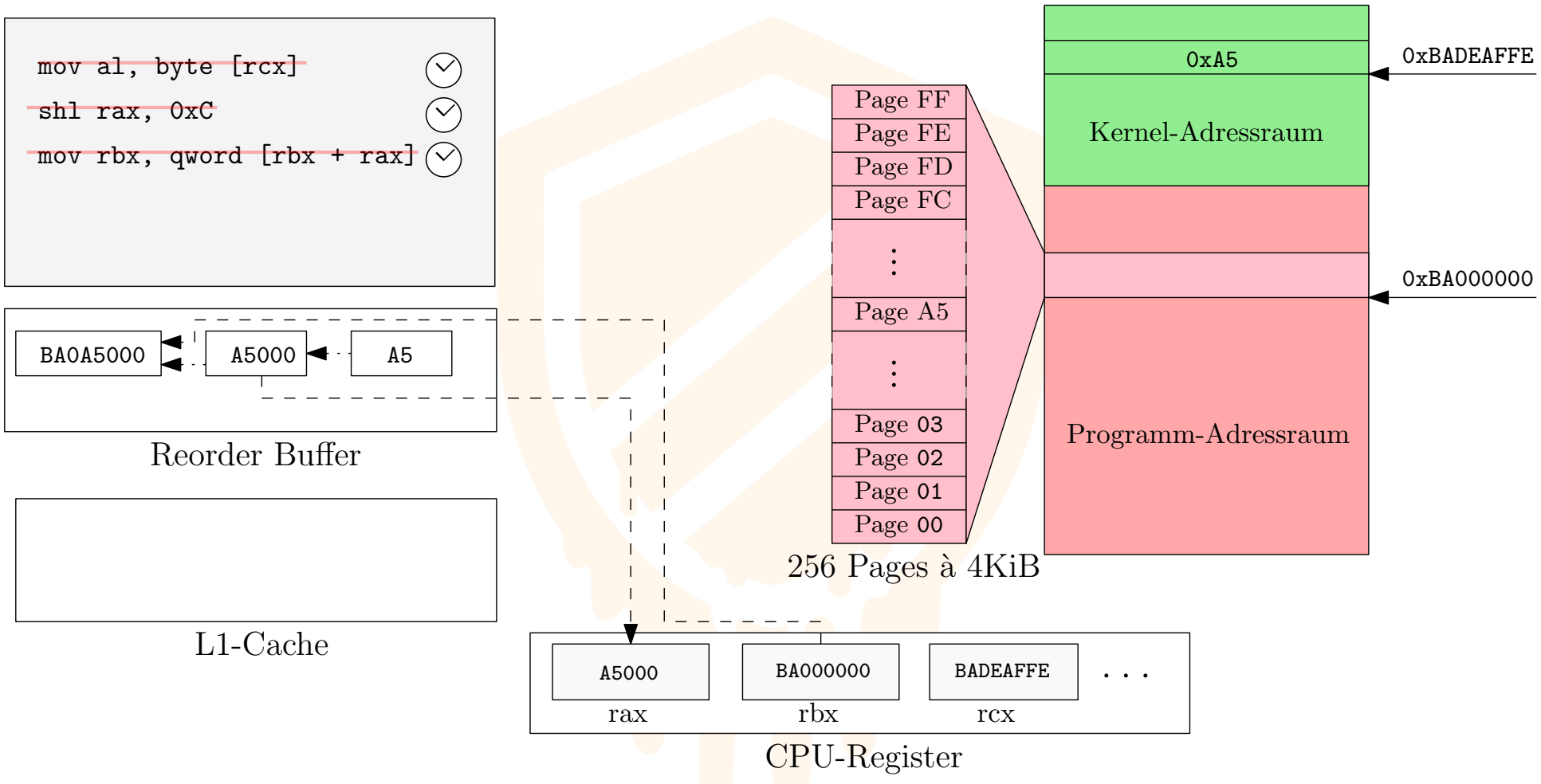
Meltdown - Vorgehensweise



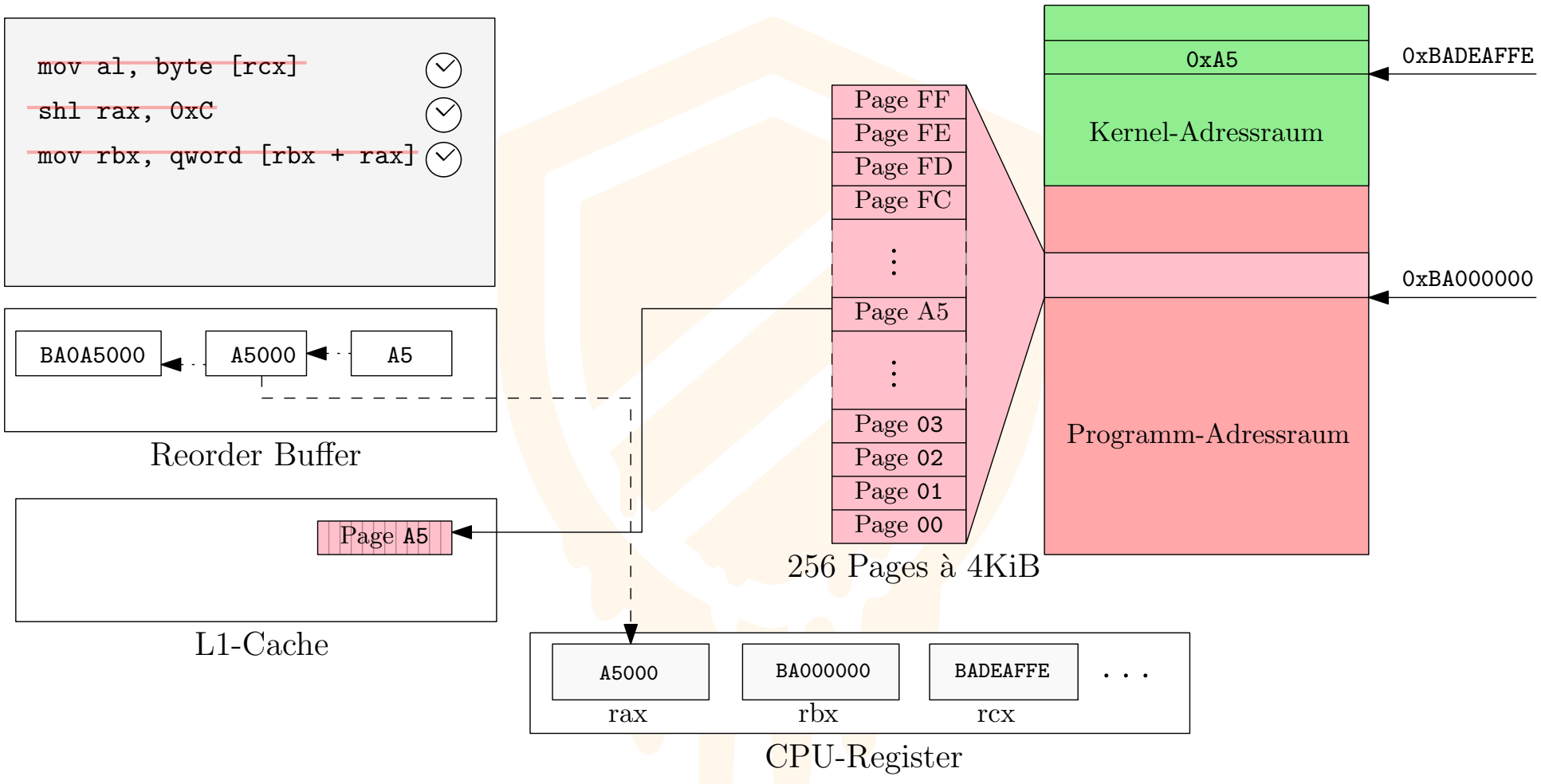
Meltdown - Vorgehensweise



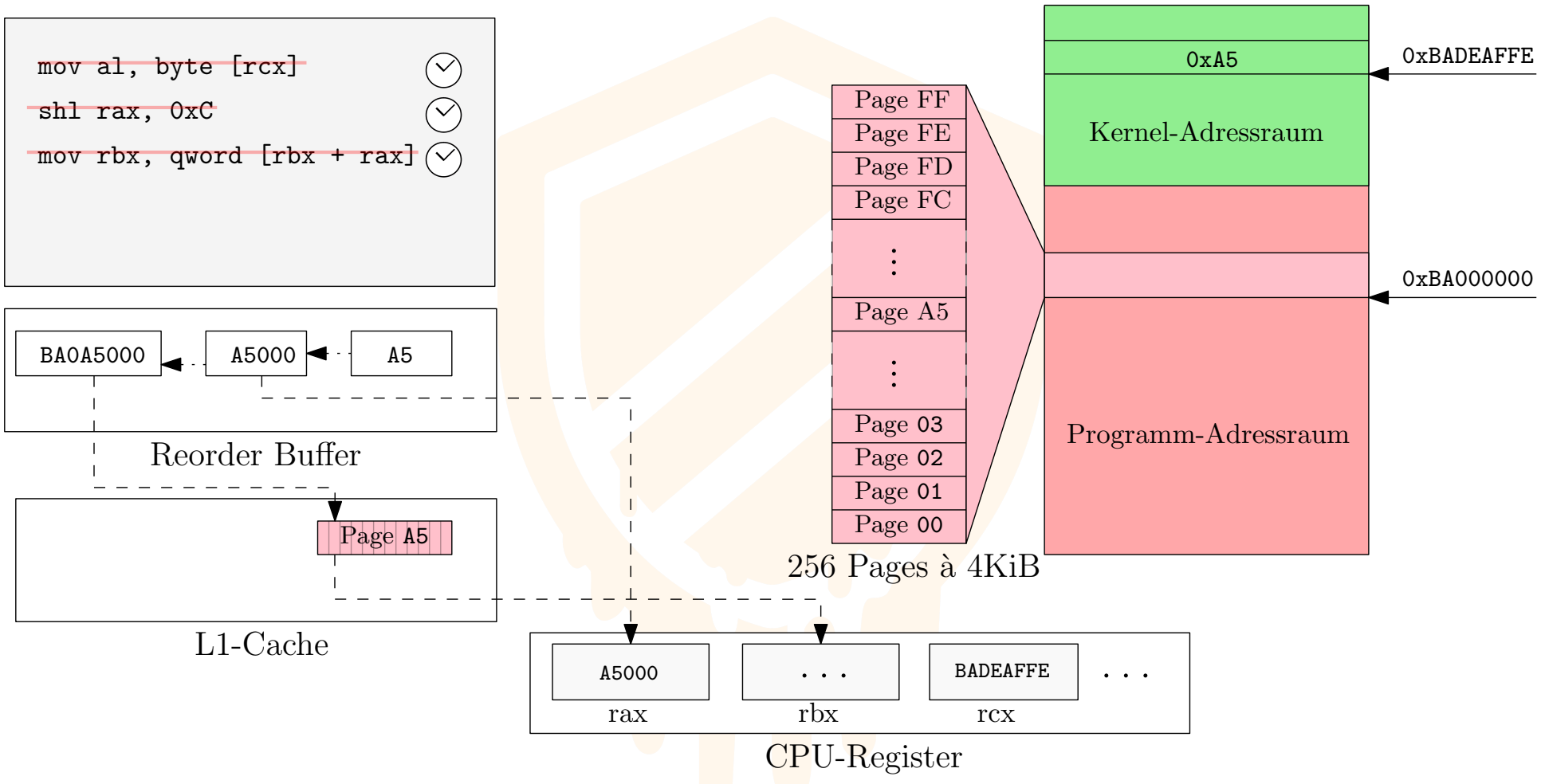
Meltdown - Vorgehensweise



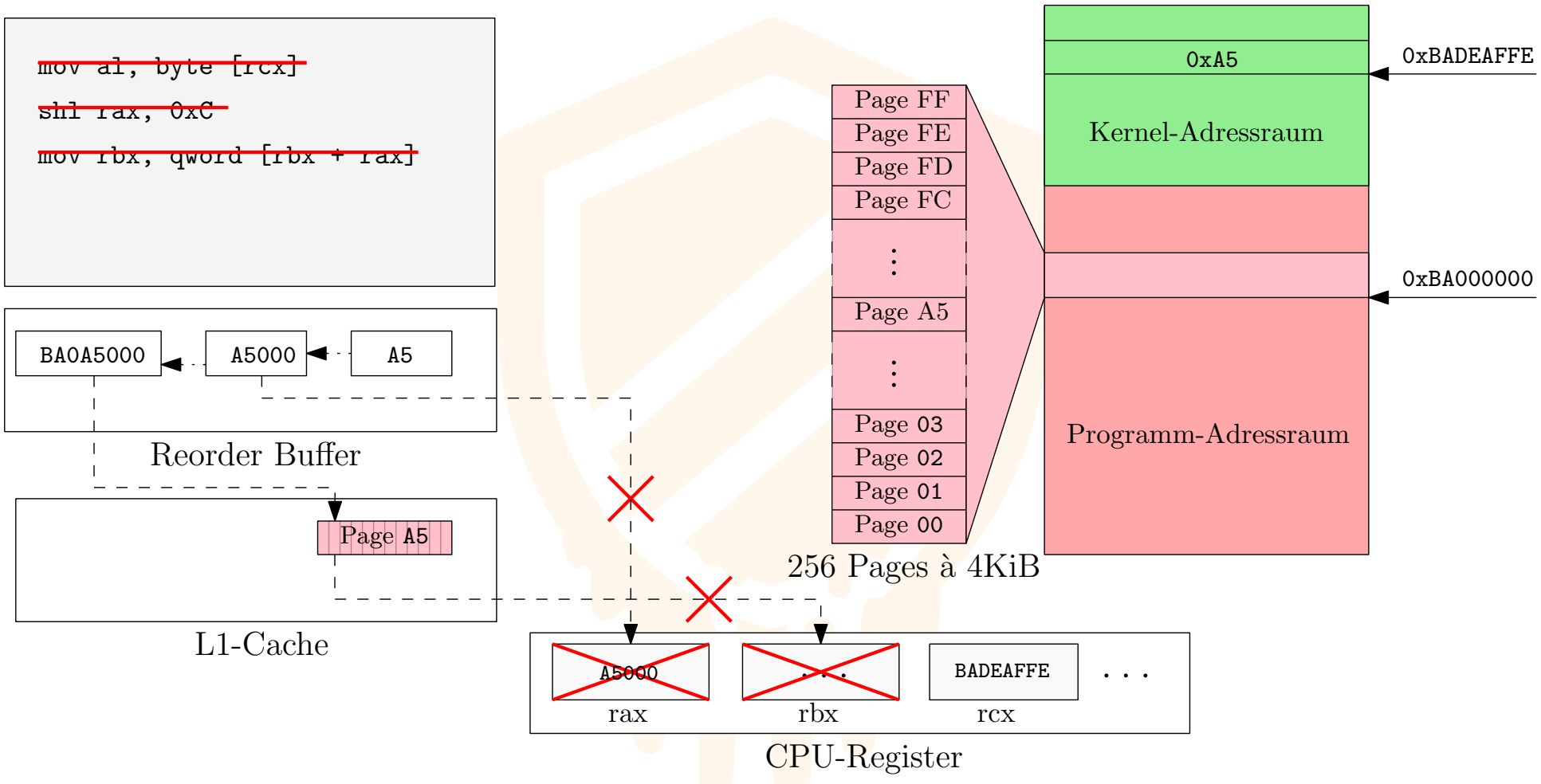
Meltdown - Vorgehensweise



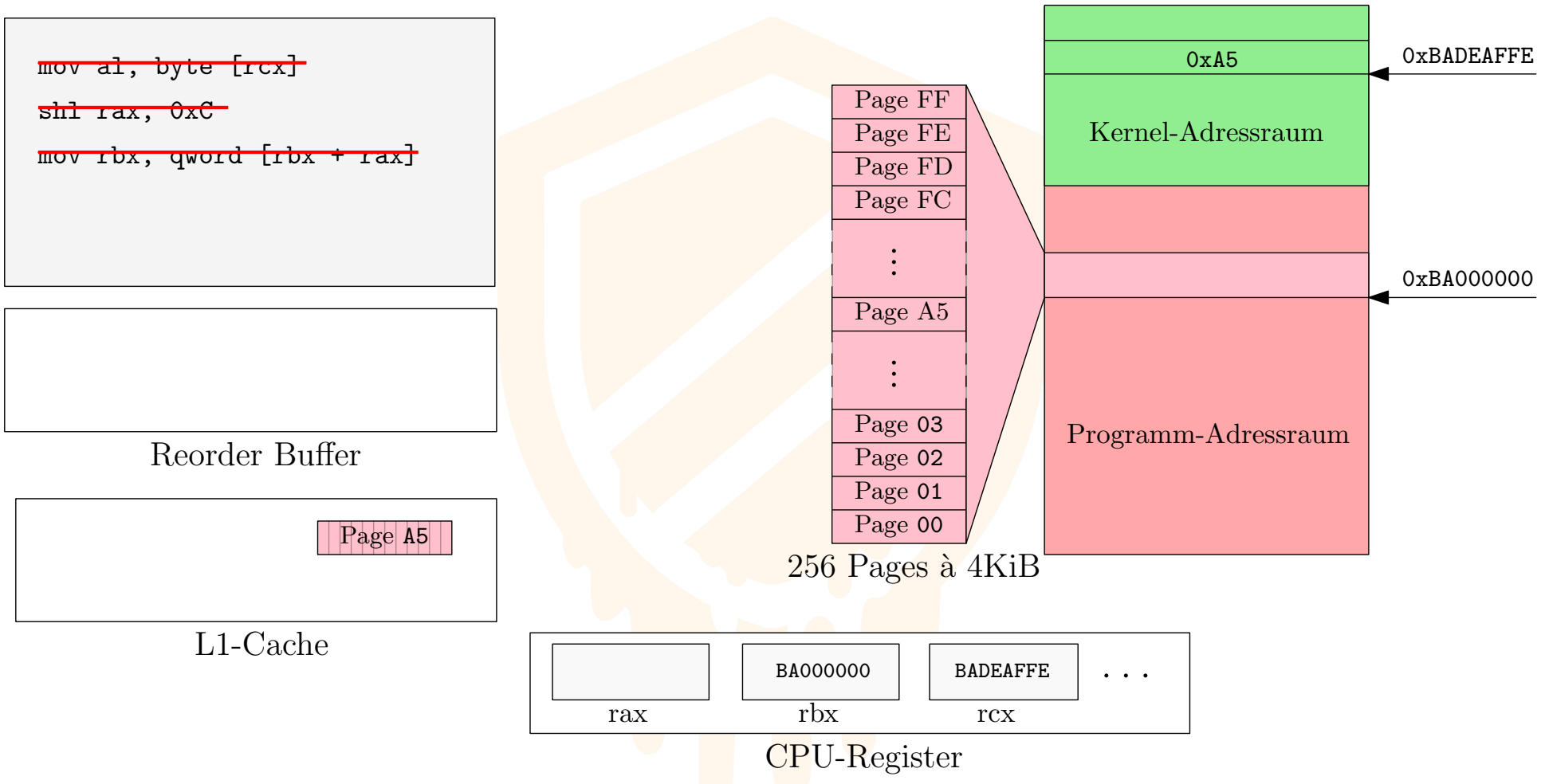
Meltdown - Vorgehensweise



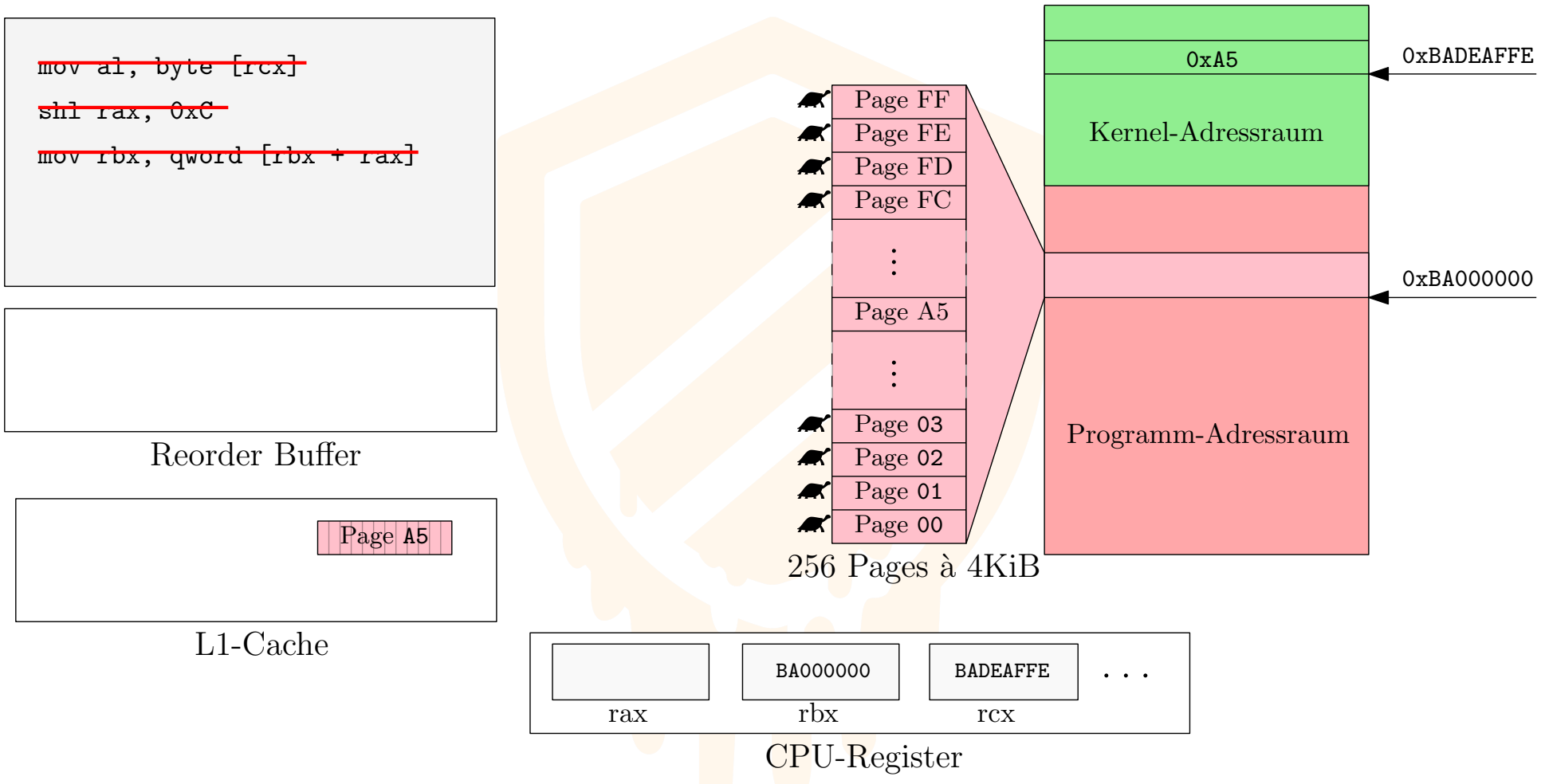
Meltdown - Vorgehensweise



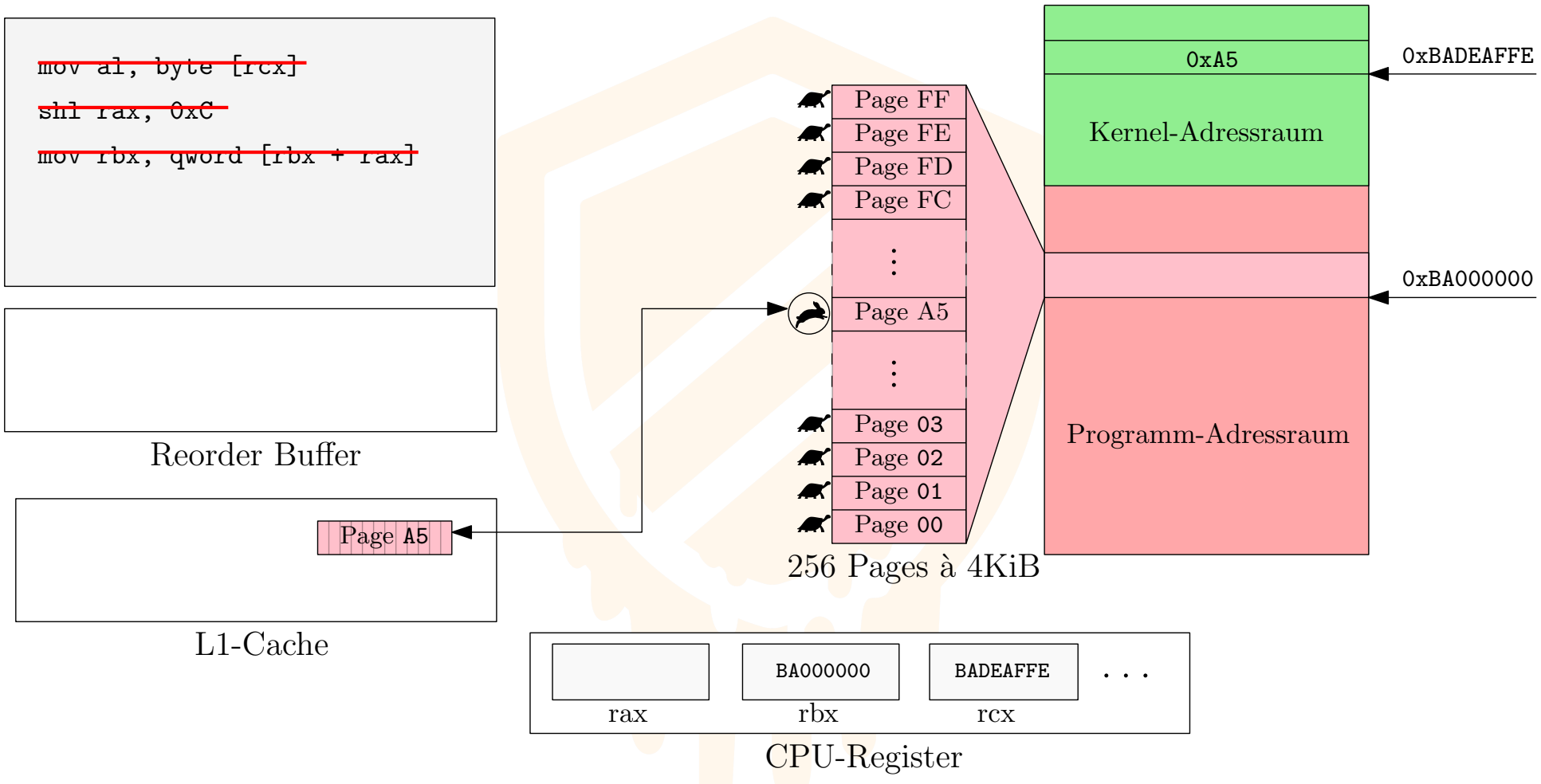
Meltdown - Vorgehensweise



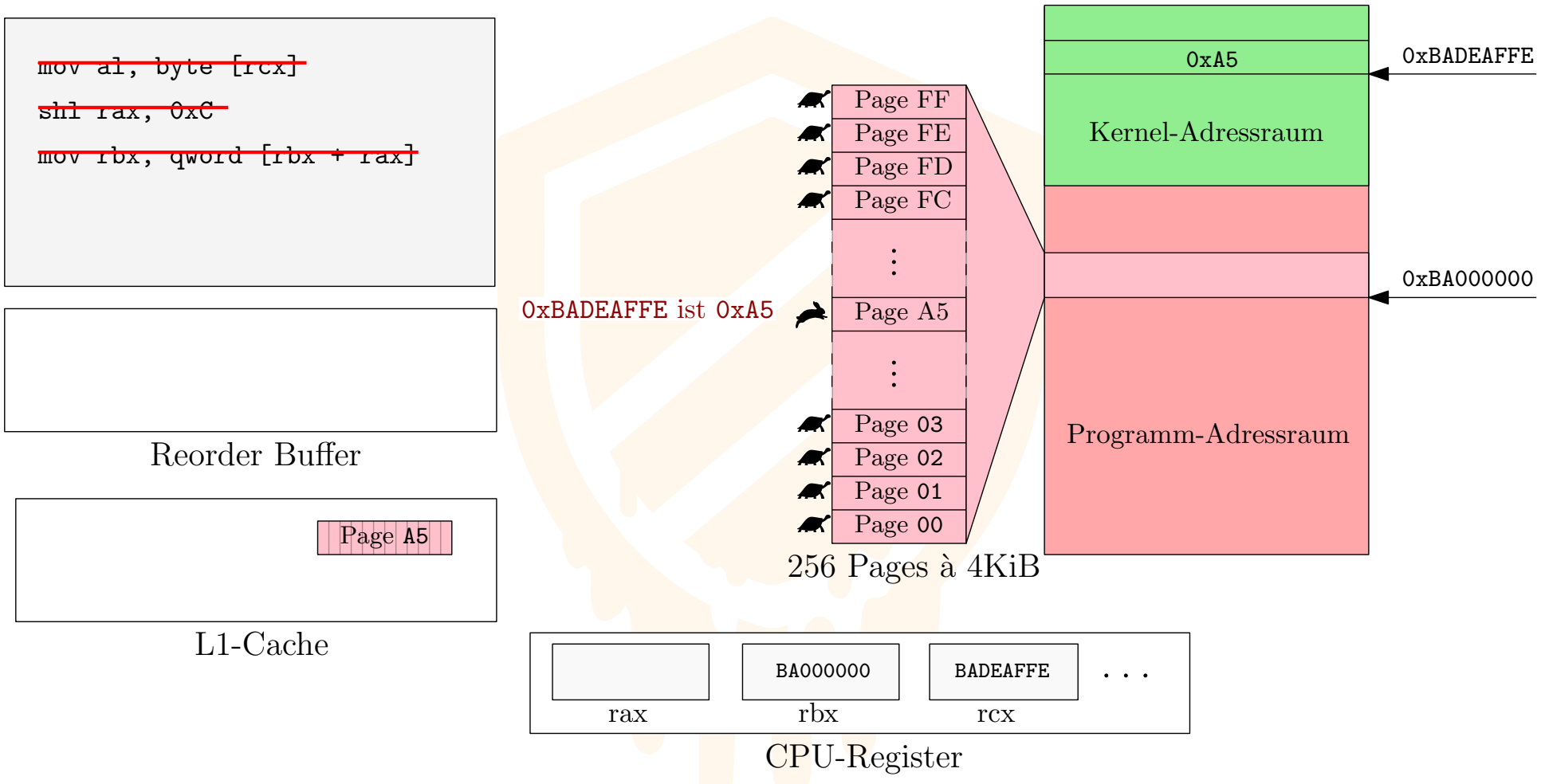
Meltdown - Vorgehensweise



Meltdown - Vorgehensweise



Meltdown - Vorgehensweise



Meltdown - Unterschied zu Spectre

Meltdown unterscheidet sich von Spectre in vielen Hinsichten:

Meltdown	Spectre

Meltdown - Unterschied zu Spectre

Meltdown unterscheidet sich von Spectre in vielen Hinsichten:

	Meltdown	Spectre
Prozessoren	Viele Intel CPUs Einige ARM CPUs	Unter anderem viele Intel, AMD und ARM CPUs

Meltdown - Unterschied zu Spectre

Meltdown unterscheidet sich von Spectre in vielen Hinsichten:

	Meltdown	**Spectre**
Prozessoren	Viele Intel CPUs Einige ARM CPUs	Unter anderem viele Intel, AMD und ARM CPUs
Mechanismus	Race Condition: Berechtigungsprüfung nach spekulativer Ausführung	Branch Prediction

Meltdown - Unterschied zu Spectre

Meltdown unterscheidet sich von Spectre in vielen Hinsichten:

	Meltdown	**Spectre**
Prozessoren	Viele Intel CPUs Einige ARM CPUs	Unter anderem viele Intel, AMD und ARM CPUs
Mechanismus	Race Condition: Berechtigungsprüfung nach spekulativer Ausführung	Branch Prediction
Datenzugriff	Kernel-Speicher und somit **gesamter** physikalischer Speicher	Andere User-Prozesse

Meltdown - Gegenvorkehrungen / „Fixes“

Meltdown - Gegenvorkehrungen / „Fixes“

- Vollständige Behebung nur über Austausch von Hardware möglich
  (z.B. Whiskey Lake für Laptops oder Cascade Lake für Server)

Meltdown - Gegenvorkehrungen / „Fixes“

- Vollständige Behebung nur über Austausch von Hardware möglich
  (z.B. Whiskey Lake für Laptops oder Cascade Lake für Server)

- KPTI - Workaround: Jeder Prozess erhält zwei Page-Tabellen:

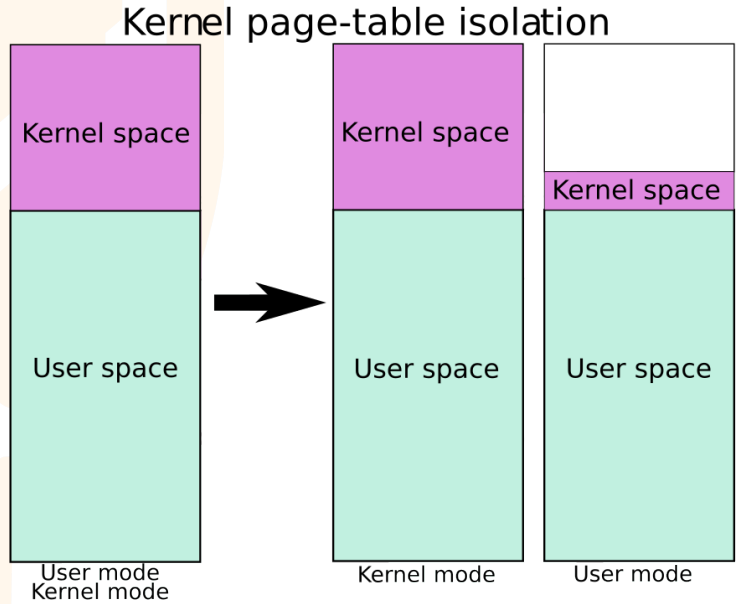


Abbildung: KPTI[2]

[2] Quelle: Wikimedia Foundation

Meltdown - Gegenvorkehrungen / „Fixes“

- Vollständige Behebung nur über Austausch von Hardware möglich
  (z.B. Whiskey Lake für Laptops oder Cascade Lake für Server)

- KPTI - Workaround: Jeder Prozess erhält zwei Page-Tabellen:
  - Nur essentieller Kernel-Code und -Daten werden im Ring 3 gemapped

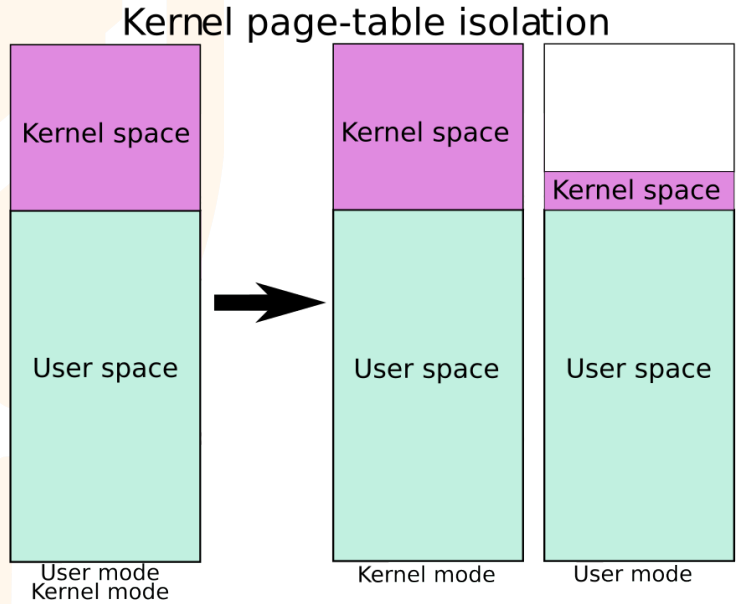


Abbildung: KPTI[2]

[2] Quelle: Wikimedia Foundation

Meltdown - Gegenvorkehrungen / „Fixes“

- Vollständige Behebung nur über Austausch von Hardware möglich
  (z.B. Whiskey Lake für Laptops oder Cascade Lake für Server)

- KPTI - Workaround: Jeder Prozess erhält zwei Page-Tabellen:
  - Nur essentieller Kernel-Code und -Daten werden im Ring 3 gemapped
  - Bei Wechsel in Ring 0 wird gesamter Kernel eingehängt

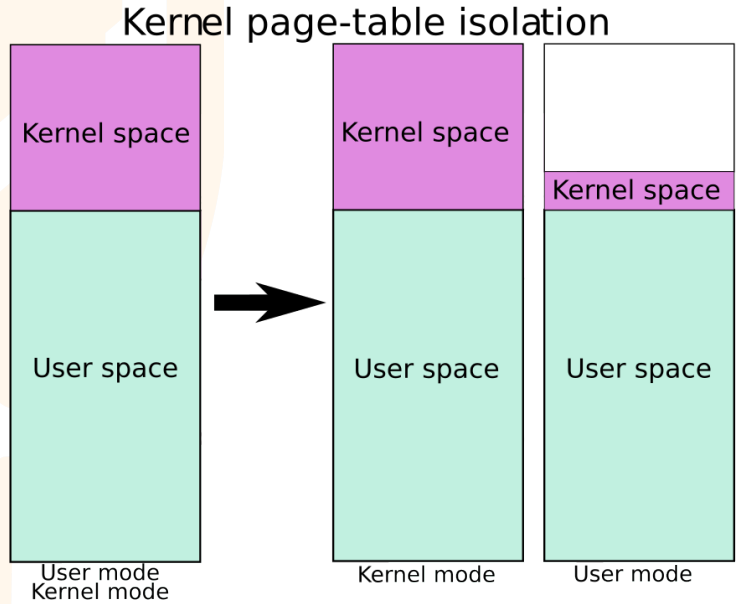


Abbildung: KPTI[2]

[2] Quelle: Wikimedia Foundation

Weiterführende Literatur

1. Generell
   - Meltdown / Spectre Webpage und Paper (https://meltdownattack.com/)
   - Google Project Zero Blog (https://googleprojectzero.blogspot.com/...)
2. Meltdown-spezifisch
   - Referenz-Implementation der TU Graz (Github: IAIK/meltdown)
   - G DATA Analytics Blog (https://cyber.wtf/...)

Vielen Dank für Ihre Aufmerksamkeit