Securing Cryptographic Modules: A Shades of Gray Story

Matthieu Rivain
matthieu.rivain@cryptoexperts.com

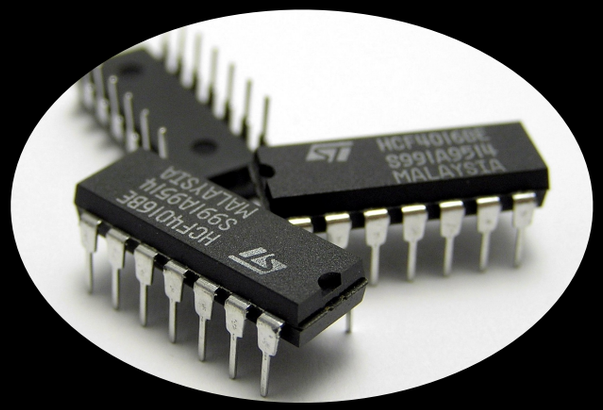
ICMC 2019 - Vancouver - 16 May 2019

CryptoExperts

- Founded in 2009, based in Paris
- Research team & service company
- Strong focus on cryptography & security of embedded systems
- Services of custom crypto design, implementation, evaluation
- Software & technologies
  - Secure embedded crypto libraries
  - White-box cryptography
  - Encryption for Pay-TV
  - Fully Homorphic Encryption (FHE)
- Visit our website: **www.cryptoexperts.com**

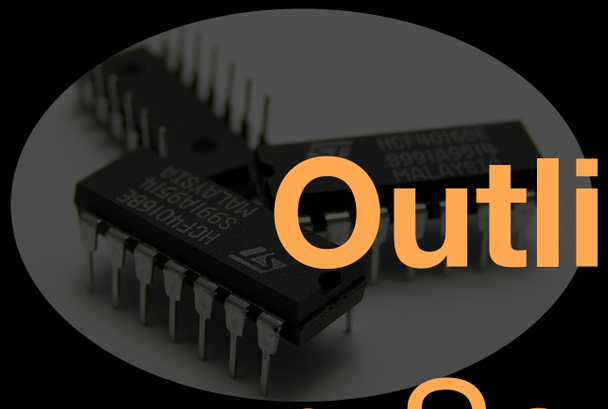
What I will (not) talk about

What I will (not) talk about



Securing Cryptographic Modules: A ~~Fifty~~ Story

What I will (not) talk about



Outline

- Security models
- Security assessment
- Evolution of CM security

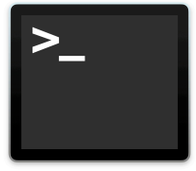
Securing Cryptographic Modules: A ~~Fifty Shades of Grey~~ Story

Cryptographic modules

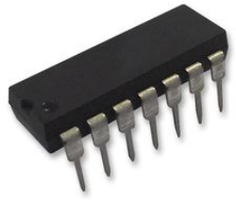
Smart cards

HSMs

CM galaxy



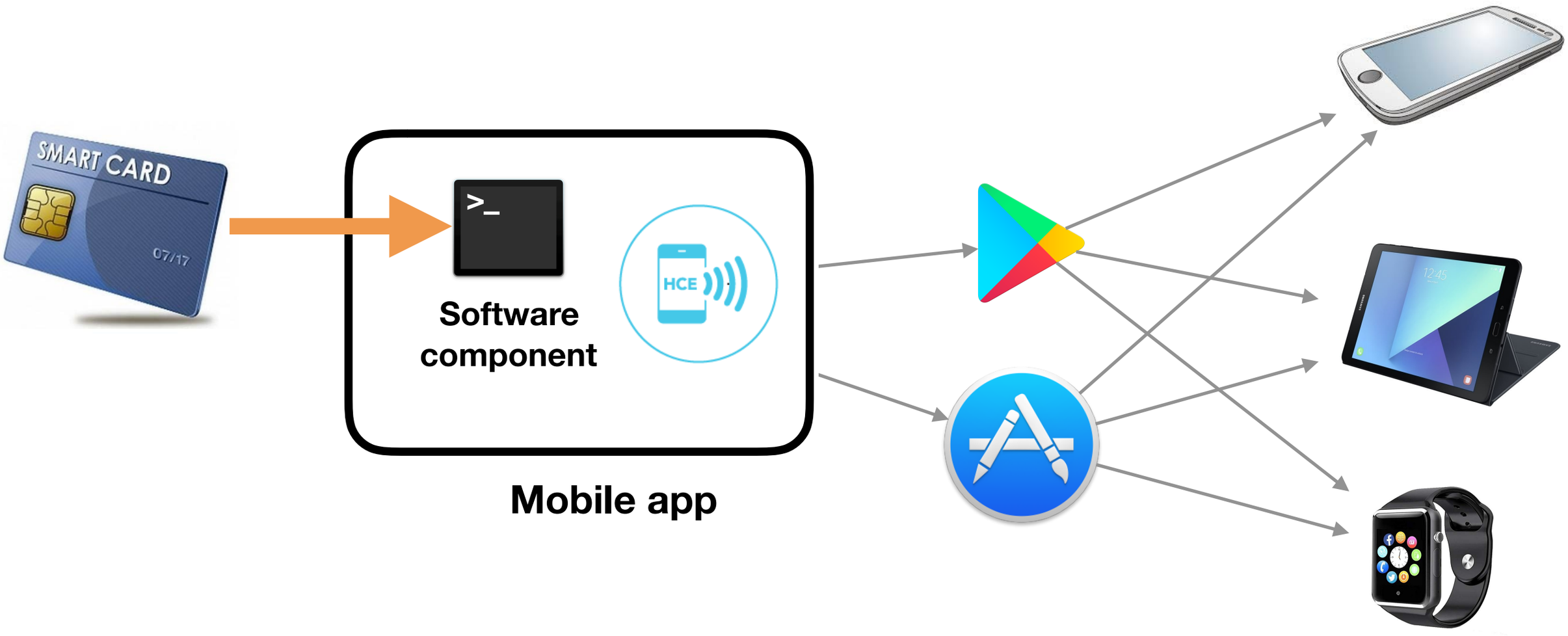
Software CM



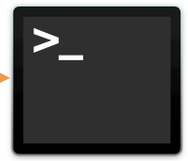
Security ICs / TPMs

Systems on Chip / Microcontroller

Current trend



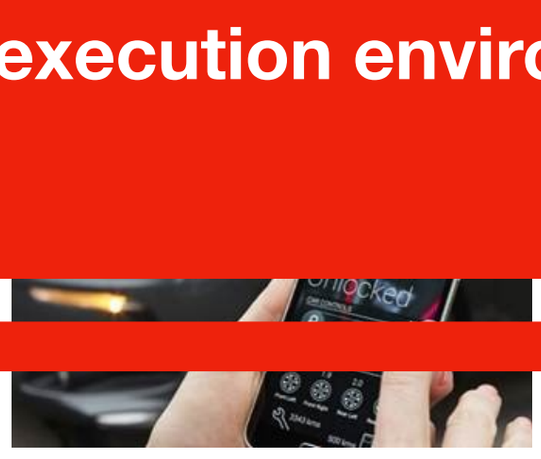
Current trend

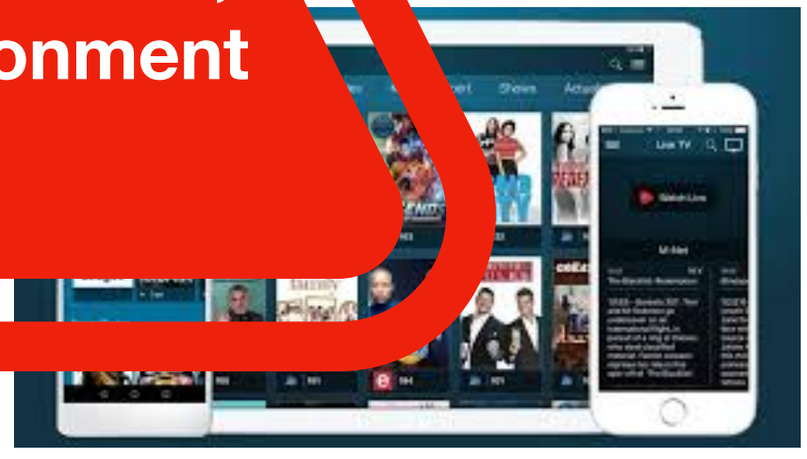


Software component

Lot of potential vulnerabilities:

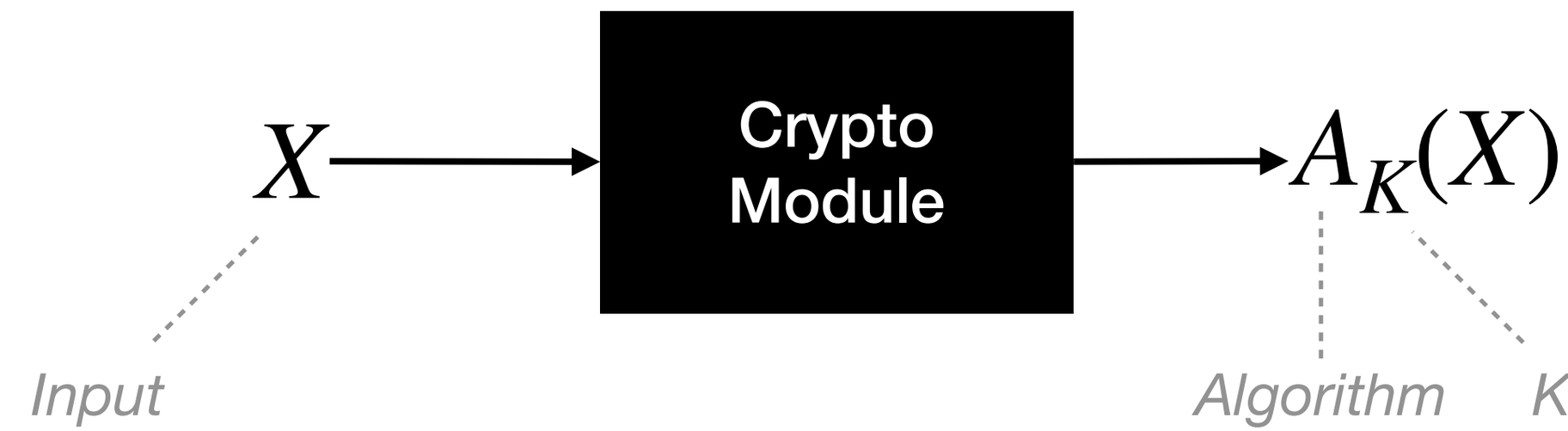
software copyable, apps available on internet, rich execution environment



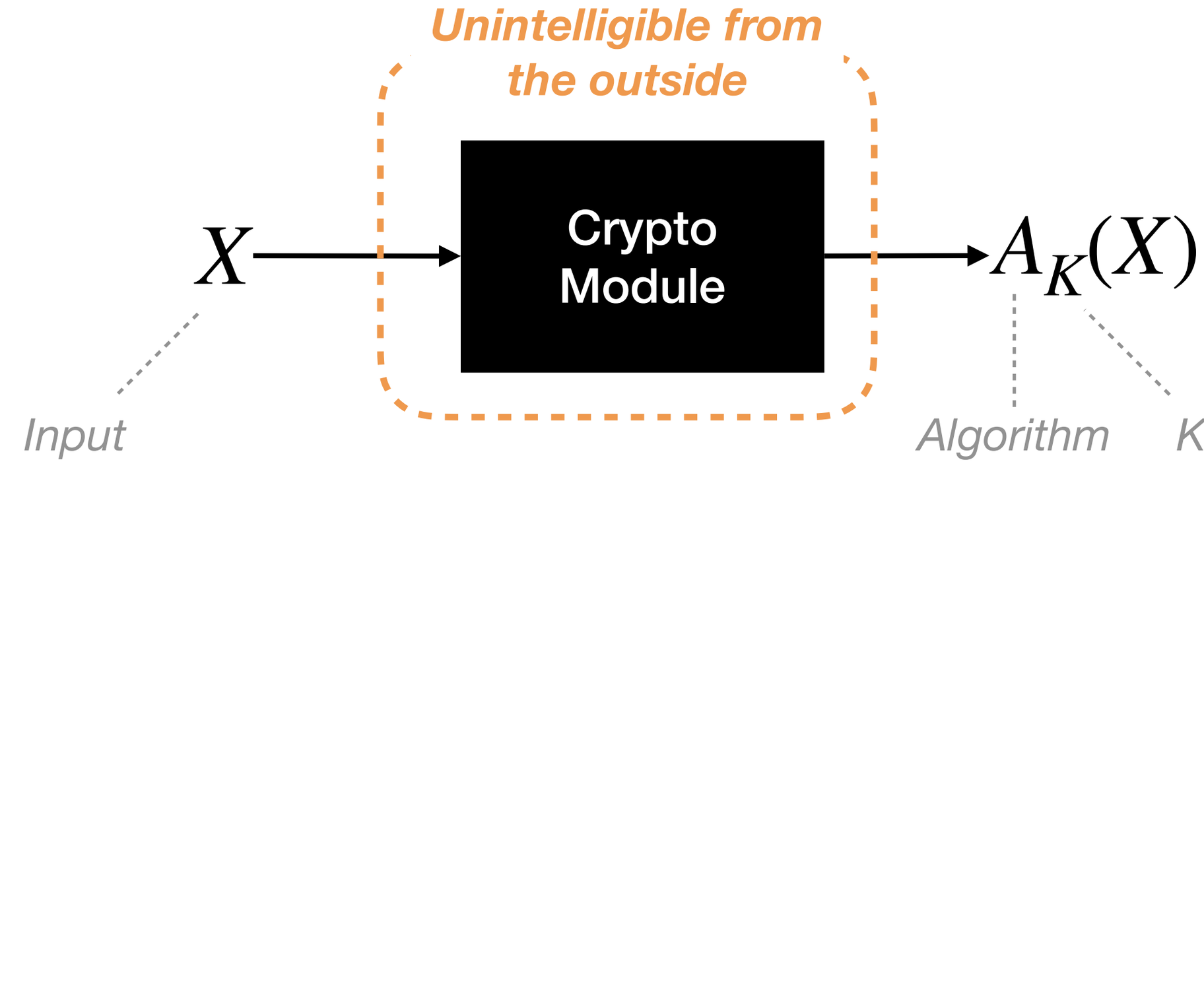


Security models

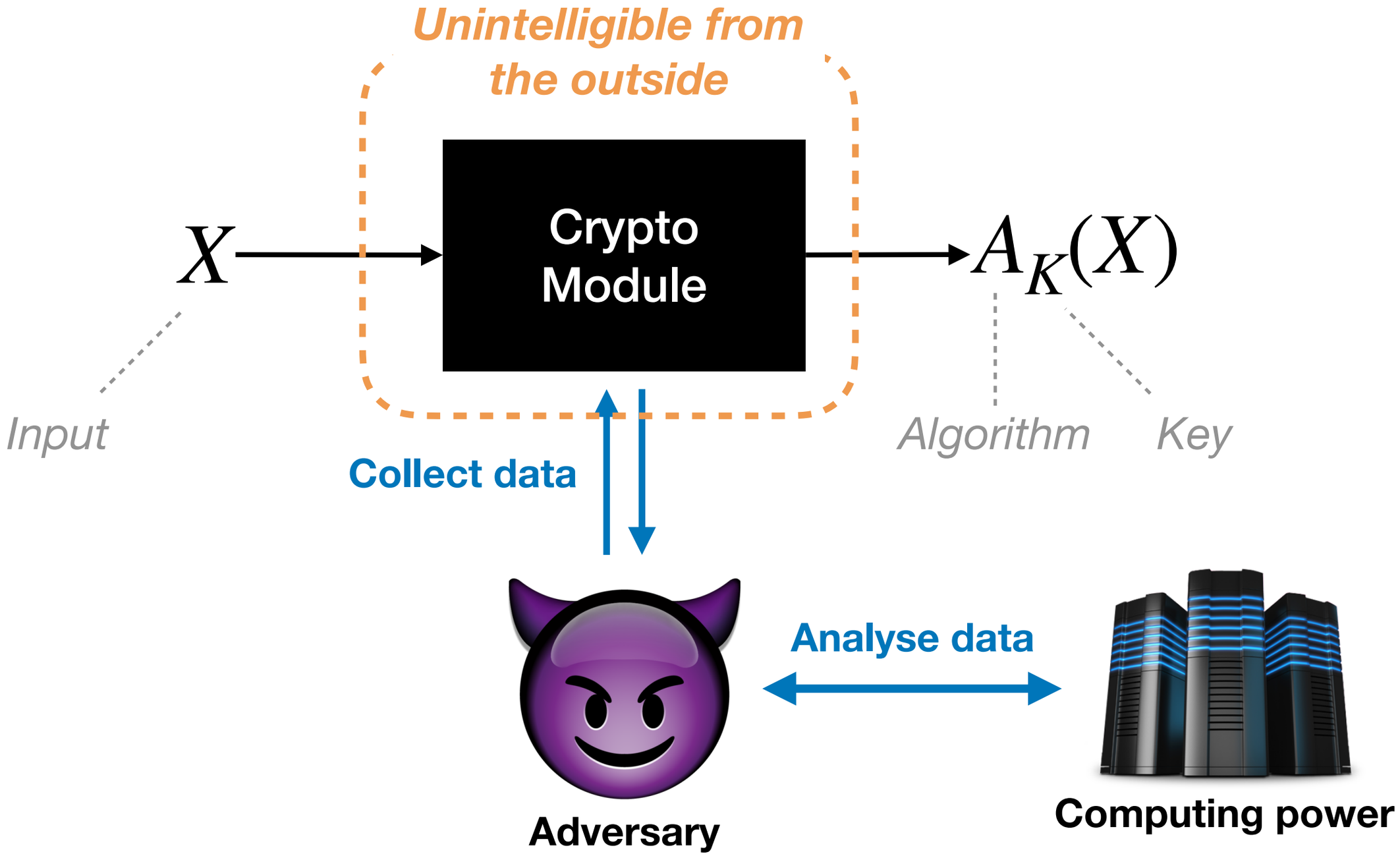
Black-box model



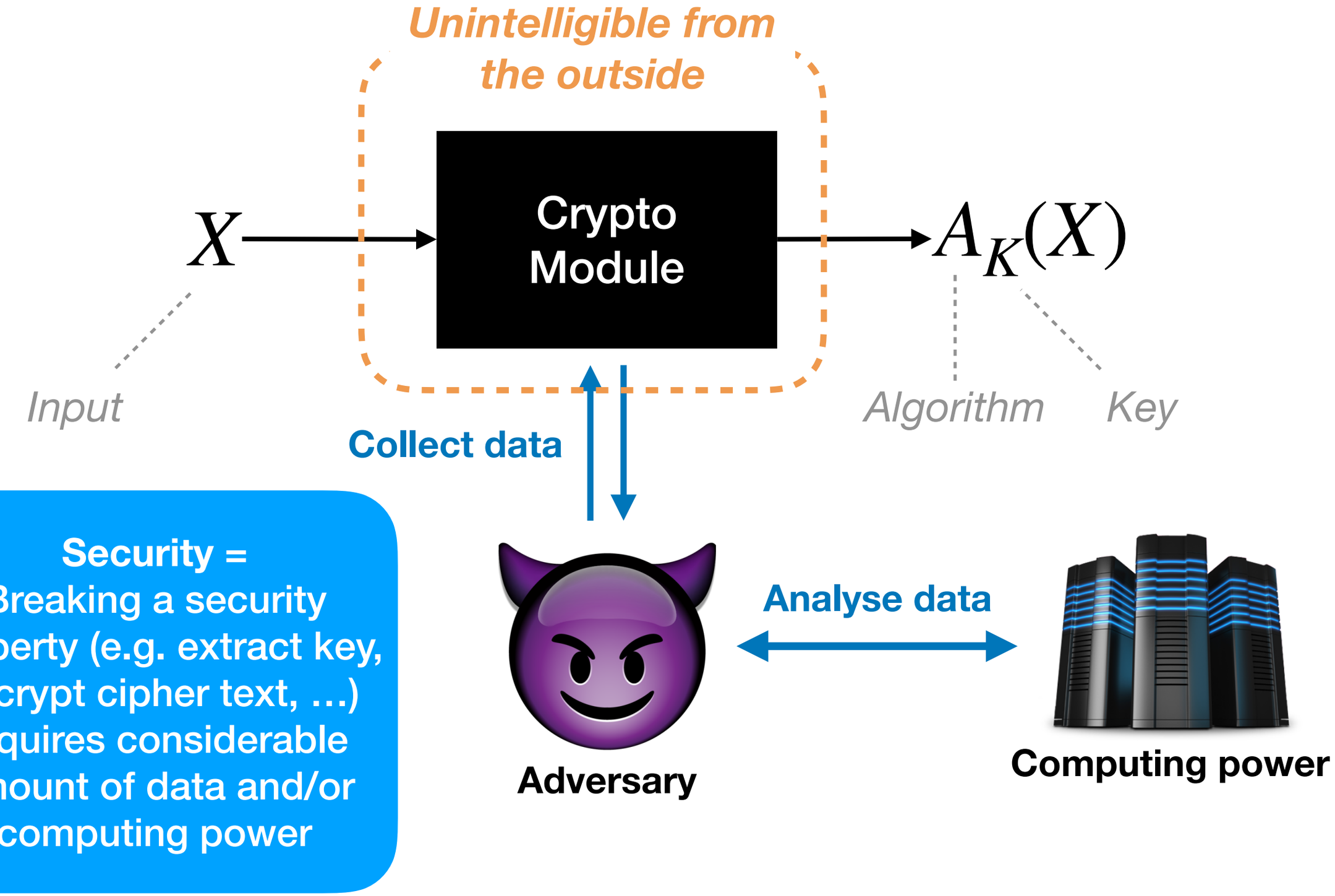
Black-box model



Black-box model

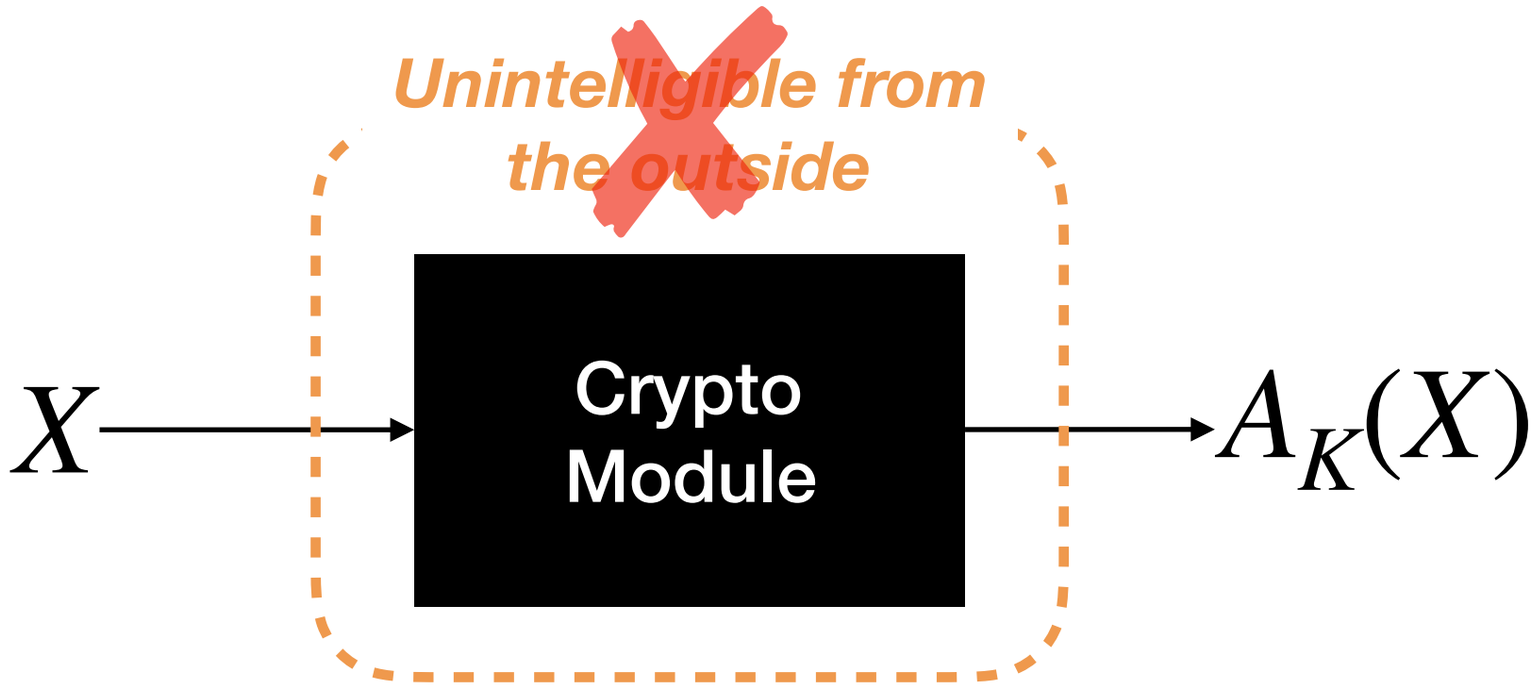


Black-box model

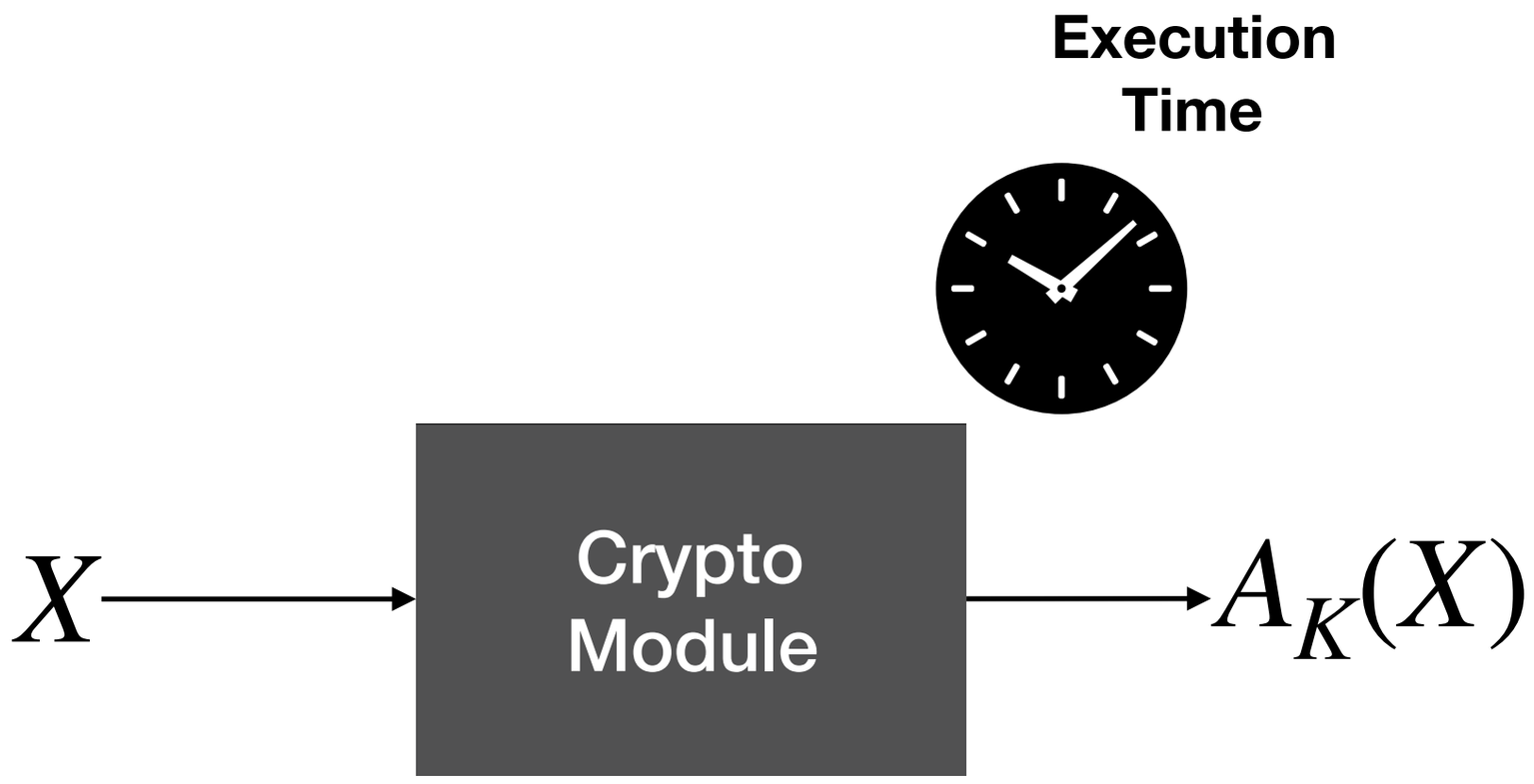


Security =
Breaking a security property (e.g. extract key, decrypt cipher text, …) requires considerable amount of data and/or computing power

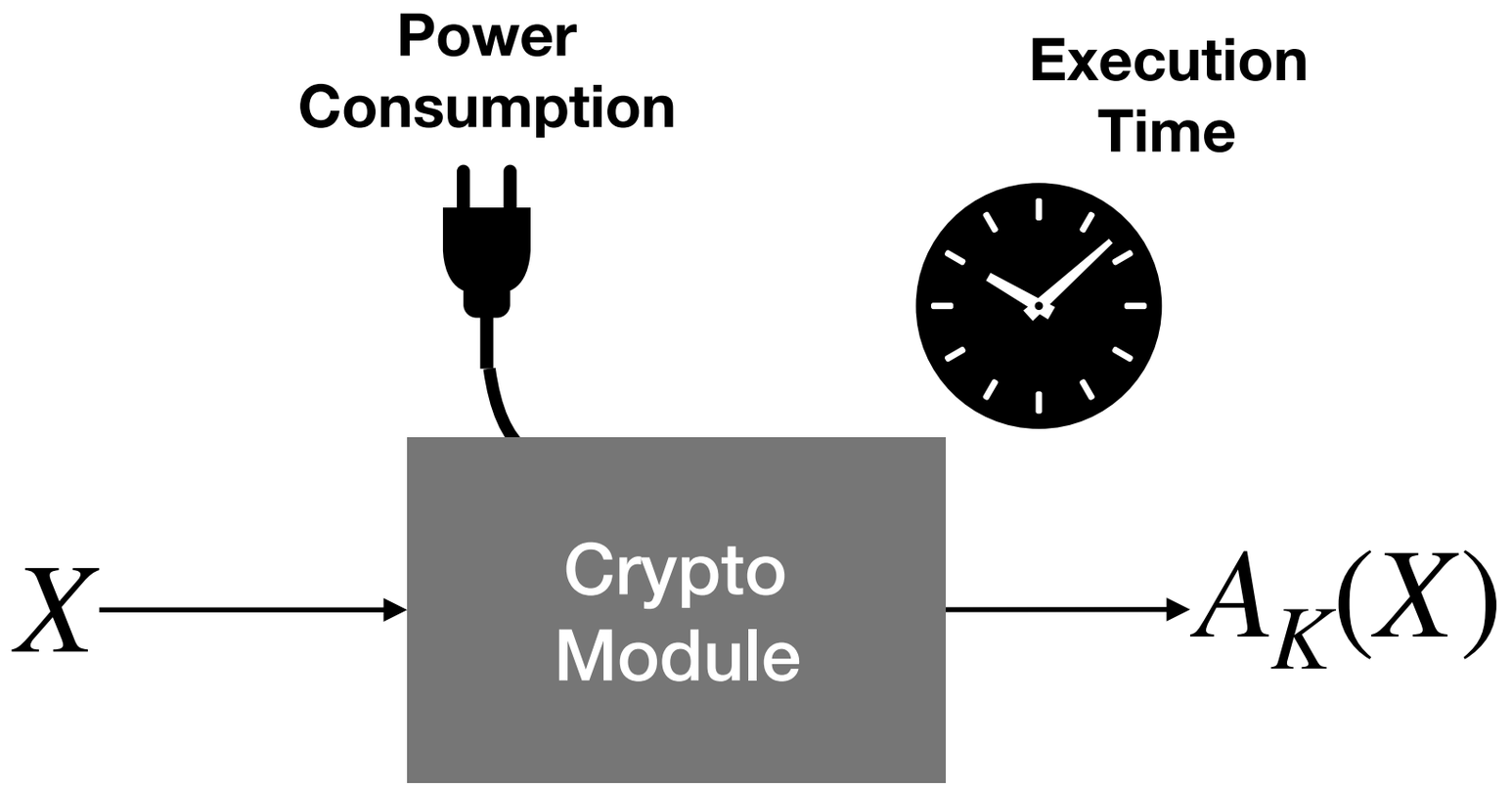
Side-channel attacks



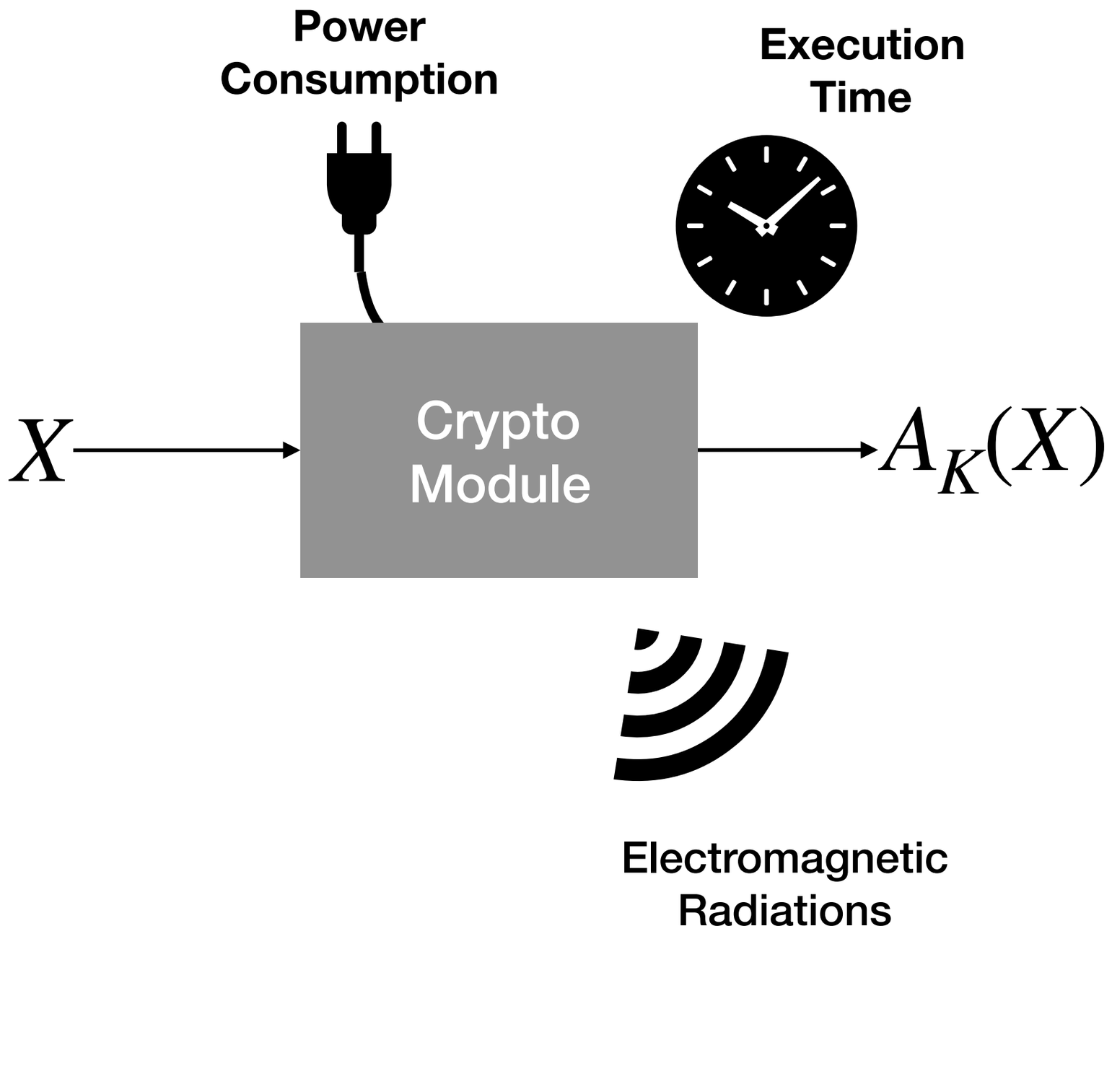
Side-channel attacks



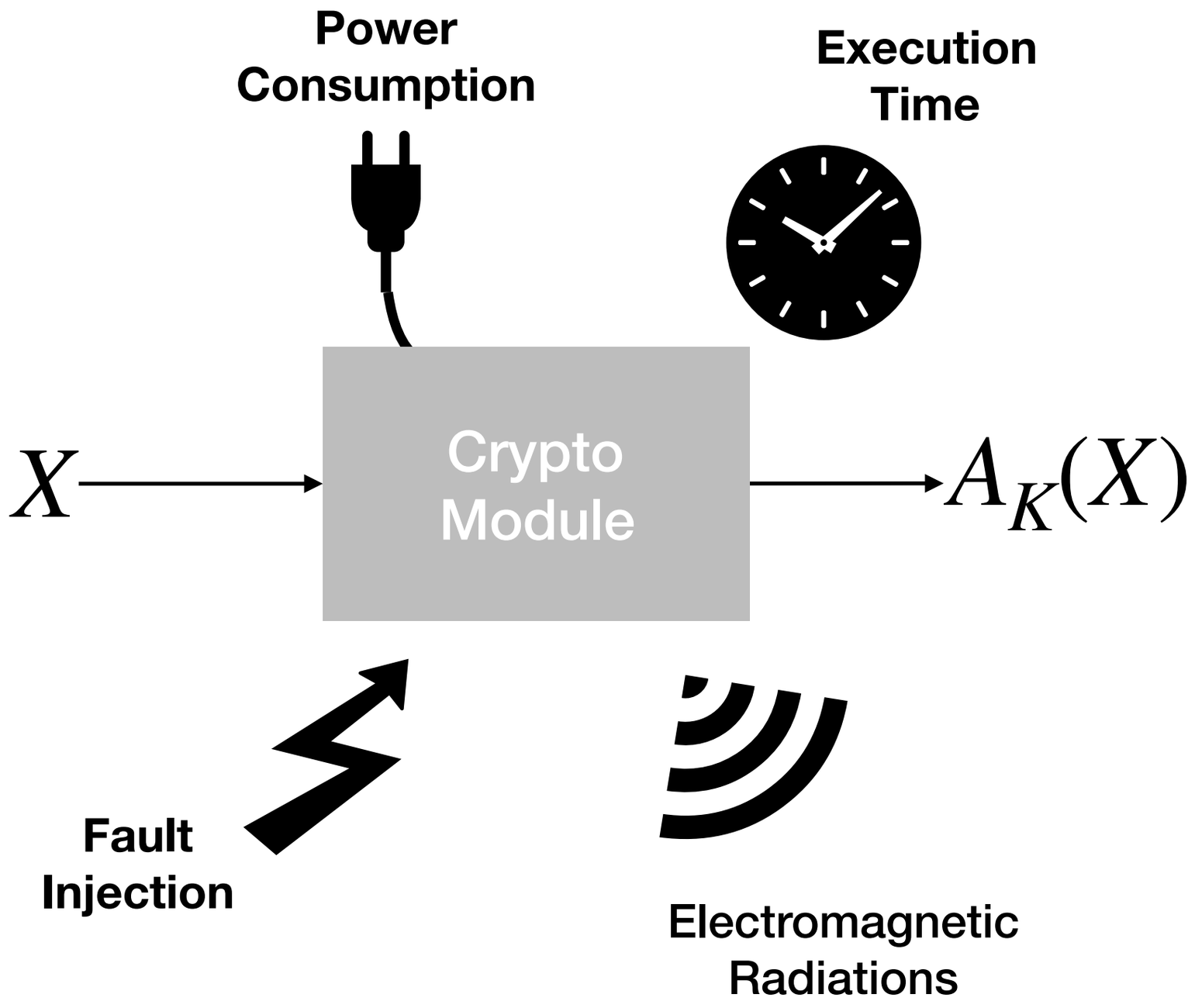
Side-channel attacks



Side-channel attacks

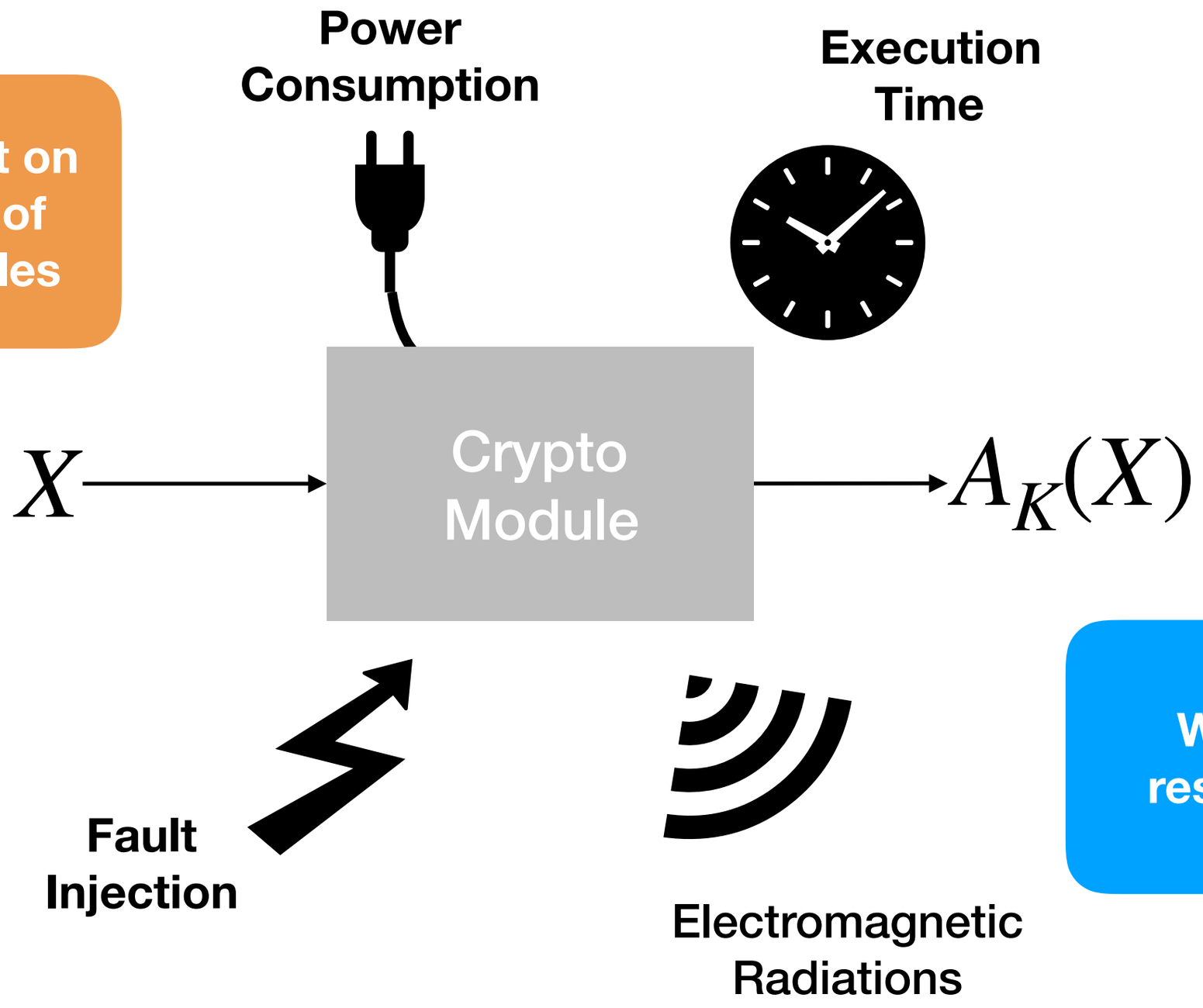


Side-channel attacks



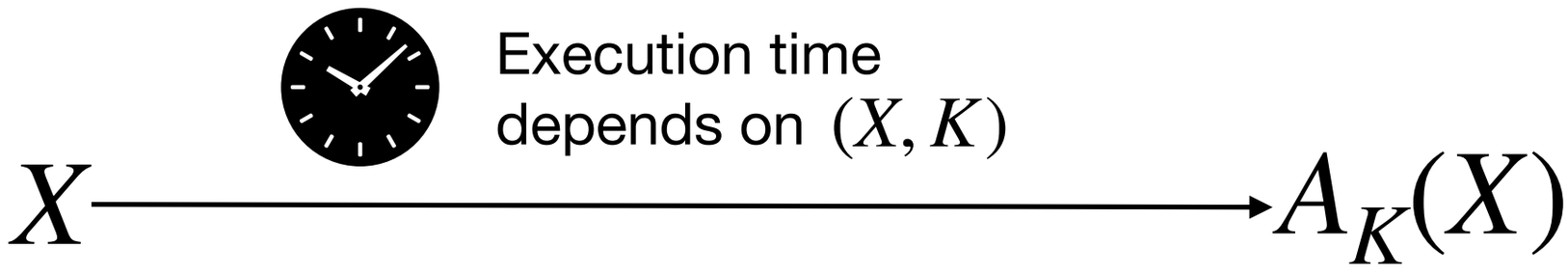
Side-channel attacks

Strong impact on the security of crypto modules



Whole new research area

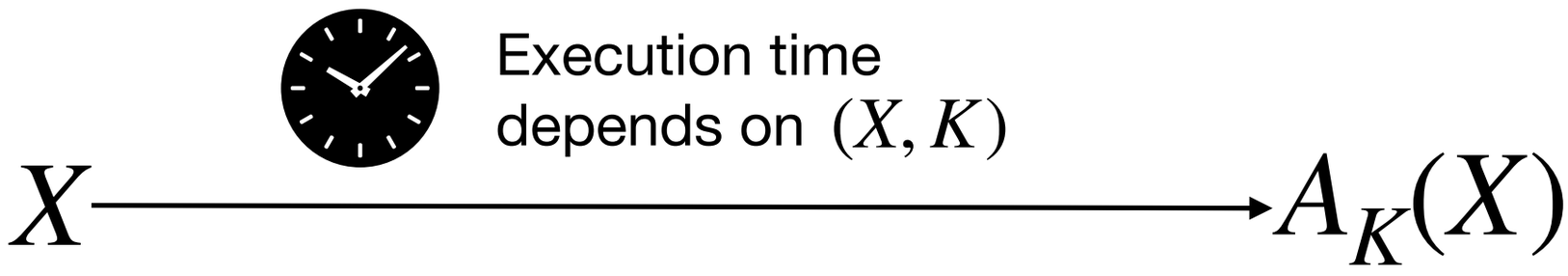
Timing attacks




```
[...]

if (key_dependent_bit == 0)
{
    do_something();
}
else
{
    do_something_else();
}

[...]
```

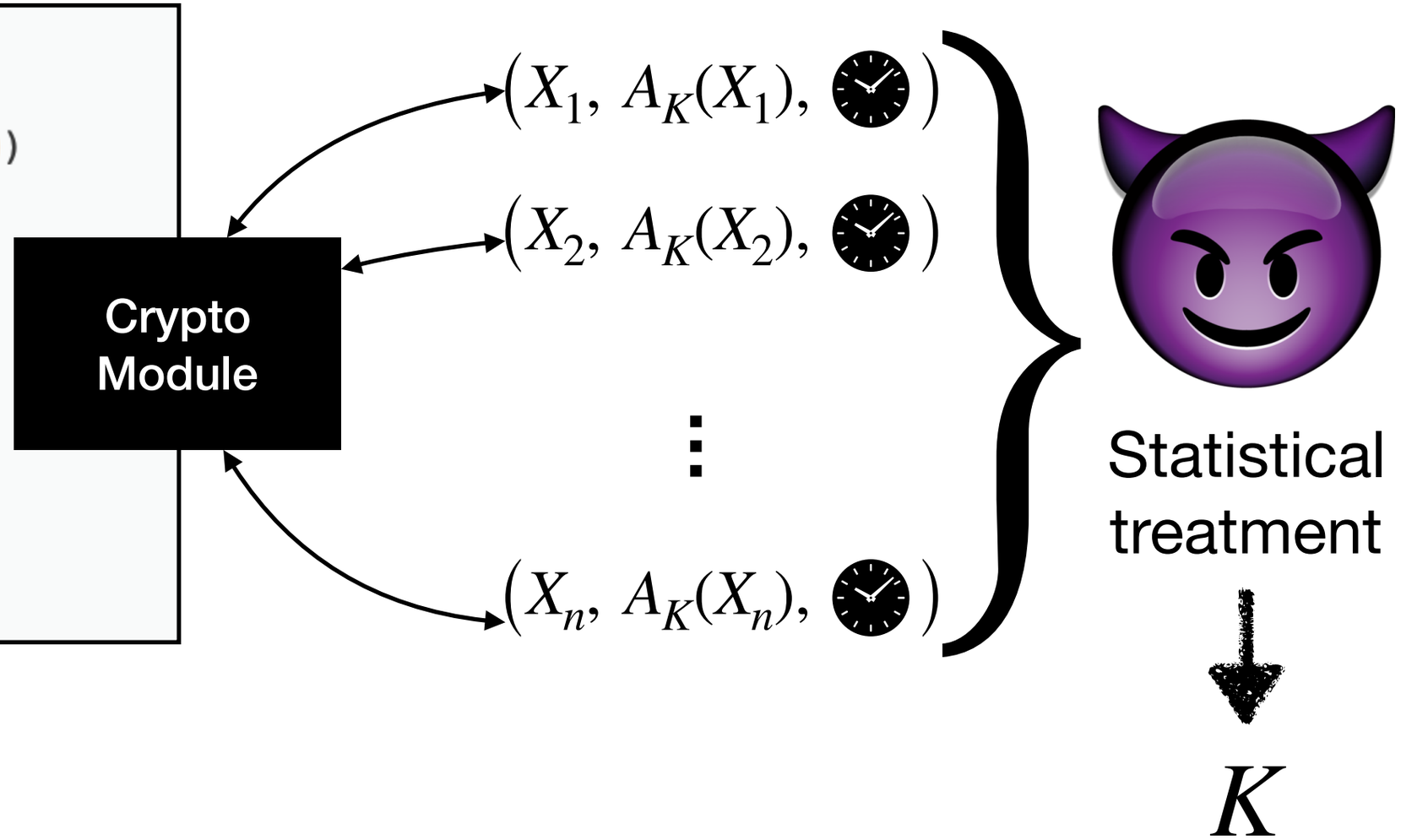
Simple example

Timing attacks




```
[...]

if (key_dependent_bit == 0)
{
    do_something();
}
else
{
    do_something_else();
}

[...]
```

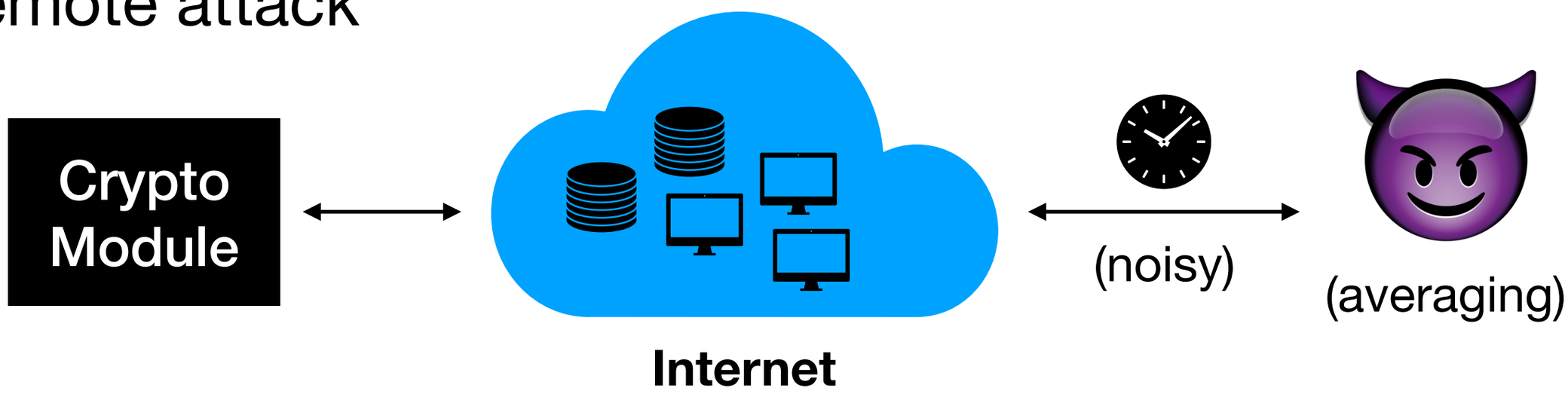
Simple example



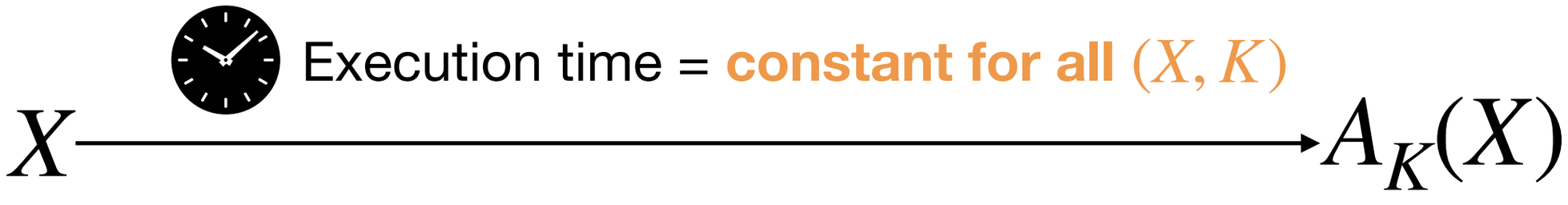
Timing attacks

- Lot of (naive) crypto implementations are vulnerable

- Remote attack

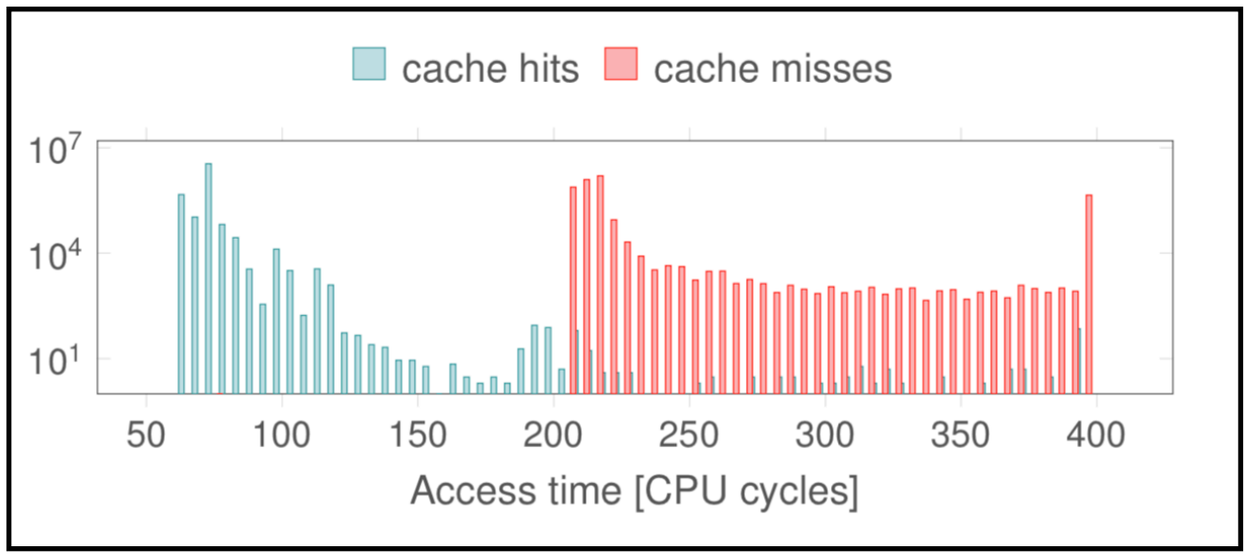


- Solution: constant-time



Timing attacks

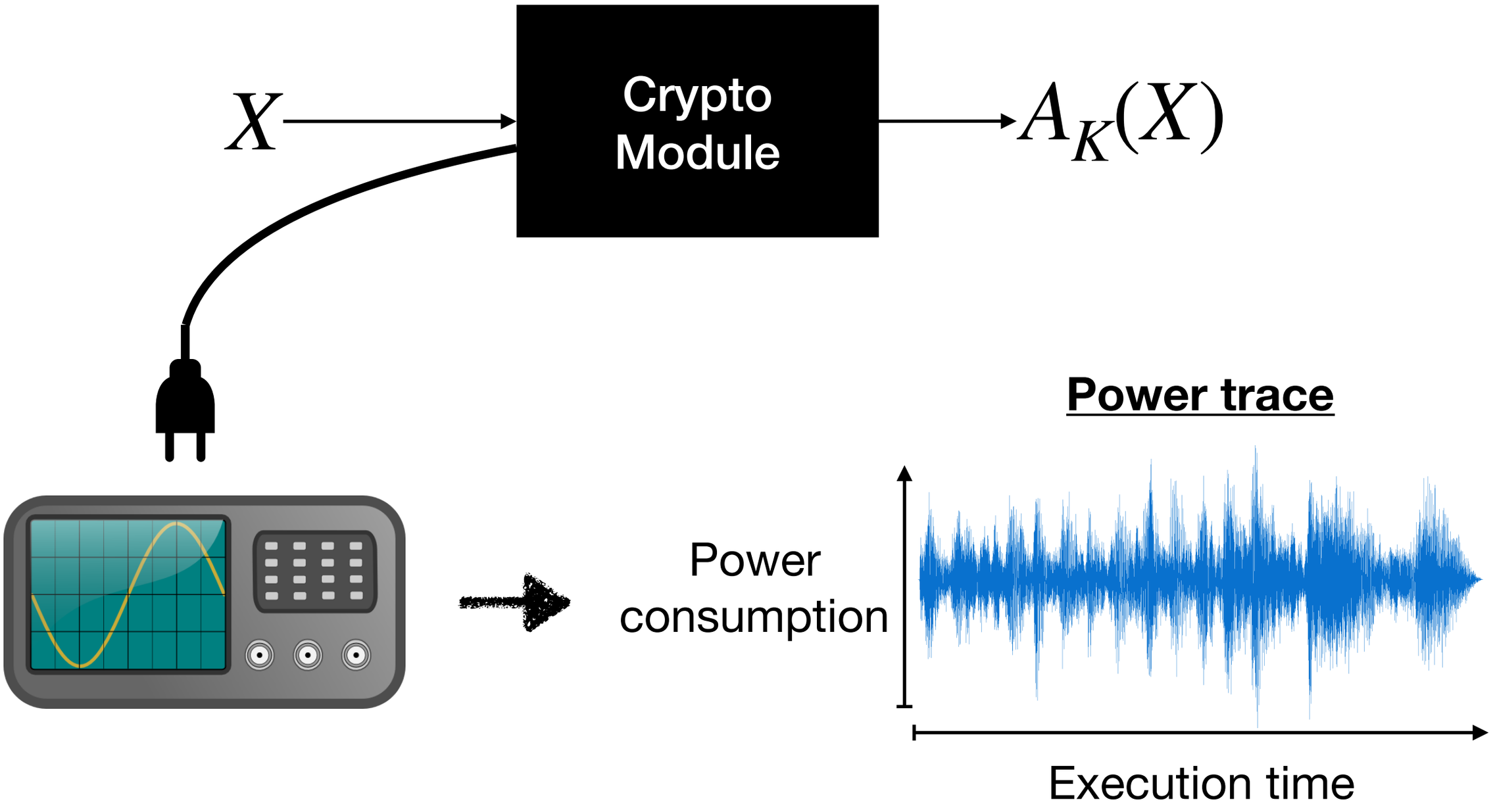
- Today: constant-time = must-have for crypto
- Constant-time algorithm ≠ constant-time implementation
- Cache timing attacks



Source: **`gruss.cc/files/microarchitecturalincontinence.pdf`**

- Avoid data-dependent memory look-up

Power analysis



Differential Power analysis

X

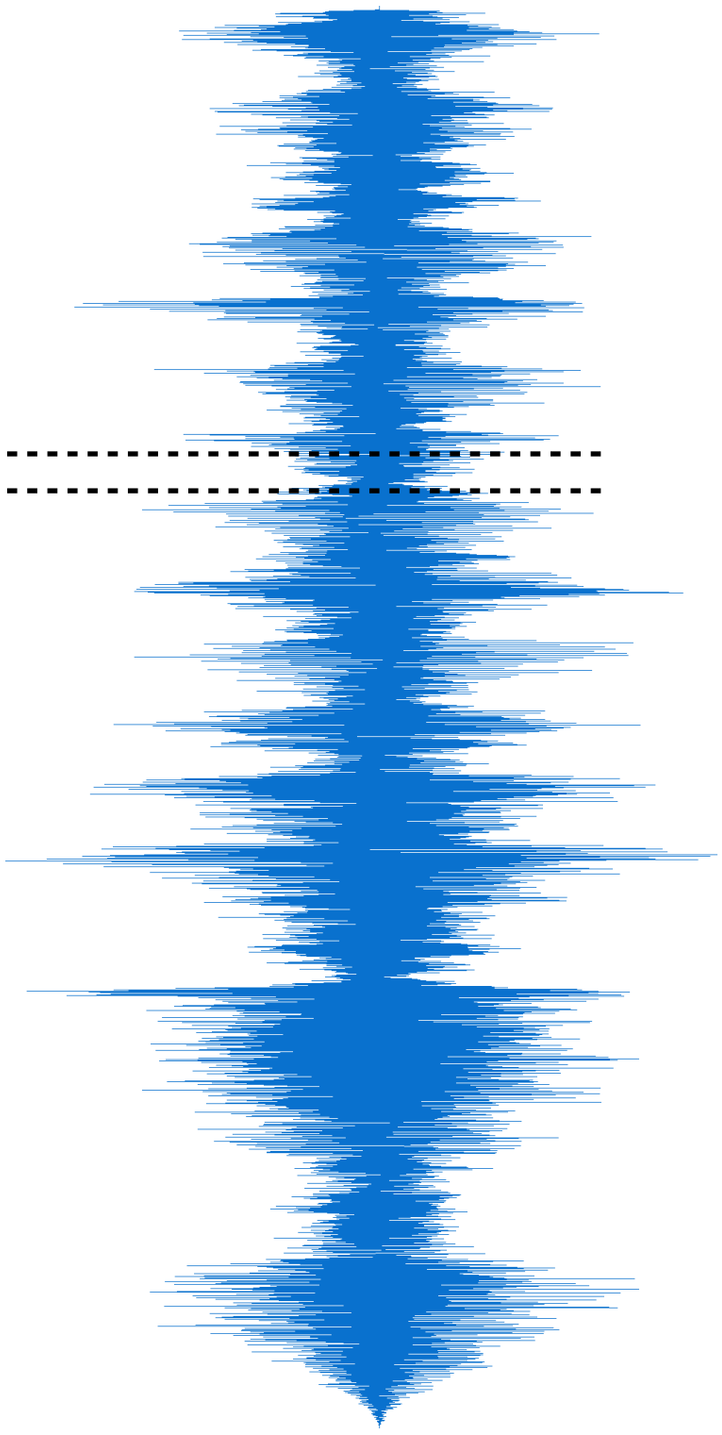
Key byte

$IR = f(X, k_1)$

Intermediate result

$A_K(X)$

```
...

EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R2
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R3
MOV     R11, R0, ROR #32-8
AND     R11, R0, ROR #32-1
EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R4
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R5
EOR     R6, R3, R5, ROR #3
EOR     R6, R6, ROR, #1
EOR     R6, R2

...
```



Differential Power analysis

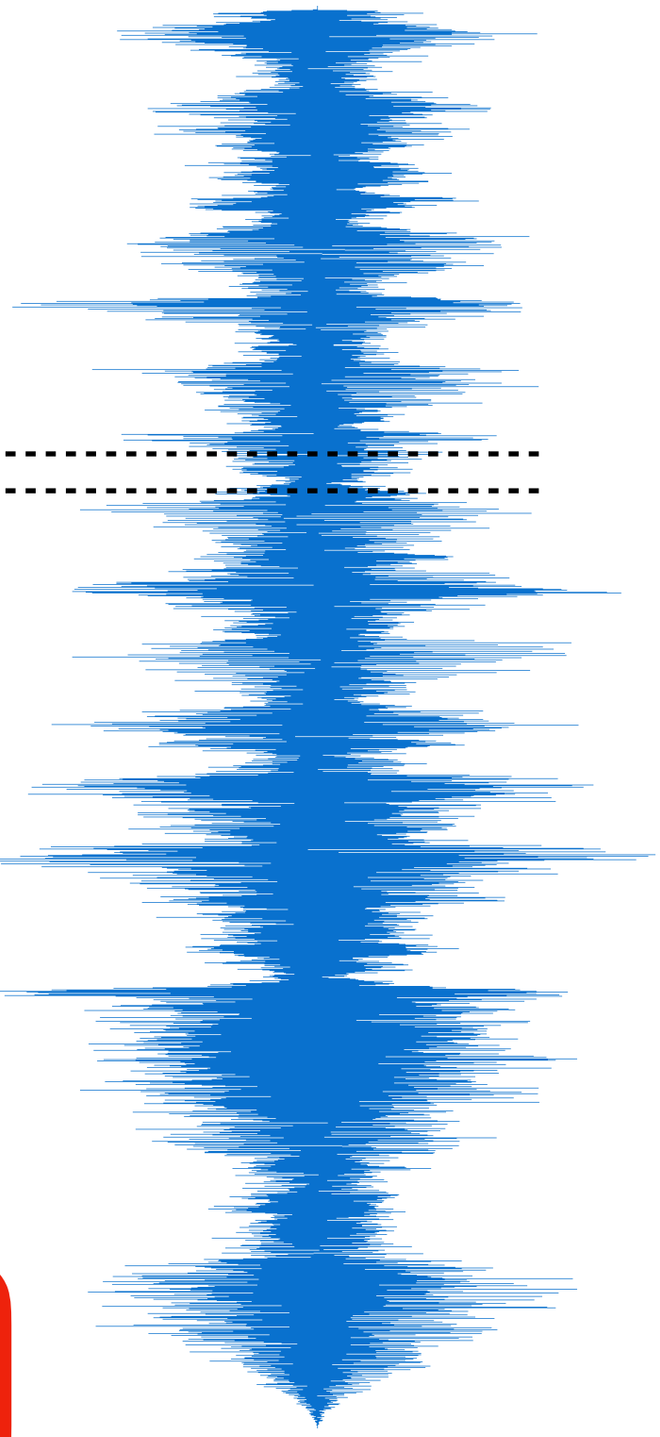
X

Key byte

$IR = f(X, k_1)$

Intermediate result

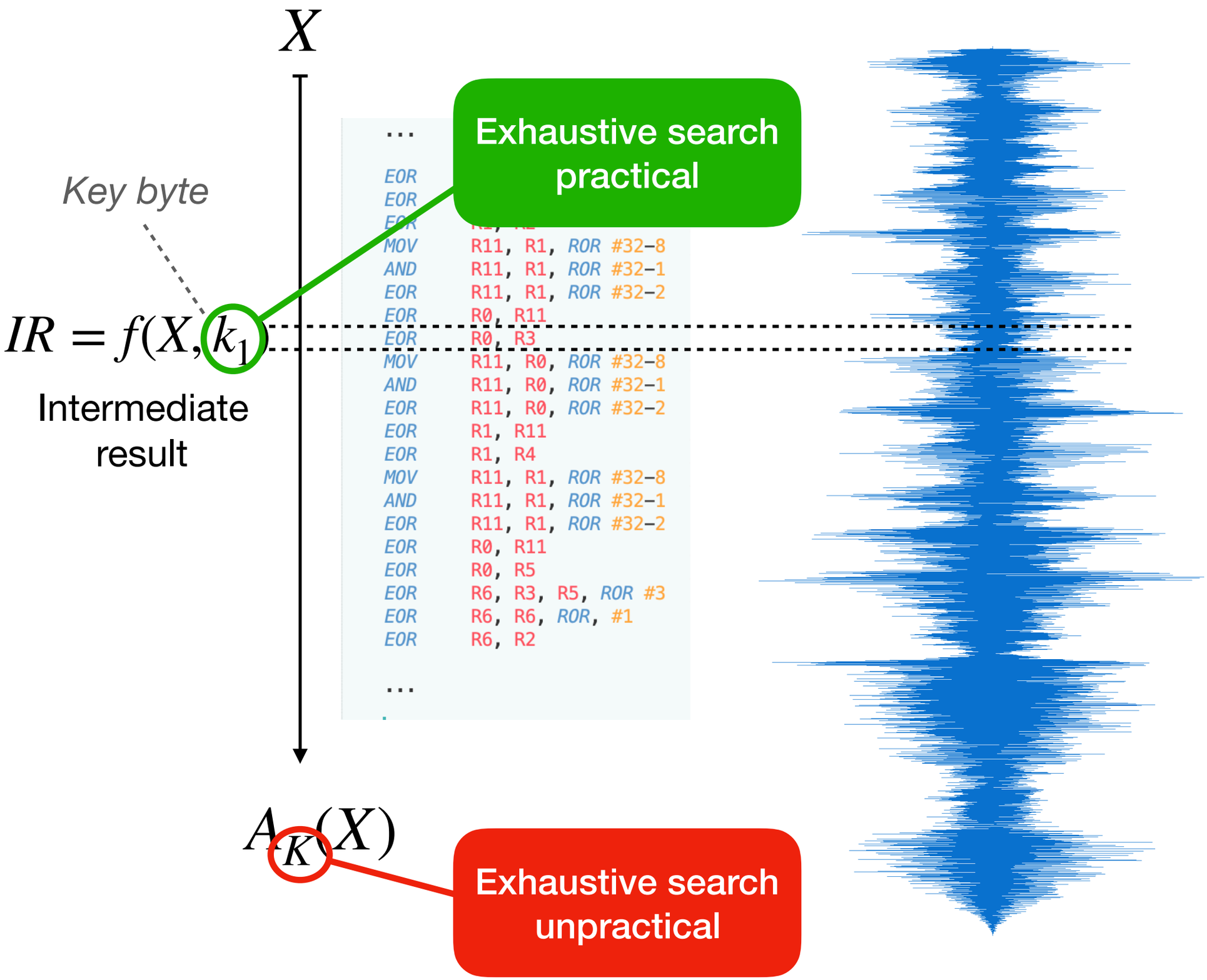
```
...

EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R2
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R3
MOV     R11, R0, ROR #32-8
AND     R11, R0, ROR #32-1
EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R4
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R5
EOR     R6, R3, R5, ROR #3
EOR     R6, R6, ROR, #1
EOR     R6, R2

...
```



$A_K(X)$

Exhaustive search unpractical

Differential Power analysis



Differential Power analysis

X

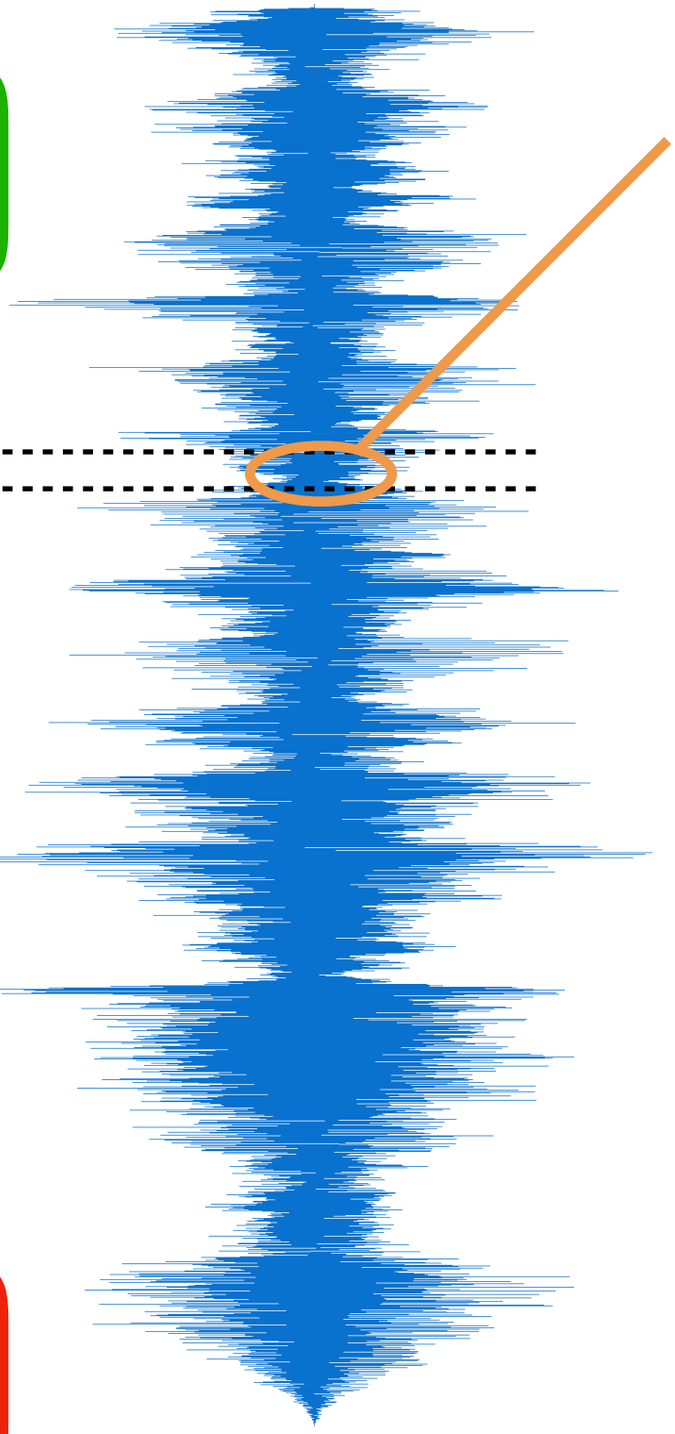
Key byte

$IR = f(X, k_1)$

Intermediate result

```
...
EOR     R1, R1
EOR     R2, R2
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R3
MOV     R11, R0, ROR #32-8
AND     R11, R0, ROR #32-1
EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R4
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R5
EOR     R6, R3, R5, ROR #3
EOR     R6, R6, ROR, #1
EOR     R6, R2
...
```

Exhaustive search practical



Statistically dependent on IR

$A_K(X)$

Exhaustive search unpractical

Differential Power analysis

X

Key byte

$IR = f(X, k_1)$

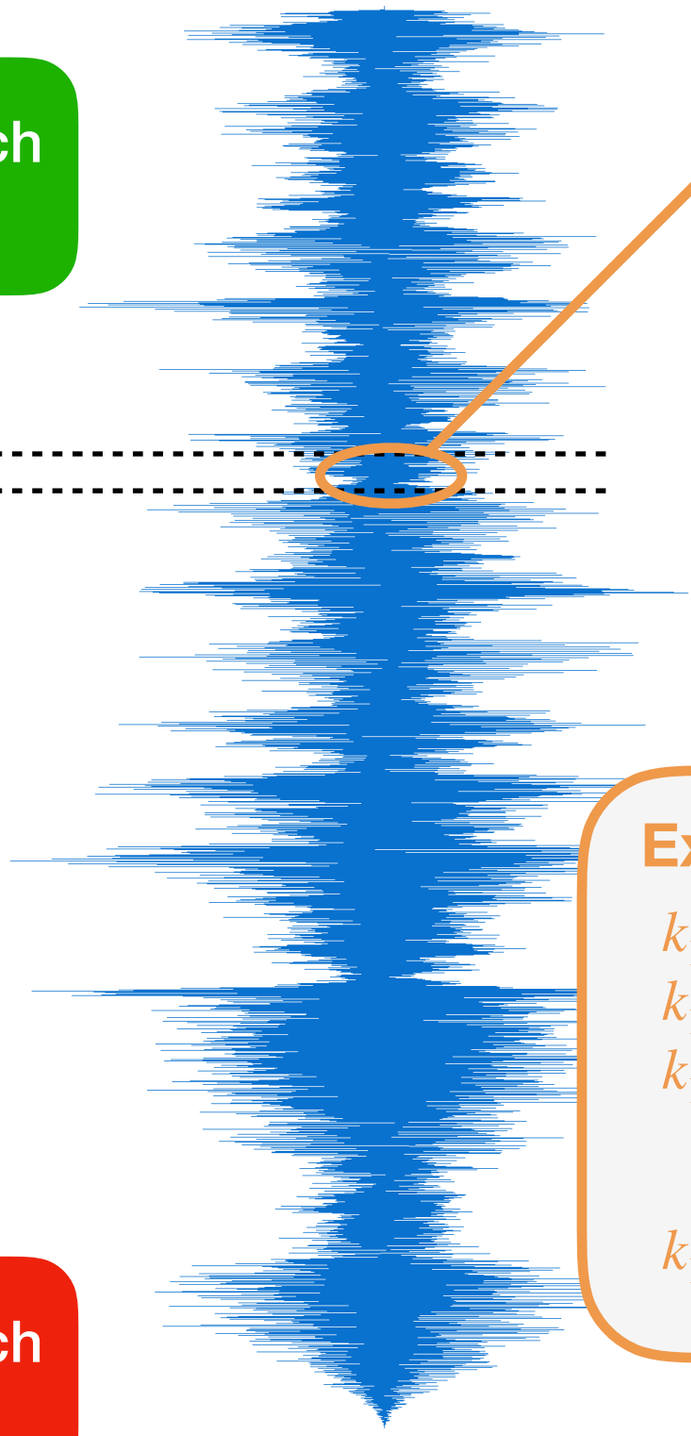
Intermediate result

$A_K(X)$

```
...
EOR     R1, R1
EOR     R2, R2
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R3
MOV     R11, R0, ROR #32-8
AND     R11, R0, ROR #32-1
EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R4
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R5
EOR     R6, R3, R5, ROR #3
EOR     R6, R6, ROR, #1
EOR     R6, R2
...
```

Exhaustive search practical

Exhaustive search unpractical



Statistically dependent on IR

Exhaustive search:

$k_1 = 0x00 \Rightarrow IR = 0x63$
$k_1 = 0x01 \Rightarrow IR = 0xA0$
$k_1 = 0x02 \Rightarrow IR = 0x3E$
...
$k_1 = 0xFF \Rightarrow IR = 0x11$

Differential Power analysis

X

Key byte

$IR = f(X, k_1)$

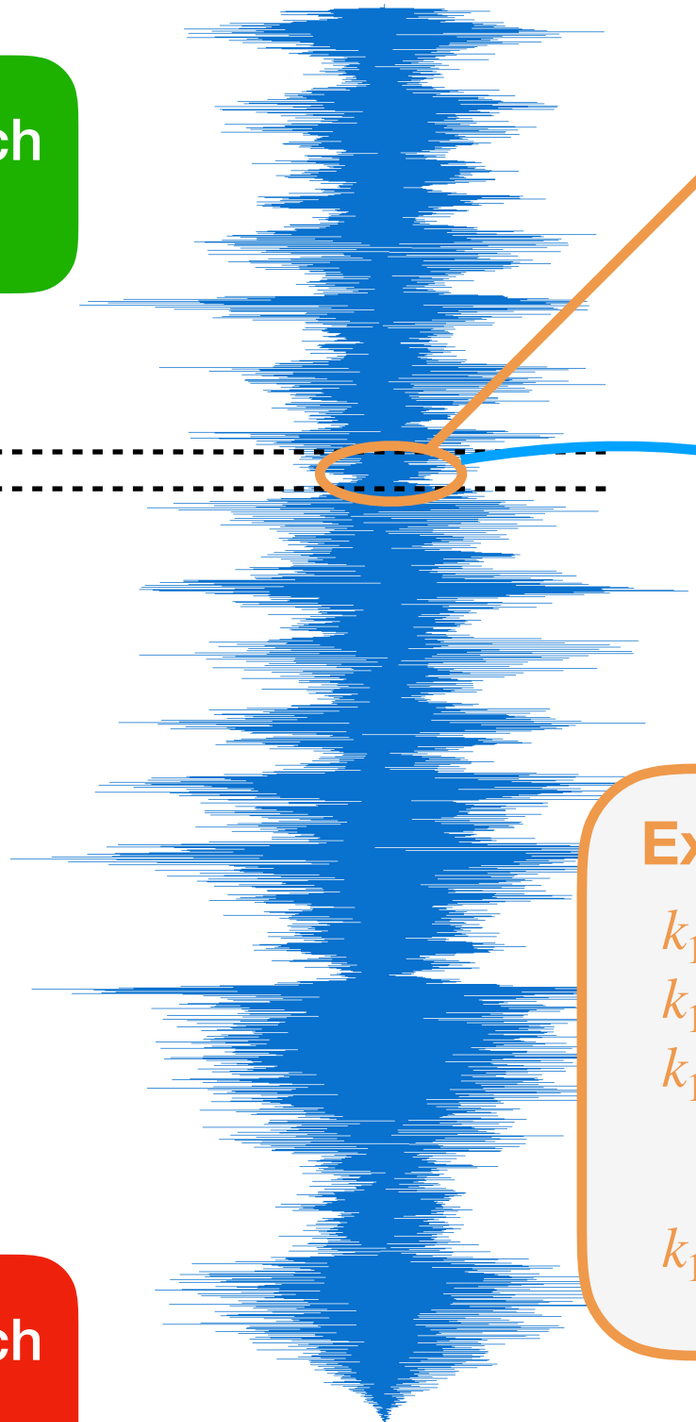
Intermediate result

```
...
EOR     R0, R0
EOR     R0, R0
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R3
MOV     R11, R0, ROR #32-8
AND     R11, R0, ROR #32-1
EOR     R11, R0, ROR #32-2
EOR     R1, R11
EOR     R1, R4
MOV     R11, R1, ROR #32-8
AND     R11, R1, ROR #32-1
EOR     R11, R1, ROR #32-2
EOR     R0, R11
EOR     R0, R5
EOR     R6, R3, R5, ROR #3
EOR     R6, R6, ROR, #1
EOR     R6, R2
...
```

Exhaustive search practical

$A_K(X)$

Exhaustive search unpracticall



Statistically dependent on IR

Which prediction matches the most?

Exhaustive search:

$k_1 = 0x00 \Rightarrow IR = 0x63$
$k_1 = 0x01 \Rightarrow IR = 0xA0$
$k_1 = 0x02 \Rightarrow IR = 0x3E$
...
$k_1 = 0xFF \Rightarrow IR = 0x11$

Differential Power analysis

Key guess
$k_1 = 0$

$f(X_1, 0)$

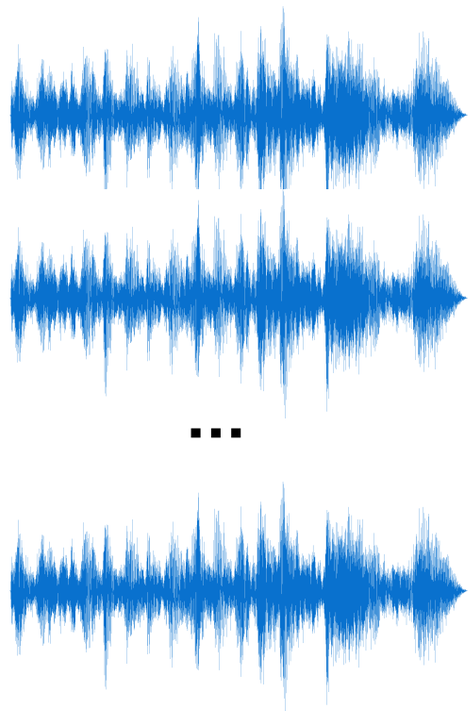
$f(X_2, 0)$

...

$f(X_n, 0)$

predictions

$$\frac{\sum_i (x_i - \bar{x}) \cdot (y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2} \cdot \sqrt{\sum_i (y_i - \bar{y})^2}}$$

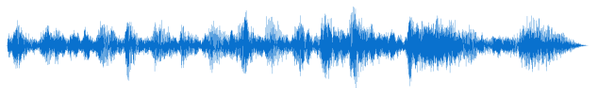


power traces

Statistics

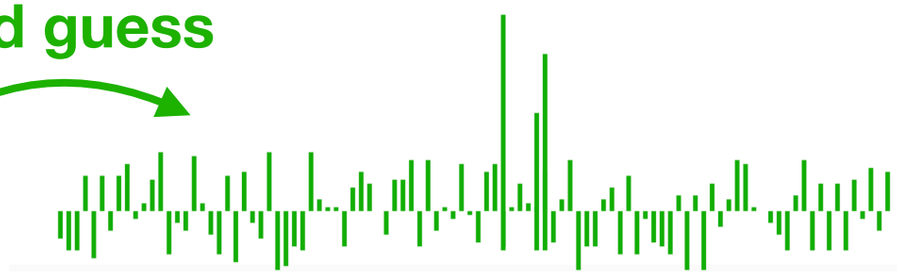
Bad guess

No correlation peaks



correlation trace

Good guess



Correlation peaks

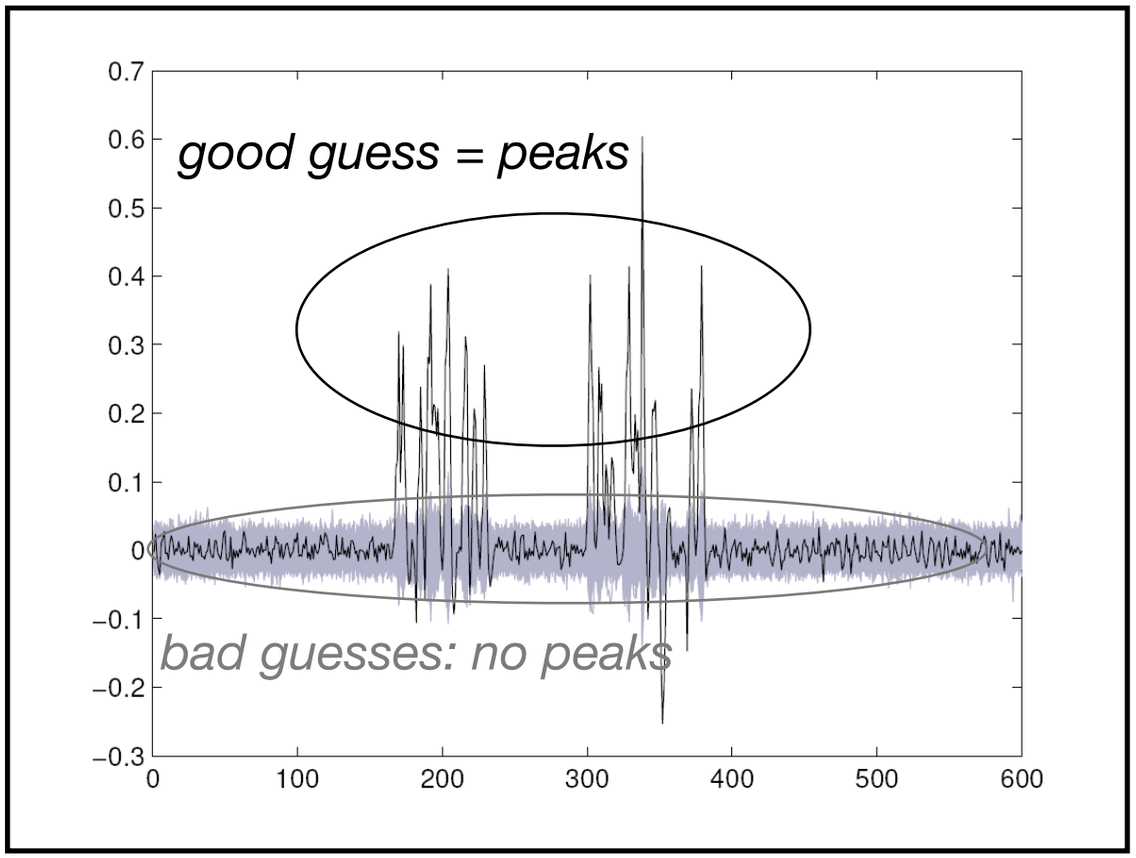
Yes, it works!

Power analysis station

Source: **ninjalab.io**

Price ~ $10K

Practical attack results



AES implementation on a secure chip

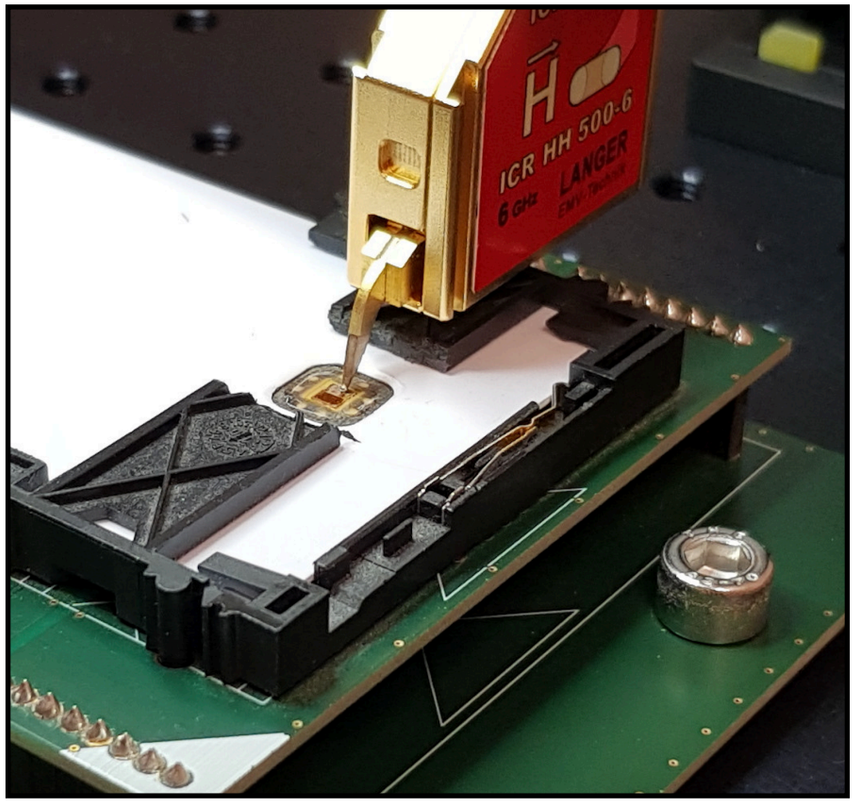
Electromagnetic analysis

- Similar to PA: power traces ⟶ EM traces
- More powerful in two (opposite) ways

Relax physical access requirement

Improved signal

Source: **m.tau.ac.il/~tromer/radioexp/**



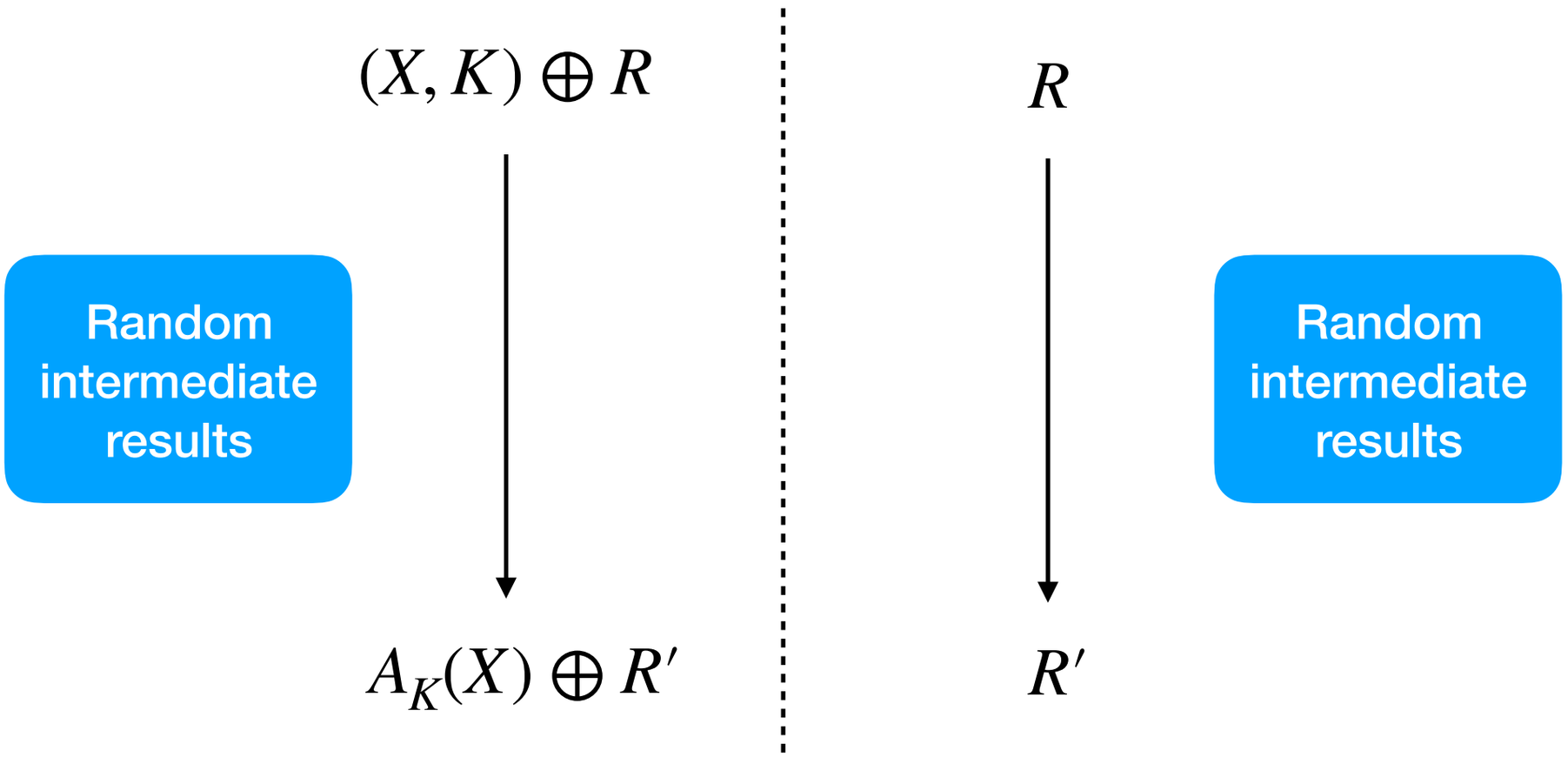
Source: **ninjalab.io**

Countermeasures

- Use of randomisation
  - Make the leakage **noisy**
  - Make intermediate results **unpredictable**

Countermeasures

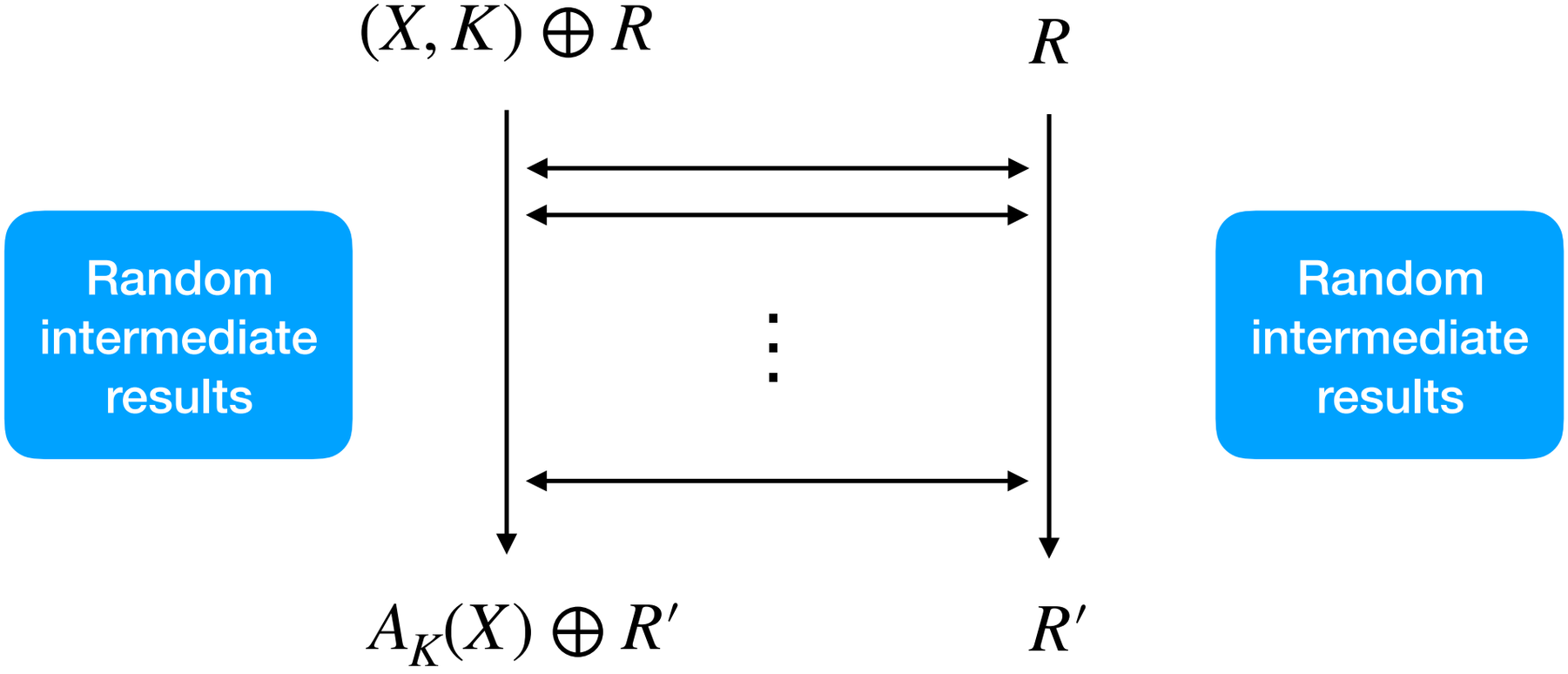
- Use of randomisation
  - Make the leakage **noisy**
  - Make intermediate results **unpredictable**



Masking

Countermeasures

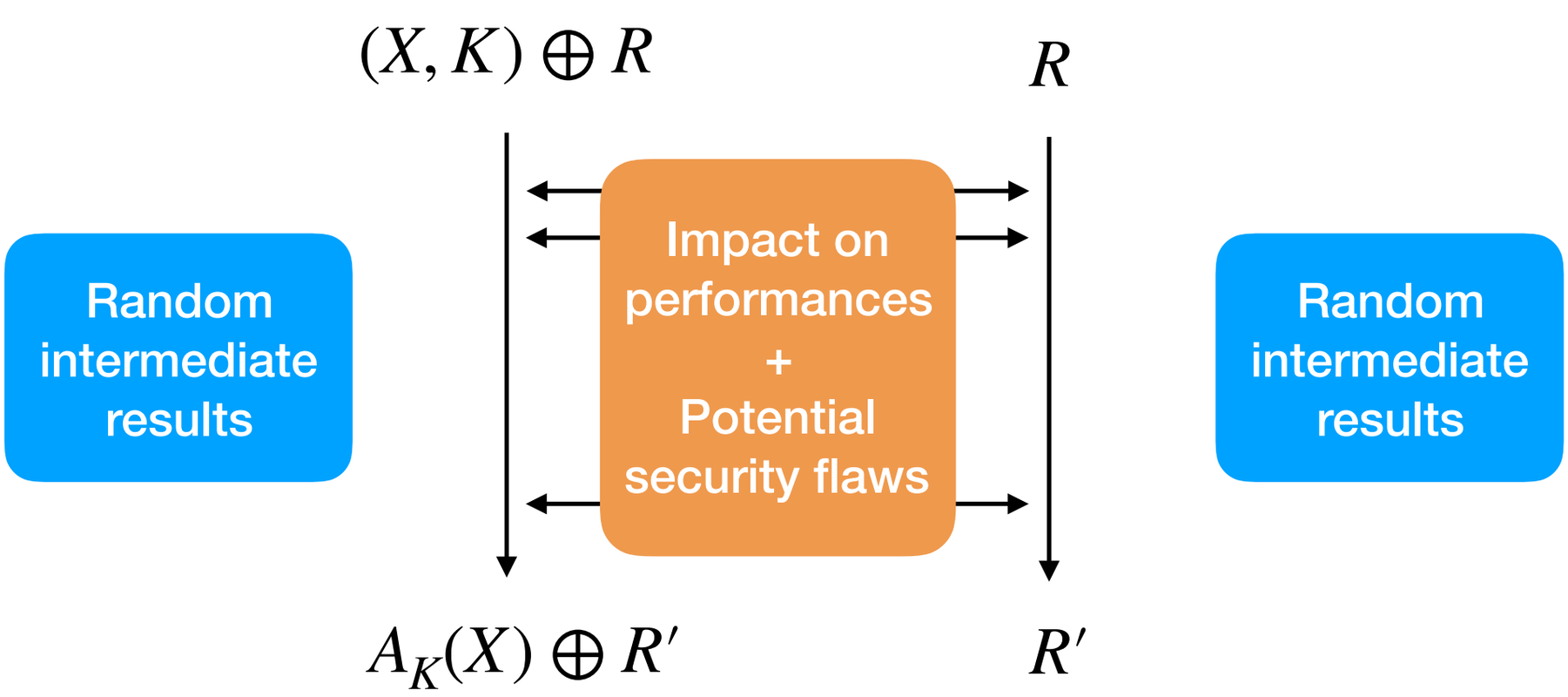
- Use of randomisation
  - Make the leakage **noisy**
  - Make intermediate results **unpredictable**



Masking

Countermeasures

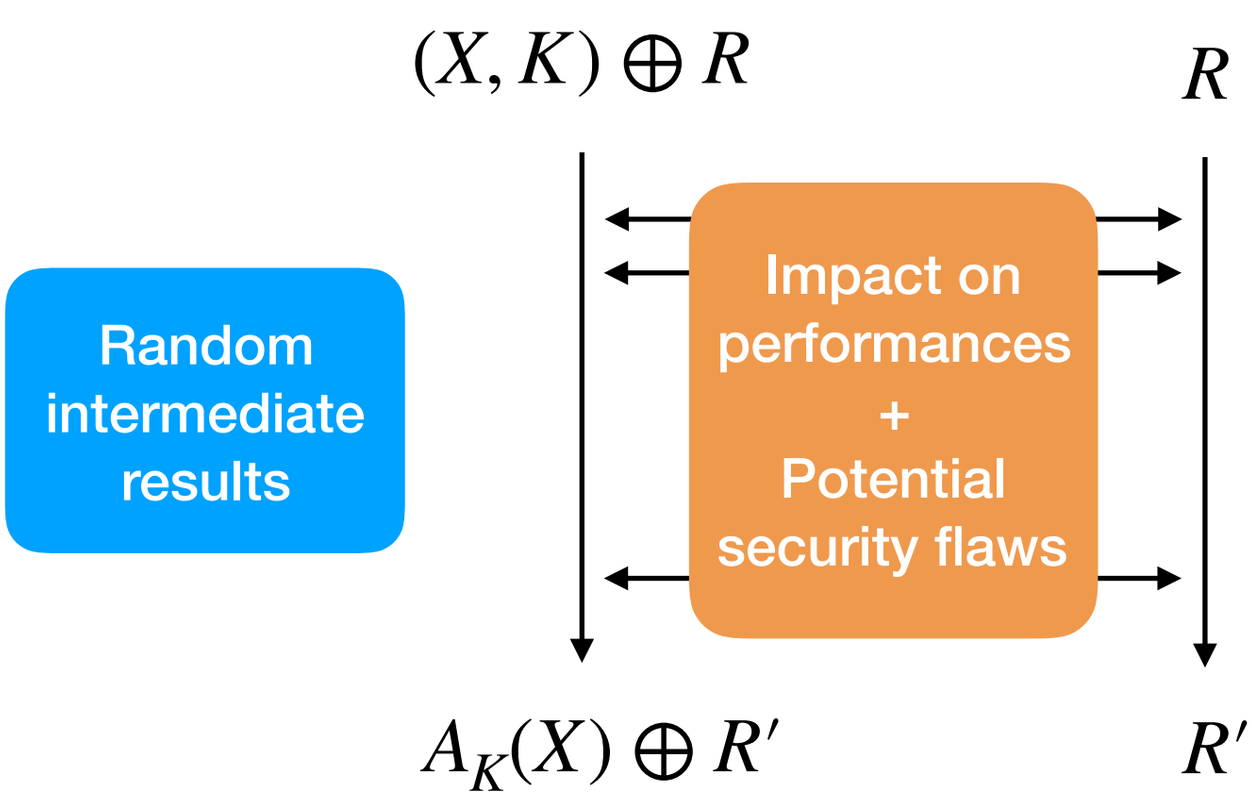
- Use of randomisation
  - Make the leakage **noisy**
  - Make intermediate results **unpredictable**

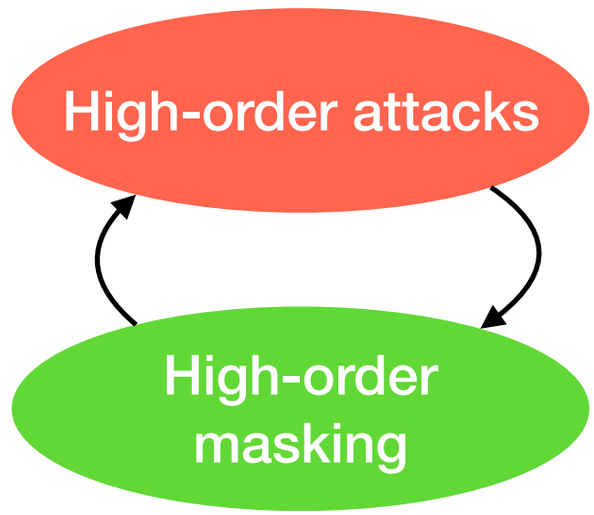


Masking

Countermeasures

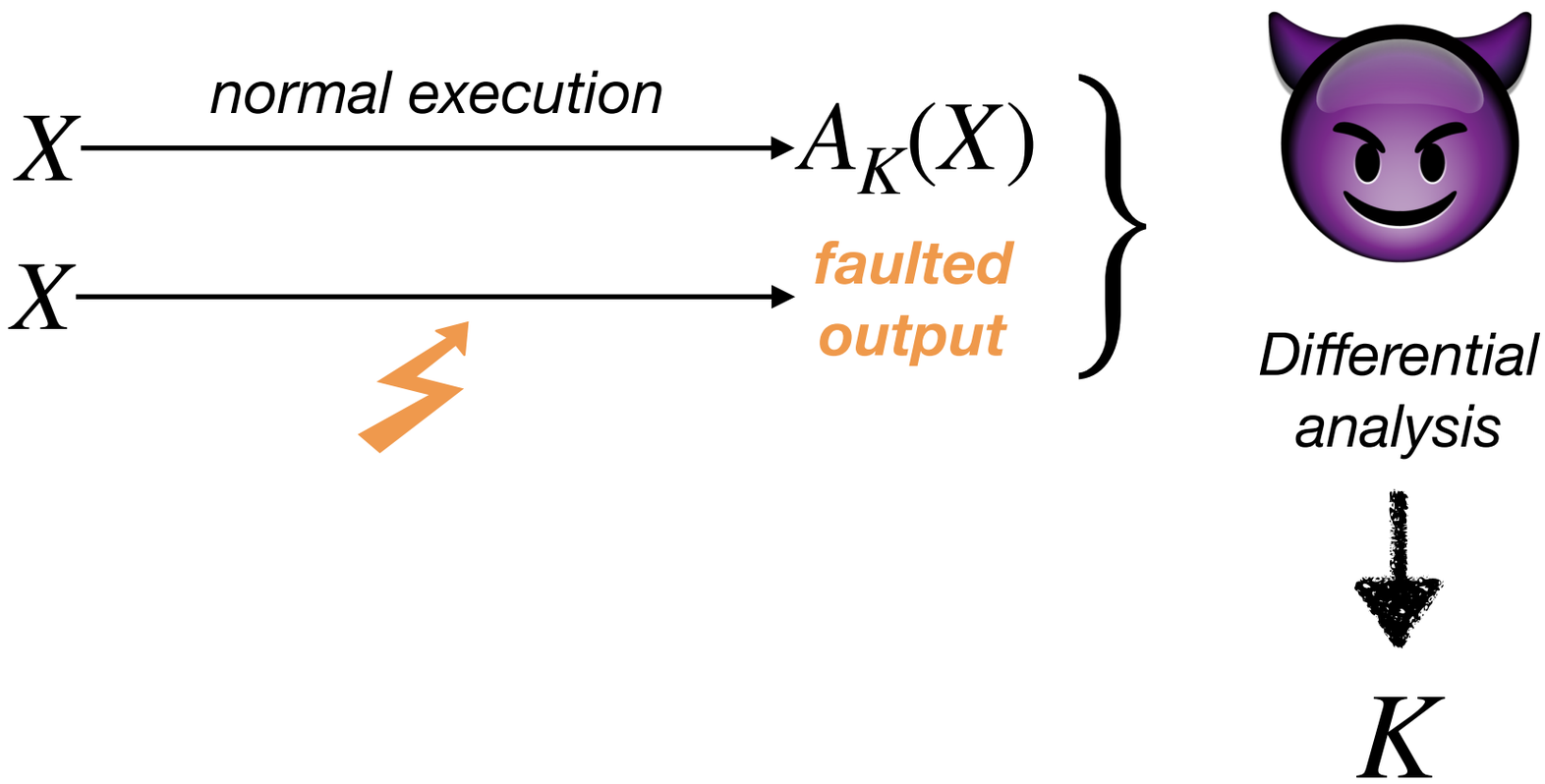
- Use of randomisation
  - Make the leakage **noisy**
  - Make intermediate results **unpredictable**





Masking

Fault attacks

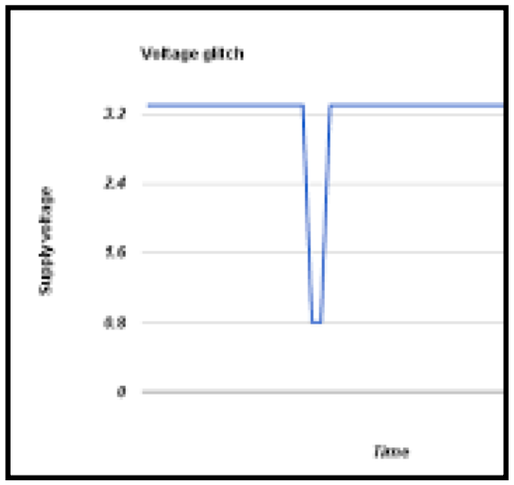


- Very powerful
- A few pairs of correct/faulted outputs reveal the key

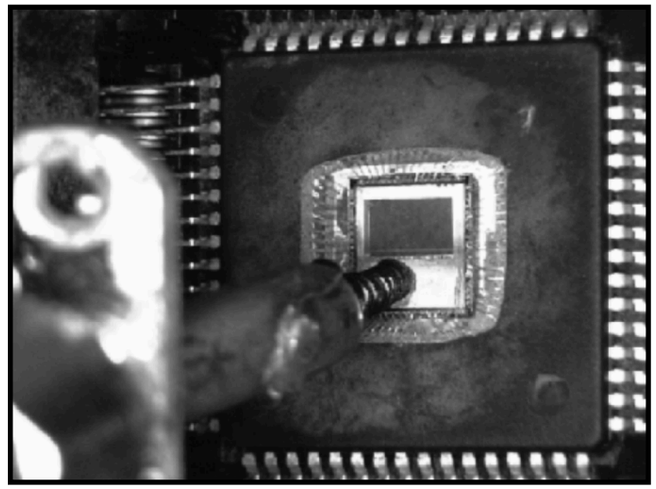
Fault attacks

- Several fault injection means

Power glitch / clock glitch

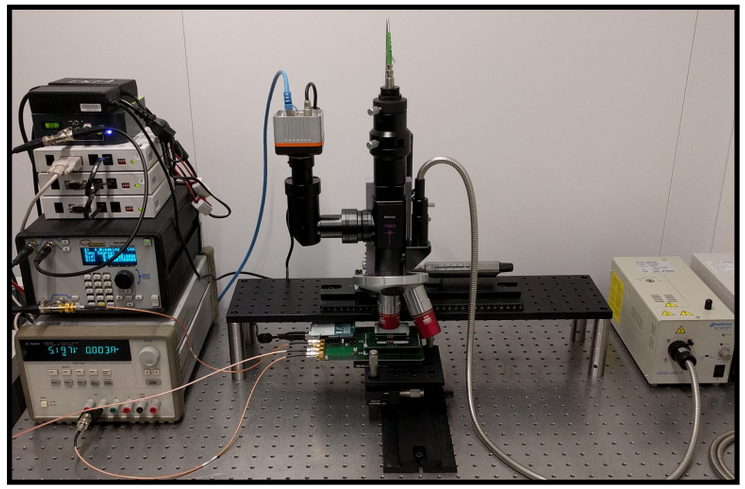


EM injection



Source: **ia.cr/2012/123**

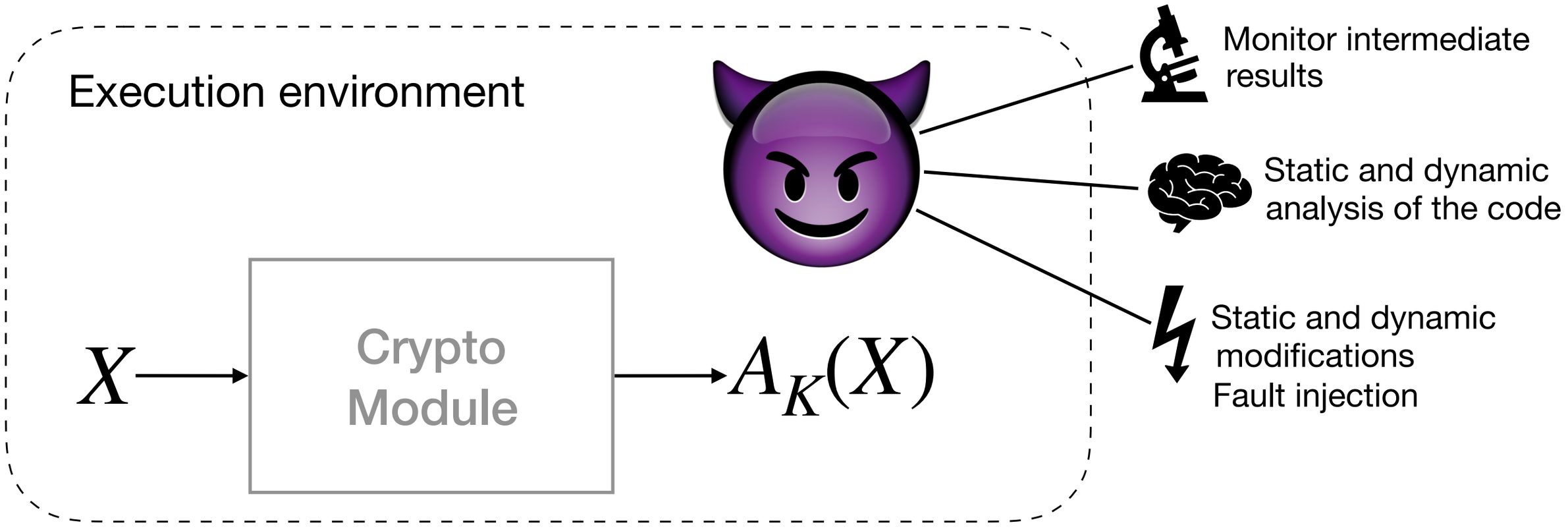
Laser injection



Source: **ninjalab.io**

- (Semi) invasive attacks
- Countermeasure: check correctness
- Multiple fault injections

White-box model



- Omniscient adversary
- Full control of the execution environment
- Full access to the code and data
- e.g. malware

White-box model

- Standard implementations completely broken

Illustration: Shamir, van Someren. *Playing hide and seek with stored keys.*

White-box model

- Standard implementations completely broken

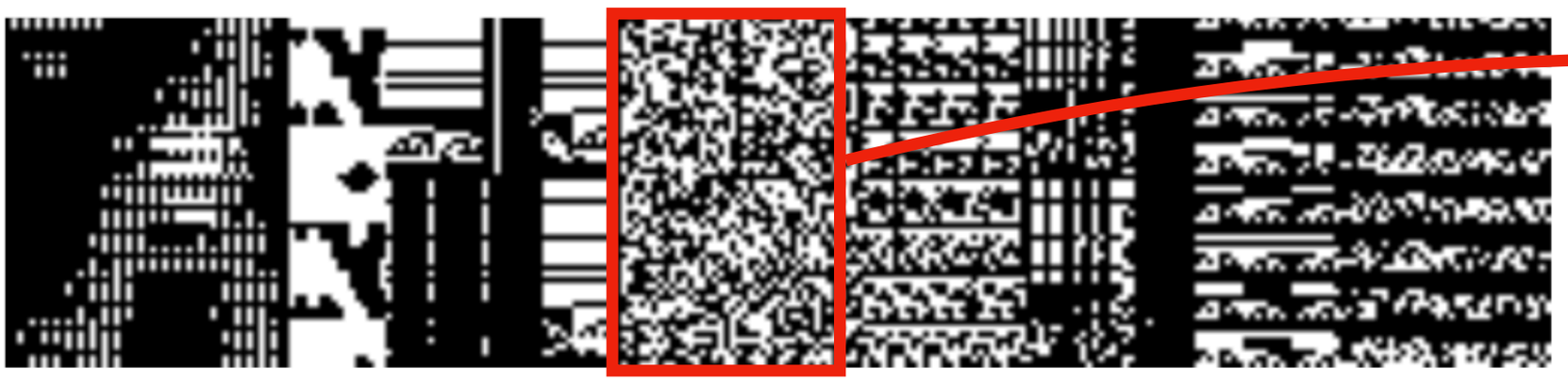


Illustration: Shamir, van Someren. *Playing hide and seek with stored keys.*

White-box model

- Standard implementations completely broken

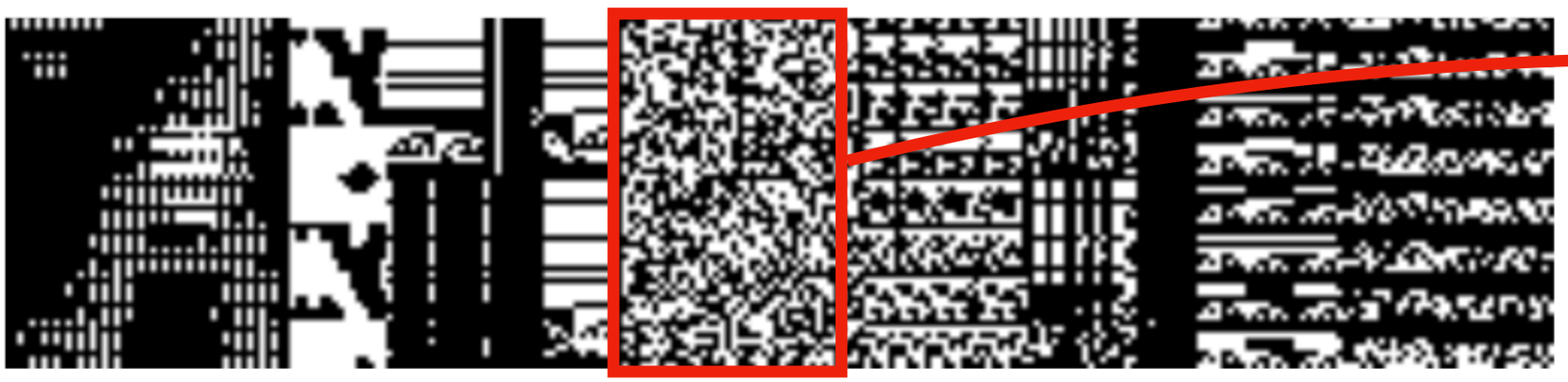
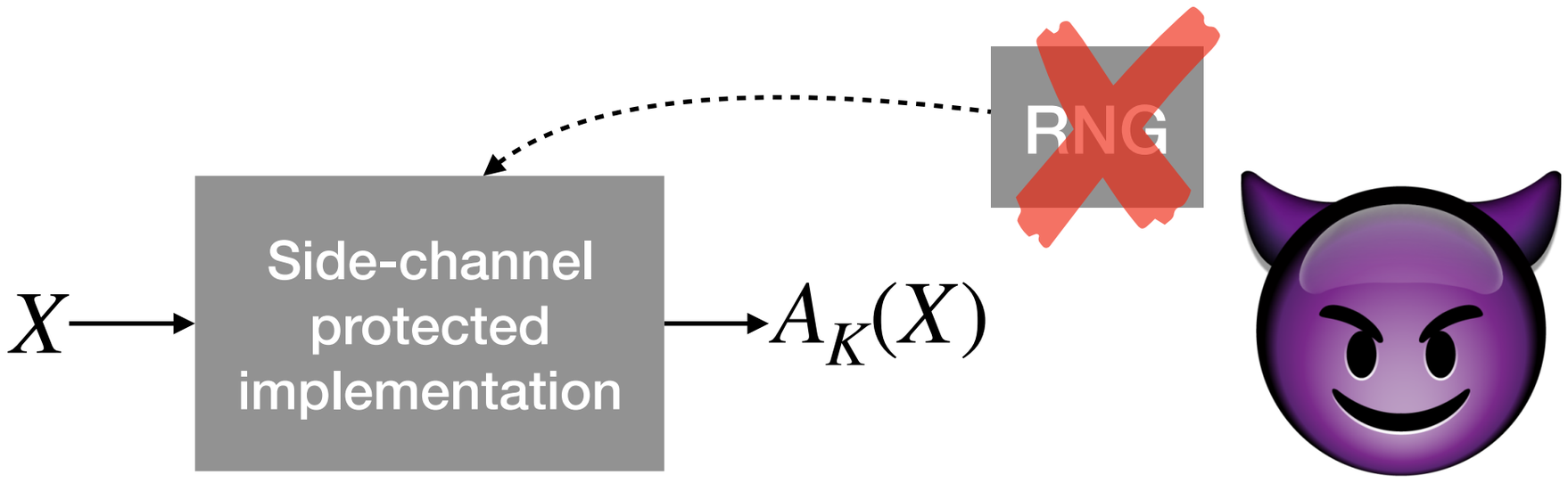


Illustration: Shamir, van Someren. *Playing hide and seek with stored keys.*

- Side-channel countermeasures insufficient



White-box cryptography

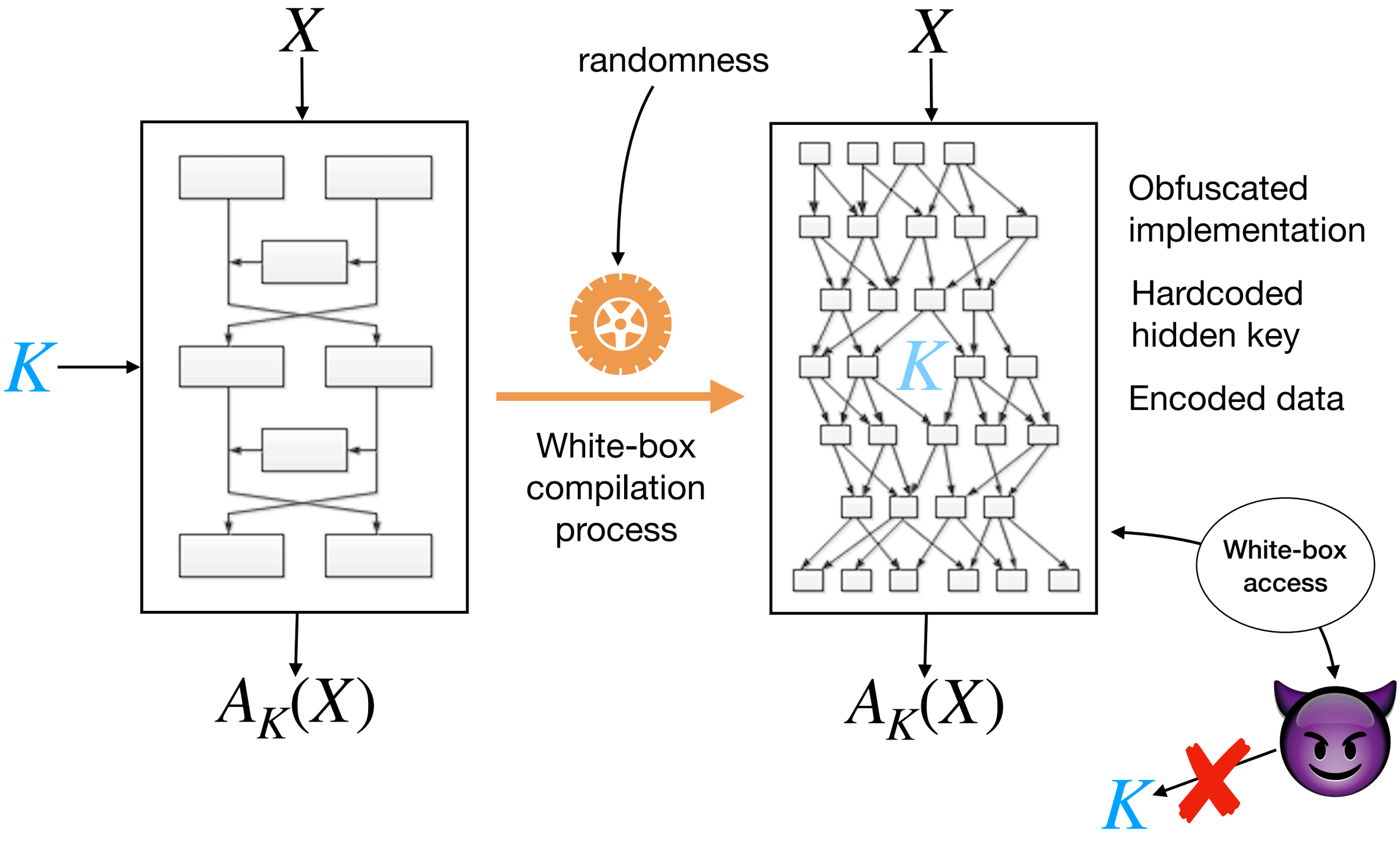
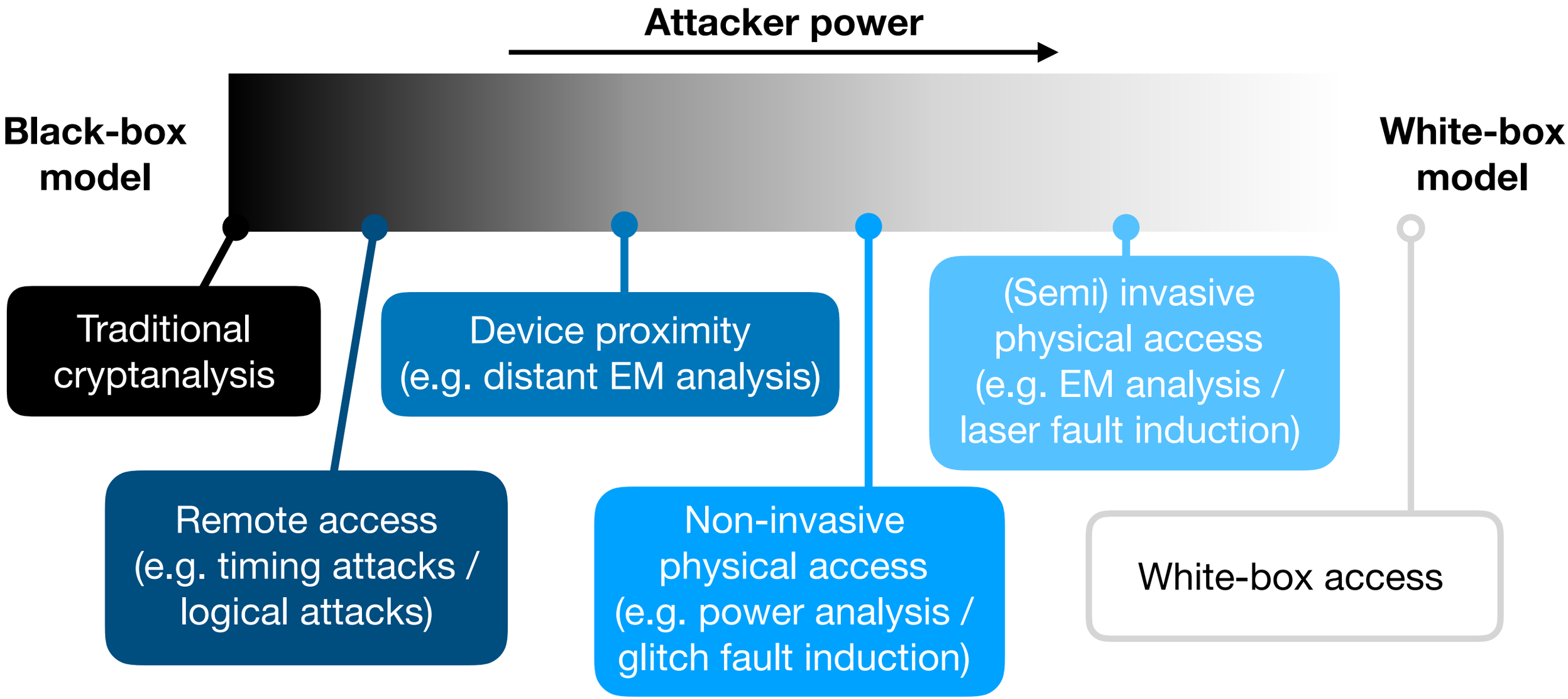
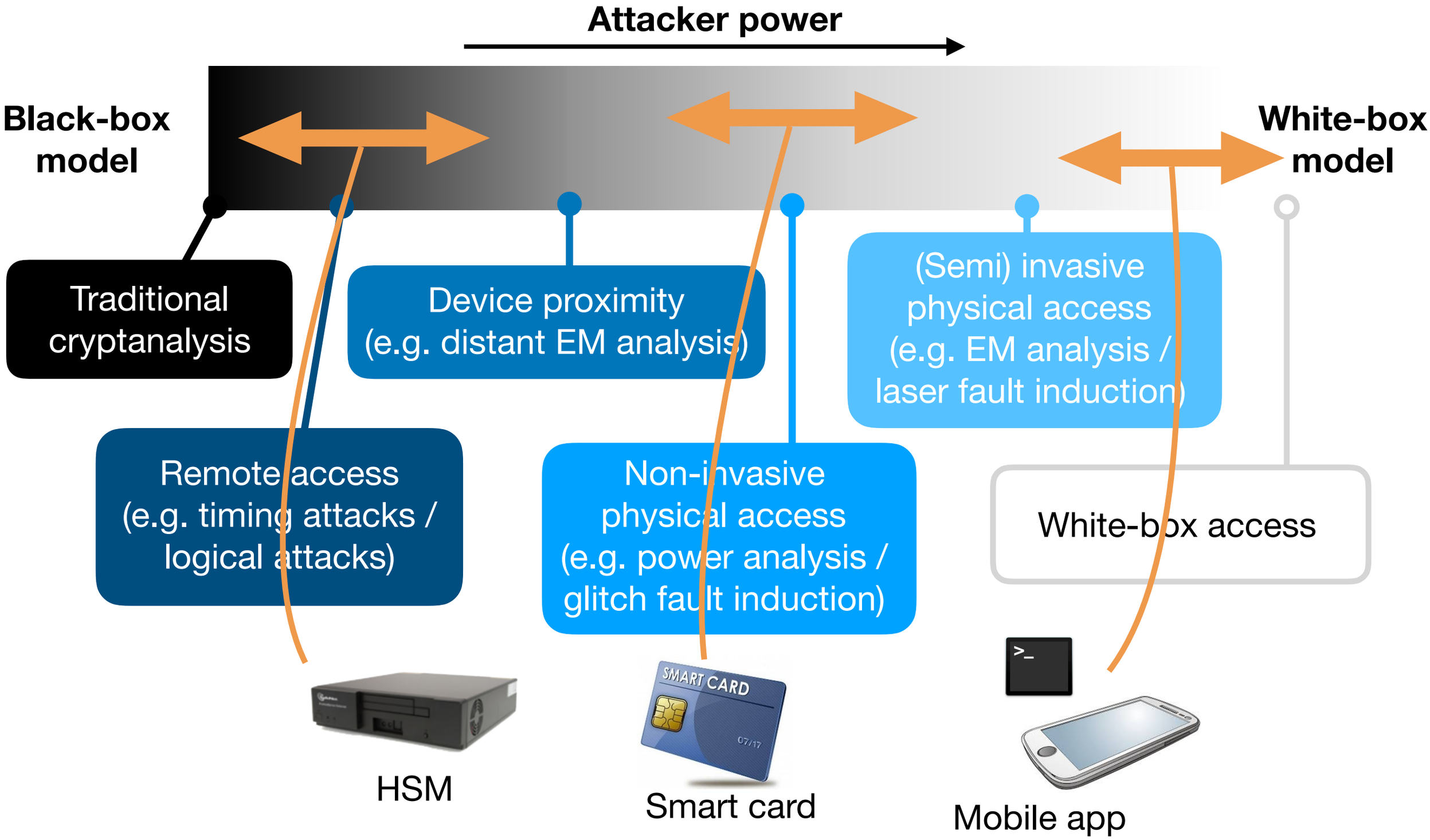


Illustration: **www.whiteboxcrypto.com**

Model grayscale



Model grayscale



Don’t choose the wrong gray!

2008: EM analysis of KeeLoq remote **car door system** (remote control cloning)

Source: `www.iacr.org/archive/crypto2008/51570204/51570204.pdf`

2016: EM key extraction on iOS devices (OpenSSL and CoreBitcoin signing keys)

Source: `https://m.tau.ac.il/~tromer/mobilesc/`

Recently: Power analysis of **cryptocurrency hardware wallet** (PIN and signing key recovery)

Source: `ia.cr/2019/401`

OpenSSL
Cryptography and SSL/TLS Toolkit

2018: four different timing attack vulnerabilities reported on **OpenSSL** RSA / DSA / ECDSA signatures

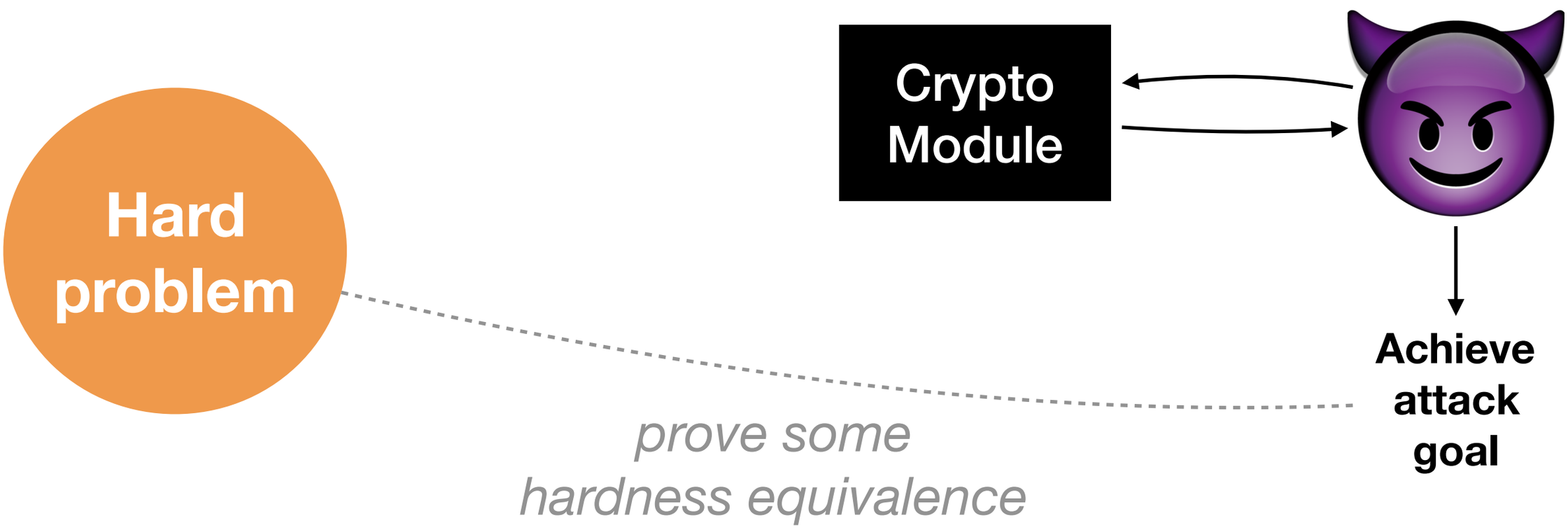
Source: `https://www.openssl.org/news/vulnerabilities.html`

Security assessment

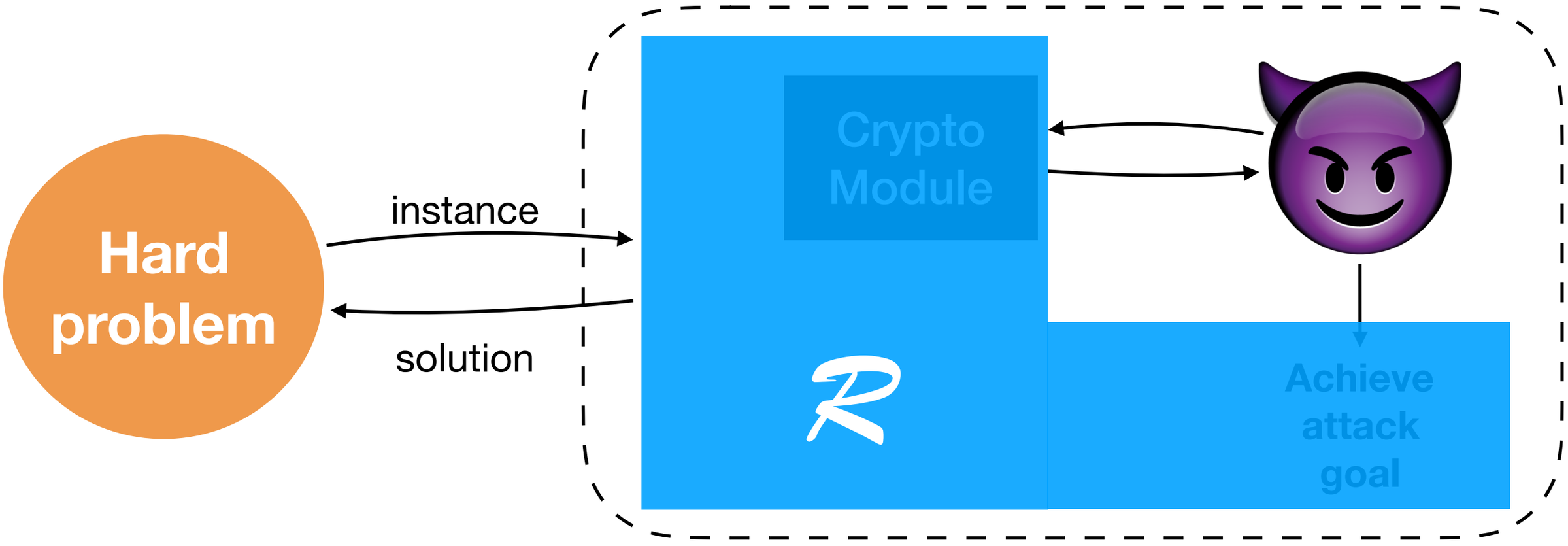
Security assessment

- An attack = a **target**, a **goal**, some **means**
- Example:
  - Target: smart-card computing RSA signatures
  - Goal: extract the RSA private key
  - Means:
    - (non-invasive) physical access for 30mn,
    - $100K of computing power from cloud provider
- **Security assessment:** the attack goal cannot be achieved given the attack means
  - can be more or less formal
  - possibly based on some well-defined assumptions

Provable security



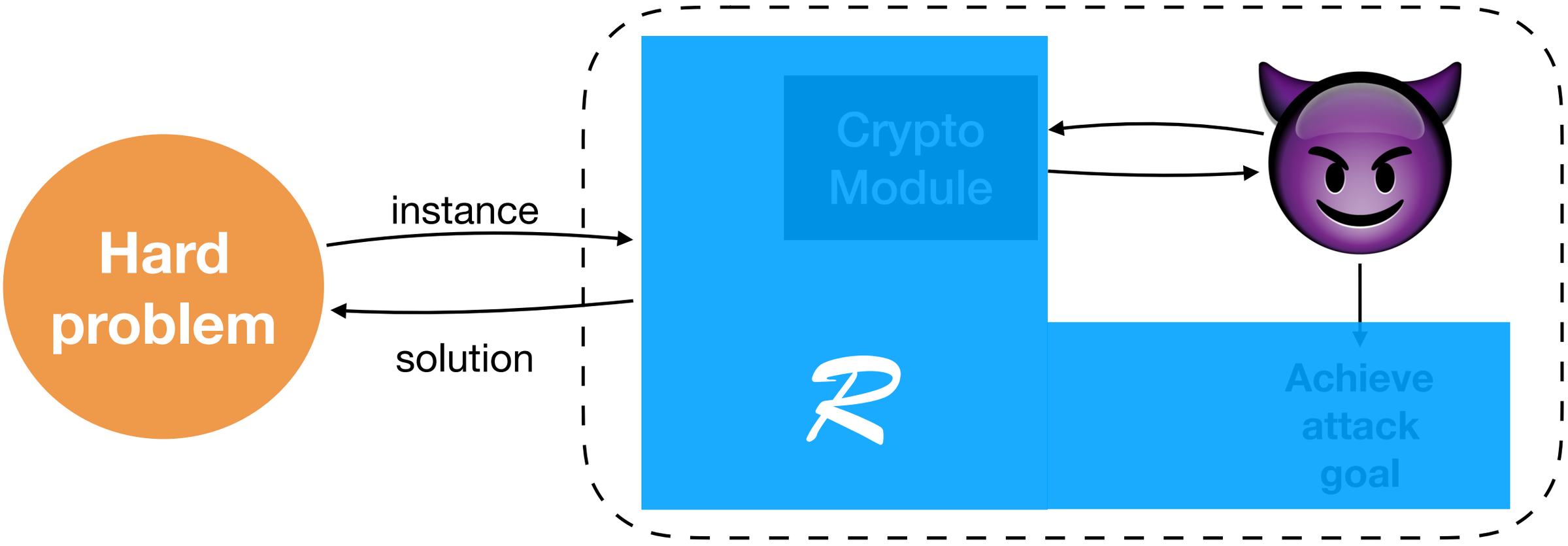
Provable security



- **Security reduction** = define algorithm $\mathcal{R}$ s.t.

  😈 + $\mathcal{R}$ solves **hard problem**

Provable security



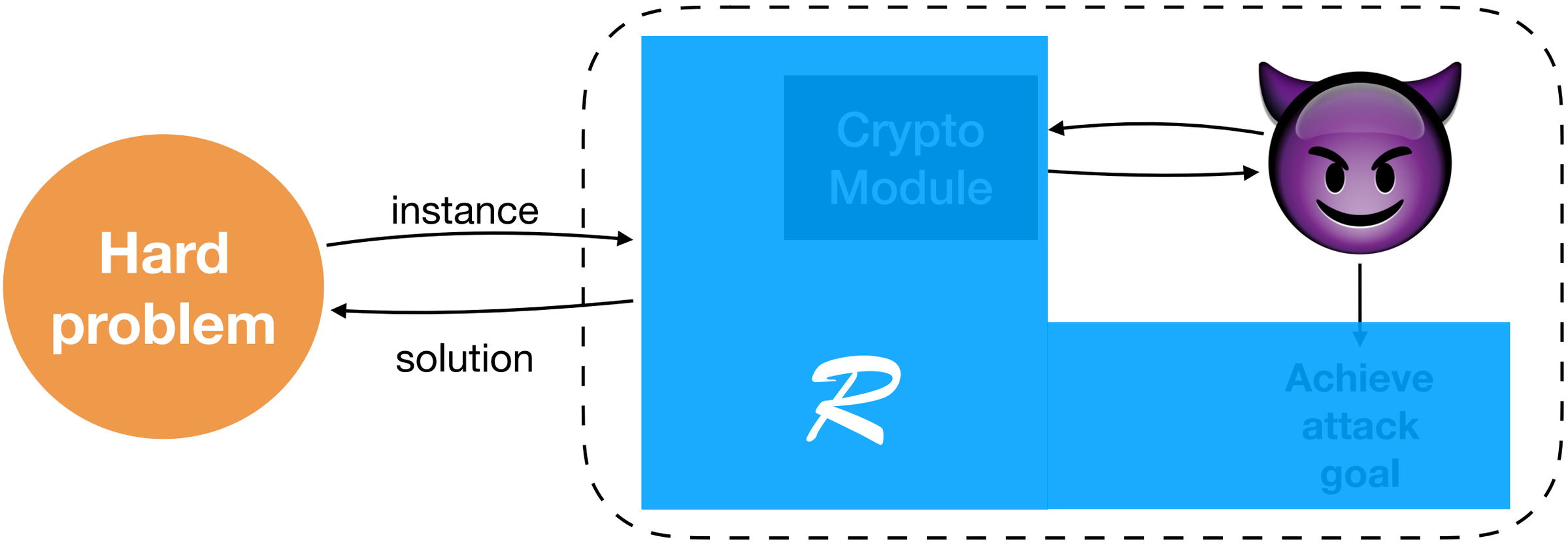
- **Security reduction** = define algorithm $\mathcal{R}$ s.t.

  😈 + $\mathcal{R}$ solves **hard problem**

- If solving **hard problem** costs at least **X** then

  😈 + $\mathcal{R}$ costs at least **X**

Provable security



- **Security reduction** = define algorithm $\mathcal{R}$ s.t.

  😈 + $\mathcal{R}$ solves **hard problem**

- If solving **hard problem** costs at least **X** then

  😈 + ~~$\mathcal{R}$~~ costs at least **X** $-\varepsilon$

Provable security

- Examples:

Recovering RSA secret key (from public key)

factoring large integer ***N*** = ***p*** x ***q***

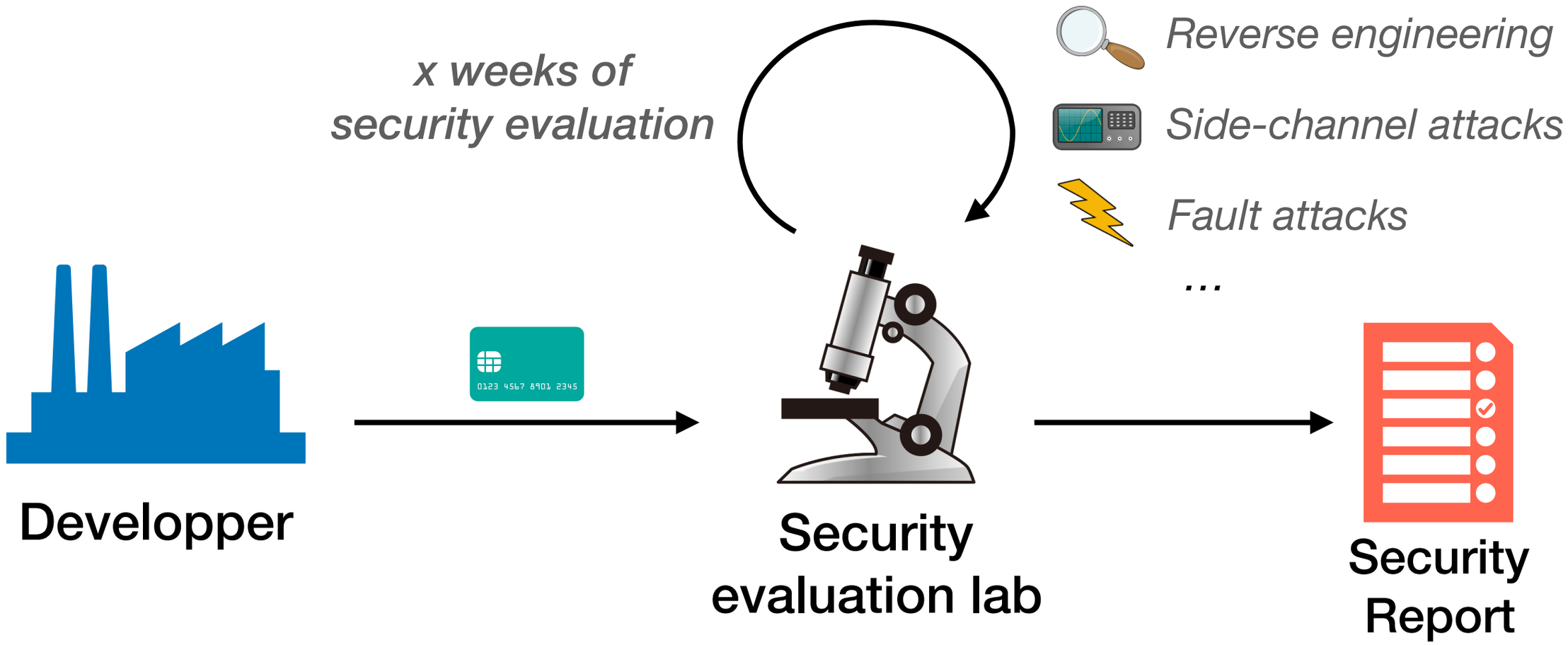
Forging RSA signature

solving RSA problem *(for some signature schemes)*

- Not always available (e.g. ECDSA)
- Desired property for new standards

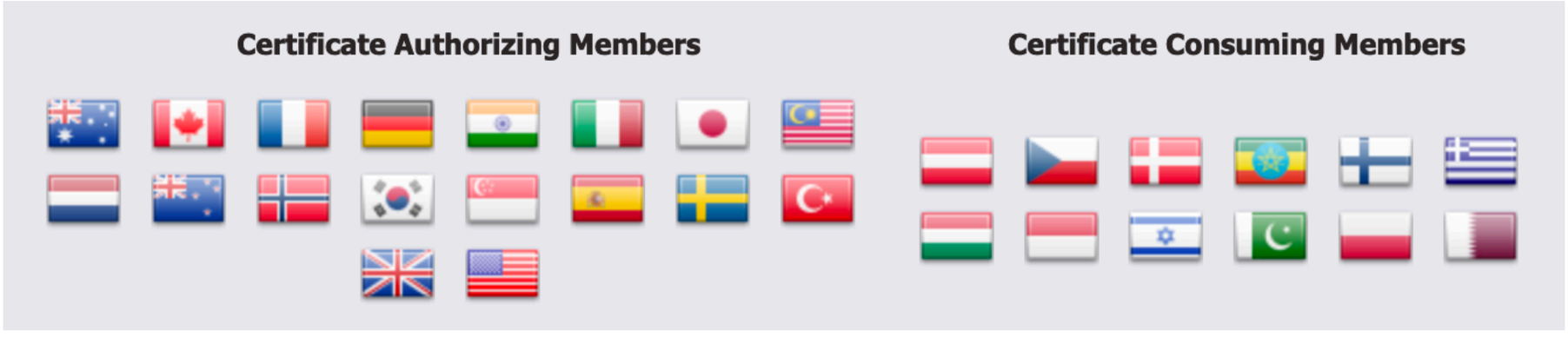
Security evaluation

- Lack of provable security outside the black-box model
- Evaluation paradigm

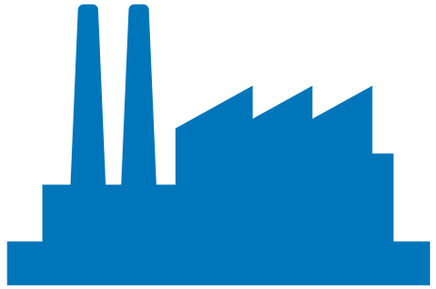


Common criteria

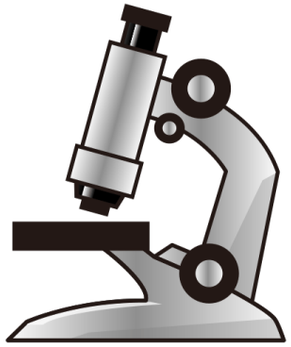
- *Common Criteria for IT Security Evaluation*
  - International standard (ISO/IEC 15408)
- Common evaluation methodology for all kind of IT products
- Evaluations overseen by certification bodies
- Mutual recognition arrangement



Common criteria



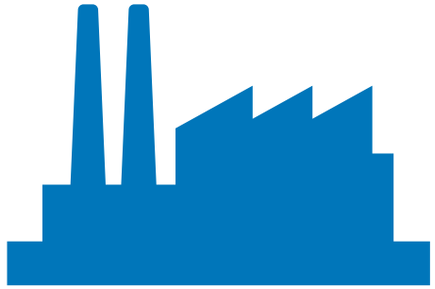
Developper



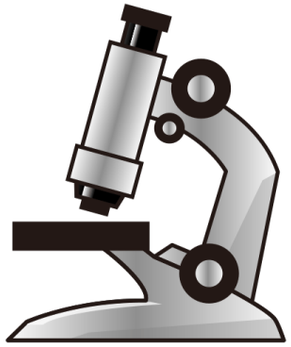
ITSEF Lab

Certification body

Common criteria



Developper



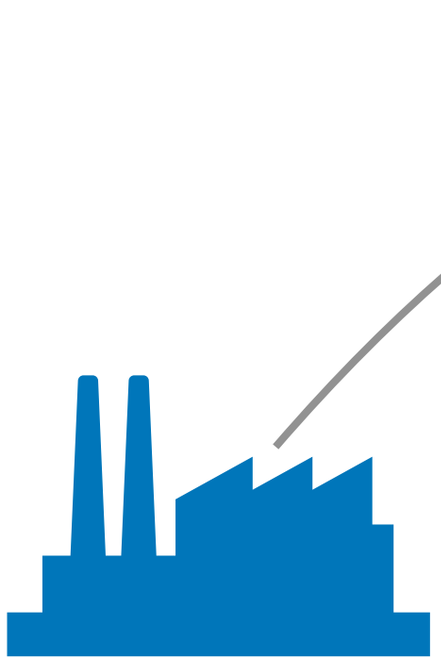
ITSEF Lab

Accreditation

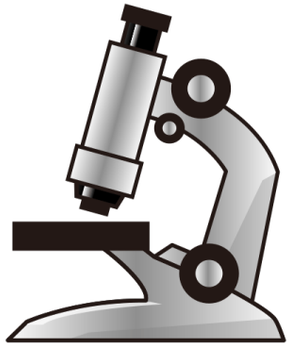
Certification body

Common criteria

(1) Certification feasibility?



Developper



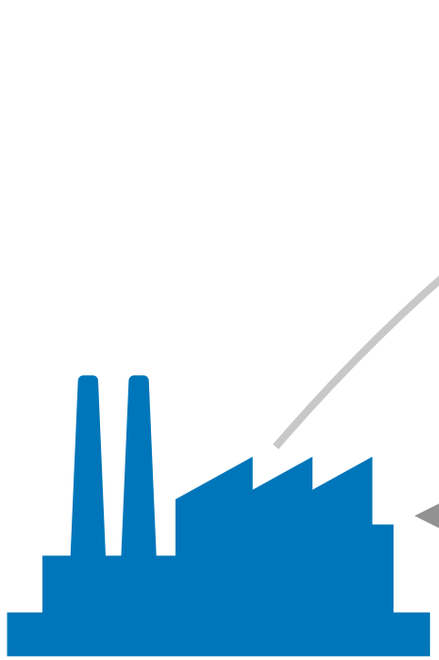
ITSEF Lab

Accreditation

Certification body

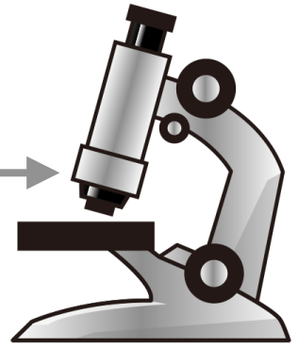
Common criteria

(1) Certification feasibility?



Developper

(2) Contract

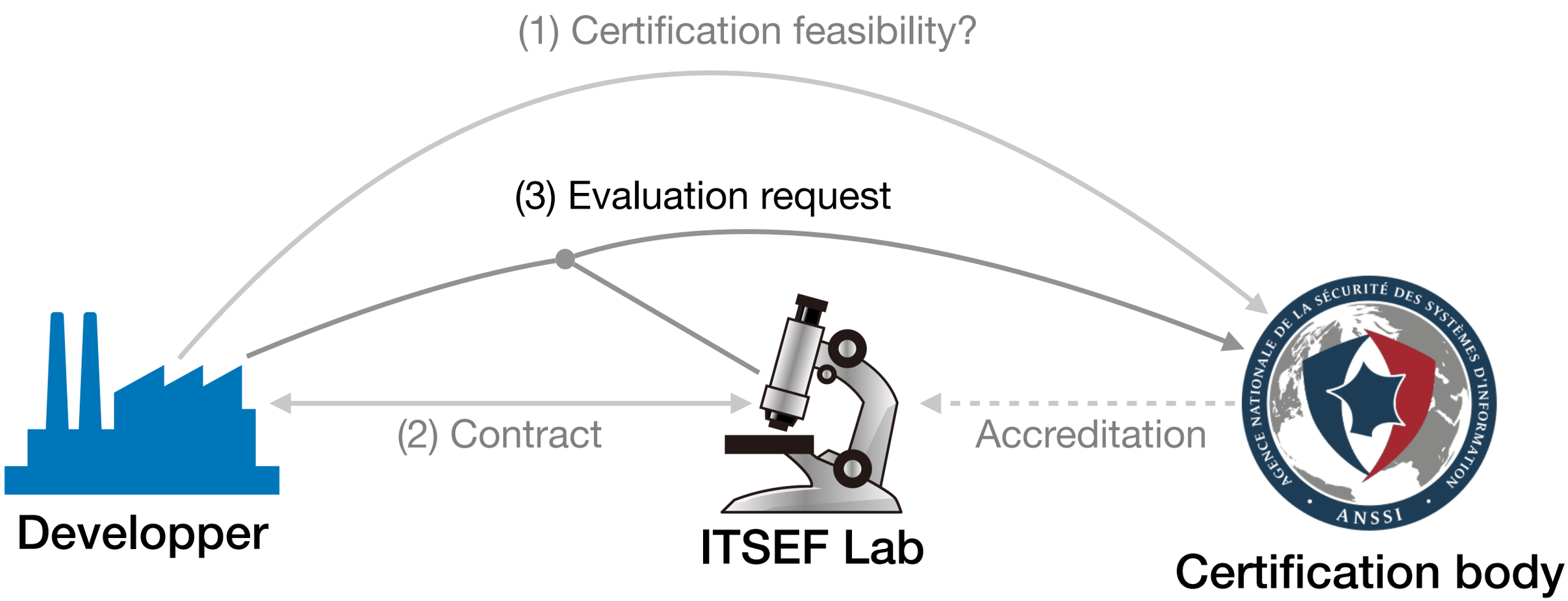


ITSEF Lab

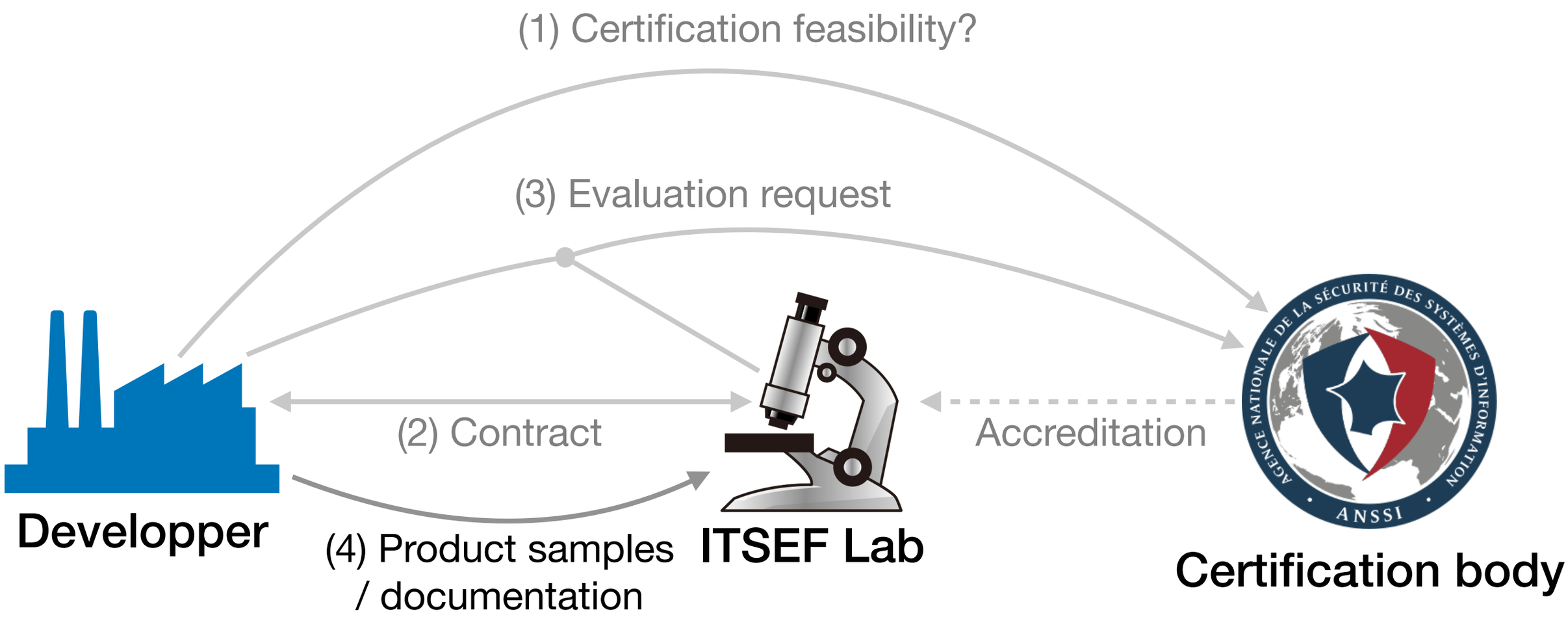
Accreditation

Certification body

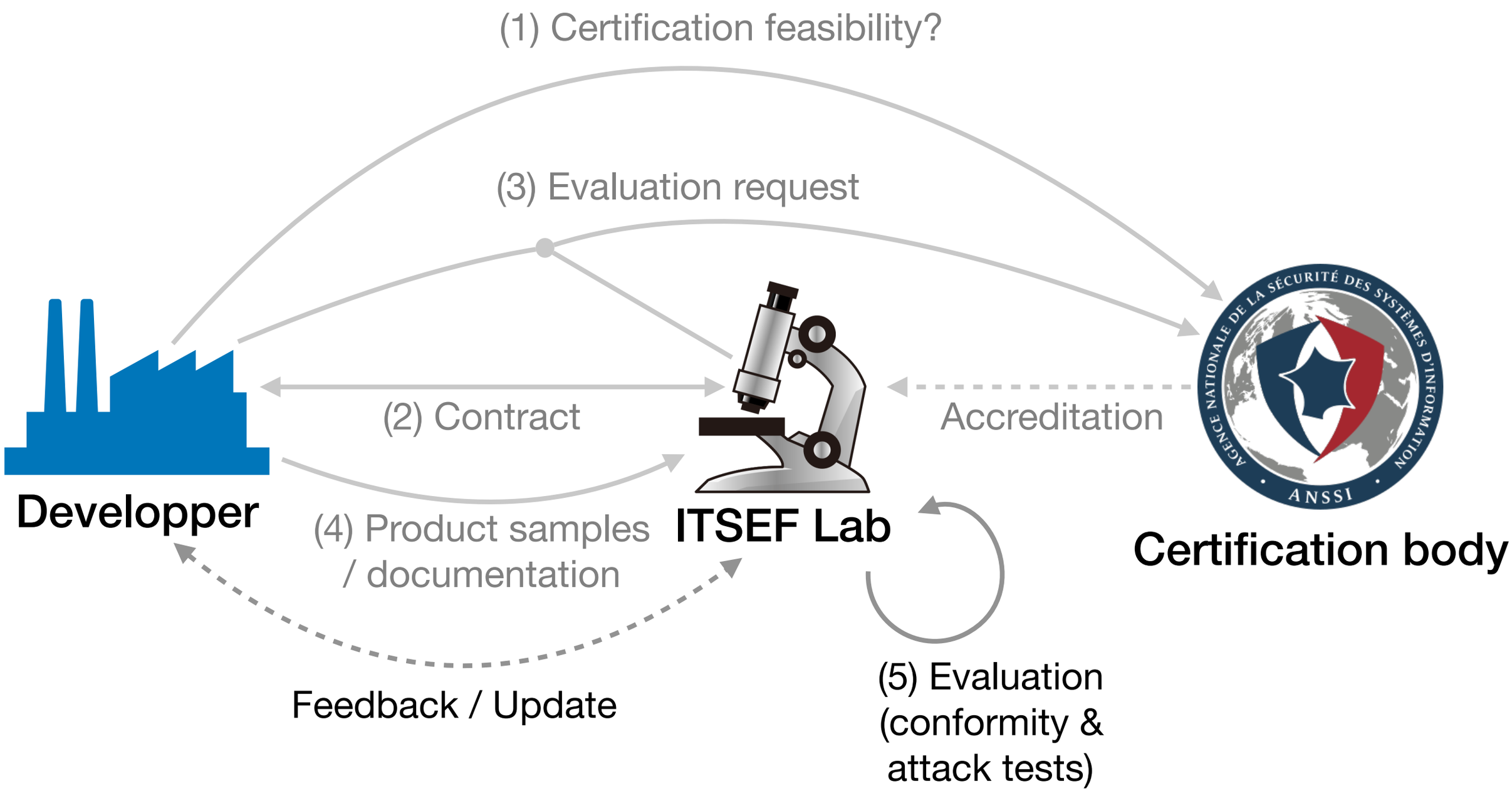
Common criteria



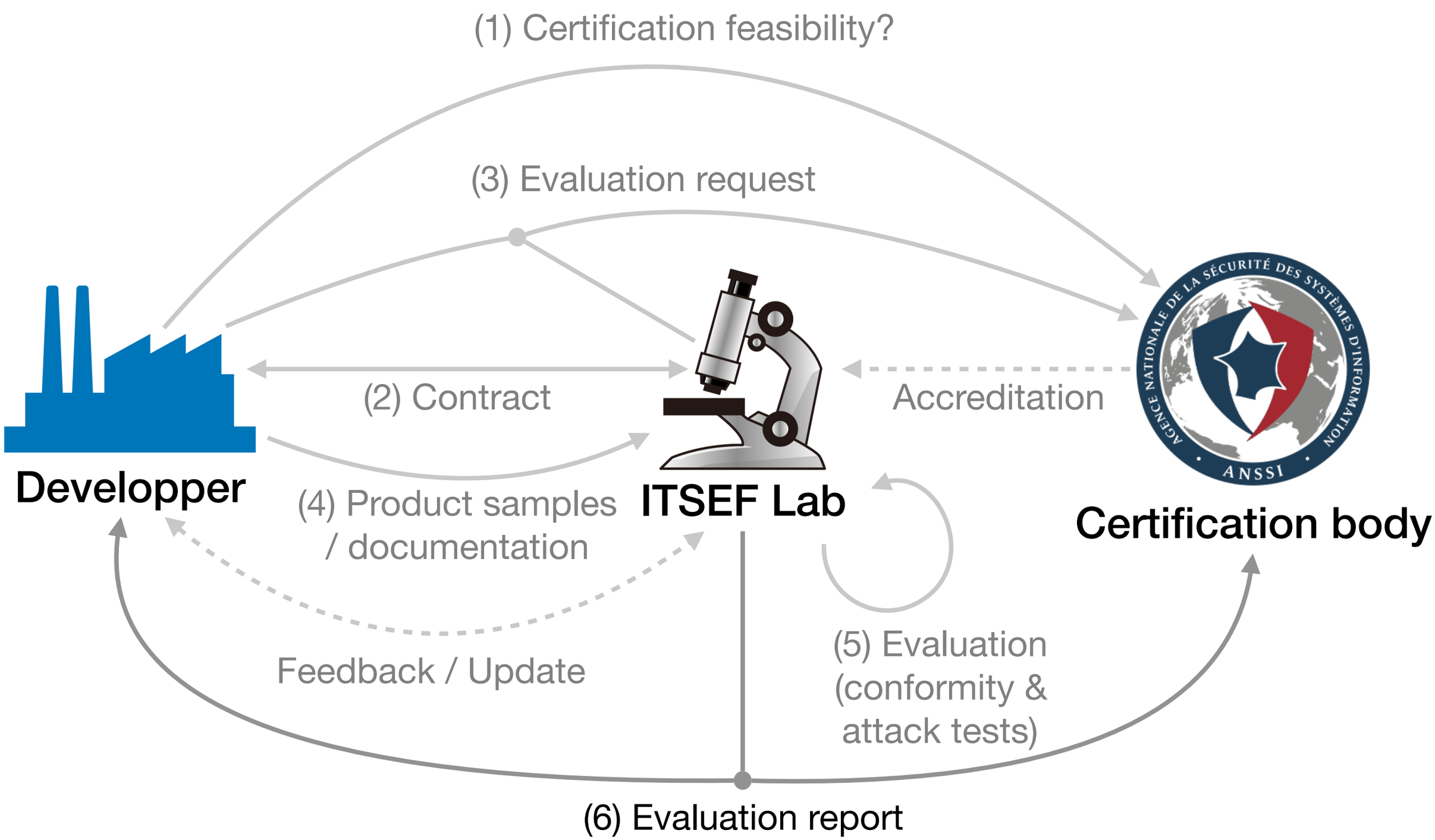
Common criteria



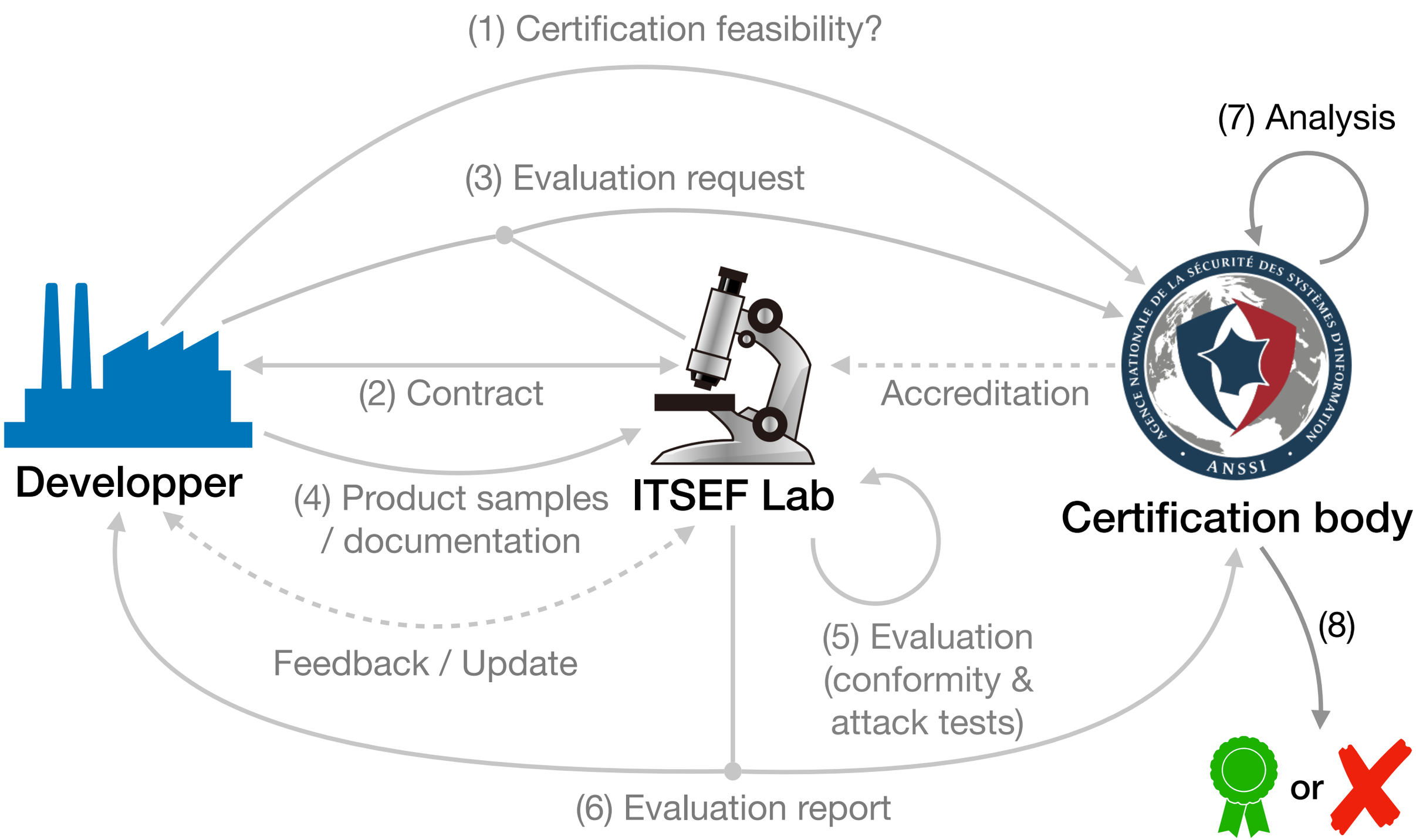
Common criteria



Common criteria



Common criteria



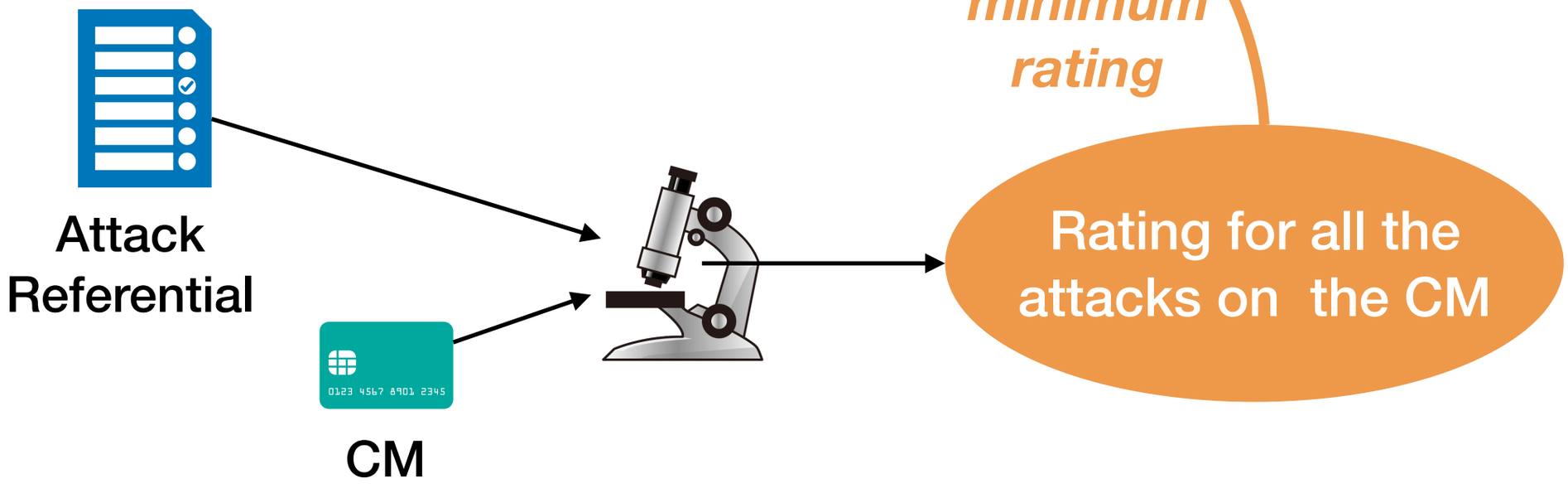
Vulnerability Analysis (VAN) level

VAN level	Range of values	TOE resistant to attackers with attack potential of:
N/A	0 - 15	No rating
1 / 2	16 - 20	Basic
3	21 - 24	Enhanced Basic
4	25 - 30	Moderate
5	≥ 31	High

Vulnerability Analysis (VAN) level

VAN level	Range of values	TOE resistant to attackers with attack potential of:
N/A	0 - 15	No rating
1 / 2	16 - 20	Basic
3	21 - 24	Enhanced Basic
4	25 - 30	Moderate
5	≥ 31	High

minimum rating



Attack rating

- Referential for smart cards
  - SOG-IS / JHAS (Hardware Attack Subgroup)
- **Two steps** x **Seven factors**
  - Rating = sum of scores

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Referential for smart cards
  - SOG-IS / JHAS (Hardware Attack Subgroup)
- **Two steps** x **Seven factors**
  - Rating = sum of scores

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
	2	4
	3	6
	*	*
	0	0
	1	2
	3	4
	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Identification: effort to identify and setup the attack the first time

Exploitation: effort to reproduce the attack after identification

Attack rating

- Referential for smart cards
  - SOG-IS / JHAS (Hardware Attack Subgroup)
- **Two steps** x **Seven factors**
  - Rating = sum of scores

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Data collection, leakage detection, DPA < 1 day

Data collection, reproduce DPA < 1 hour

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Expert for attack setup

Proficient for attack reproduction

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

No required knowledge of the ToE

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

One sample is enough

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Power analysis station (specialized)

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

No open sample required

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Identification total: 1 + 5 + 0 + 0 + 3 + 0 = 9

Exploitation total: 0 + 2 + 0 + 0 + 4 = 6

} **Attack rating: 9 + 6 = 15**

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Factors	Identification	Exploitation
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Identification total: 1 + 5 + 0 + 0 + 3 + 0 = 9

Exploitation total: 0 + 2 + 0 + 0 + 4 = 6

} **Attack rating: 9 + 6 = 15**

VAN level	Range of values	TOE resistant to attackers with attack potential of:
N/A	0 - 15	No rating
1 / 2	16 - 20	Basic
3	21 - 24	Enhanced Basic
4	25 - 30	Moderate
5	≥ 31	High

Attack rating

- Example: differential power analysis on AES implementation w/o countermeasures

Identification total: 1 + 5 + 0 + 0 + 3 + 0 = 9

Exploitation total: 0 + 2 + 0 + 0 + 4 = 6

Attack rating: 9 + 6 = 15

VAN level	Range of values	TOE resistant to attackers with attack potential of:
N/A	0 - 15	No rating
1 / 2		sic
3		anced Basic
4	25 - 30	Moderate
5	≥ 31	High

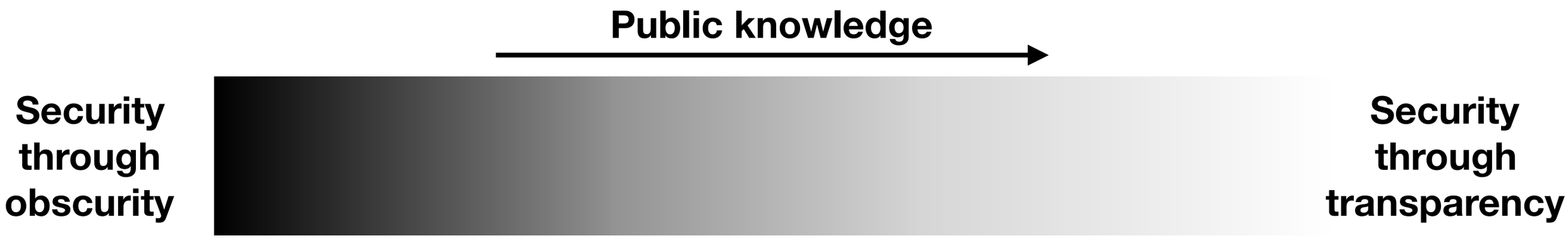
Fail evaluation at any vulnerability level

Moving state of the art

- Constant evolution of attacks and countermeasures
- Active research community

- Regular updates of the attack referentials
- ITSEF labs challenged by certification bodies

Evaluation grayscale



Evaluation grayscale

Public knowledge

Security through obscurity

Security through transparency

Kerckhoffs's principle

*A cryptosystem should be secure even if everything about the system, **except the key**, is **public knowledge**.*

Evaluation grayscale

Public knowledge

Security through obscurity

Security through transparency

Kerckhoffs's principle

*A cryptosystem should be secure even if everything about the system, **except the key**, is **public knowledge**.*

Cryptographers' dogma

Evaluation grayscale

Public knowledge

Security through obscurity

Security through transparency

More points in CC evaluation

Kerckhoffs's principle

*A cryptosystem should be secure even if everything about the system, **except the key**, is **public knowledge**.*

Cryptographers' dogma

Evaluation grayscale

Public knowledge

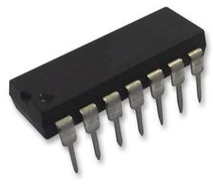
Security through obscurity

Security through transparency

More points in CC evaluation

Kerckhoffs's principle

Hardware crypto module



*A cryptosystem should be secure even if everything about the system, **except the key**, is **public knowledge**.*

Cryptographers' dogma

Evaluation grayscale

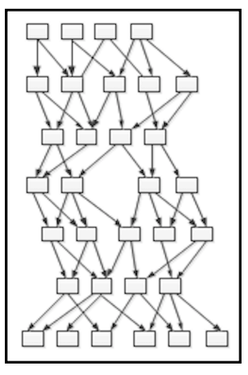
Public knowledge

Security through obscurity

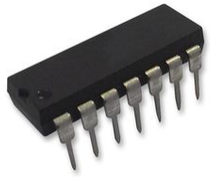
Security through transparency

More points in CC evaluation

White-box crypto



Hardware crypto module



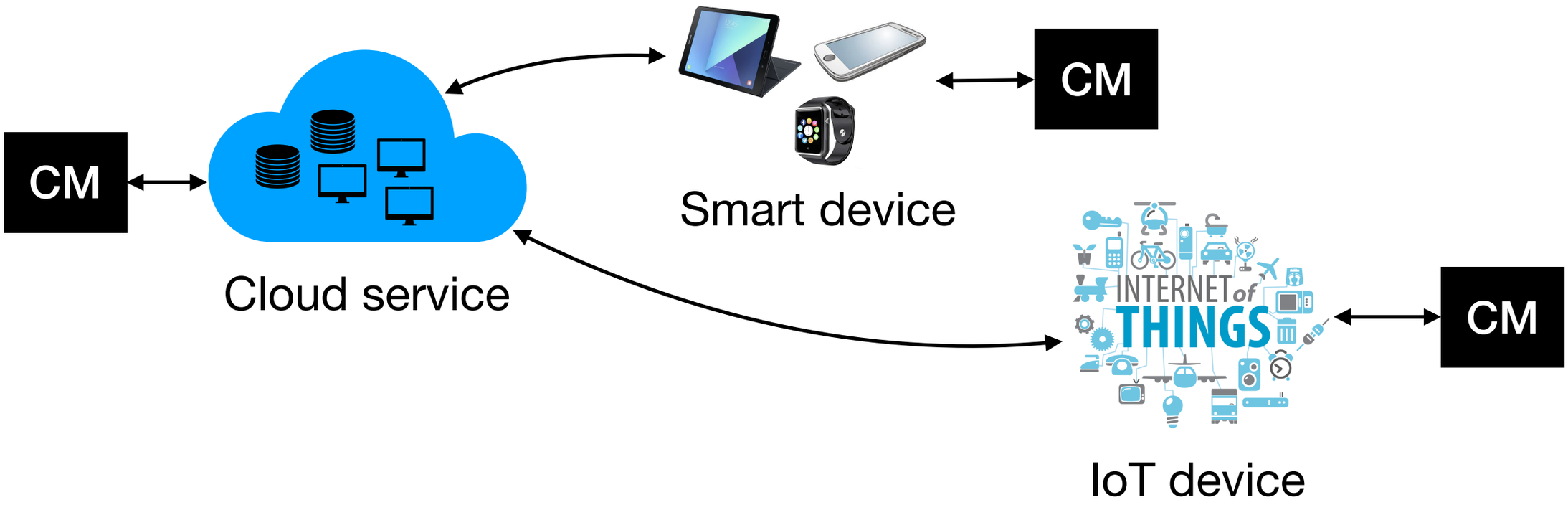
Kerckhoffs's principle

*A cryptosystem should be secure even if everything about the system, **except the key**, is **public knowledge**.*

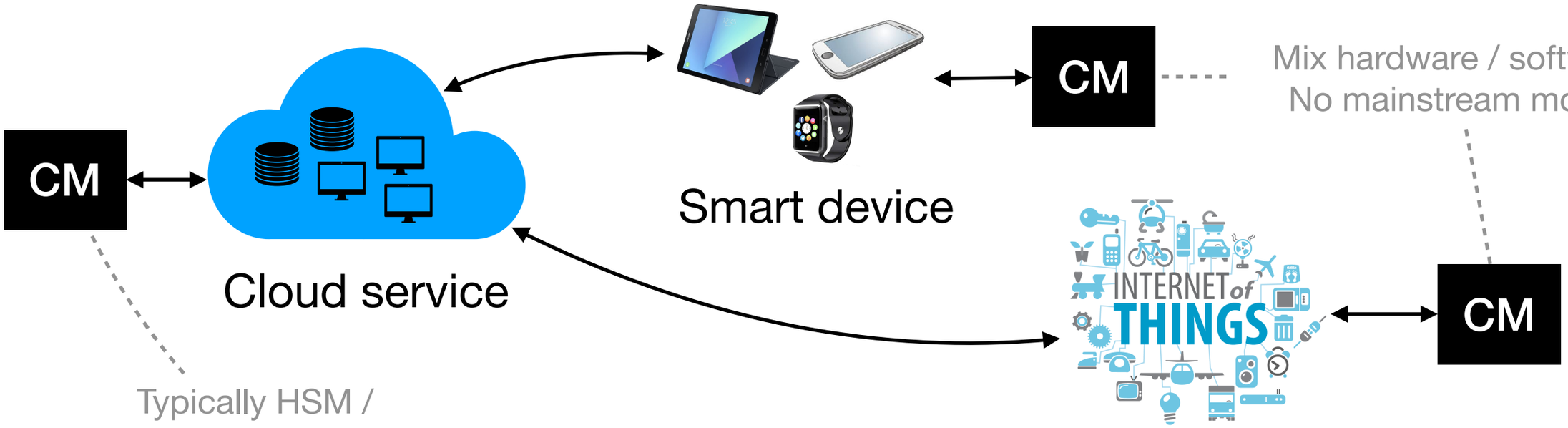
Cryptographers' dogma

Evolution of CM security

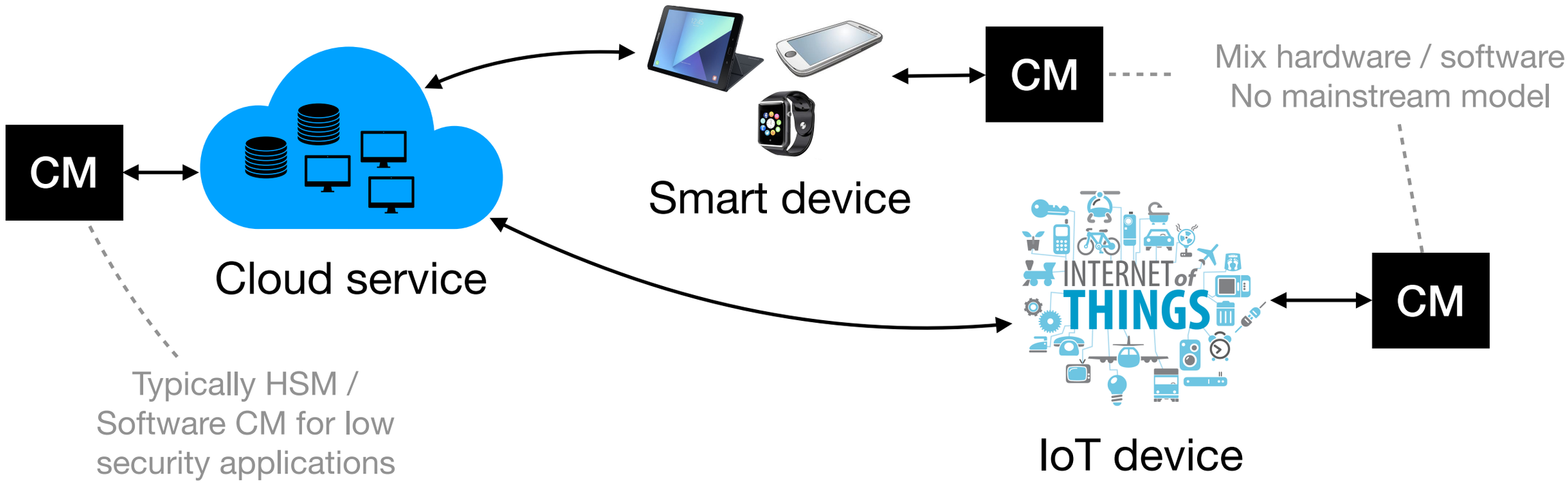
Evolution of cryptographic modules



Evolution of cryptographic modules



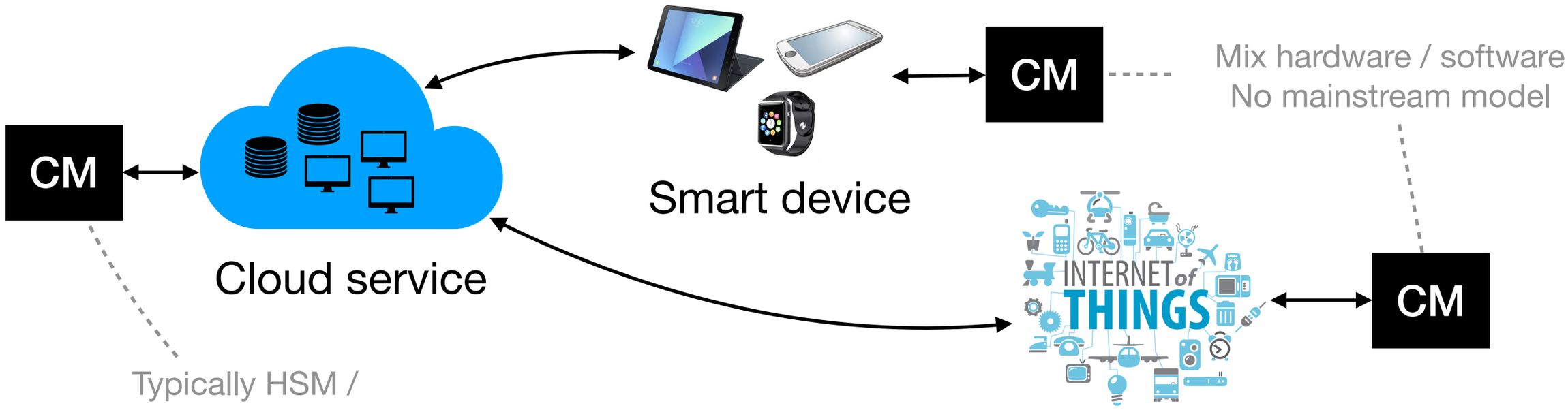
Evolution of cryptographic modules



- **Ideal setting**
  - Hardware secure element on all devices
  - Minimalist API (for security)
  - Open to app developpers

- **Alternatives**
  - Trusted execution environment (TEE)
  - Tokenisation
  - White-box cryptography

Evolution of cryptographic modules



- **Ideal setting**
  - Hardware secure element on all devices
  - Minimalist API (for security)
  - Open to app developpers
- **Alternatives**
  - Trusted execution environment (TEE)
  - Tokenisation
  - White-box cryptography

Software CM ≠ hardware CM

Where do we stand in terms of security?

More threats addressed

More security guaran-ties

	Black-box model	Gray-box model	White-box model
Evaluation & secret design	-	-	(✓)
Evaluation & partial public information	-	✓	✗
Formal proof & public review	✓	✗	✗

✓ Running smoothly

(✓) New trend

✗ Not available (yet)

Evolution of gray-box security

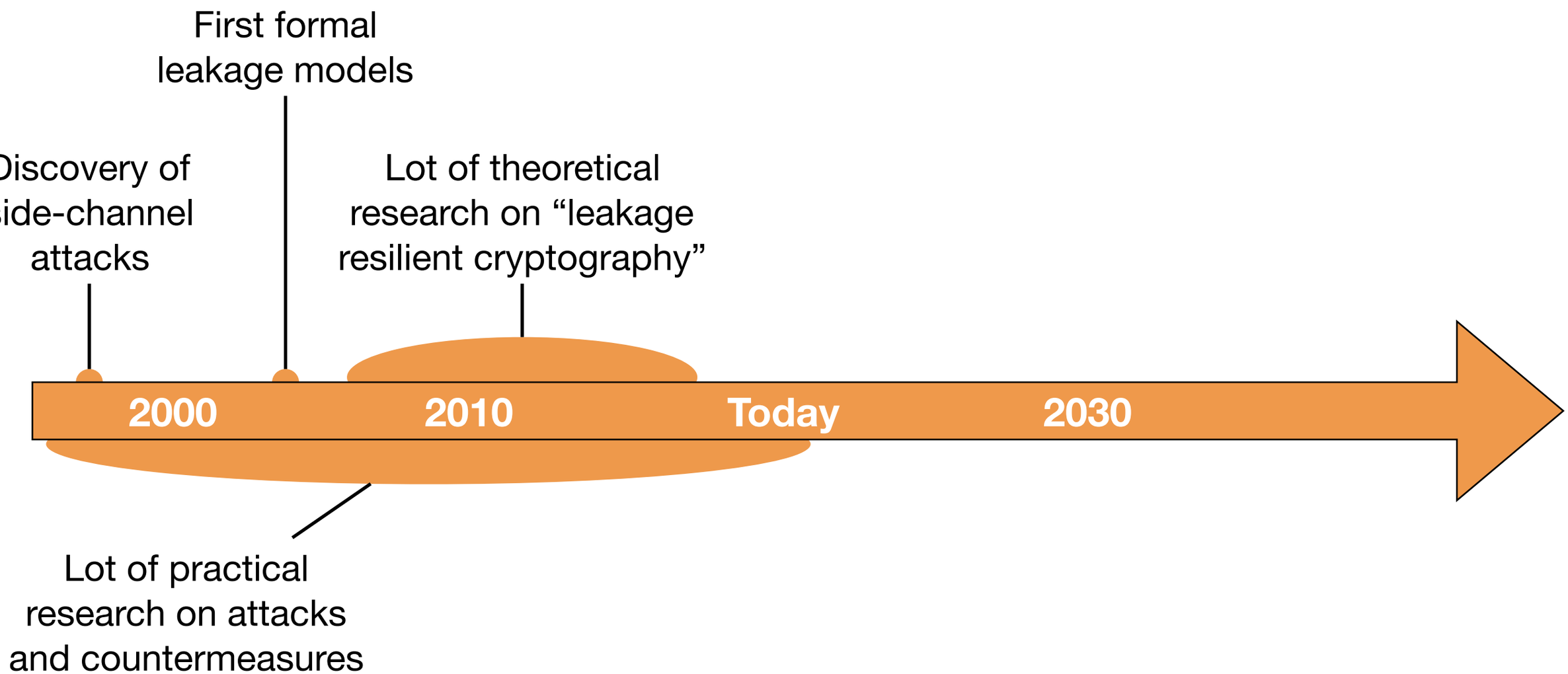
Evolution of gray-box security

Discovery of side-channel attacks

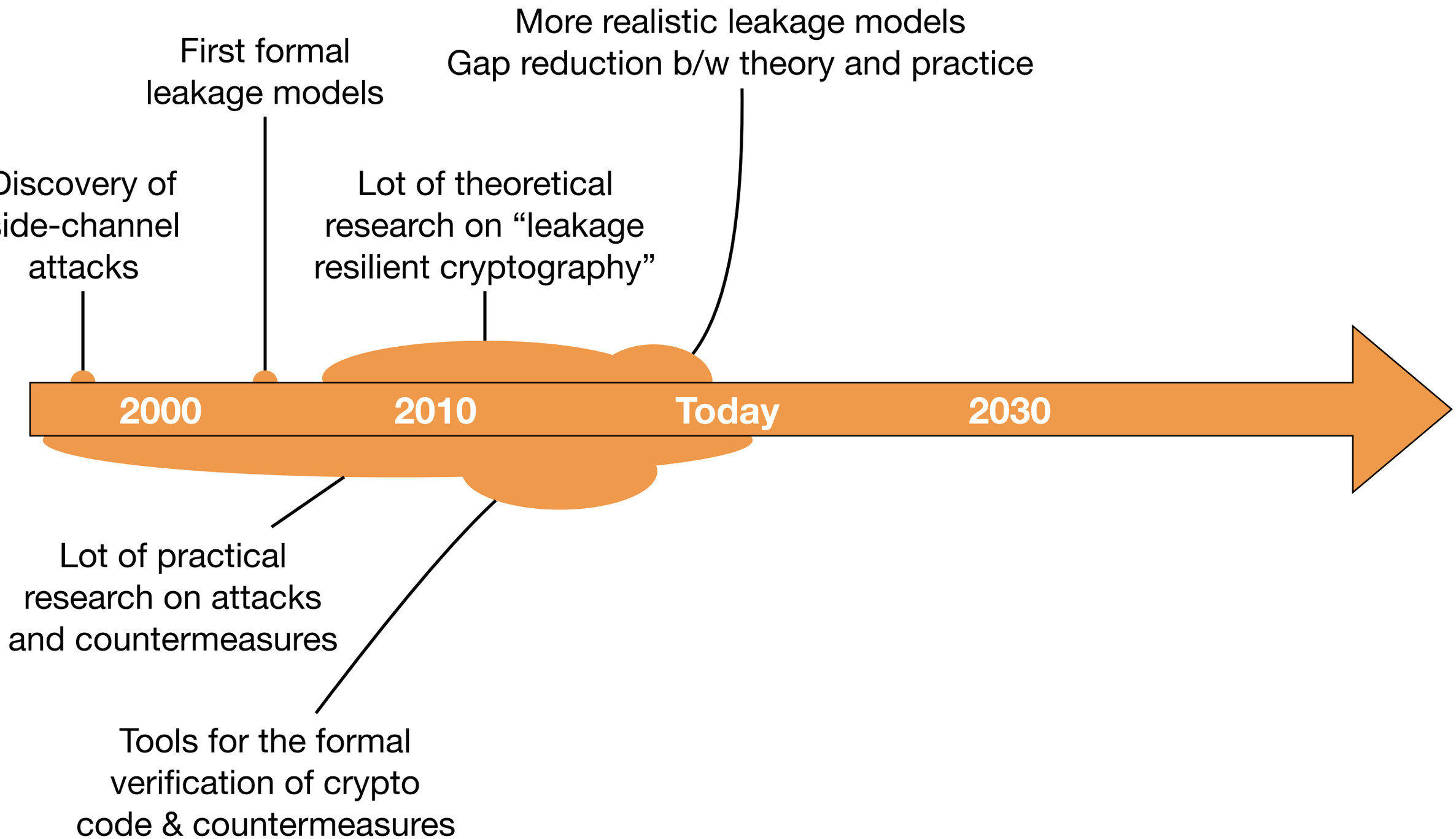
2000 2010 Today 2030

Lot of practical research on attacks and countermeasures

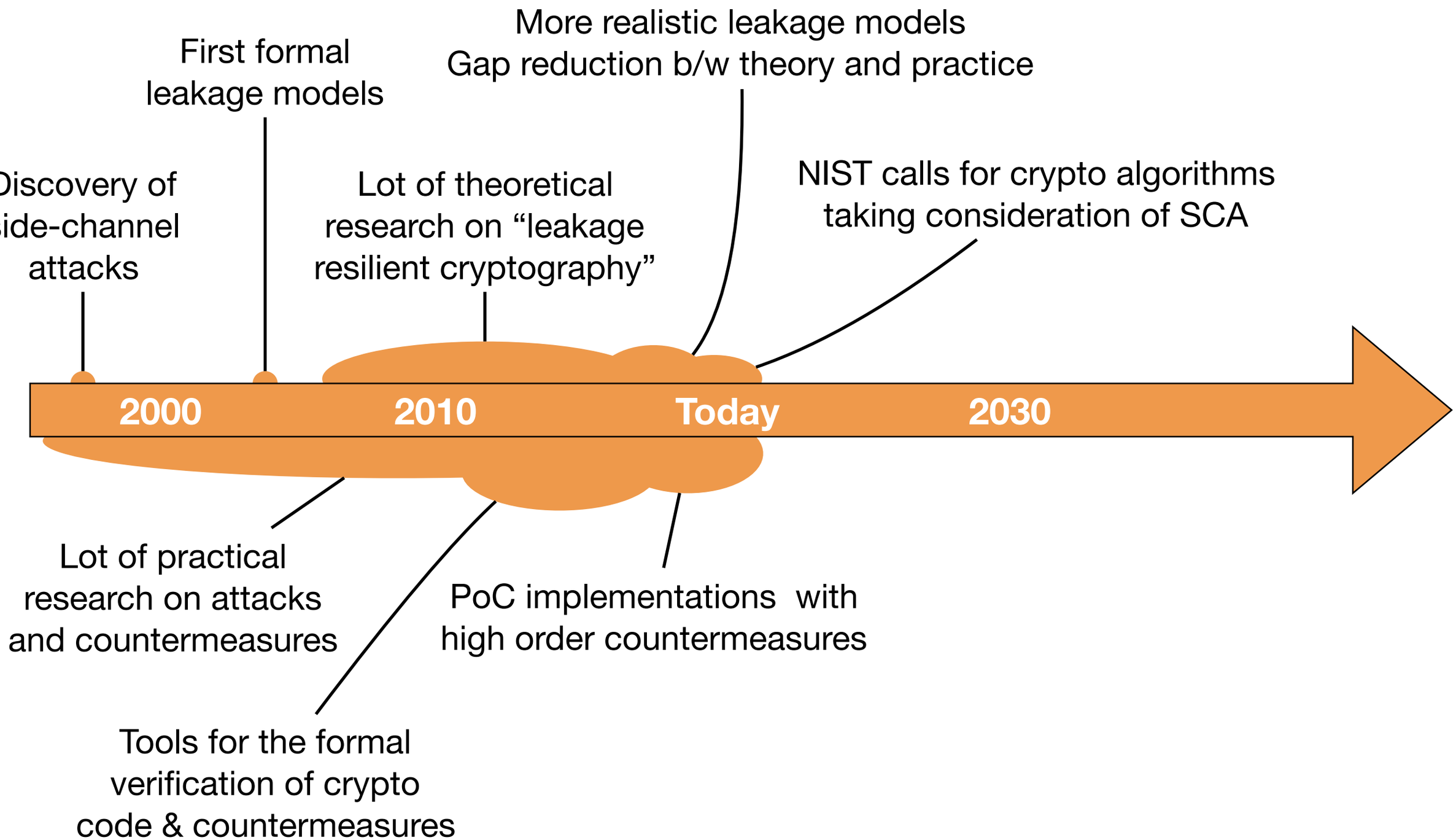
Evolution of gray-box security



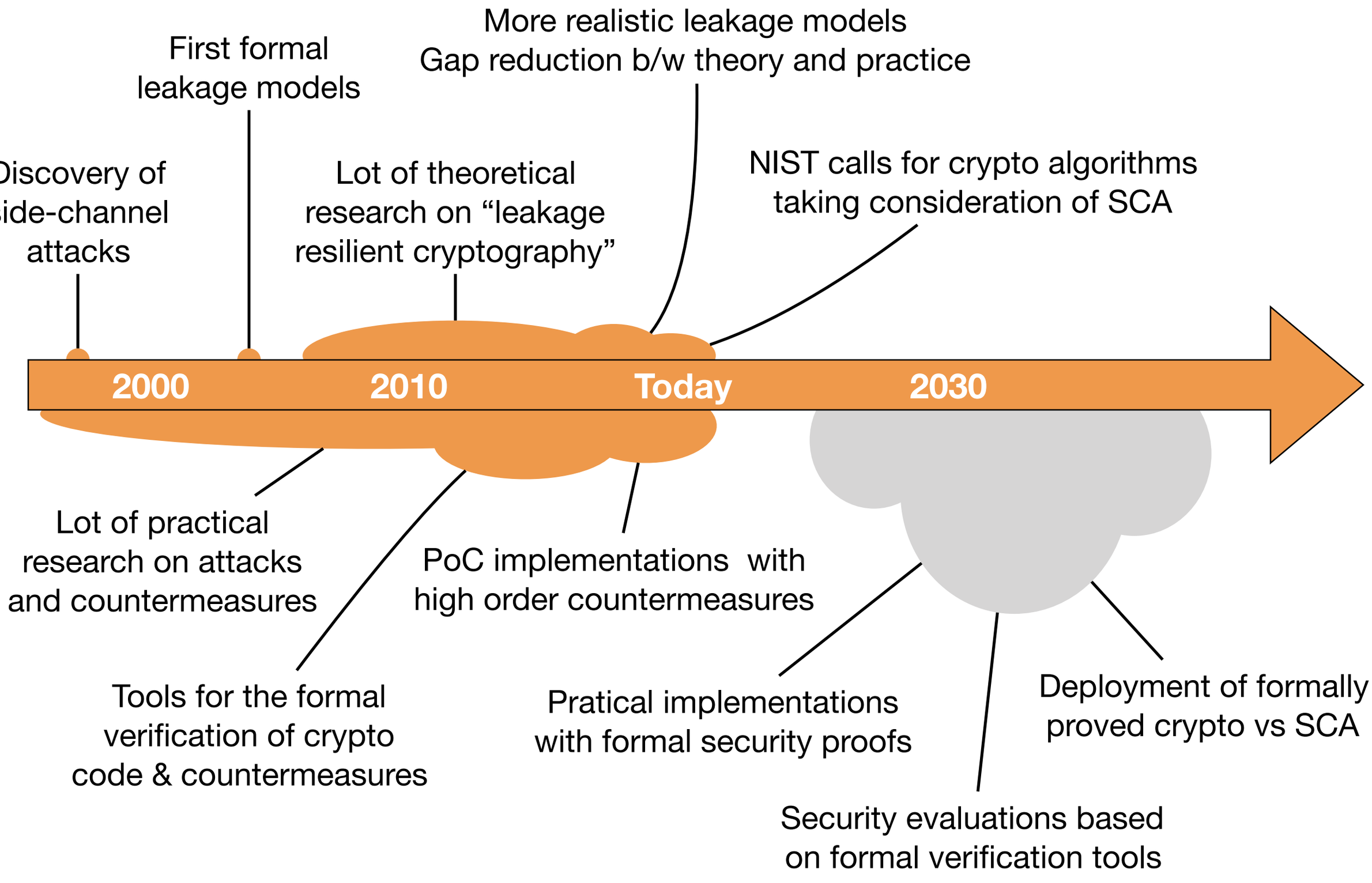
Evolution of gray-box security



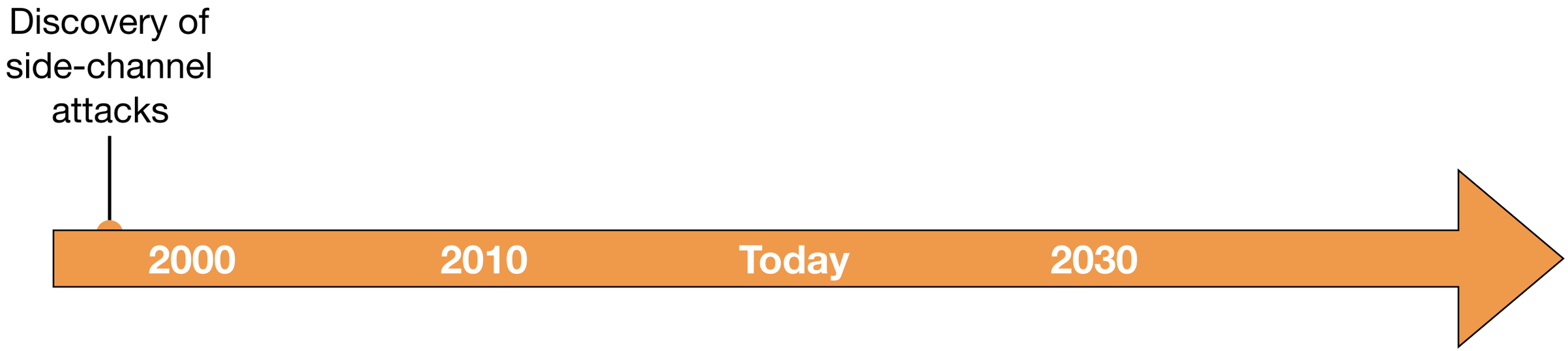
Evolution of gray-box security



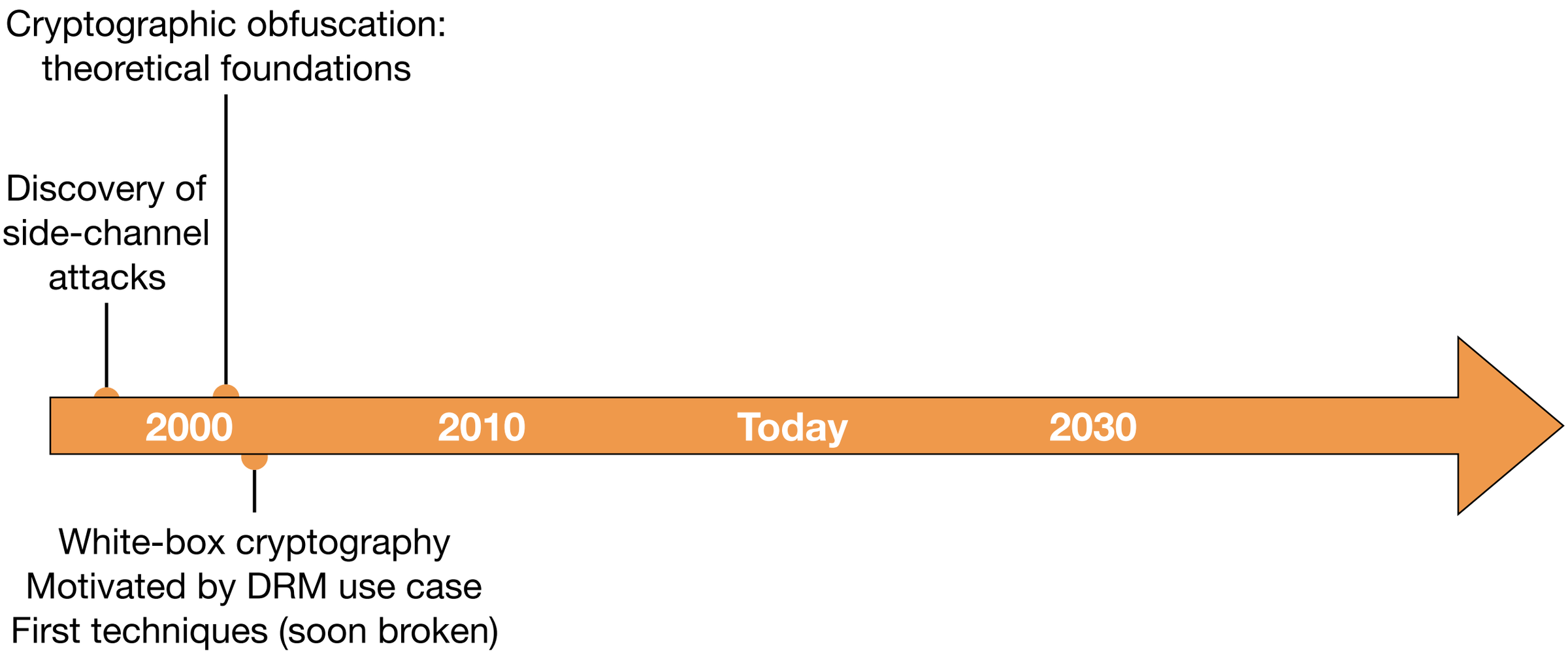
Evolution of gray-box security



Evolution of white-box security



Evolution of white-box security



Evolution of white-box security

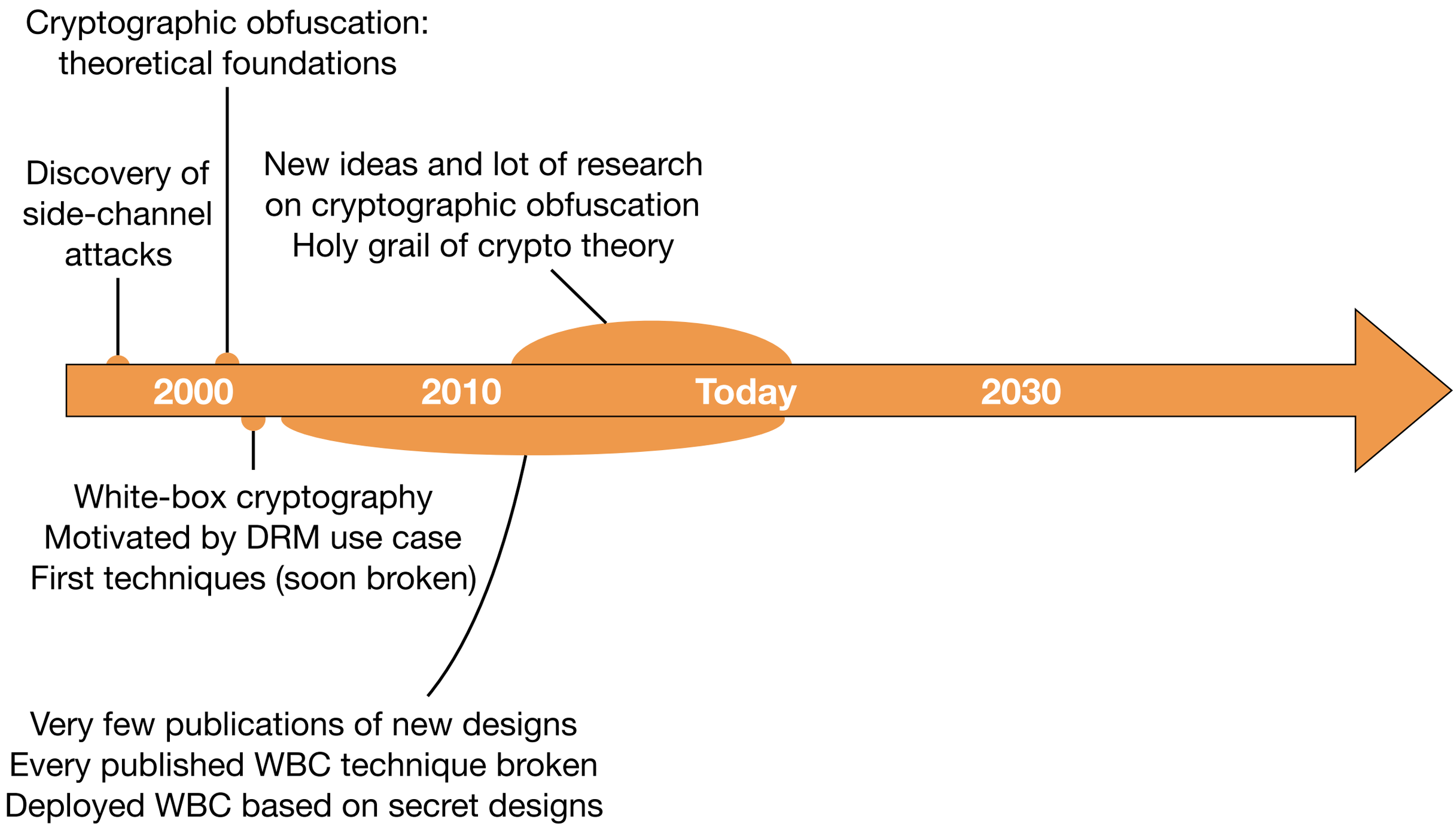
Cryptographic obfuscation:
theoretical foundations

Discovery of
side-channel
attacks

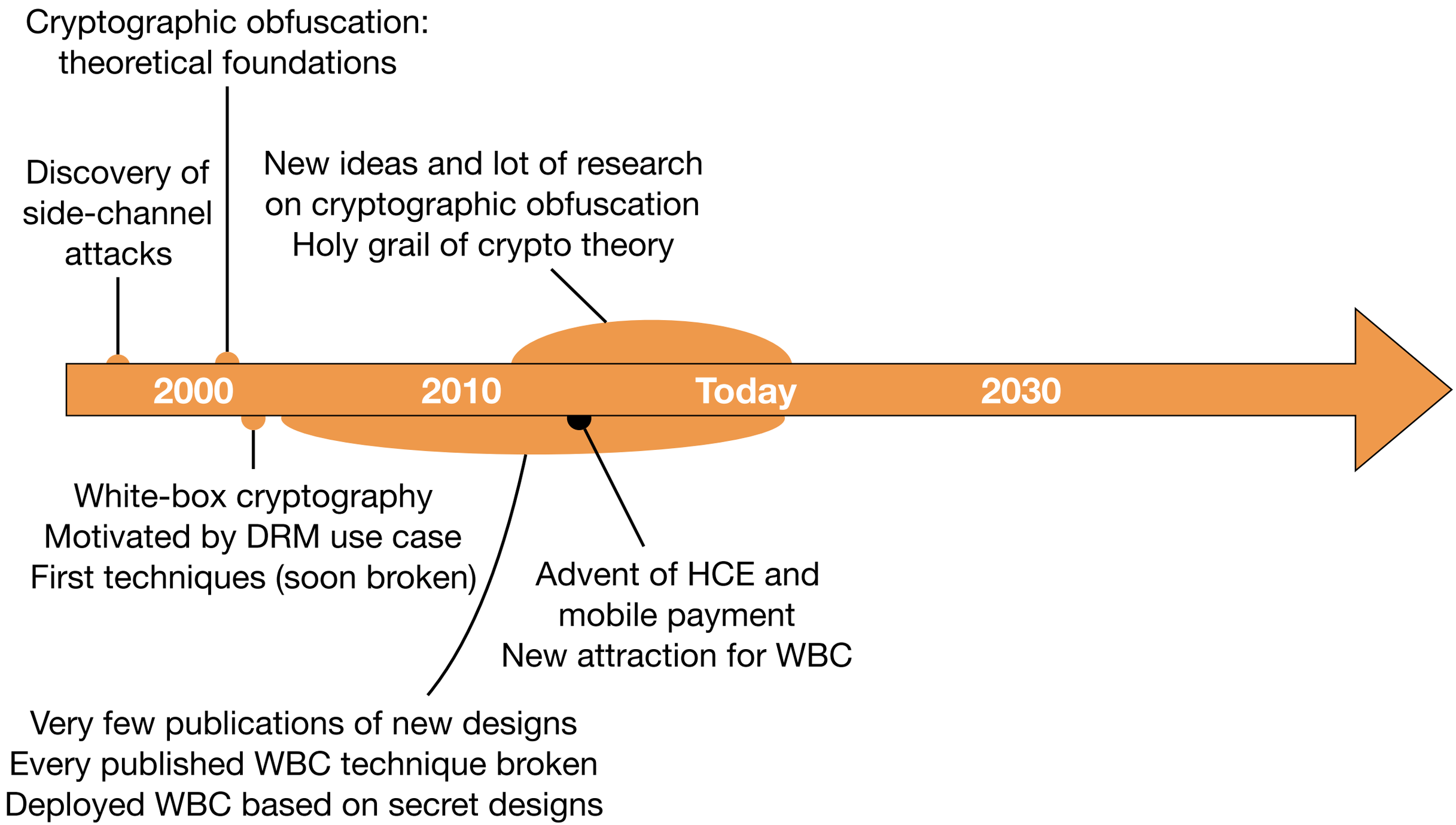
White-box cryptography
Motivated by DRM use case
First techniques (soon broken)

Very few publications of new designs
Every published WBC technique broken
Deployed WBC based on secret designs

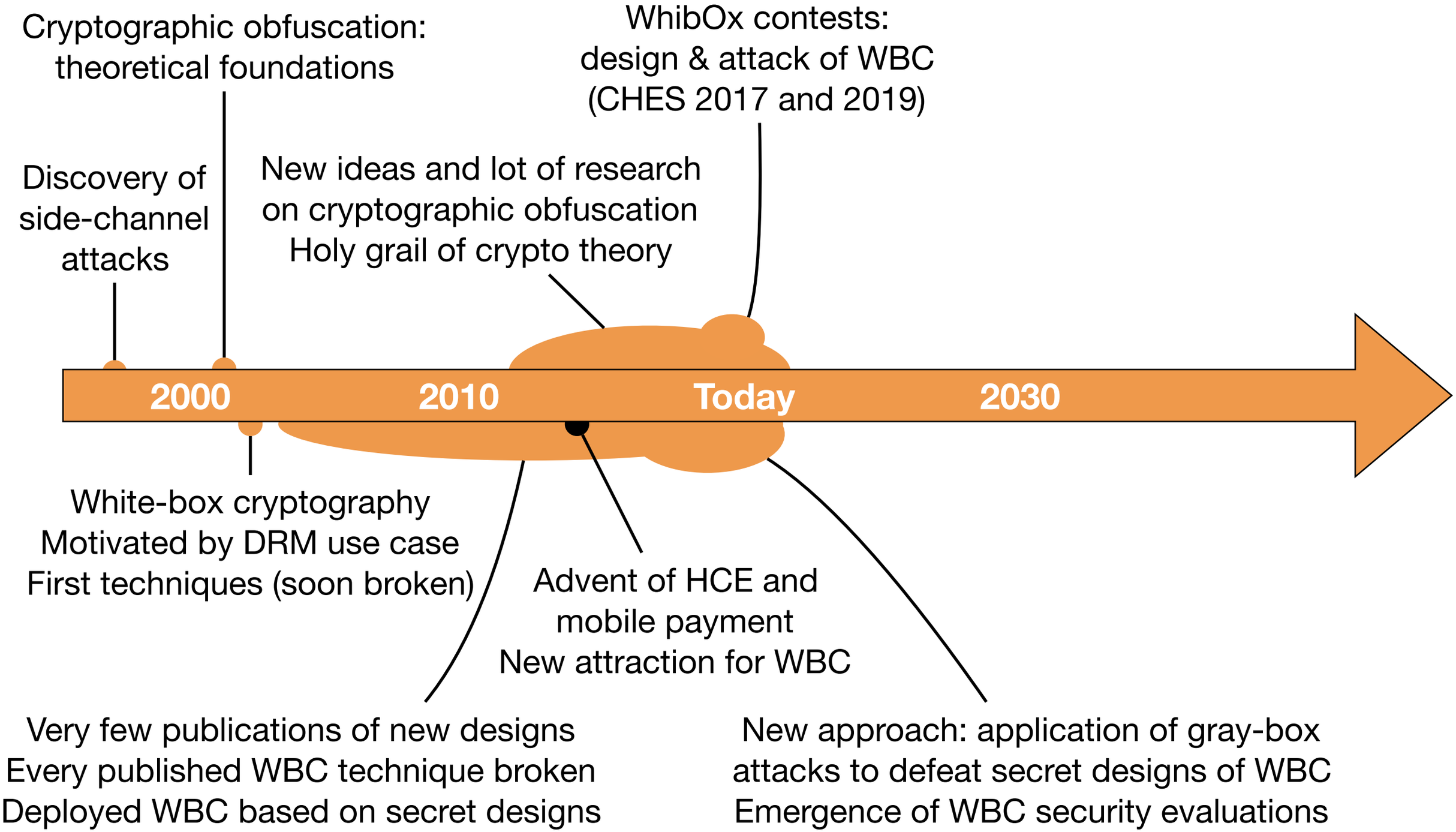
Evolution of white-box security



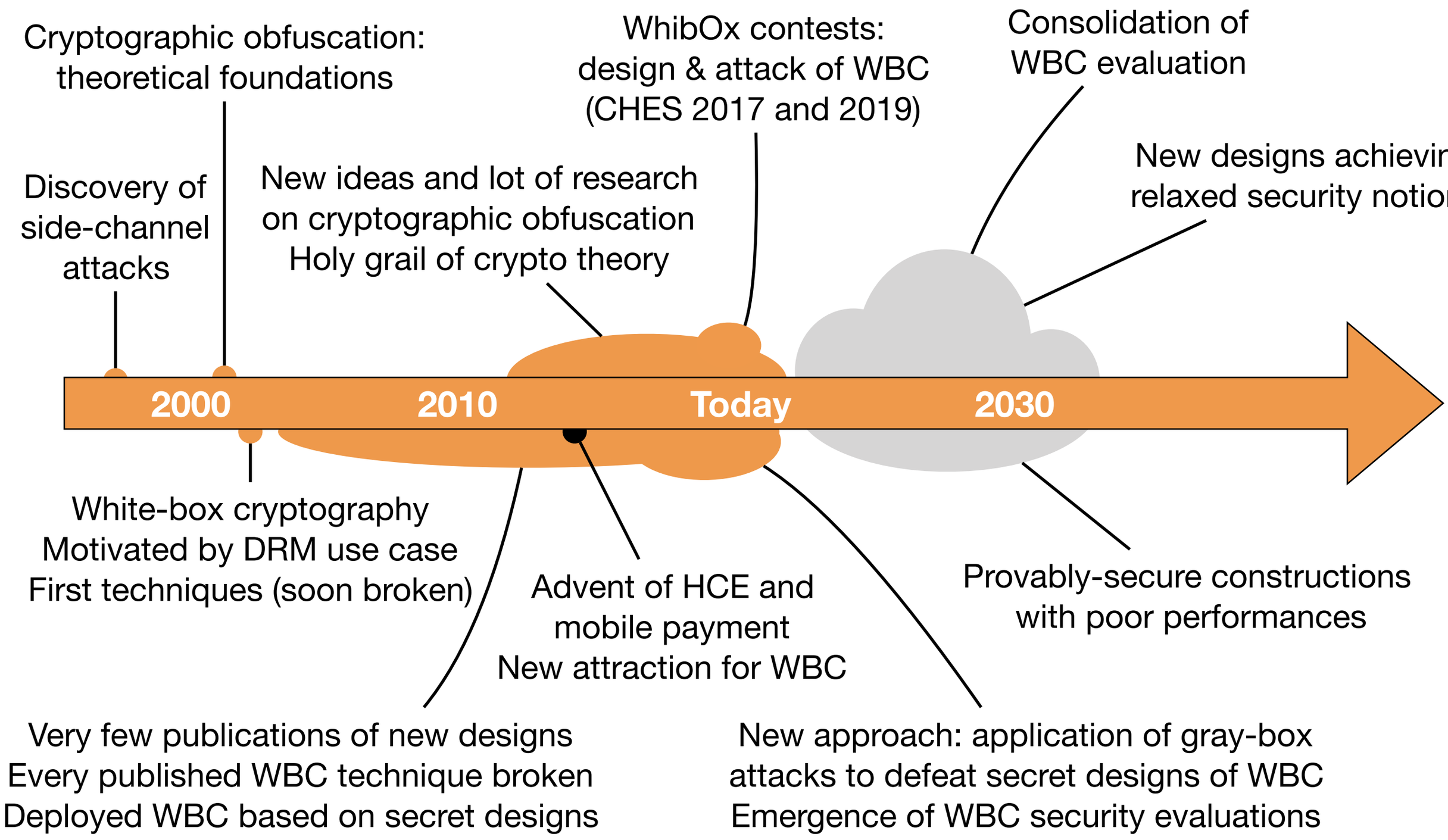
Evolution of white-box security



Evolution of white-box security



Evolution of white-box security



Conclusions

- Several shades of gray for the security of CM
- Don’t underestimate the practicability of side-channel attacks
- Gray-box security
  - Evaluation model running well
  - Transition to formal tools / proofs
- White-box cryptography
  - Solution of smart devices w/o accessible secure elements
  - Partly based on security through obscurity
  - Emergence of WBC evaluation (needs consolidation)

Questions?

What?

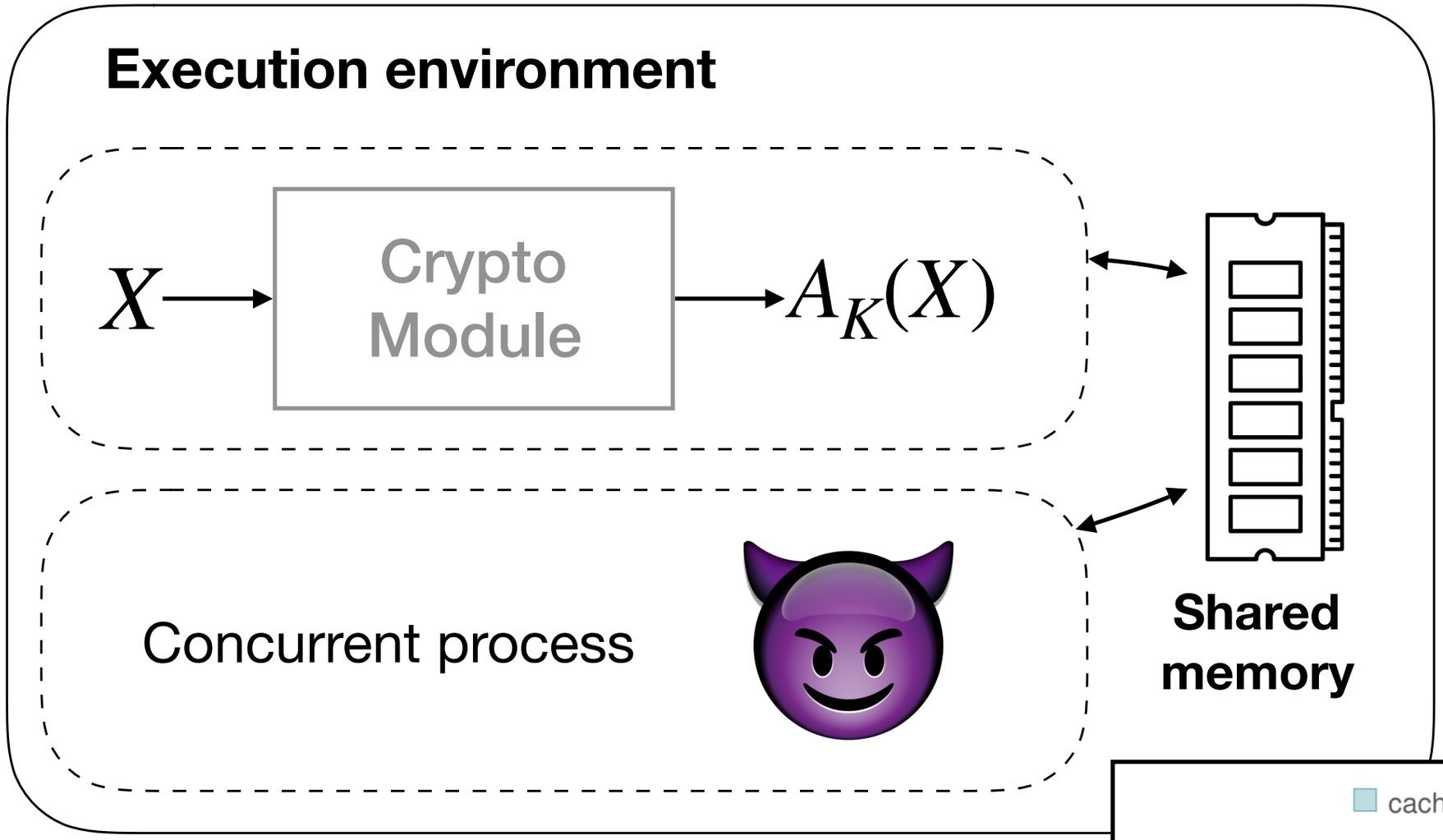
Why?

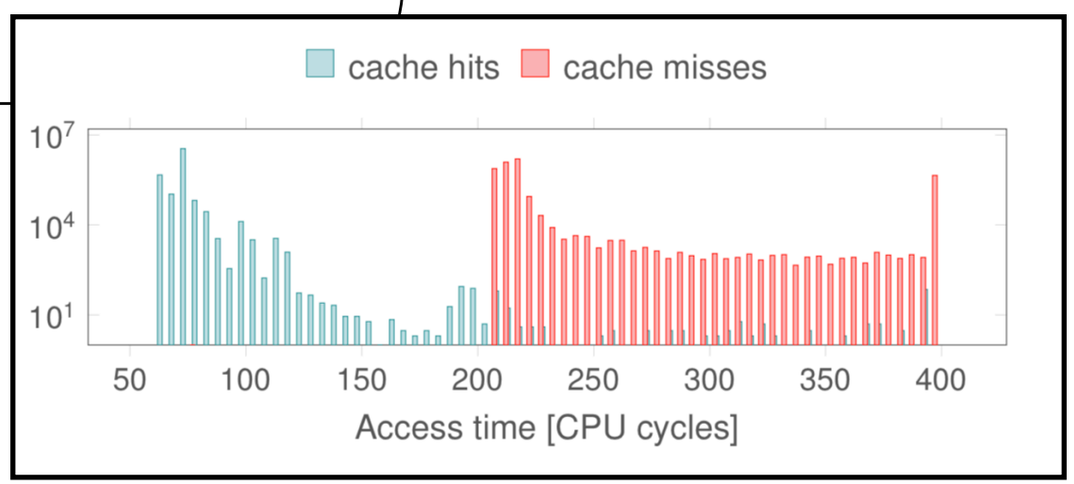
Securing Cryptographic Modules: A ~~Fifty~~ Story

Related links

- Common criteria: https://www.commoncriteriaportal.org/
- SOG-IS: https://www.sogis.eu/
- CHES conference: https://ches.iacr.org/
- Smart card certification tutorial: https://iacr.org/workshops/ches/ches2016/presentations/CHES16-Tutorial1.pdf
- WhibOx contest (white-box design and attack competition)
  - 2017: https://whibox-contest.github.io/
  - 2019: https://www.cyber-crypt.com/whibox-contest/
- VERISICC project (Verification of side-channel countermeasures): https://www.cryptoexperts.com/verisicc/

Microarchitectural attacks





- Concurrent execution leaks information through shared memory / cache
- Avoid data-dependent look-up
- Or use white-box cryptography