Kleptographic Attacks against Implicit Rejection

Antoine Joux, Julian Loss, Benedikt Wagner

Proxy Speaker: Yanbo Chen

eprint 2024/260

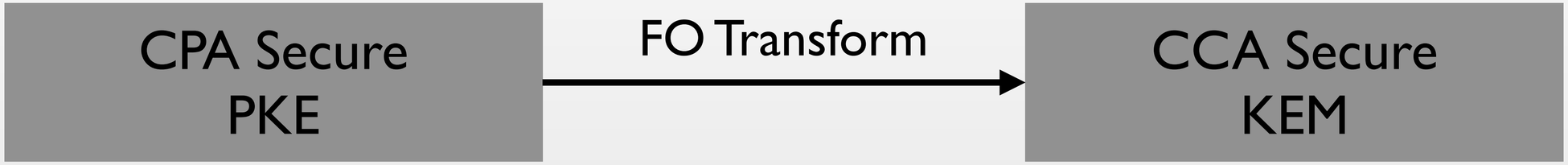
Fujisaki-Okamoto Transform

Fujisaki-Okamoto Transform

Fujisaki-Okamoto Transform

- Analysis in the QROM

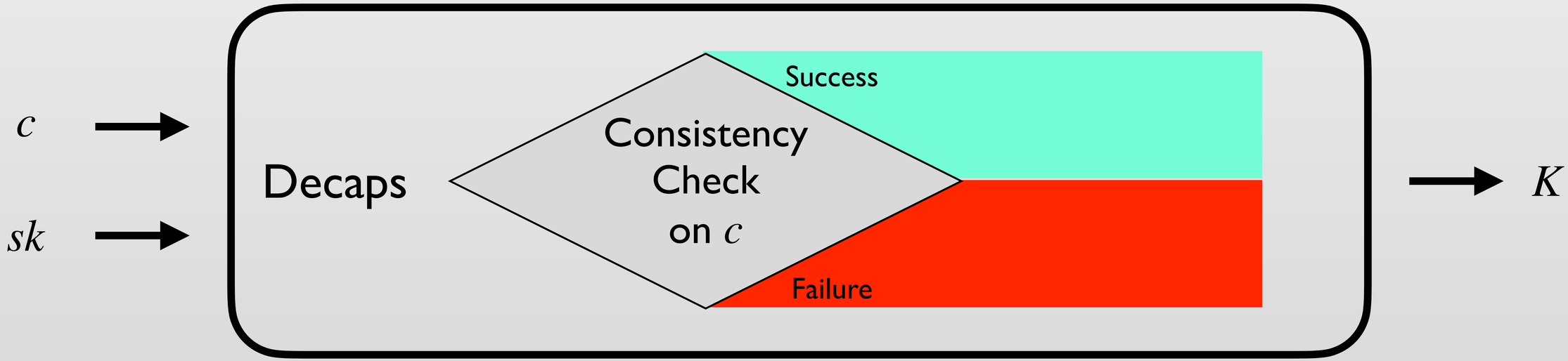
Fujisaki-Okamoto Transform



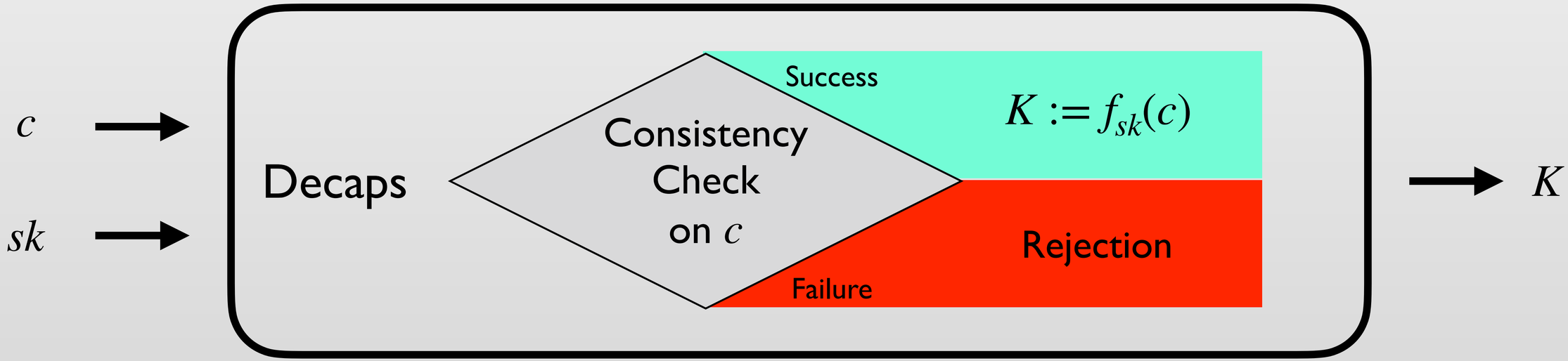
- Analysis in the QROM
- Used in NIST PQC Submissions, e.g., Kyber

Fujisaki-Okamoto Transform

Fujisaki-Okamoto Transform



Fujisaki-Okamoto Transform



How to Reject

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

Implicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := H(c, s)$

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

Implicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := H(c, s)$

Independent seed

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

Implicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := H(c, s)$

Independent seed

- Implicit rejection: tighter bounds

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

Implicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := H(c, s)$

Independent seed

- Implicit rejection: tighter bounds
- Implicit rejection in Kyber

How to Reject

Explicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := \perp$

Implicit Rejection

Success	$K := f_{sk}(c)$
Failure	$K := H(c, s)$

Independent seed

- Implicit rejection: tighter bounds
- Implicit rejection in Kyber

Our Observation:

Implicit rejection can be less secure!

Our Work

Our Work

Implicit rejection in a kleptographic setting

Our Work

Implicit rejection in a kleptographic setting

Kleptographic attacker can break it!

Our Work

Implicit rejection in a kleptographic setting

Kleptographic attacker can break it!

	Subvert	Memory	Time Offline	Time Online	Advantage
Attack 1	Decaps	2^8	2^0	2^2	0.997
Attack 2	Key Gen	2^7	2^0	2^{130}	0.999
Attack 3	Key Gen	2^{111}	2^{154}	2^{106}	0.692

* applied to Kyber

Kleptography

Kleptography

Cryptographic Algorithm

Kleptography

Cryptographic Algorithm

Subverted Algorithm

- Kleptographic attacker subverts algorithm

Kleptography

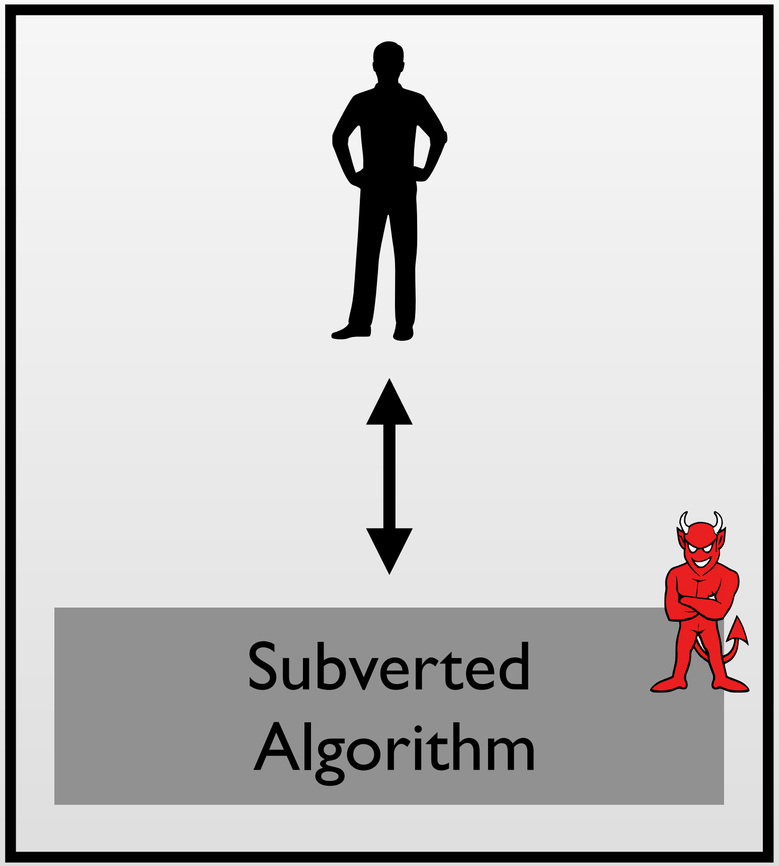
Cryptographic Algorithm

Subverted Algorithm

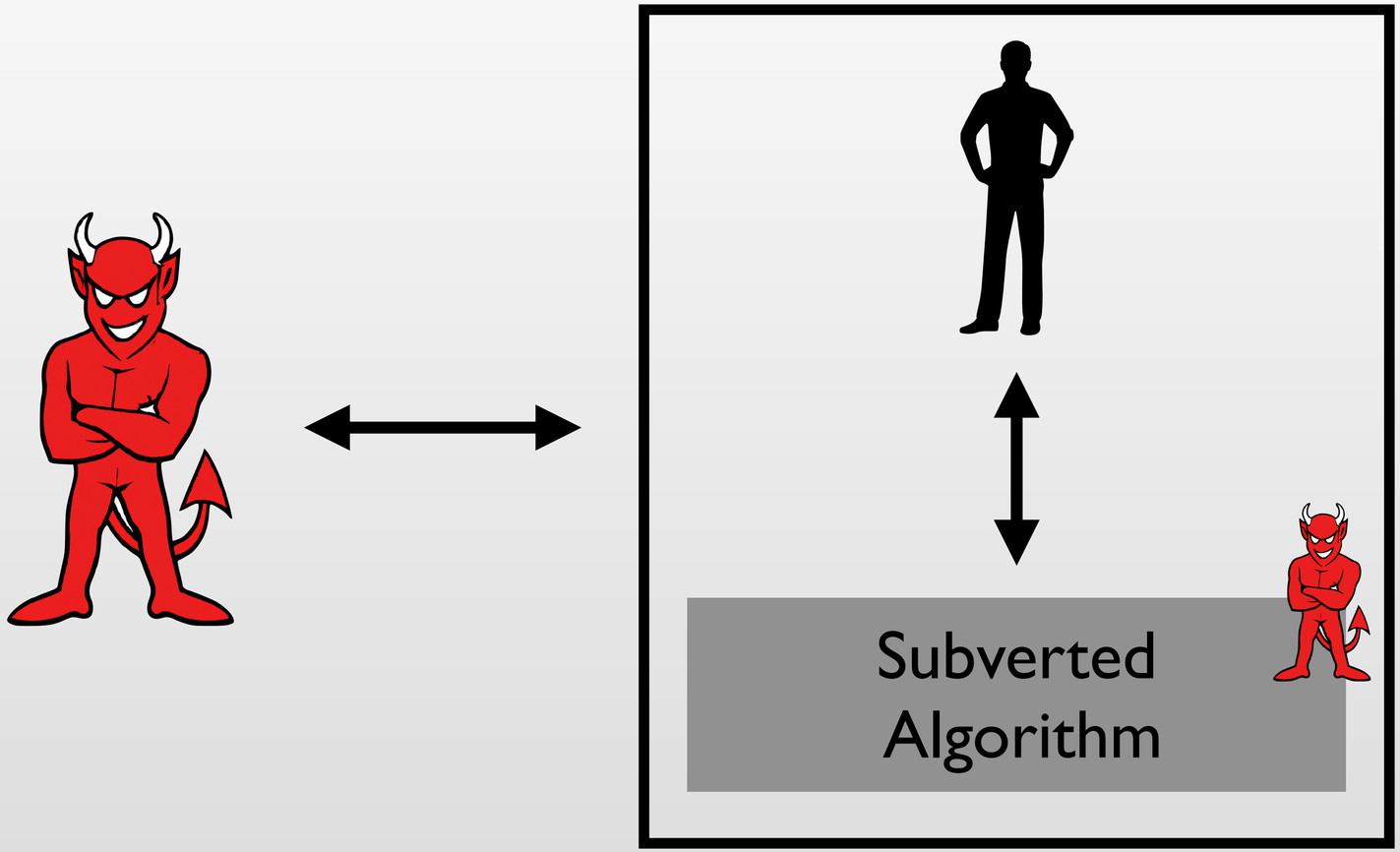
- Kleptographic attacker subverts algorithm
- Attacker's goals: Success and Undetectability

Kleptographic Attacker's Goals

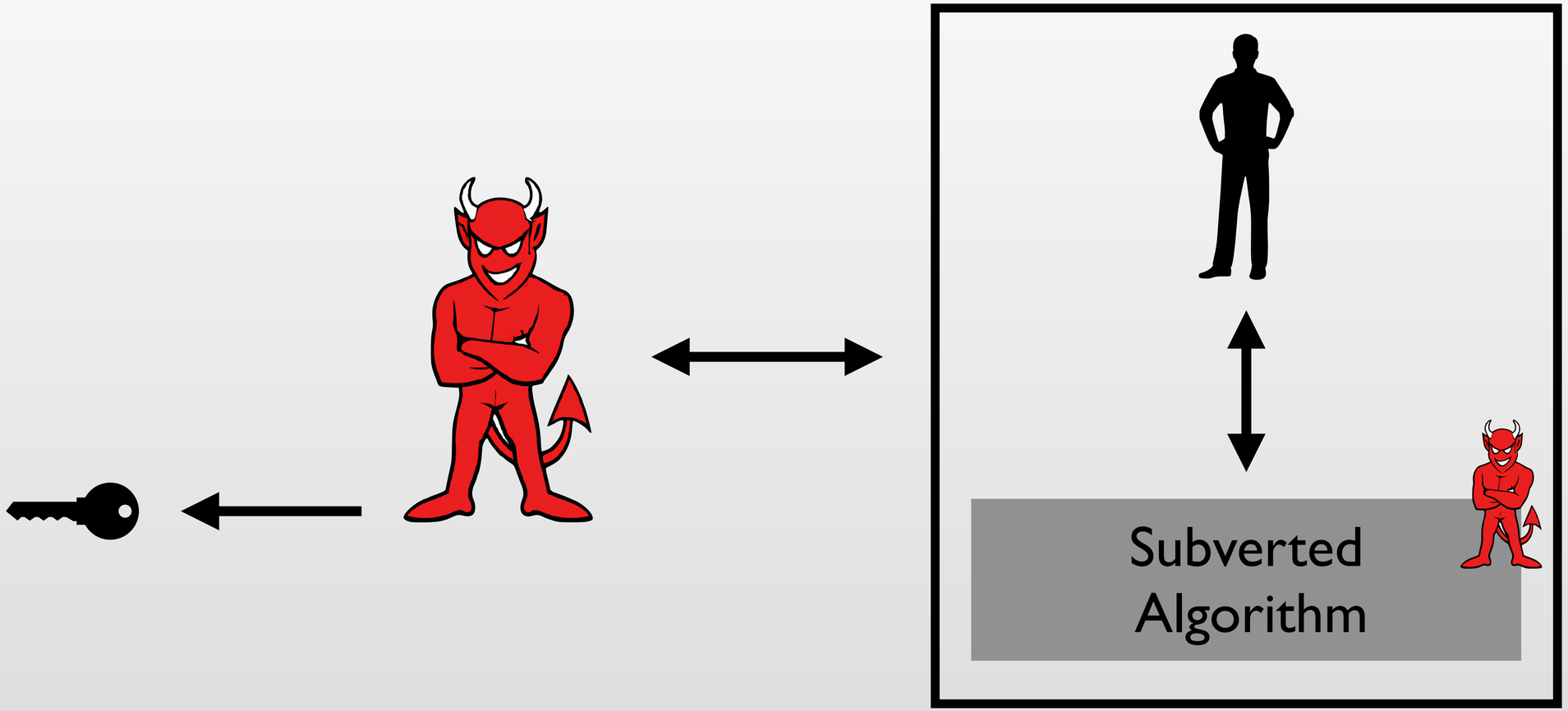
Kleptographic Attacker's Goals



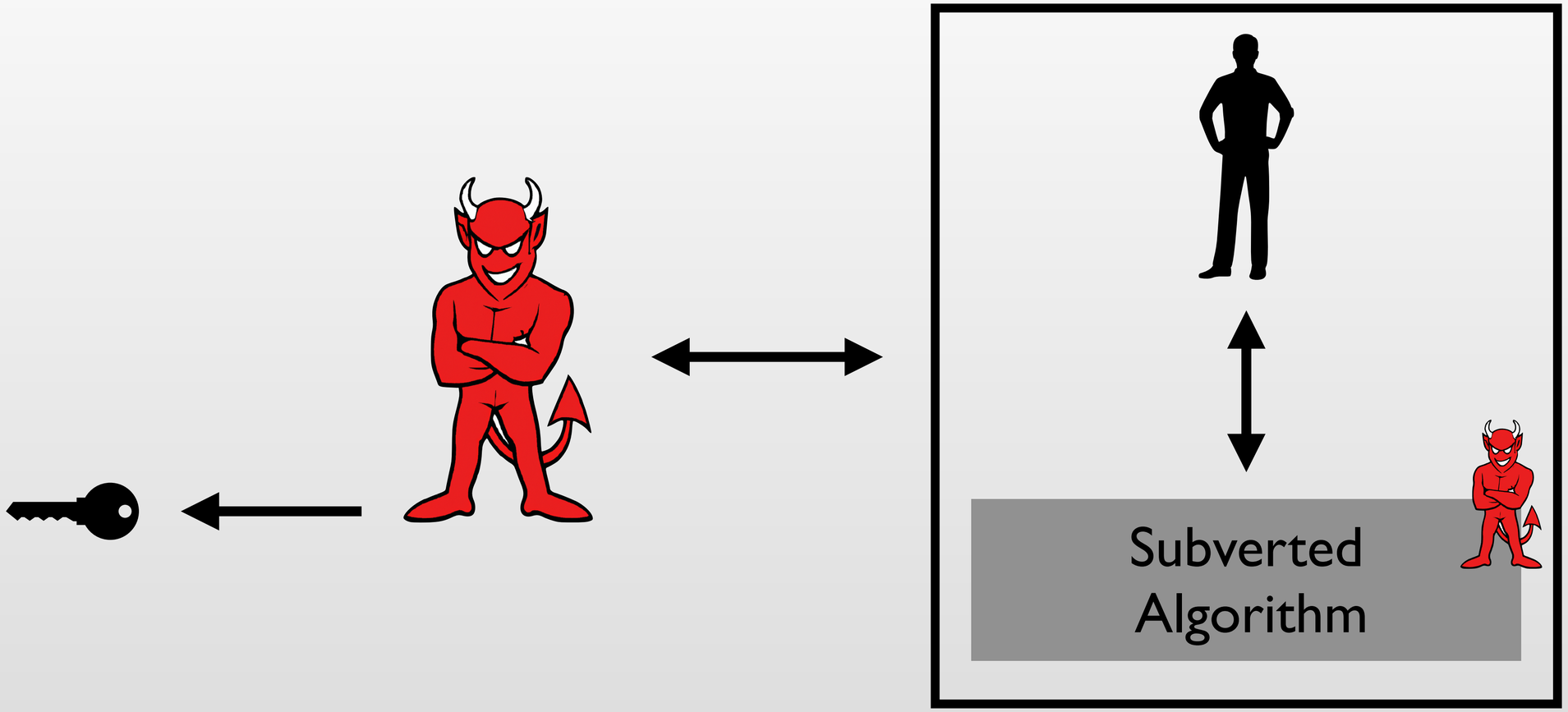
Kleptographic Attacker's Goals



Kleptographic Attacker's Goals



Kleptographic Attacker's Goals



- Success: attacker breaks security for subverted user

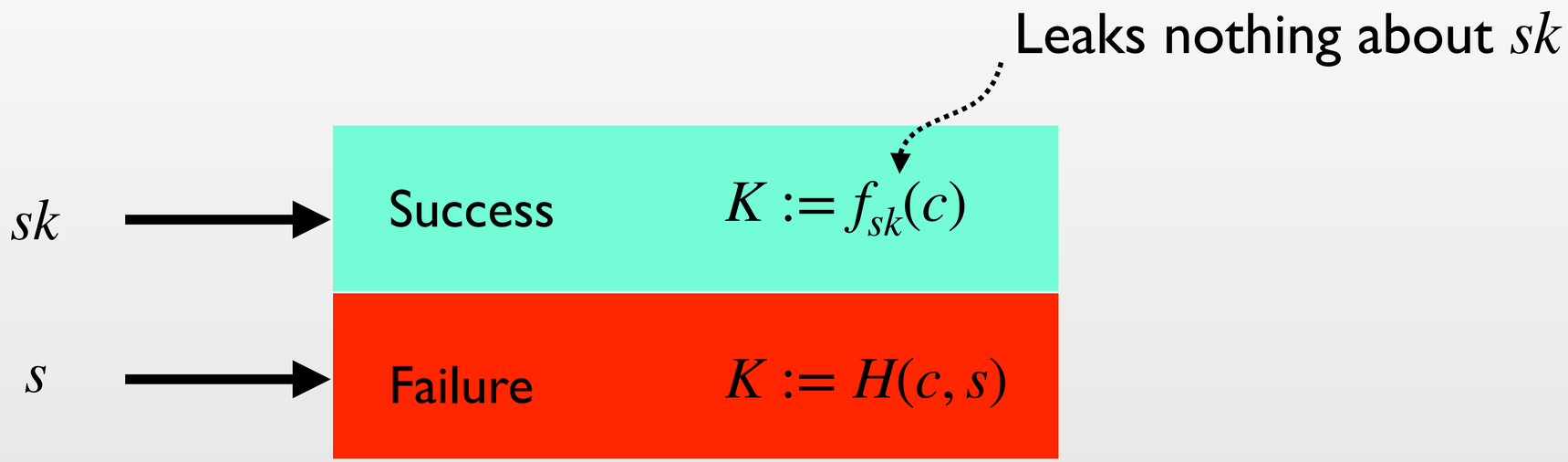
Kleptographic Attacker's Goals

- Undetectability: user cannot detect subversion

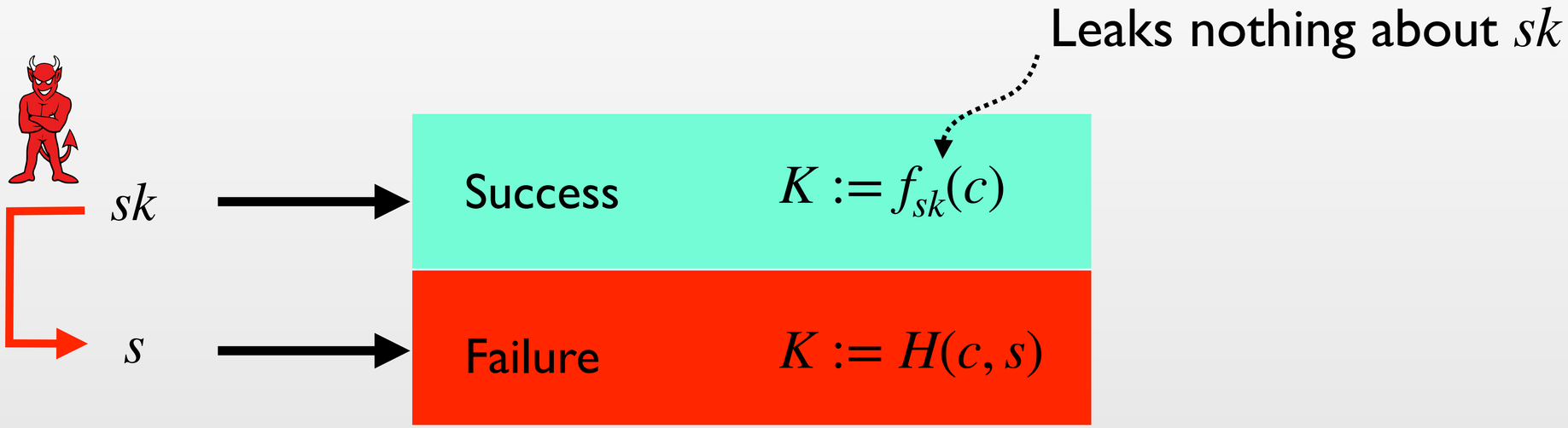
Main Idea of Our Attacks (#2 and #3)

Main Idea of Our Attacks (#2 and #3)

Main Idea of Our Attacks (#2 and #3)

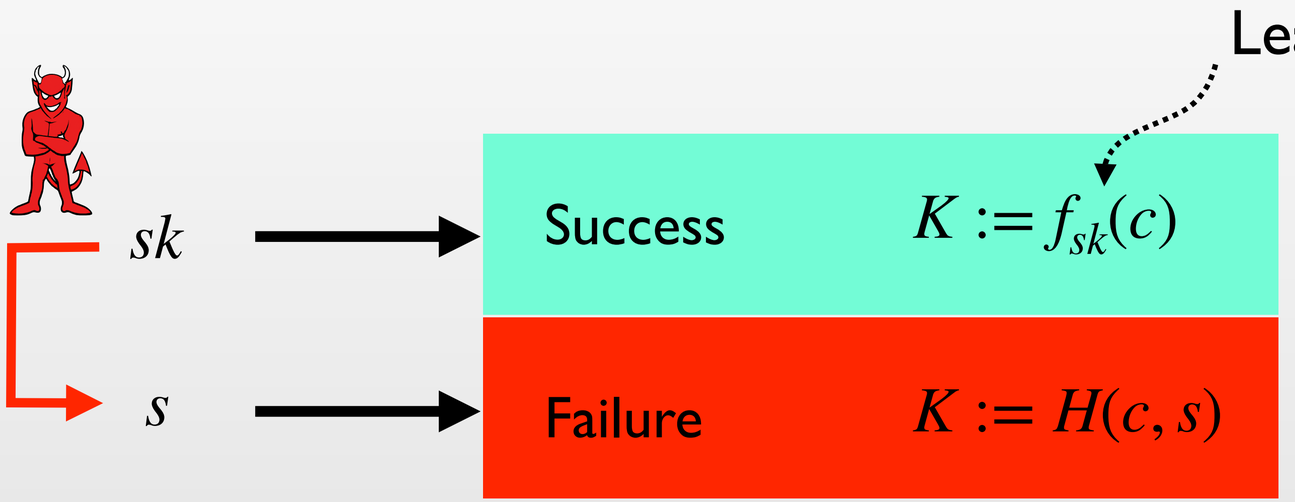


Main Idea of Our Attacks (#2 and #3)



- Make seed s depend on sk

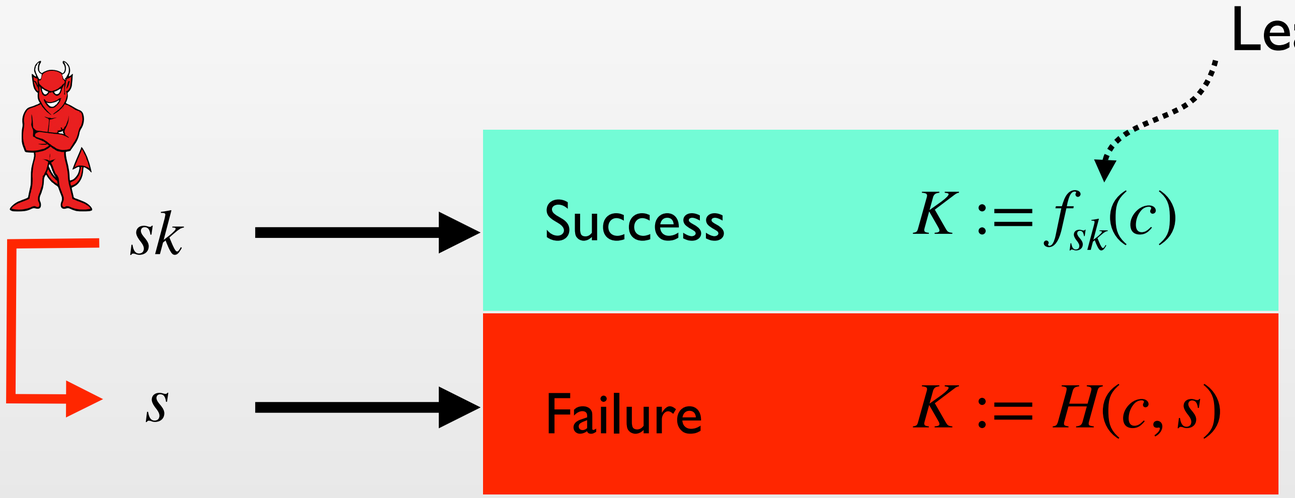
Main Idea of Our Attacks (#2 and #3)



$s = H(ak, \text{truncate}(sk))$

- Make seed s depend on sk

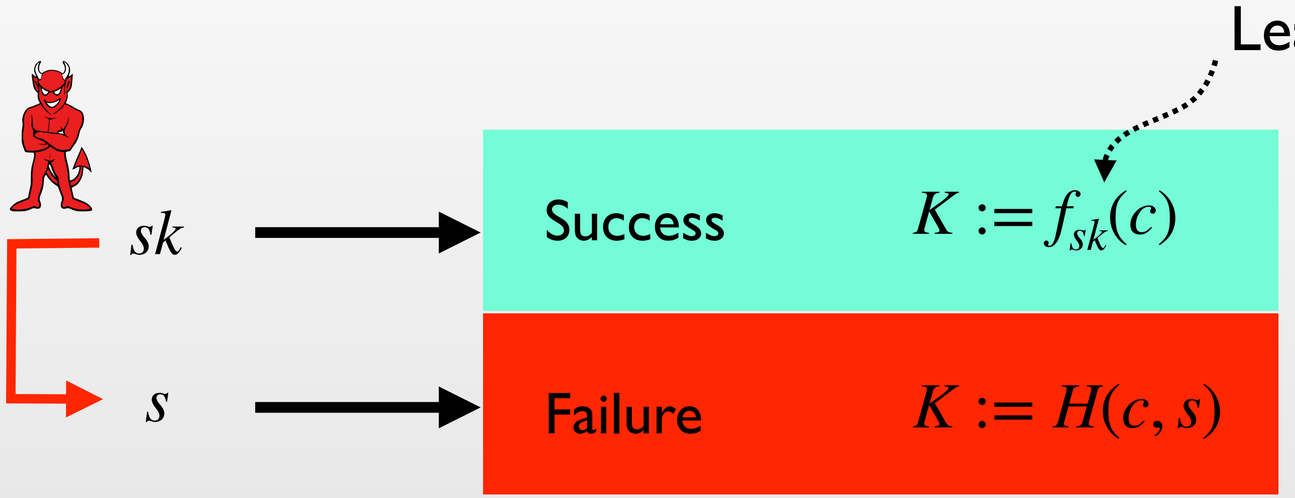
Main Idea of Our Attacks (#2 and #3)



$s = H(ak, \text{truncate}(sk))$

- Make seed s depend on sk
- Undetectable if ak is random

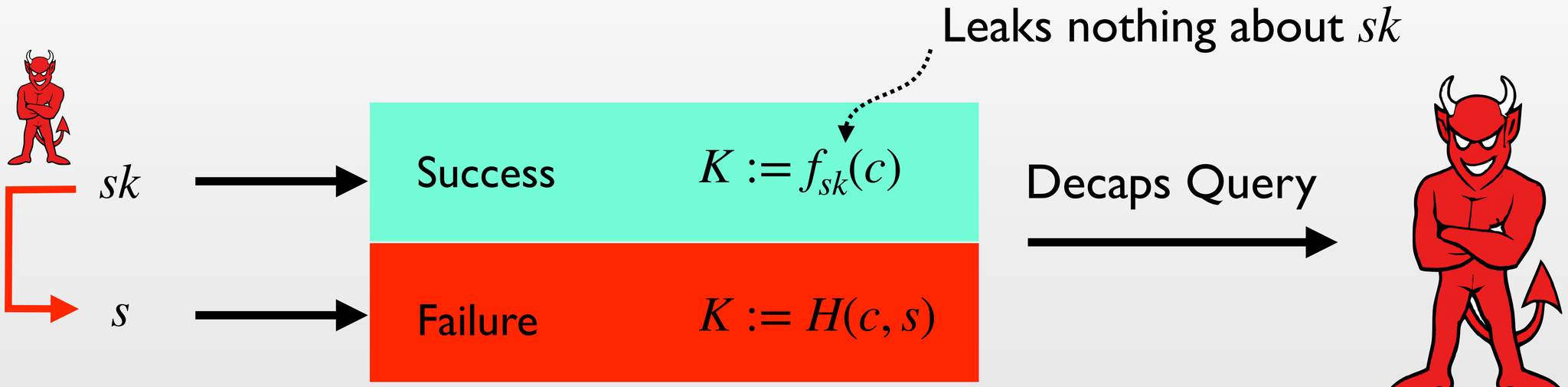
Main Idea of Our Attacks (#2 and #3)



$s = H(ak, \text{truncate}(sk))$

- Make seed s depend on sk
- Undetectable if ak is random
- Rejection keys K leak bits of sk

Main Idea of Our Attacks (#2 and #3)



- Make seed s depend on sk
- Undetectable if ak is random
- Rejection keys K leak bits of sk

Open Questions

Open Questions

- Mitigations?

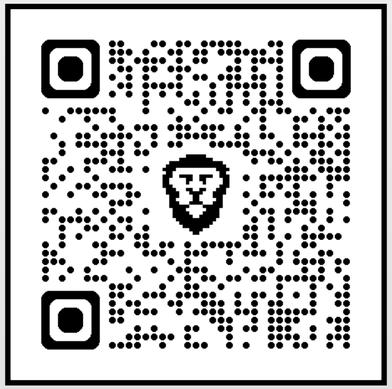
Open Questions

- Mitigations?
- Conclusion for NIST PQC Standardization?

Open Questions

- Mitigations?
- Conclusion for NIST PQC Standardization?
- Can we apply technique to other primitives, like PAKE?

Thank you!



eprint 2024/260