A Security Model for Randomization-based Protected Caches

Jordi Ribes-González, Oriol Farràs
Universitat Rovira i Virgili

Carles Hernández
Universitat Politècnica de València

Vatistas Kostalabros, Miquel Moretó
Barcelona Supercomputing Center

Cryptographic Hardware and Embedded Systems (CHES)

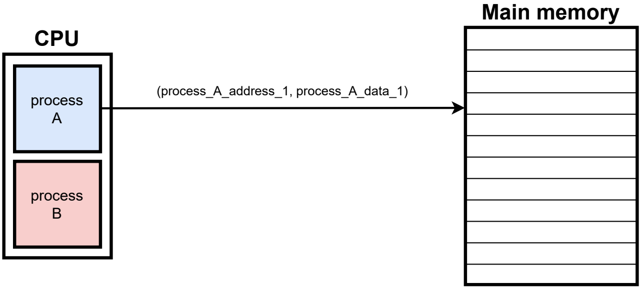
19th September 2022

Table of Contents

Table of Contents

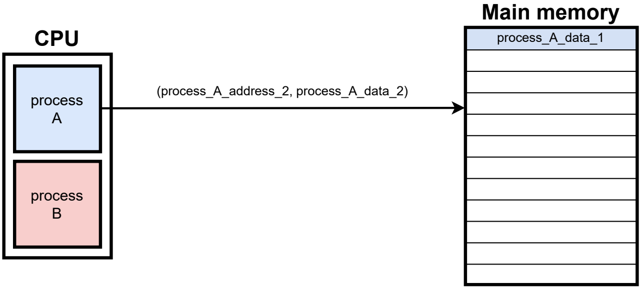
Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



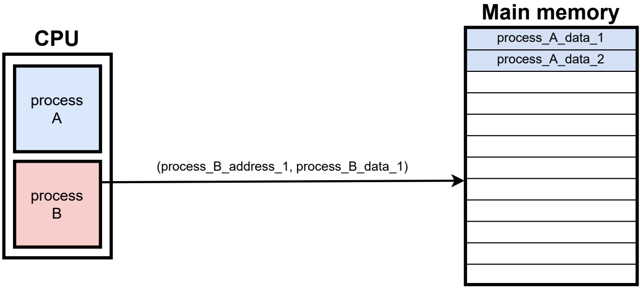
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



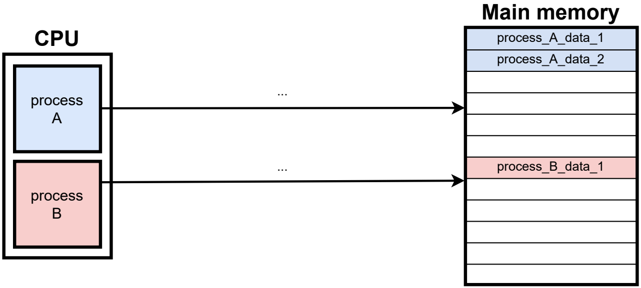
Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

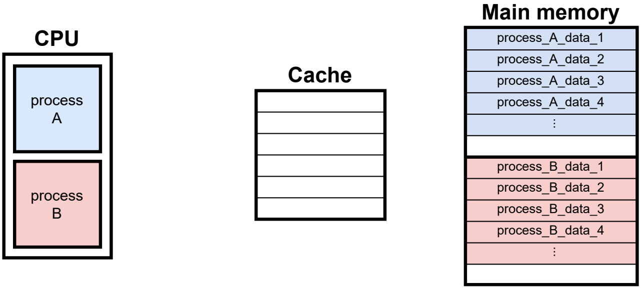
Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks

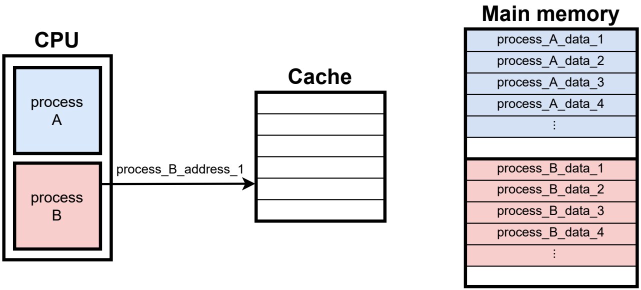
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses

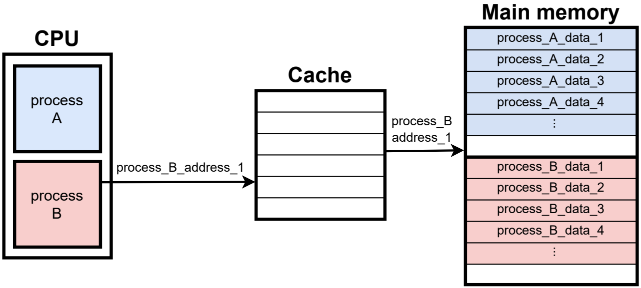
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



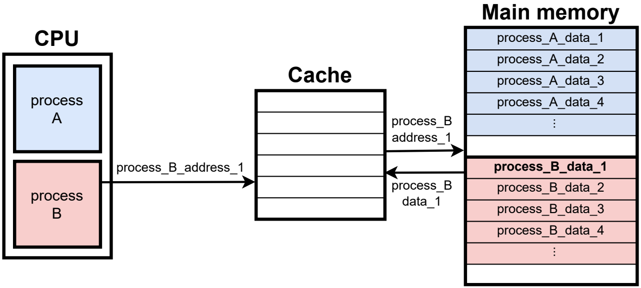
- Cache memories **reduce the latency** of memory accesses

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



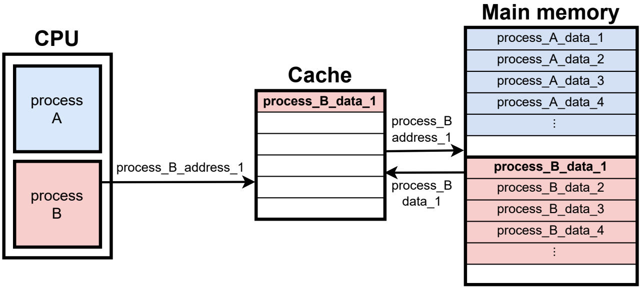
- Cache memories **reduce the latency** of memory accesses

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

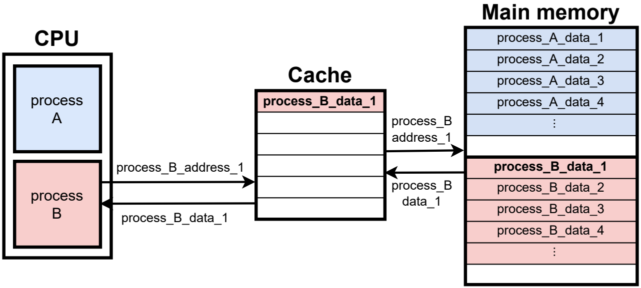


- Cache memories **reduce the latency** of memory accesses

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

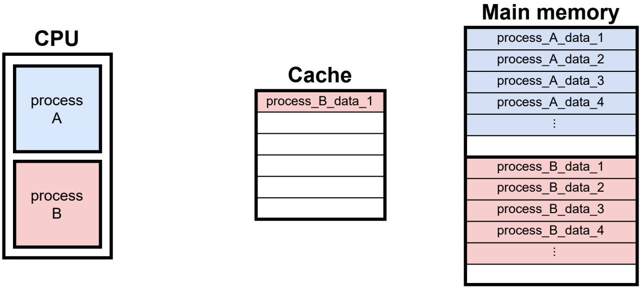


- Cache memories **reduce the latency** of memory accesses



- Cache memories **reduce the latency** of memory accesses

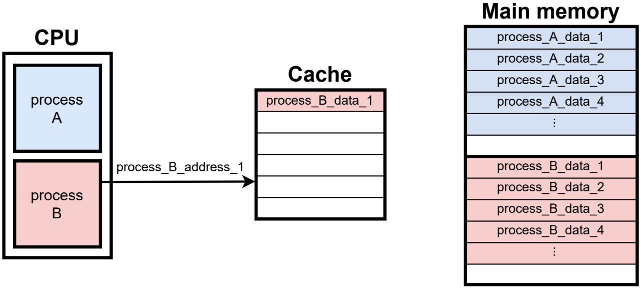
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses

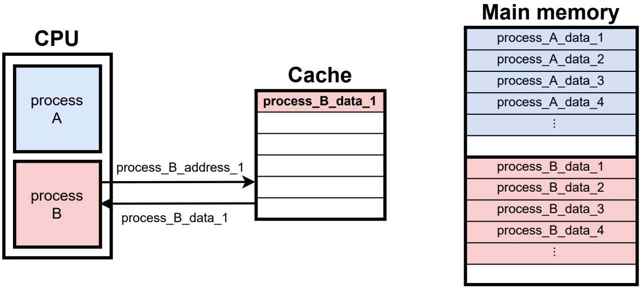
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



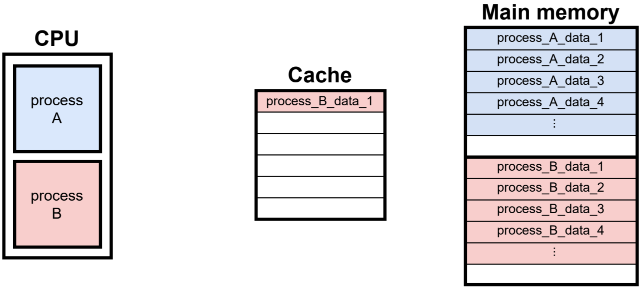
- Cache memories **reduce the latency** of memory accesses

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses

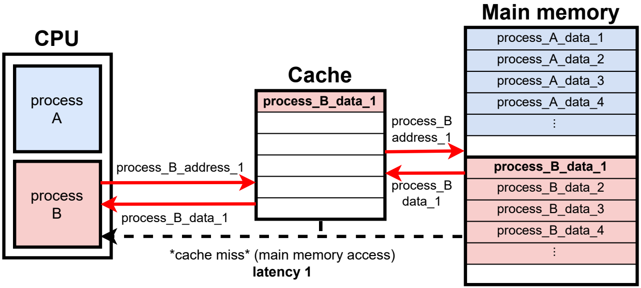
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

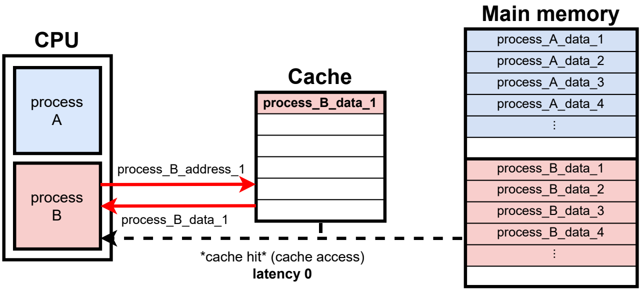
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

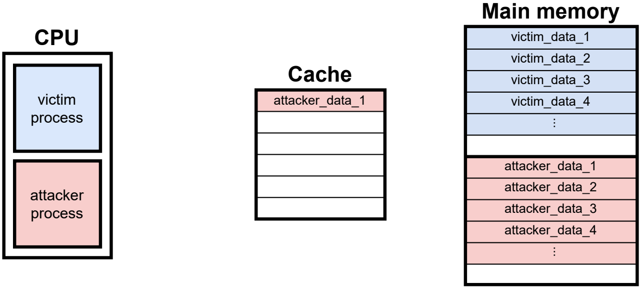
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

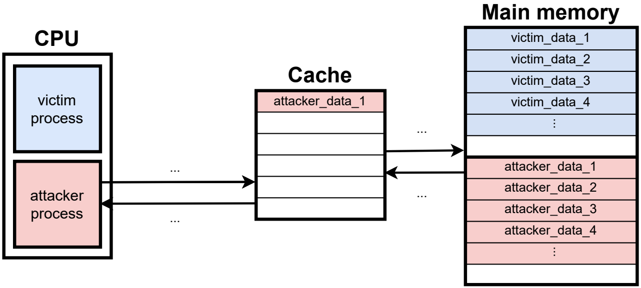
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

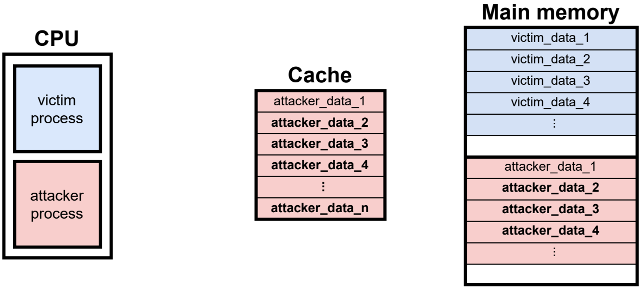
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

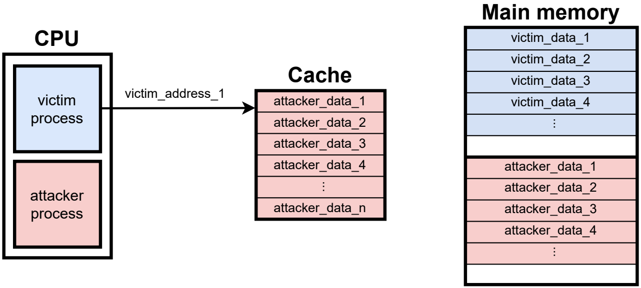
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

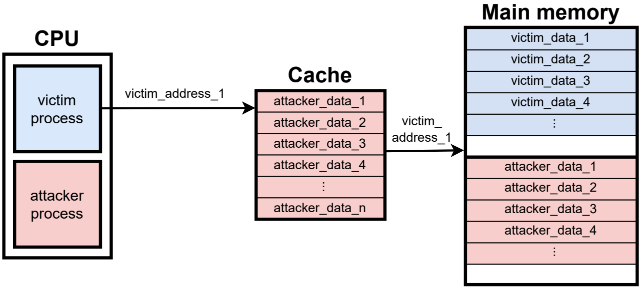
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

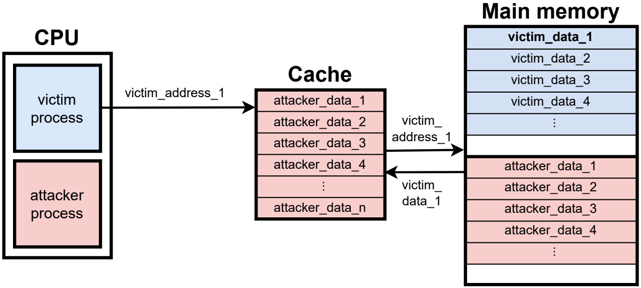
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

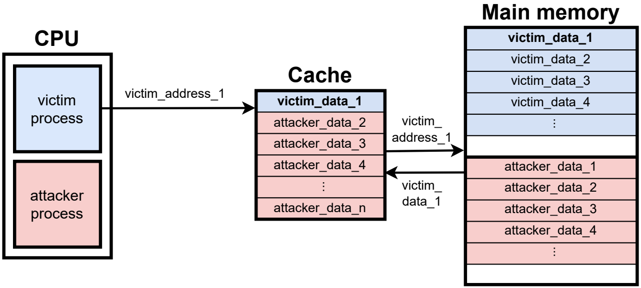
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

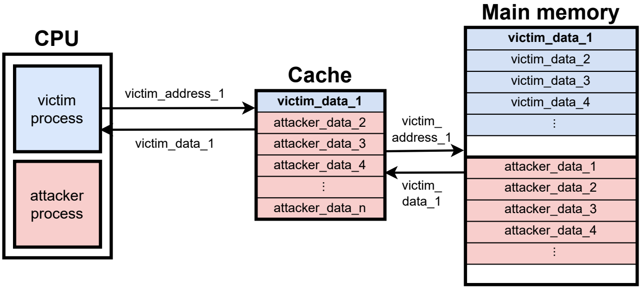
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

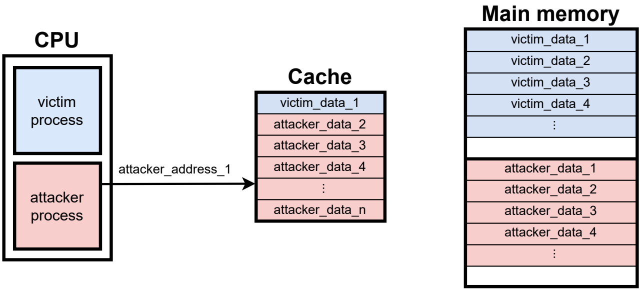
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

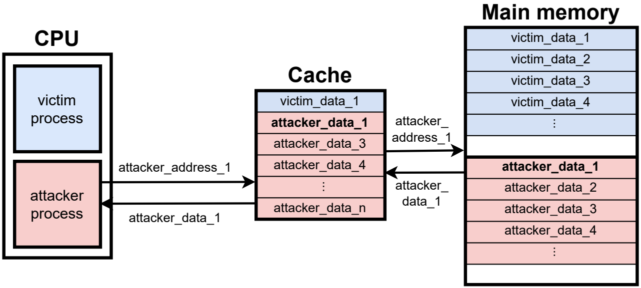
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

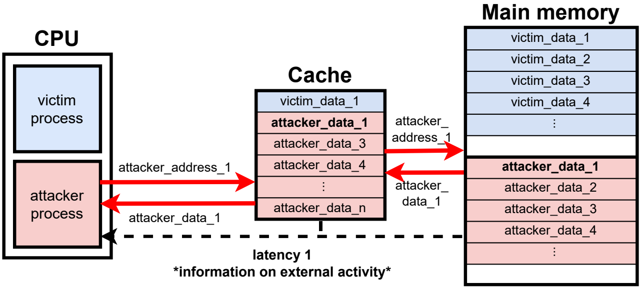
An Overview of Cache Side-channel Attacks



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**

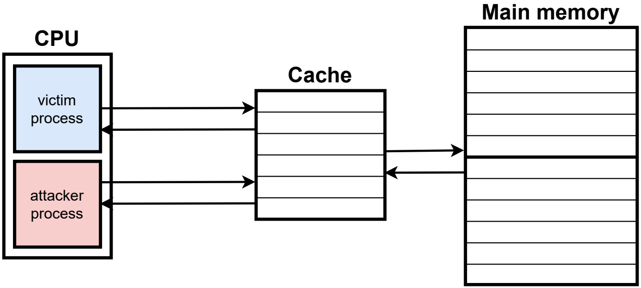
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

An Overview of Cache Side-channel Attacks



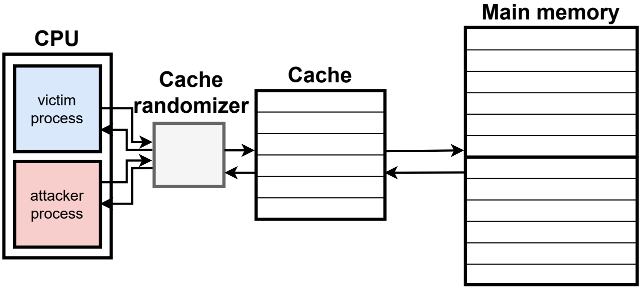
- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**
- Exploit access latency to eavesdrop on **external** processes

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**
- Exploit access latency to eavesdrop on **external** processes

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



- Cache memories **reduce the latency** of memory accesses
- Cache side-channel: access **latency** reveals if data is **already cached**
- Exploit access latency to eavesdrop on **external** processes
- Randomization-based Protected Caches: **randomize** cache addresses

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Outline of Our Work

Study the security of RPCs

- against **single-target access-based** attacks in
- **shared large** caches (LLC)

In particular, resistance against **Prime+Probe** and **Evict+Probe** attacks.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Outline of Our Work

Study the security of RPCs

- against **single-target access-based** attacks in
- **shared large** caches (LLC)

In particular, resistance against **Prime+Probe** and **Evict+Probe** attacks.

Several previous RPCs have been found **insecure**. Aims:

- address the **break-and-repair cycle**
- analyze the **impact of access-based attacks**

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Outline of Our Work

Study the security of RPCs

- against **single-target access-based** attacks in
- **shared large** caches (LLC)

In particular, resistance against **Prime+Probe** and **Evict+Probe** attacks.

Several previous RPCs have been found **insecure**. Aims:

- address the **break-and-repair cycle**
- analyze the **impact of access-based attacks**

Provable security approach to RPCs:

1. **model RPCs**
2. characterize security through **game-based definitions**
3. analyze security through **security proofs** and **attacks**
4. evaluate performance through a **simulation**

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache side-channel attacks exploit:

- Own **access** latency
- **Timing** external processes
- Cache **flushing**
- Cache **collisions**
- Cache **coherence**

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache side-channel attacks exploit:

- Own **access** latency
- **Timing** external processes
- Cache **flushing**
- Cache **collisions**
- Cache **coherence**

Focus on **access-based attacks** as Prime+Probe and Evict+Probe.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache side-channel attacks exploit:

- Own **access** latency
- **Timing** external processes
- Cache **flushing**
- Cache **collisions**
- Cache **coherence**

Focus on **access-based attacks** as Prime+Probe and Evict+Probe.

Mitigation strategies:

- cache **partitioning**
- **table-based** randomization
- **randomization**-based protected caches

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache side-channel attacks exploit:

- Own **access** latency
- **Timing** external processes
- Cache **flushing**
- Cache **collisions**
- Cache **coherence**

Focus on **access-based attacks** as Prime+Probe and Evict+Probe.

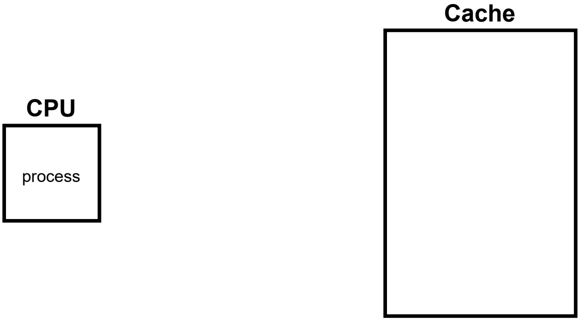
Mitigation strategies:

- cache **partitioning** (bad for performance)
- **table-based** randomization (inefficient for LLC)
- **randomization**-based protected caches

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Table of Contents

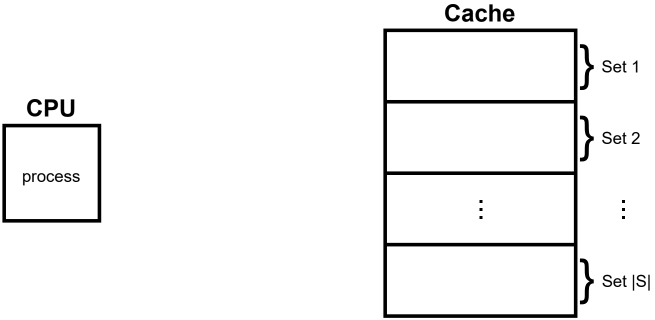
Our Cache Model and Access-based Attacks



Cache memories

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks

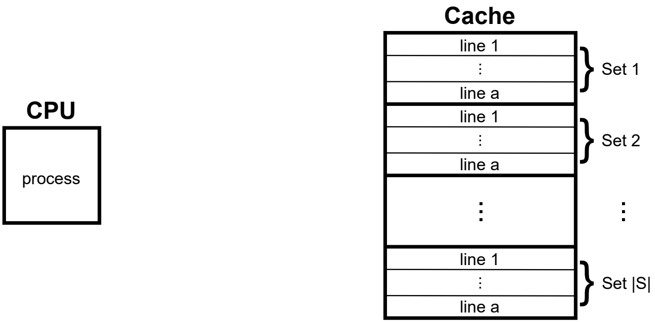


Cache memories

- consist of $|S|$ **cache sets**,

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks

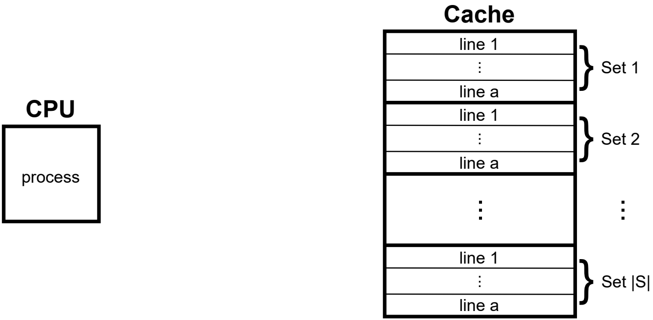


Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks

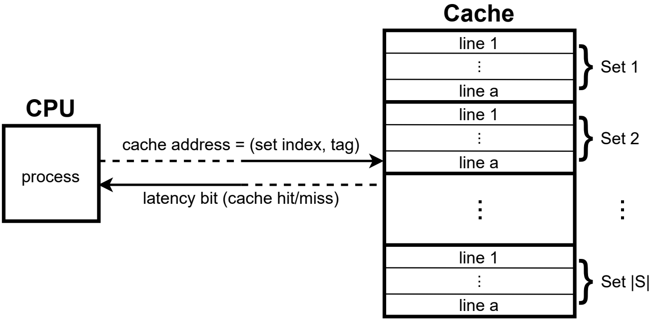


Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

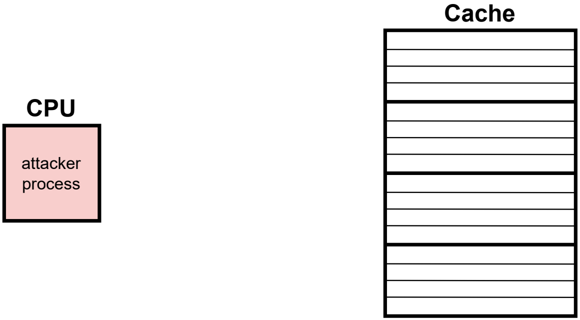
- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

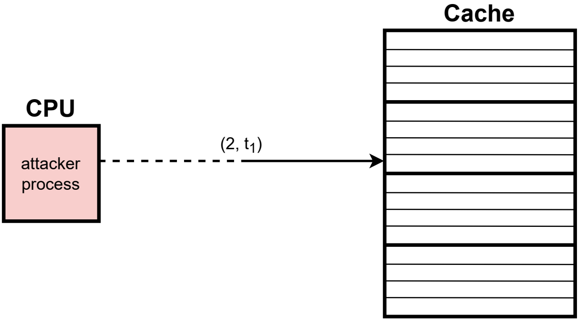
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya
Departament de Recerca
i Universitats
Unió Europea
Fons Europeu
de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

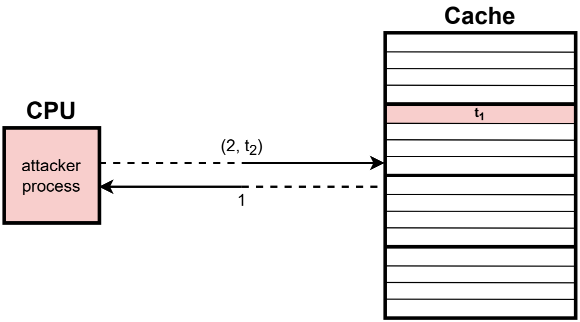
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

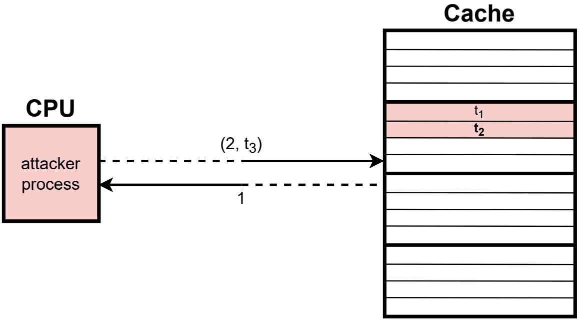
- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

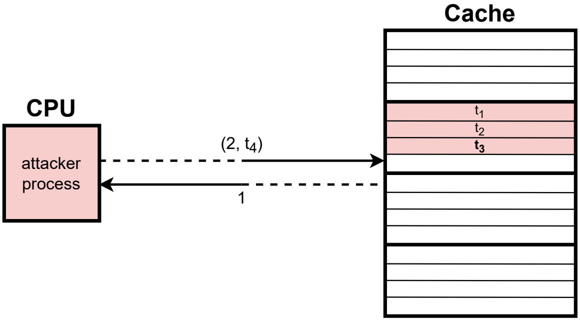
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

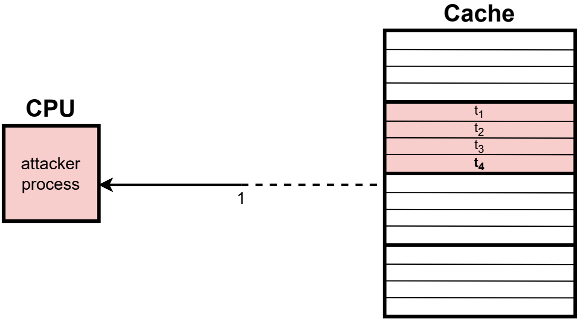
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

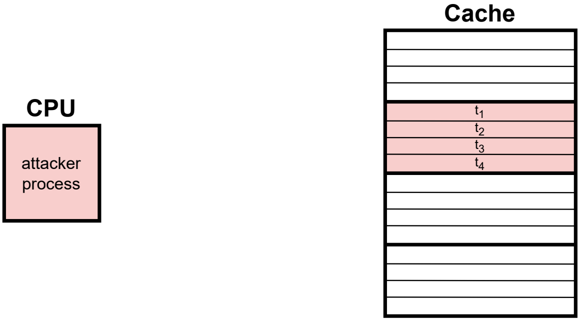
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

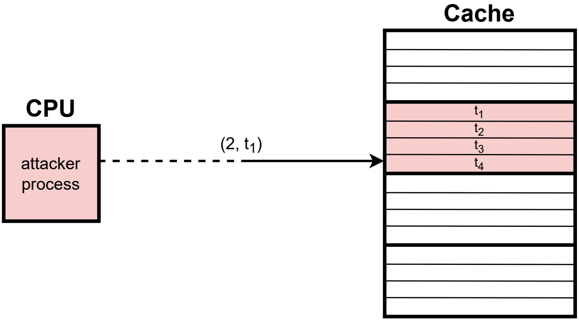
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

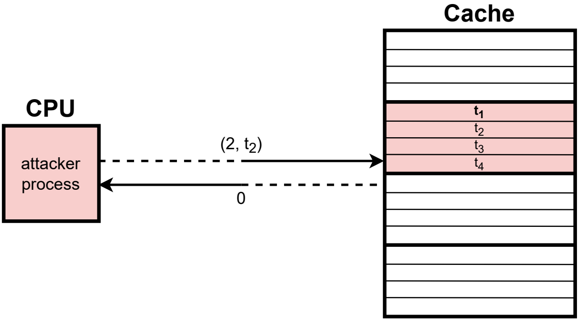
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

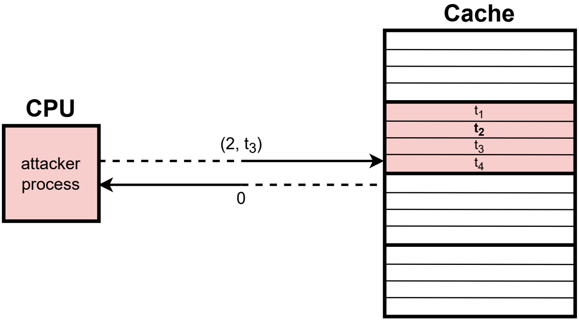
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

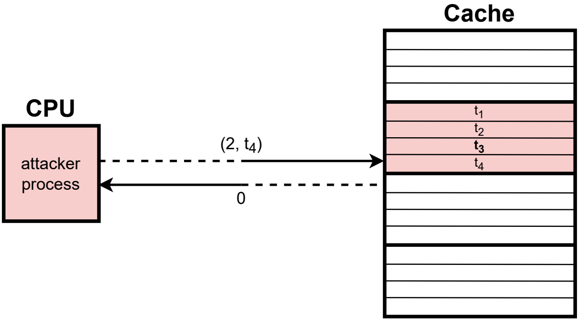
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

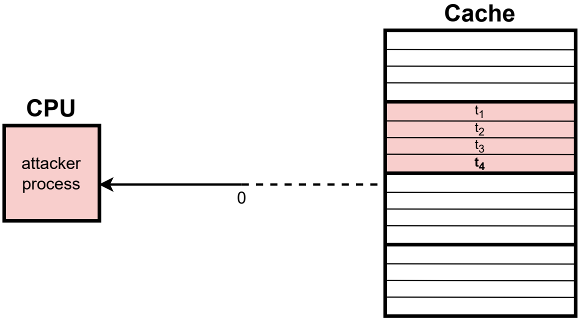
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

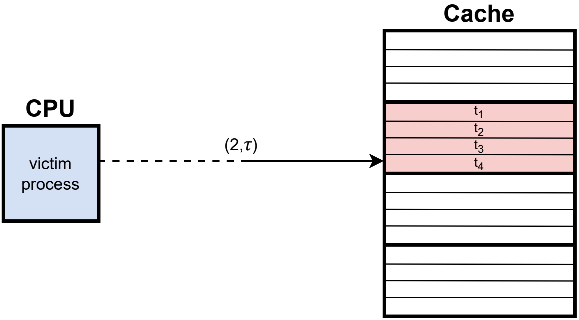
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

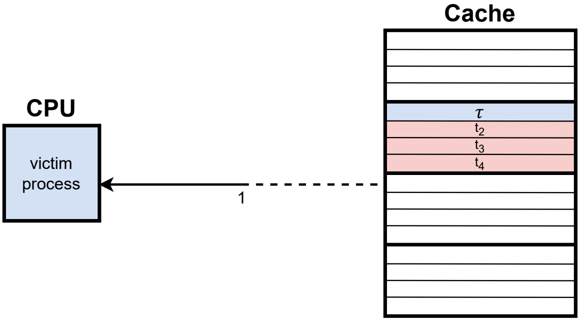
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

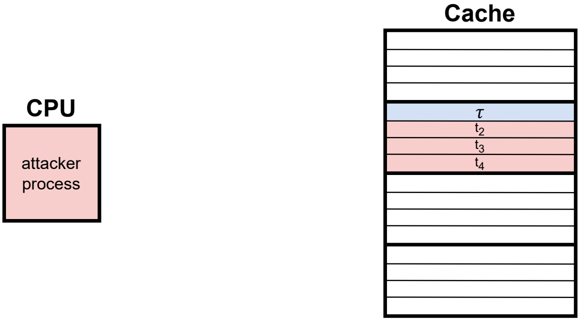
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

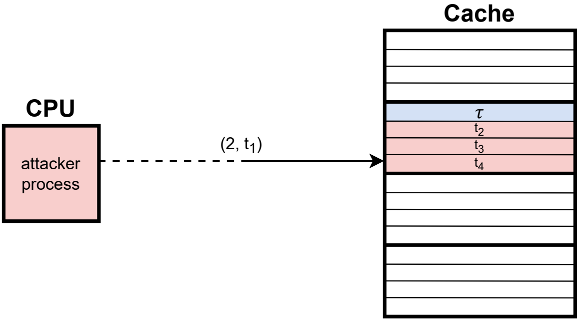
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

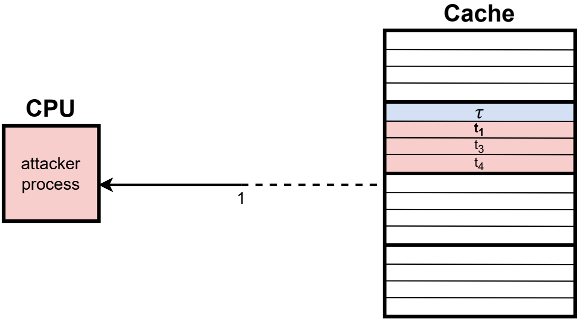
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

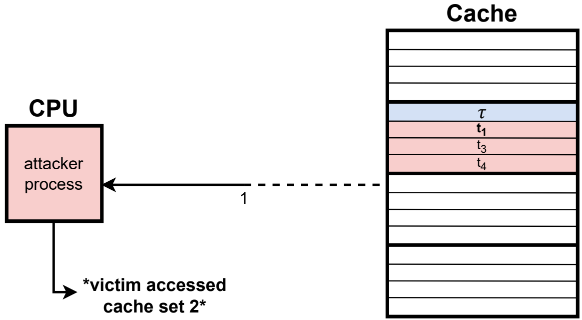
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Our Cache Model and Access-based Attacks



Cache memories

- consist of $|S|$ **cache sets**, with a **lines** each (associativity),
- and a **replacement policy** RP.

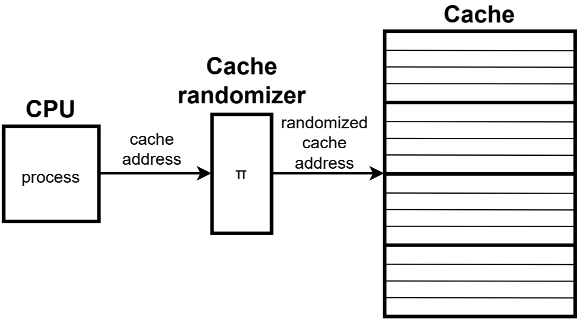
Cache addresses comprise

- a **set index** which addresses cache sets, and
- a **tag** which is stored in some line according to RP.

Access-based attack in this context (with $|S| = a = 4$).

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

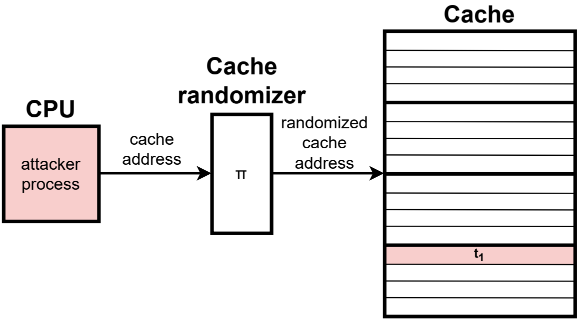
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

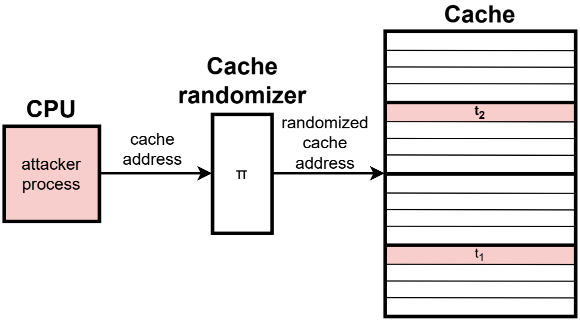
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

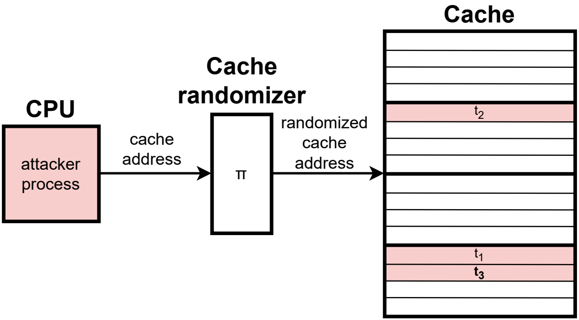
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

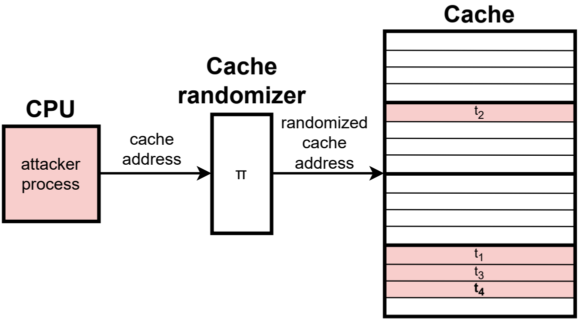
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

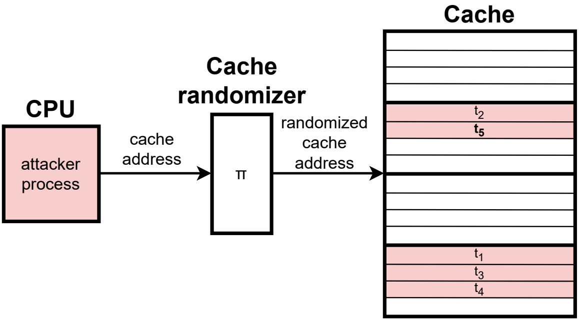
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.



Address randomization: Hamper attacks by **scattering** accesses.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

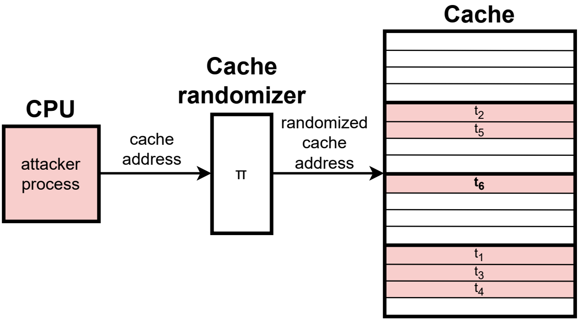
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

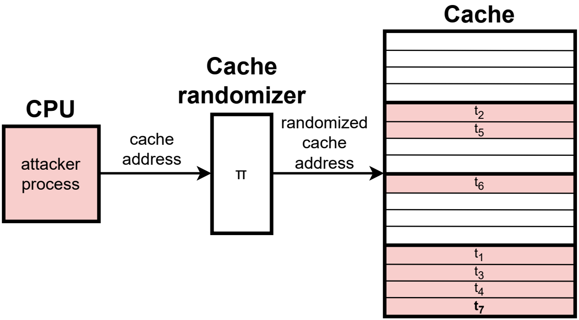
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

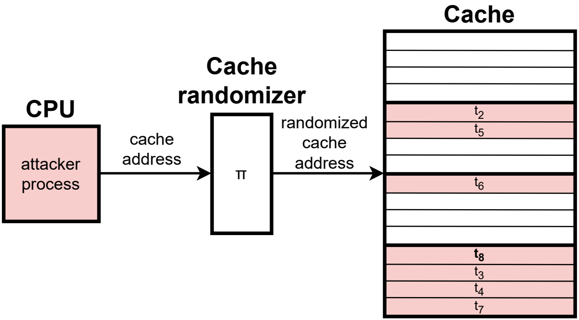
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

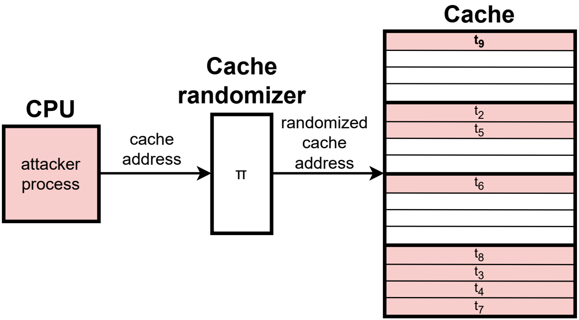
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

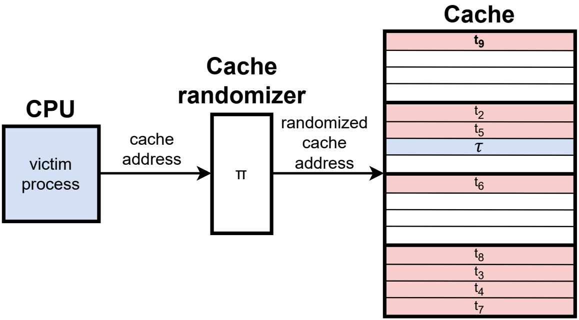
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

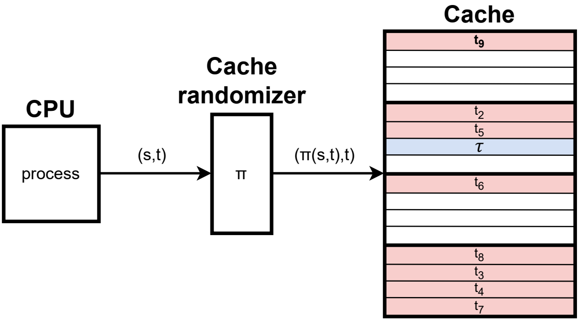
Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.
Access-based attacks *take longer* and are *more difficult*!

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Randomization-based Protected Caches

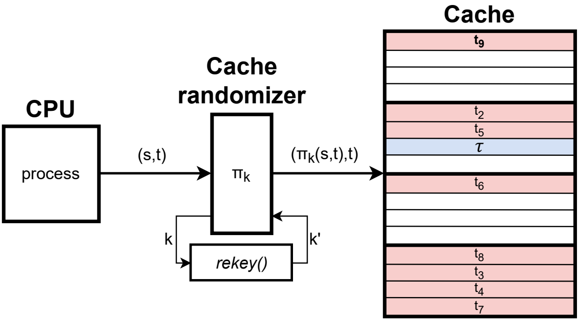


Address randomization: Hamper attacks by **scattering** accesses.
Access-based attacks *take longer* and are *more difficult*!

- **Set-index randomization** $(s, t) \rightarrow (\pi(s, t), t)$

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Randomization-based Protected Caches



Address randomization: Hamper attacks by **scattering** accesses.

Access-based attacks *take longer* and are *more difficult*!

- **Set-index randomization** $(s,t) \to (\pi_k(s,t),t)$
- Modeled as a keyed **pseudo-random function** (rekey,π)

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Table of Contents

Even with RPCs, **attacks are possible** given enough cache accesses [Bourgeat et al.'20, Purnal et al.'21, our work].

RPCs establish a **rekeying period**.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Questions Addressed in Our Work

Even with RPCs, **attacks are possible** given enough cache accesses [Bourgeat et al.'20, Purnal et al.'21, our work].

RPCs establish a **rekeying period**.

Up until now, **rekeying has been set heuristically** to thwart **particular attacks**, leading to **insecure RPCs**.

Can some rekeying periods provide provable **security guarantees**?

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Even with RPCs, **attacks are possible** given enough cache accesses [Bourgeat et al.'20, Purnal et al.'21, our work].

RPCs establish a **rekeying period**.

Up until now, **rekeying has been set heuristically** to thwart **particular attacks**, leading to **insecure RPCs**.

Can some rekeying periods provide provable **security guarantees**?

Moreover, **key-invariant information** about the cache randomizer can be exploited [Bourgeat et al.'20].

Can security be enforced **across different epochs**?

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Formally **define and prove security** against **all attacks** that

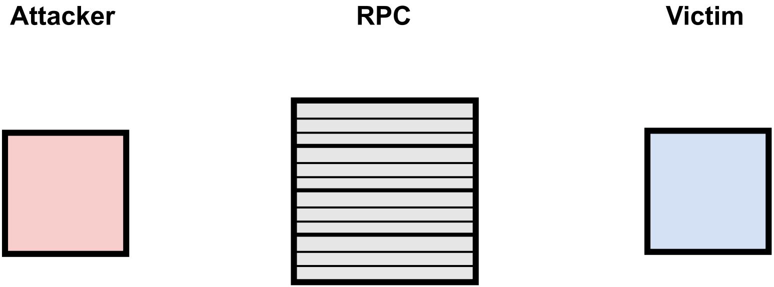
- aim to detect a victim access to a **single target address**
- are considered to succeed if their **advantage crosses some threshold**
- only **exploit access latency** information

This approach allows

- to provide **concrete security guarantees**
- to **quantify the success of an attack** under specific conditions

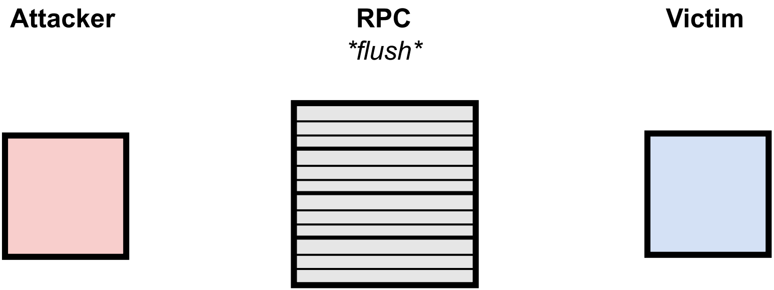
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



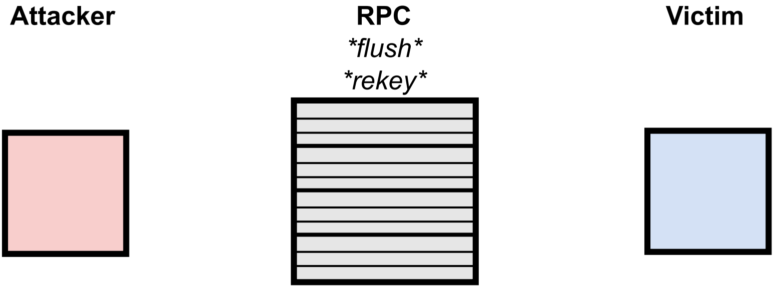
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



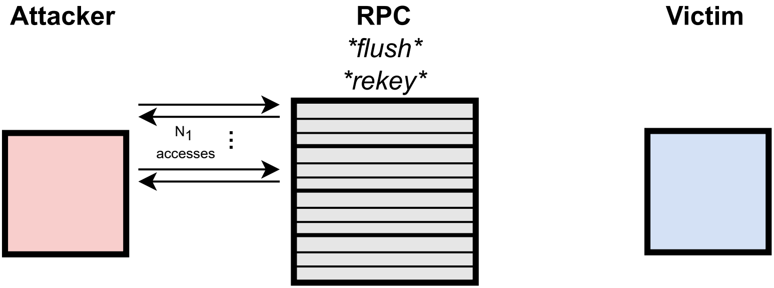
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



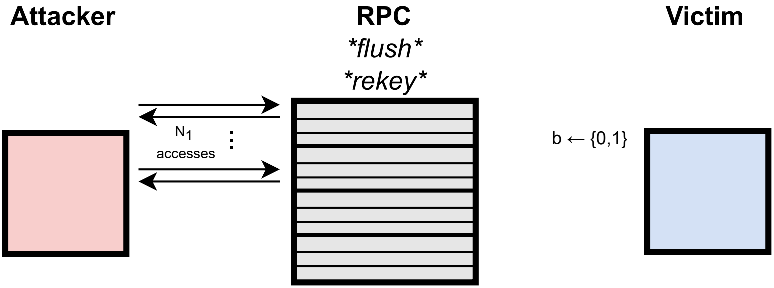
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



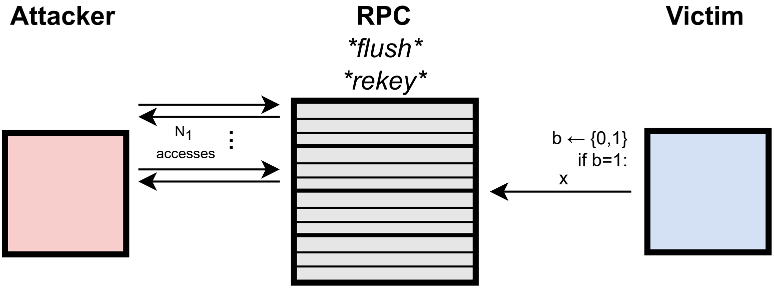
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



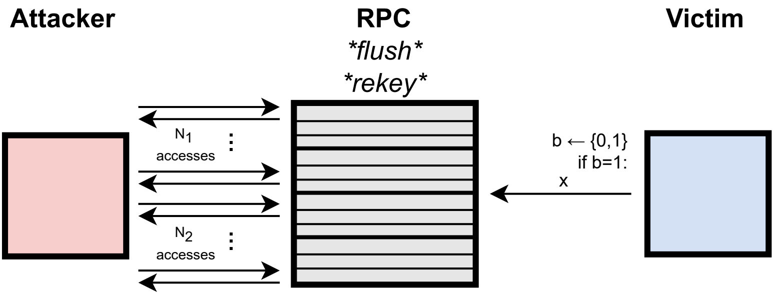
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



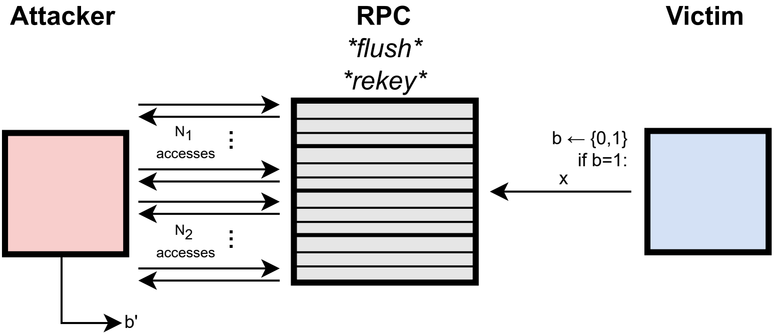
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



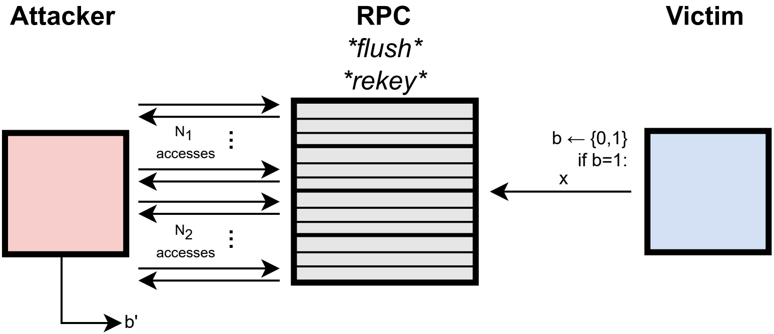
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Definition



The RPC $\mathcal{C}$ **is** N**-access secure with advantage at most** p if, for every x, for every N_1, N_2 such that $N_1 + N_2 = N$, and for every adversary $\mathcal{A}$,

$$\mathrm{Adv}^{\mathrm{RPC}}_{\mathcal{C},\mathcal{A}}(N_1, N_2) := 2 \cdot \left|\Pr\left[b' = b\right] - 1/2\right| \leq p.$$

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

As a first step, we assume an **ideal cache randomizer** $(\overline{\mathsf{rekey}}, \bar{\pi})$ that behaves as a random oracle for functions from addresses to set indexes.

Ideal Cache Randomizer

For every $k \leftarrow \overline{\mathsf{rekey}}()$, choose $\bar{\pi}_k$ uniformly at random.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

As a first step, we assume an **ideal cache randomizer** $(\overline{\text{rekey}}, \bar{\pi})$ that behaves as a random oracle for functions from addresses to set indexes.

Ideal Cache Randomizer

For every $k \leftarrow \overline{\text{rekey}}()$, choose $\bar{\pi}_k$ uniformly at random.

We obtain:

Let $p \in [0, 1]$. Then $\bar{\mathcal{C}}$ is N-**access secure with advantage at most** p for

$$N = \max\left\{ N' \ : \ \sum_{i=0}^{N'-a} \binom{N'}{i} (1/|S|)^{N'-i} (1 - 1/|S|)^{i} \leq p \right\}.$$

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

As a first step, we assume an **ideal cache randomizer** $(\overline{\text{rekey}}, \bar{\pi})$ that behaves as a random oracle for functions from addresses to set indexes.

Ideal Cache Randomizer

For every $k \leftarrow \overline{\text{rekey}}()$, choose $\bar{\pi}_k$ uniformly at random.

We obtain:

Let $p \in [0,1]$. Then $\bar{\mathcal{C}}$ is N-**access secure with advantage at most** p for

$$N = \max\left\{ N' \; : \; \sum_{i=0}^{N'-a} \binom{N'}{i} (1/|S|)^{N'-i} (1 - 1/|S|)^{i} \leq p \right\}.$$

This result has been slightly improved in a scenario with **noise**.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

We consider the Intel® Core **i7-8700K (Coffee Lake)** 12**MB LLC**:

associativity a: 16

slices: 12

cache sets per slice: 1024

cache sets $|S|$: $12 \cdot 1024 = 12288$

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

We consider the Intel® Core **i7-8700K (Coffee Lake)** 12**MB LLC**:

associativity a: 16

slices: 12

cache sets per slice: 1024

cache sets $|S|$: $12 \cdot 1024 = 12288$

Suppose we want to thwart attacks with advantage **bigger than 1%**.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Application Example: Setting and Ideal Case

We consider the Intel® Core **i7-8700K (Coffee Lake)** 12**MB LLC**:

- **associativity** a: 16
- slices: 12
- cache sets per slice: 1024
- **cache sets** $|S|$: $12 \cdot 1024 = 12288$

Suppose we want to thwart attacks with advantage **bigger than 1%**.

Ideal Case:

The ideal RPC $\bar{\mathcal{C}}$ is N-access secure with advantage at most 0.01 for

$$N = \max\left\{ N' \;:\; \sum_{i=0}^{N'-a} \binom{N'}{i} (1/|S|)^{N'-i} (1 - 1/|S|)^{i} \leq 0.01 \right\}.$$

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

We consider the Intel® Core **i7-8700K (Coffee Lake)** 12**MB LLC**:

- **associativity** a: 16
- slices: 12
- cache sets per slice: 1024
- **cache sets** $|S|$: $12 \cdot 1024 = 12288$

Suppose we want to thwart attacks with advantage **bigger than 1%**.

Ideal Case:

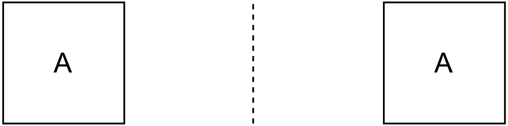
The ideal RPC $\bar{\mathcal{C}}$ is 100532-**access secure** with advantage at most 0.01.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Table of Contents

Cache randomizers are **not ideal** in practice.

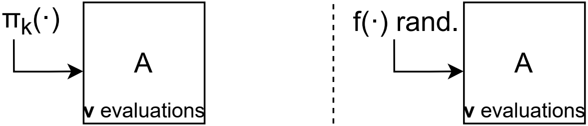
We use **pseudo-random** cache randomizers (π_k, rekey):



Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache randomizers are **not ideal** in practice.

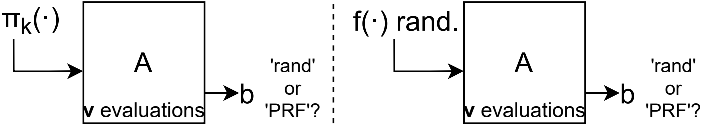
We use **pseudo-random** cache randomizers (π_k, rekey):



Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

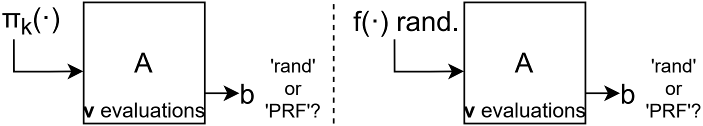
Cache randomizers are **not ideal** in practice.

We use **pseudo-random** cache randomizers (π_k, rekey):



Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Cache randomizers are **not ideal** in practice.
We use **pseudo-random** cache randomizers (π_k, rekey):

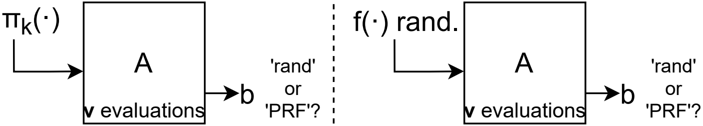


We say (π_k, rekey) **is** (ν, ε)-**pseudo-random** if every A has advantage at most ε in distinguishing the ν outputs of the oracle from random.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Security Analysis: PRF Cache Randomizer

Cache randomizers are **not ideal** in practice.
We use **pseudo-random** cache randomizers (π_k, rekey):



We say (π_k, rekey) **is** (ν, ε)**-pseudo-random** if every A has advantage at most ε in distinguishing the ν outputs of the oracle from random.

Extend previous result to **PRF cache randomizers**: advantages add up.

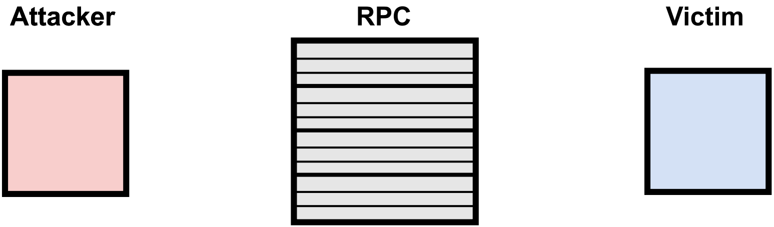
Suppose that

- the ideal RPC $\bar{\mathcal{C}}$ **is** N**-access secure with advantage at most** p,
- the cache randomizer is (N, ε)**-pseudo-random**.

Then $\mathcal{C}$ is N**-access secure with advantage at most** $p + \varepsilon$.

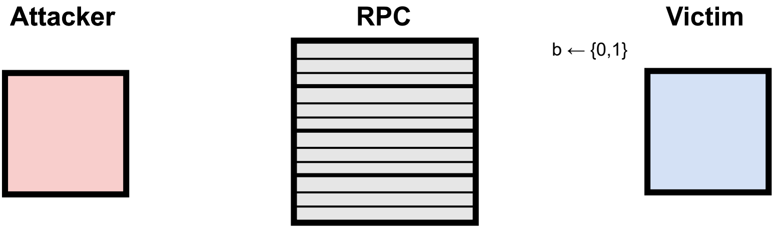
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



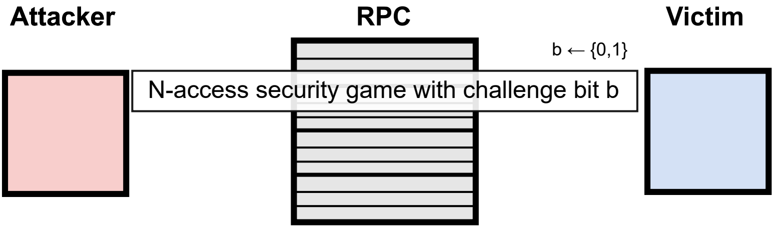
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



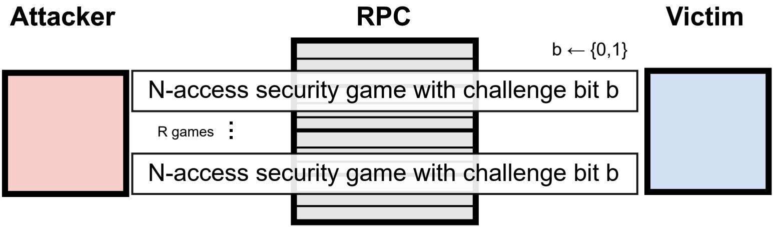
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



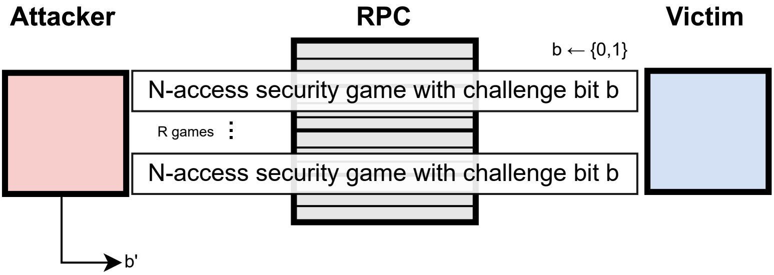
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



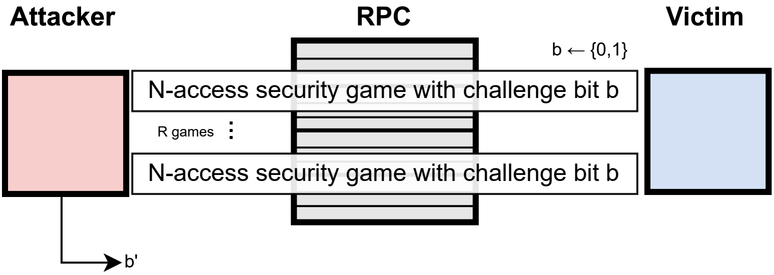
Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Multi-epoch Security Definition



The RPC $\mathcal{C}$ **is** R**-Epoch** N**-Access Secure with advantage at most** p if, for all target addresses, every $N_{1,i} + N_{2,i} = N$, and every adversary $\mathcal{A}$

$$\mathrm{Adv}_{\mathcal{C},\mathcal{A}}^{\mathrm{ME-RPC}}(R, N) := 2\left|\Pr\left[b' = b\right] - 1/2\right| \leq p.$$

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Following [Abdalla-Bellare'00], we **reduce multi-epoch security** to

- **single-epoch** security and
- the **pseudo-randomness** of the rekeying algorithm.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Following [Abdalla-Bellare'00], we **reduce multi-epoch security** to

- **single-epoch** security and
- the **pseudo-randomness** of the rekeying algorithm.

As before, all advantages add up.

Suppose

- $\mathcal{C}$ is N-**access secure with advantage at most** p,
- rekey is (R, ε)-**pseudo-random**.

Then $\mathcal{C}$ is R-**epoch** N-**access secure with advantage at most** $R \cdot p + \varepsilon$.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Following [Abdalla-Bellare'00], we **reduce multi-epoch security** to

- **single-epoch** security and
- the **pseudo-randomness** of the rekeying algorithm.

As before, all advantages add up.

Suppose

- $\mathcal{C}$ is N-**access secure with advantage at most** p,
- rekey is (R, ε)-**pseudo-random**.

Then $\mathcal{C}$ is R-**epoch** N-**access secure with advantage at most** $R \cdot p + \varepsilon$.

Rekeying **expands the time window** where security is **provably enforced**.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Suppose we want to thwart attacks with advantage **bigger than 1%**.

PRF case:

Assume the cache randomizer is $(100000, 0.001)$-pseudo-random.

Generalitat de Catalunya
Departament de Recerca
i Universitats

Unió Europea
Fons Europeu
de Desenvolupament Regional

The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Suppose we want to thwart attacks with advantage **bigger than 1%**.

PRF case:

Assume the cache randomizer is $(100000, 0.001)$-pseudo-random.
The ideal RPC $\bar{\mathcal{C}}$ is 99317-access secure with advantage at most 0.009.
The RPC $\mathcal{C}$ is 99317-**access secure** with advantage at most 0.01.

Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Application Example: PRF and Multi-epoch Cases

Suppose we want to thwart attacks with advantage **bigger than 1%**.

PRF case:

Assume the cache randomizer is $(100000, 0.001)$-pseudo-random.
The ideal RPC $\bar{\mathcal{C}}$ is 99317-access secure with advantage at most 0.009.
The RPC $\mathcal{C}$ is 99317-**access secure** with advantage at most 0.01.

Multi-epoch case:

Assume the rekeying algorithm is $(10, 0.00001)$-pseudo-random.

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Suppose we want to thwart attacks with advantage **bigger than 1%**.

PRF case:

Assume the cache randomizer is $(100000, 0.001)$-pseudo-random.
The ideal RPC $\bar{\mathcal{C}}$ is 99317-access secure with advantage at most 0.009.
The RPC $\mathcal{C}$ is 99317-**access secure** with advantage at most 0.01.

Multi-epoch case:

Assume the rekeying algorithm is $(10, 0.00001)$-pseudo-random.
The RPC $\mathcal{C}$ is 9-**epoch,** 64033-**access** secure with advantage at most 0.01.

Security is **provably enforced for** $RN = 576297$ **accesses**

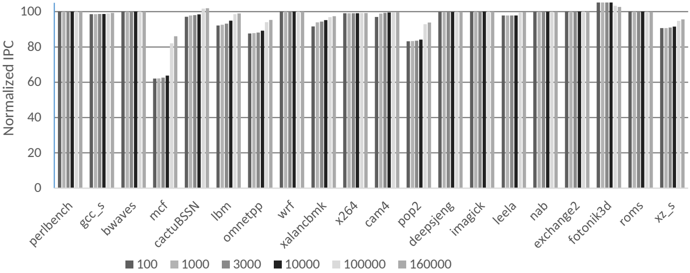
Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Table of Contents

We use **ChampSim** to simulate the RPC in our running example, with

- cache randomizer: xor-based parametric randomizer [Trilla et all'18].
- L1 and L2 private caches: 8 ways, 64 and 1024 cache sets.
- replacement policy: PLRU.
- workload: **SPEC2006 bechmark suite**.

IPC for a randomized cache for different workloads and rekeying periods, normalized to a non-randomized setting



Generalitat de Catalunya Departament de Recerca i Universitats
Unió Europea Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Table of Contents

In this work, we introduce a **security model** for RPCs.

- We present game-based **security definitions**
- We show **how to design** RPCs to obtain **security guarantees**
- We provide a **performance evaluation**

Further research in this line

- improve security through **additional hardware techniques**
- **broaden the scope** of security definitions
- **tighten the bounds** for particular replacement policies

Generalitat de Catalunya
Departament de Recerca i Universitats
Unió Europea
Fons Europeu de Desenvolupament Regional
The DRAC project, which is funded by the European Regional Development Fund (ERDF), has a total cost of €4.000.000 of which 2.000.000 (50%) are subsidized.

Thank you! Any questions?