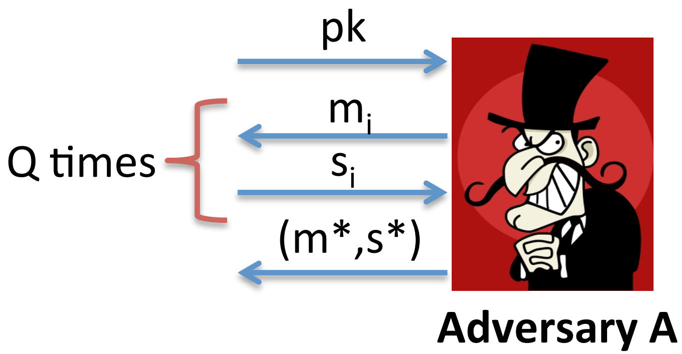
On the Impossibility of Tight Cryptographic Reductions

Christoph Bader, Tibor Jager, Yong Li, Sven Schäge
Ruhr-University Bochum

EUROCRYPT 2016

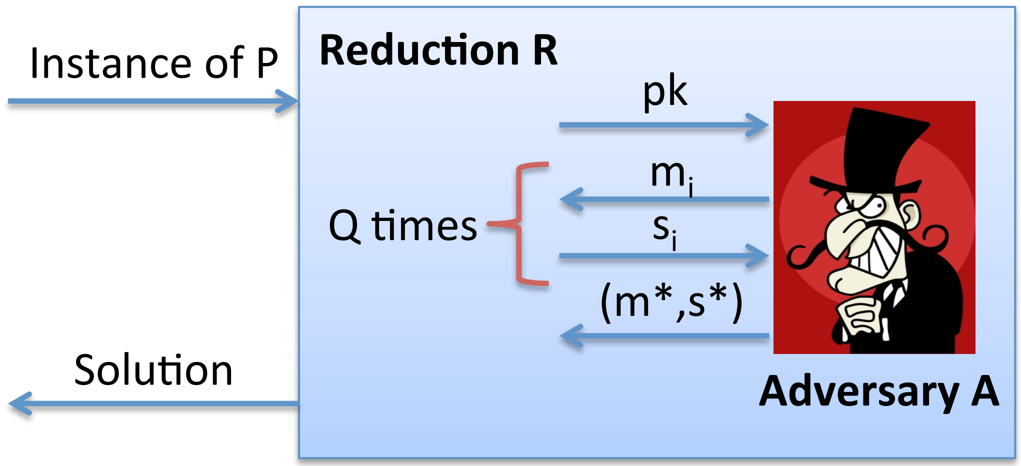
“Tight” Cryptographic Reductions

1. Define a **security model**



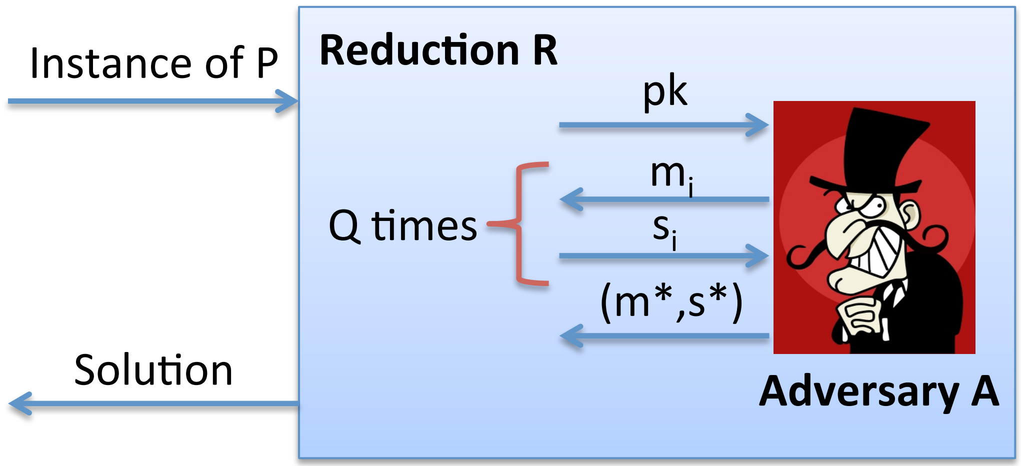
"Tight" Cryptographic Reductions

1. Define a **security model**
2. Prove: efficient **adversary A** implies efficient algorithm **R** that solves a **"hard" problem P**



“Tight” Cryptographic Reductions

1. Define a **security model**
2. Prove: efficient **adversary A** implies efficient algorithm **R** that solves a **“hard” problem P**

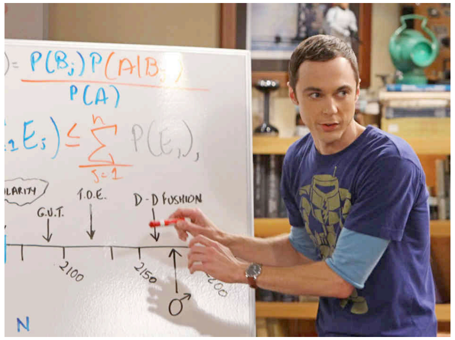


Reduction R is **tight**, if

$\mathbf{t_R} \approx \mathbf{t_A}$ and $\mathbf{succ_R} \approx \mathbf{succ_A}$

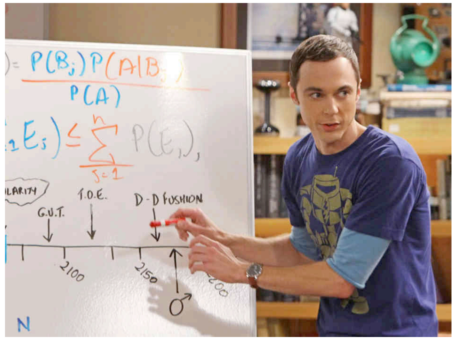
Why is tight security interesting?

- Do schemes with **tight security exist**?
  - Inherent tightness lower bounds?



Why is tight security interesting?

- Do schemes with **tight security exist**?
  – Inherent tightness lower bounds?
- Relevant for **theoretically-sound** selection of parameters
  – “Non-tight“ reduction ⇒ large parameters
  – Tight reduction ⇒ smaller parameters



Many Tightly-Secure Cryptosystems

Identity-based Encryption
- Chen, Wee (Crypto 2013)
- Blazy, Kiltz, Pan (Eurocrypt 2014)
- ...

Public-Key Encryption
- Bellare, Boldyreva, Micali (Eurocrypt 2000)
- Hofheinz, Jager (Crypto 2012)
- Gay, Hofheinz, Kiltz, Wee (Eurocrypt 2016) **(best paper)**
- ...

Key Exchange
- Bader, Hofheinz, Jager, Kiltz, Li (TCC 2015)

Digital Signatures
- Katz-Wang (CCS 2003)
- Schäge (Eurocrypt 2011)
- ...

Pseudorandom Functions
- Naor-Reingold (FOCS 1997)
- Lewko-Waters (CCS 2009)
- Jager (ePrint 2016)
- ...

Many Tightly-Secure Cryptosystems

Identity-based Encryption
- Chen, Wee (Crypto 2013)
- Blazy, Kiltz, Pan (Eurocrypt 2014)
- ...

Digital Signatures
- Katz-Wang (CCS 2003)
- Schäge (Eurocrypt 2011)
- ...

Public-Key Encryption
- Bellare, Boldyreva, Micali (Eurocrypt 2000)
- Hofheinz, Jager (Crypto 2012)
- Gay, Hofheinz, Kiltz, Wee (Eurocrypt 2016) **(best paper)**
- ...

Pseudorandom Functions
- Naor-Reingold (FOCS 1997)
- Lewko-Waters (CCS 2009)
- Jager (ePrint 2016)
- ...

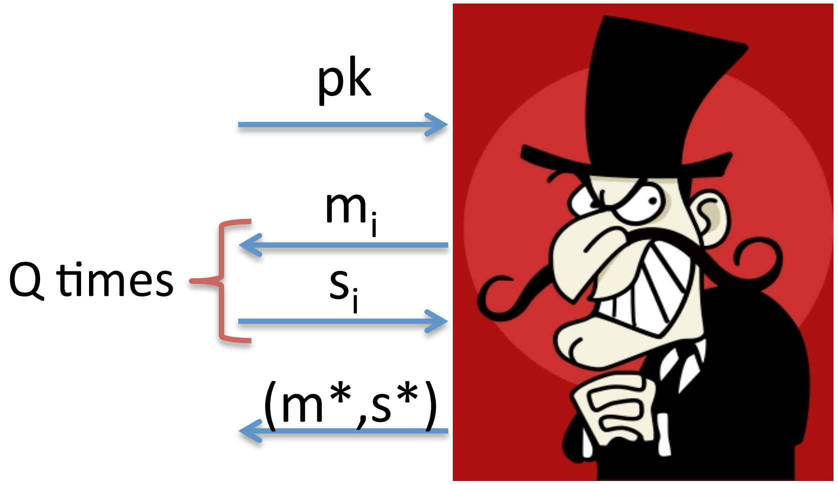
Key Exchange
- Bader, Hofheinz, Jager, Kiltz, Li (TCC 2015)

Which **properties** must a cryptosystem (not) have to allow for a **tight security** proof?

Coron's Result* (1/2)

(Eurocrypt 2002)

- Digital signatures
  - **single-user** setting
  - **unique** signatures**



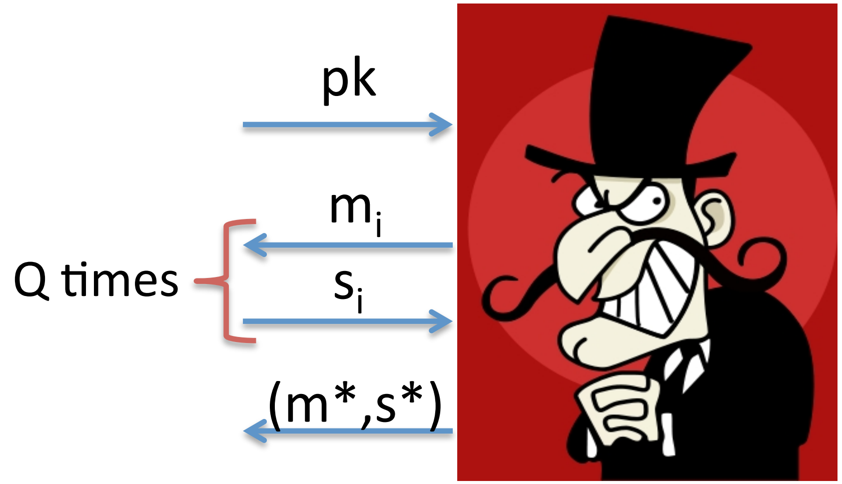
* see also Kakvi and Kiltz, Eurocrypt 2012

** generalized to re-randomizable signatures by Hofheinz et al., PKC 2012

Coron's Result* (1/2)

(Eurocrypt 2002)

- Digital signatures
  - **single-user** setting
  - **unique** signatures**

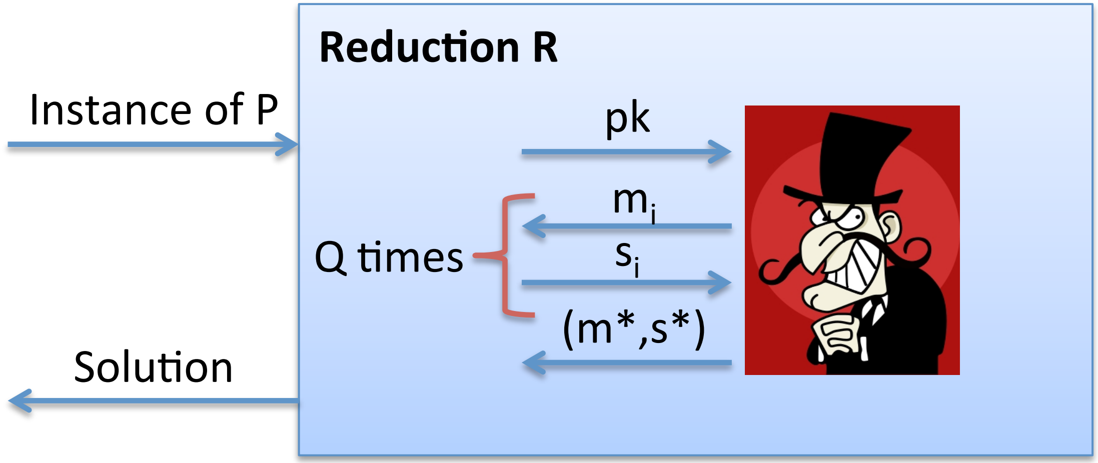


Result:
If a signature scheme has **unique signatures**, then any security reduction "loses" a factor of at least 1/Q.

* see also Kakvi and Kiltz, Eurocrypt 2012
** generalized to re-randomizable signatures by Hofheinz et al., PKC 2012

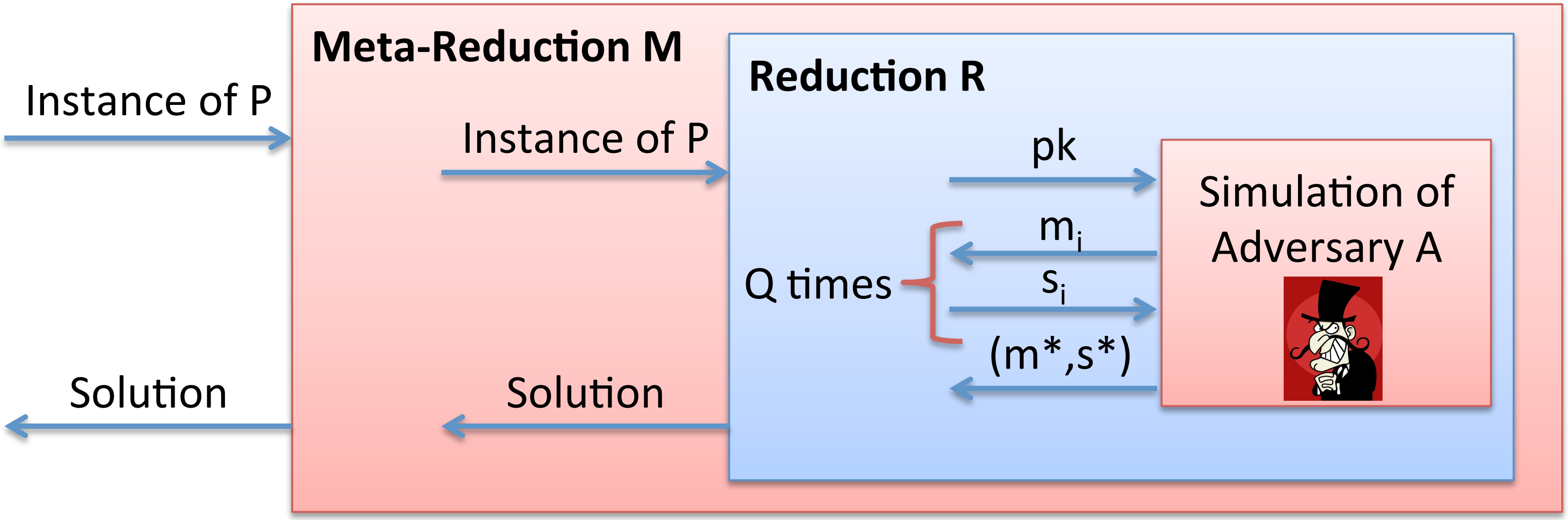
Coron's Result (2/2)

(Eurocrypt 2002)



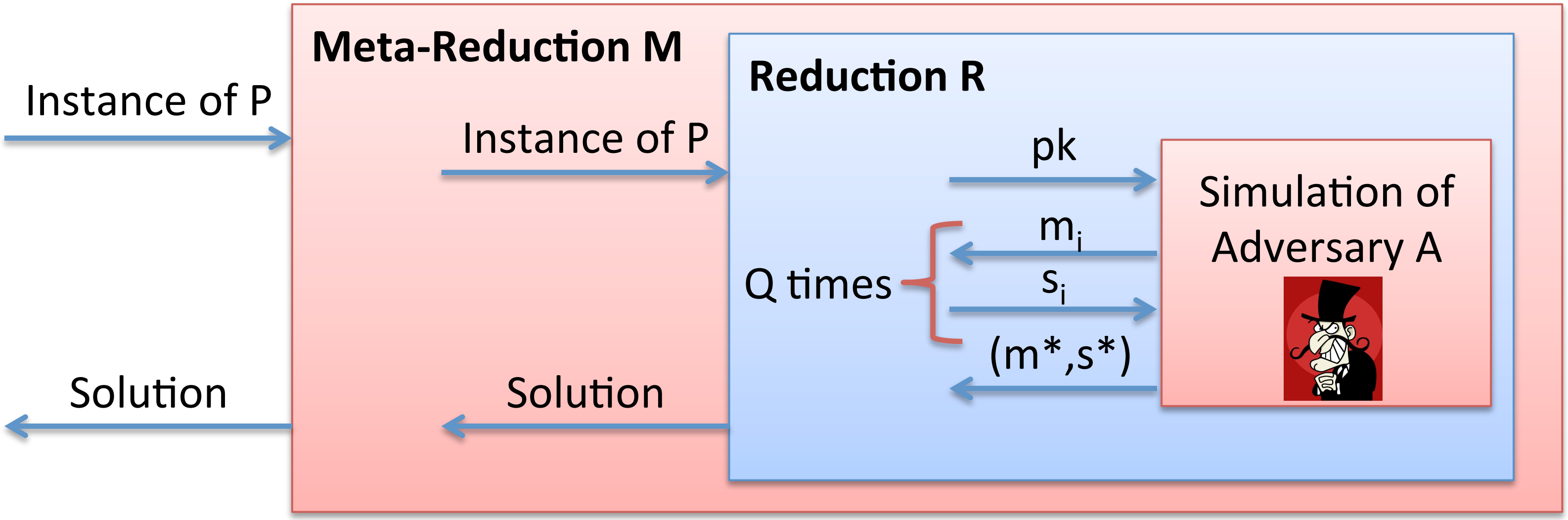
Coron's Result (2/2)

(Eurocrypt 2002)



Coron's Result (2/2)

(Eurocrypt 2002)



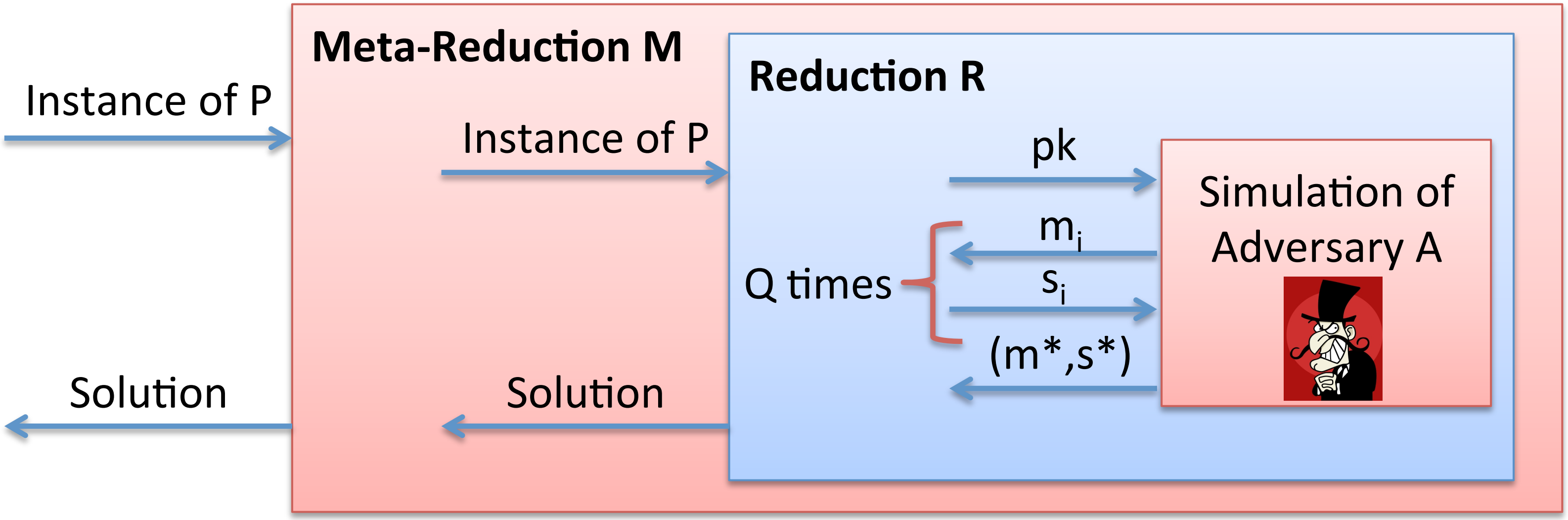
Coron shows:

If a signature scheme has **unique signatures**, then any reduction **R implies an algorithm M that solves P**

- In time $t_M \approx t_R$
- With $\epsilon_M \geq \epsilon_R - \frac{1}{Q}$

Coron's Result (2/2)

(Eurocrypt 2002)



Coron shows:

If a signature scheme has **unique signatures**, then any reduction **R implies an algorithm M that solves P**

- In time $t_M \approx t_R$
- With $\epsilon_M \geq \epsilon_R - \frac{1}{Q} \cdot \boxed{\left(1 - \frac{Q}{|\mathrm{MsgSpace}|}\right)^{-1}}$

"Annoying term"

Limitations of Coron‘s Technique

- **Restricted but reasonable** class of reductions:
  - Treat adversary A as a **black-box**
  - Few advanced capabilities (e.g. seq. rewinding)
- Relatively **complex analysis**

Limitations of Coron's Technique

- **Restricted but reasonable** class of reductions:
  - Treat adversary A as a **black-box**
  - Few advanced capabilities (e.g. seq. rewinding)
- Relatively **complex analysis**

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{Q} \boxed{\cdot \left(1 - \frac{Q}{|\mathsf{MsgSpace}|}\right)^{-1}}$$

"Annoying term"

- Only useful in settings where **Q << |MsgSpace|**
  - Acceptable for [C`02, KK`12, HJK`12]
  - Makes **application to other settings difficult**

Multi-User Security of Signatures

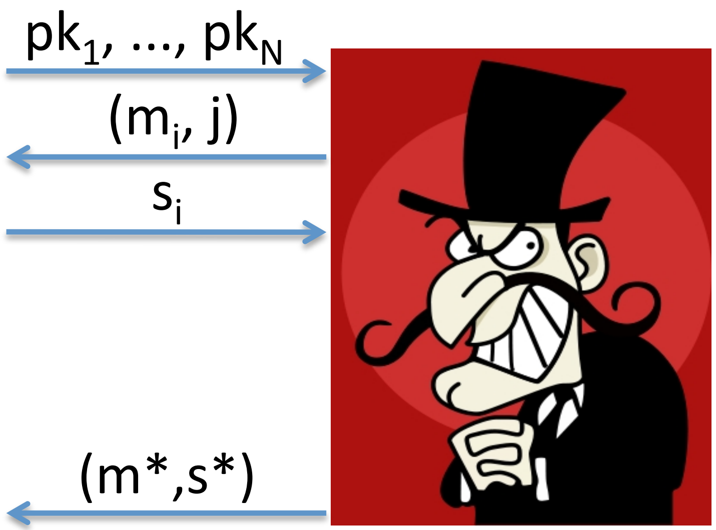
- A receives **N public keys**

$pk_1, \ldots, pk_N$

(m^*, s^*)

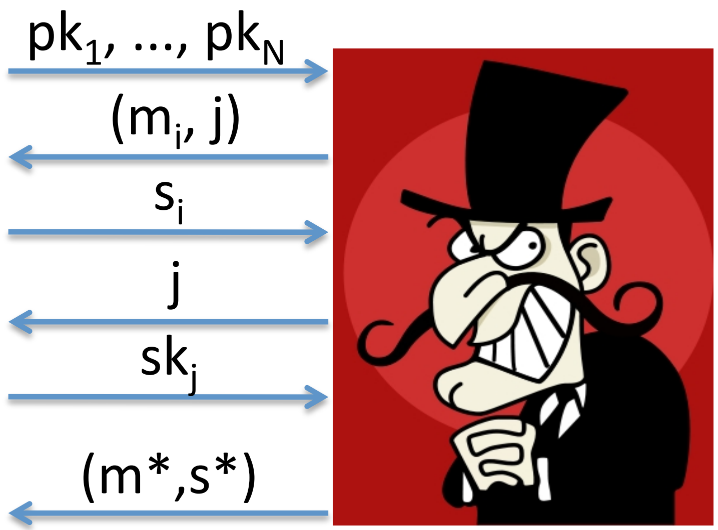
Multi-User Security of Signatures

- A receives **N public keys**
- Q signature queries



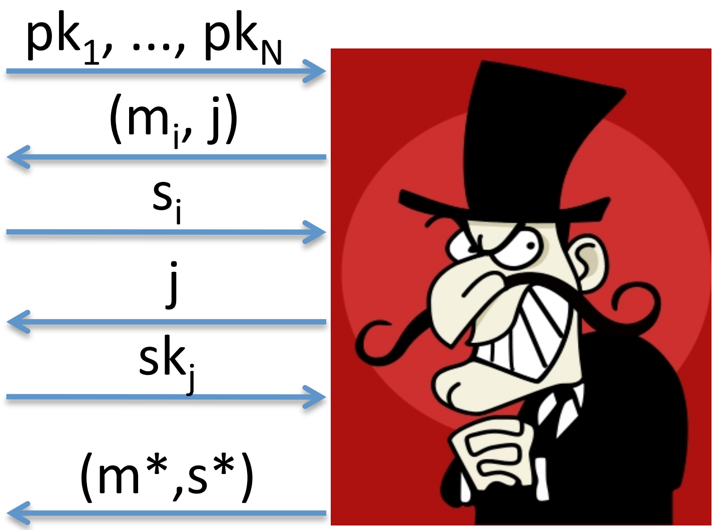
Multi-User Security of Signatures

- A receives **N public keys**
- Q signature queries
- Corrupt N-1 users



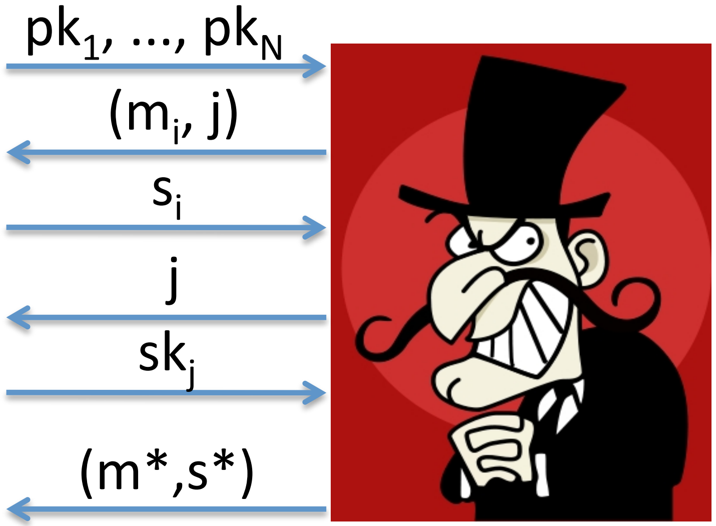
Multi-User Security of Signatures

- A receives **N public keys**
- Q signature queries
- Corrupt N-1 users
- <u>Desired:</u> **tight security** in
  - Number of signatures Q
  - Number of public keys N



Multi-User Security of Signatures

- A receives **N public keys**
- Q signature queries
- Corrupt N-1 users
- Desired: **tight security** in
  - Number of signatures Q
  - Number of public keys N



Single-user security ⇒ multi-user security

But the reduction is **not tight**, loses a factor 1/N

Applying Coron's technique to the multi-user setting

- To show that this loss is impossible to avoid:

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N}$$

Applying Coron's technique to the multi-user setting

- To show that this loss is impossible to avoid:

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N}$$

- Applying [Coron 2002], we get

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N} \boxed{\cdot \left(1 - \frac{N-1}{N}\right)^{-1}}$$

Applying Coron's technique to the multi-user setting

- To show that this loss is impossible to avoid:

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N}$$

- Applying [Coron 2002], we get

$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N} \cdot \overbrace{\boxed{\left(1 - \frac{N-1}{N}\right)^{-1}}}^{\text{Equal to N}}$$

Trivial bound, because of the "annoying term"

Our approach

<u>Goal:</u> Prove that 1/N-loss is impossible to avoid

1. Define a *weaker* security definition
   – **Counterintuitive:** Should be **more difficult** to prove impossibility of tight reductions!
2. New meta-reduction technique
   – No "annoying term"
   – Weakness of security definitions enables **simple and clean** analysis
3. **Generalize** this technique to other primitives

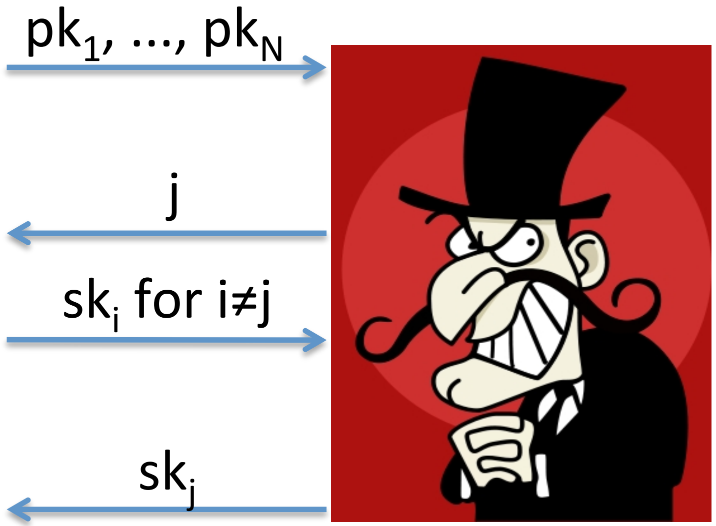
Our approach

<u>Goal:</u> Prove that 1/N-loss is impossible to avoid

1. Define a *weaker* security definition
   – **Counterintuitive:** Should be **more difficult** to prove impossibility of tight reductions!
2. New meta-reduction technique
   – No "annoying term"
   – Weakness of security definitions enables **simple and clean** analysis
3. **Generalize** this technique to other primitives

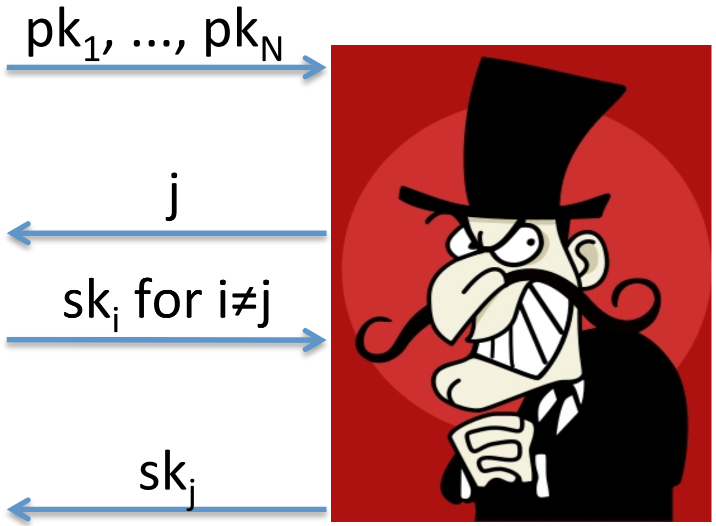
Weak Multi-User Security

- A receives N public keys
- Corrupt users
- ~~Signature queries~~
- A has to compute sk_j



Weak Multi-User Security

- A receives N public keys
- Corrupt users
- ~~Signature queries~~
- A has to compute sk_j



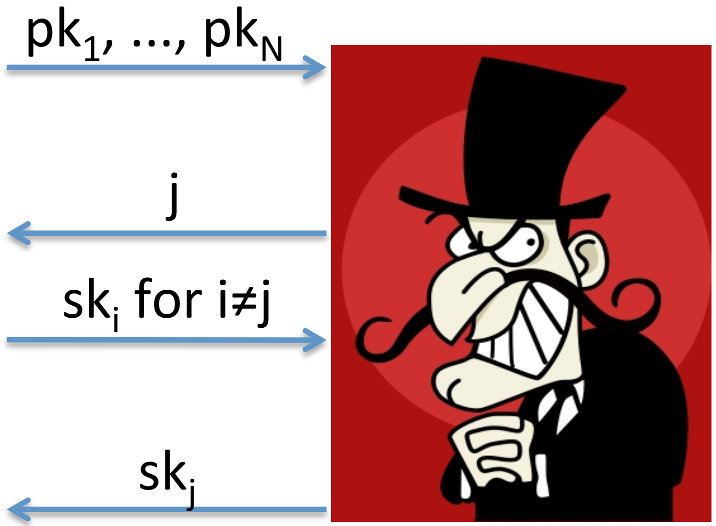
No tight security proof for “weak” security

$\Rightarrow$

No tight security proof for any “stronger” notion

Weak Multi-User Security

- A receives N public keys
- Corrupt users
- ~~Signature queries~~
- <u>A has to compute sk_j</u>



No tight security proof for “weak” security
$\Rightarrow$
No tight security proof for any “stronger” notion

Makes sense for any public-key scheme!

Our approach

Goal: Prove that 1/N-loss is impossible to avoid

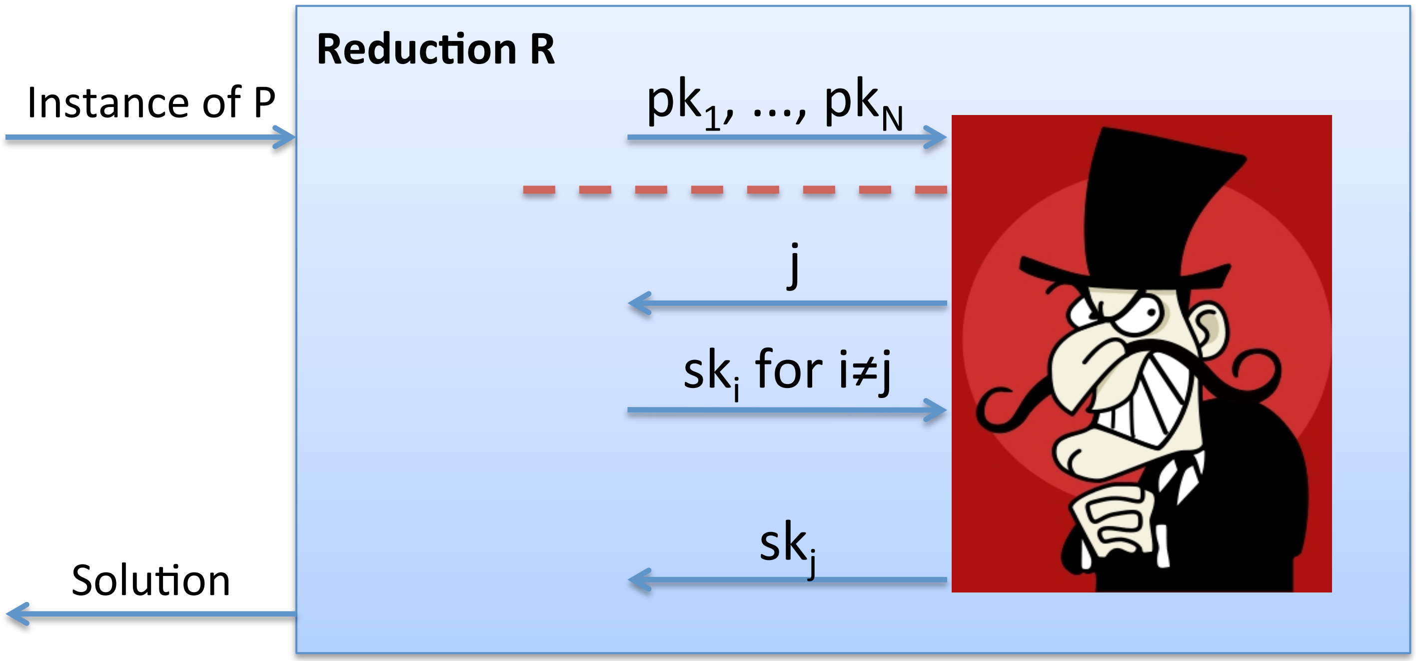
1. Define a *weaker* security definition
   - **Counterintuitive:** Should be **more difficult** to prove impossibility of tight reductions!
2. New meta-reduction technique
   - No “annoying term”
   - Weakness of security definitions enables **simple and clean** analysis
3. **Generalize** this technique to other primitives

Our result

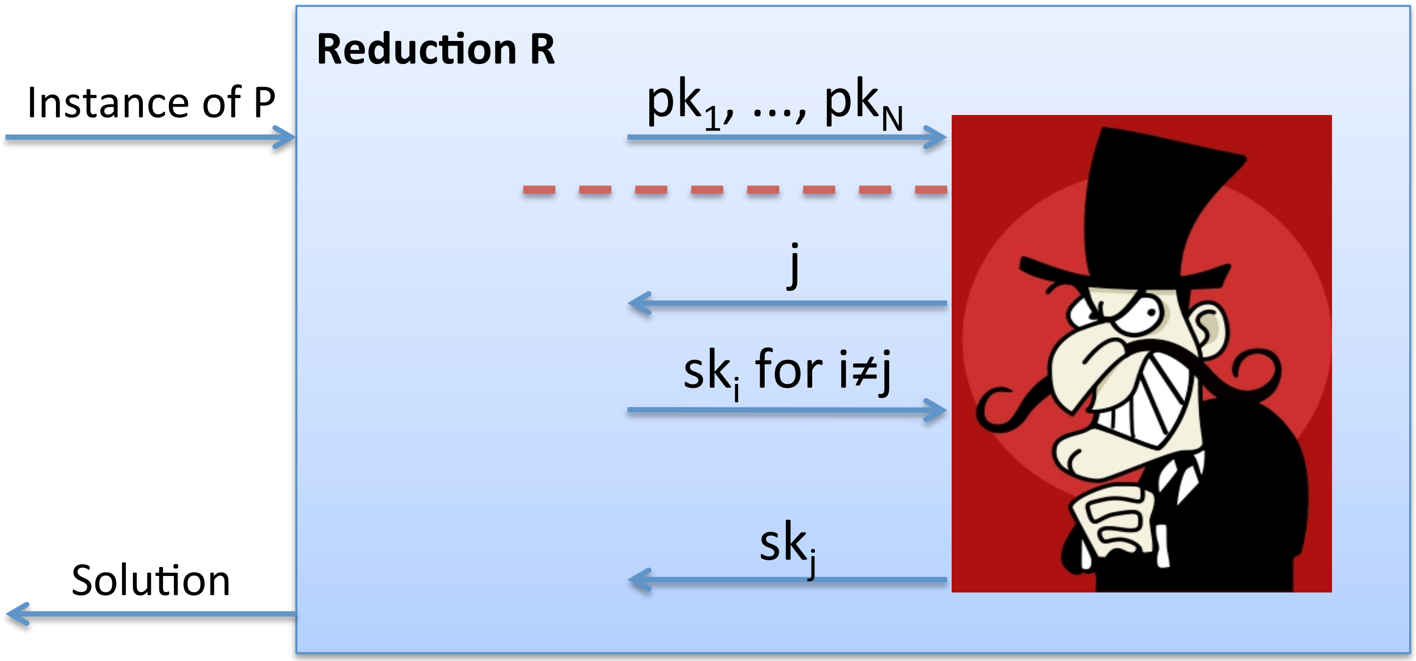
$$\epsilon_{\mathsf{M}} \geq \epsilon_{\mathsf{R}} - \frac{1}{N} \cdot \cancel{\left(1 + \frac{N-1}{N}\right)^{-1}}$$

- **Restricted but reasonable** class of reductions:
  - Use adversary A as a **black-box**
  - Few advanced capabilities (e.g. seq. rewinding)
- Relatively **simple analysis**

Tightness Bound: Intuition

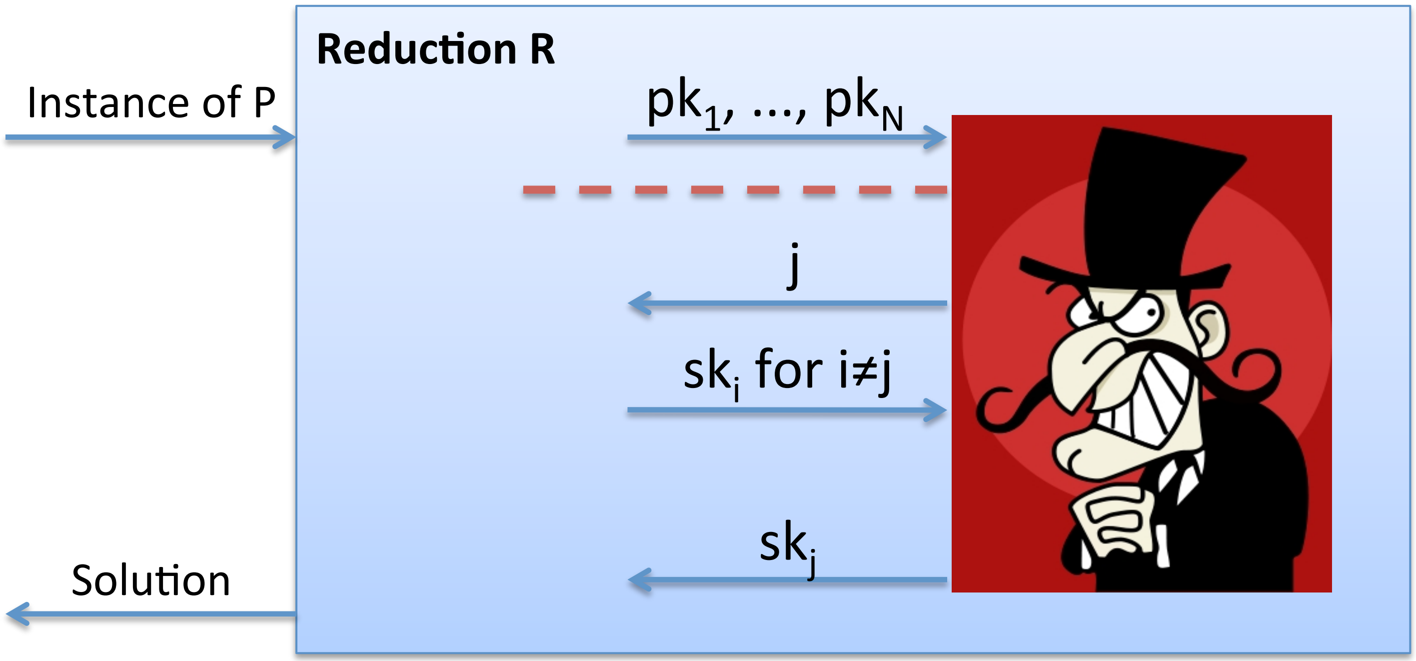


Tightness Bound: Intuition



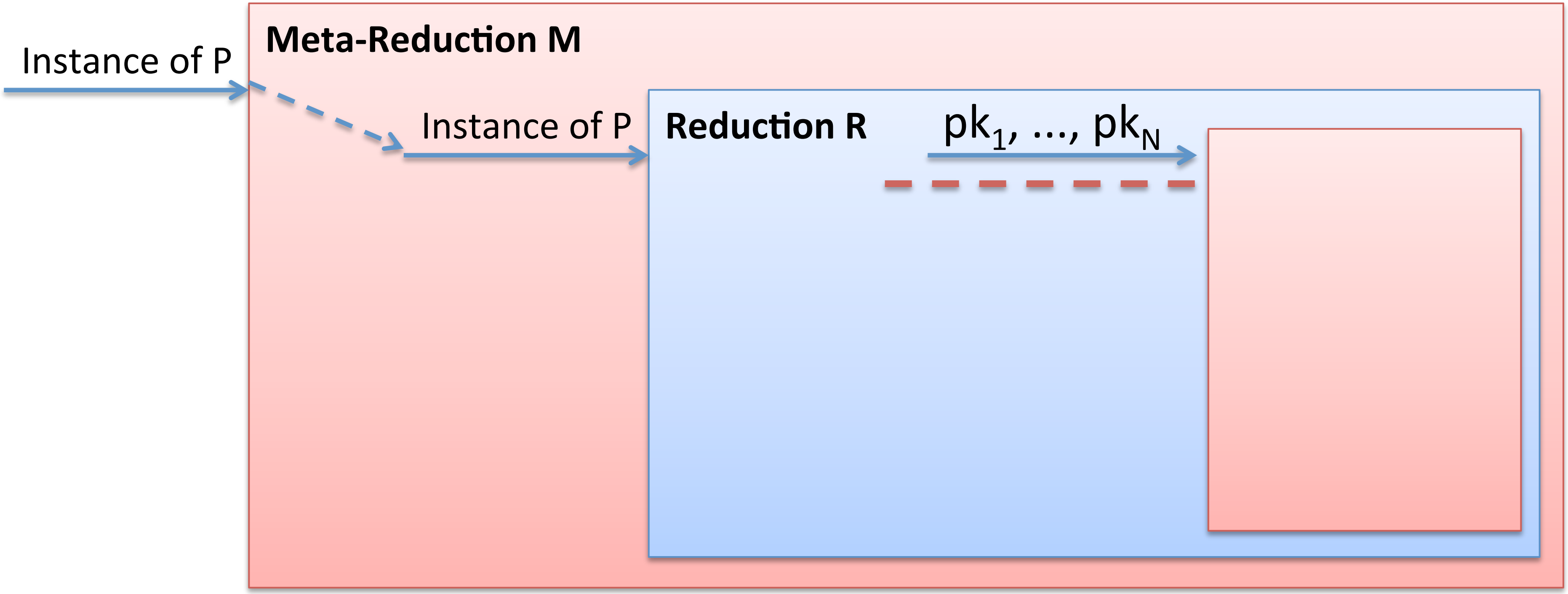
1. Only one index j such that R can output sk_i for all $i \neq j$
   ⇒ **R not tight!**
2. More than one j ⇒ **P not "hard"!**

Tightness Bound: Intuition



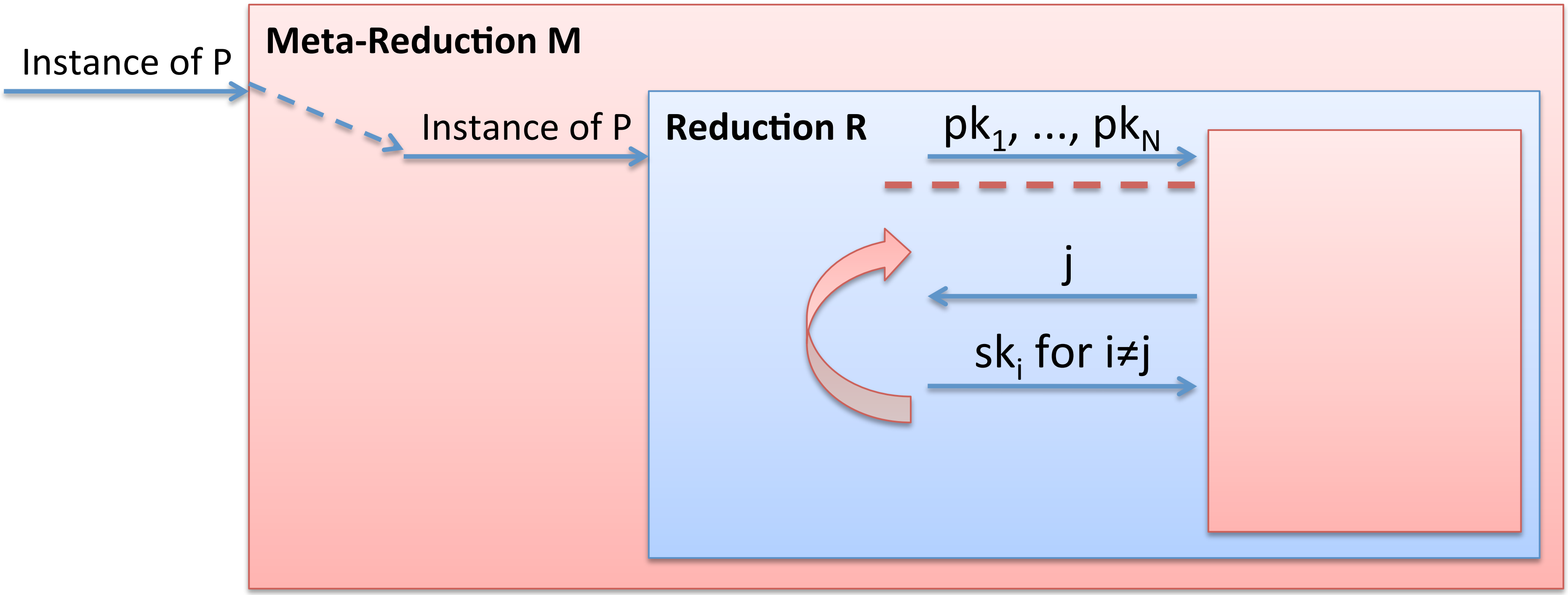
1. Only one index j such that R can output sk_i for all $i \neq j$
   ⇒ **R not tight!**
2. More than one j ⇒ **P not "hard"!**

Tightness Bound: Proof Sketch (1/2)



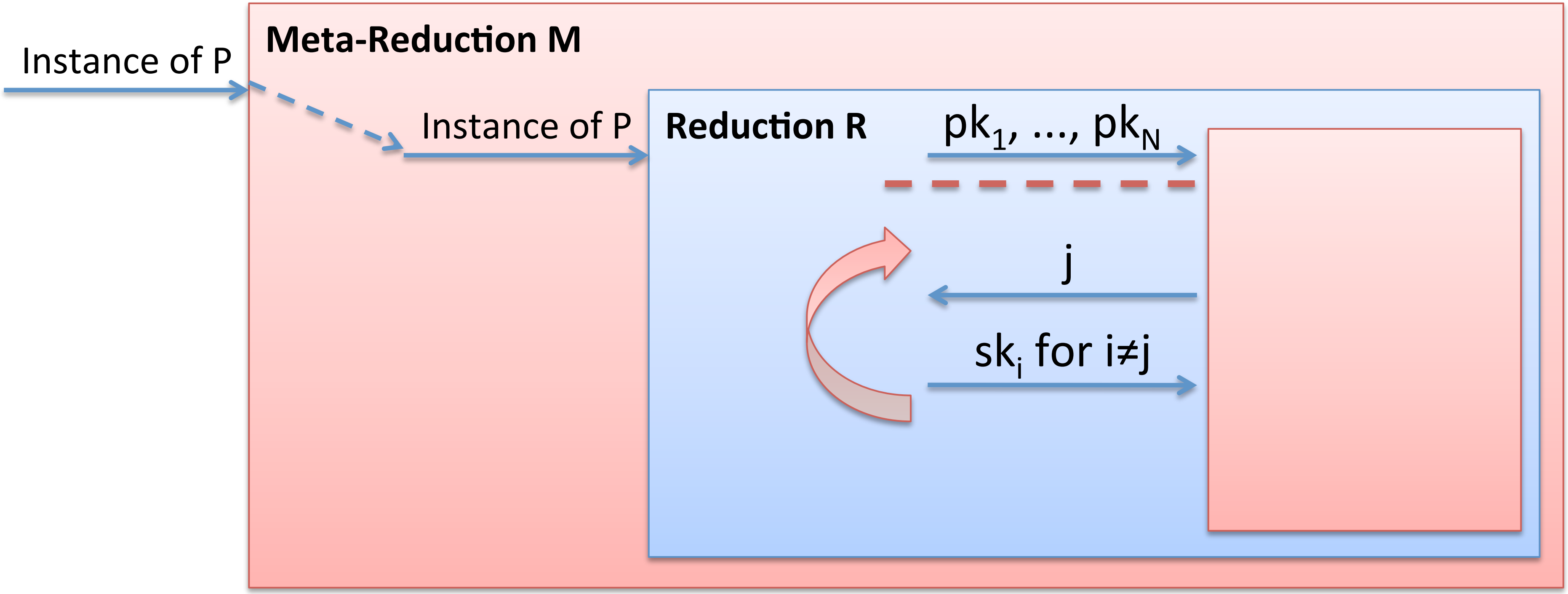
1. Run R until **right after** it outputs $pk_1, \ldots, pk_N$, **save the state** of R

Tightness Bound: Proof Sketch (1/2)



1. Run R until **right after** it outputs $pk_1, \ldots, pk_N$, **save the state** of R
2. Run R starting from this state **for all j from 1 to N**, until **R outputs the secret keys** sk_i for all i≠j

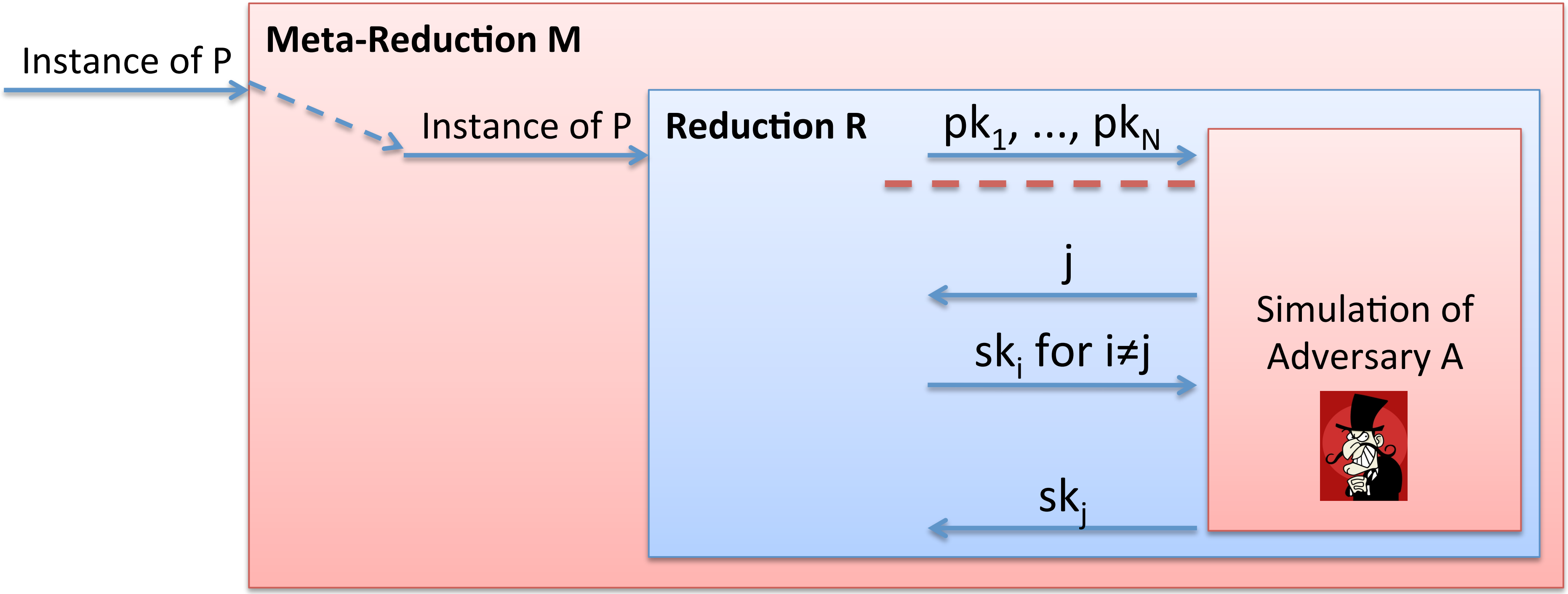
Tightness Bound: Proof Sketch (1/2)



1. Run R until **right after** it outputs $pk_1, \ldots, pk_N$, **save the state** of R
2. Run R starting from this state **for all j from 1 to N**, until **R outputs the secret keys** sk_i for all $i \neq j$

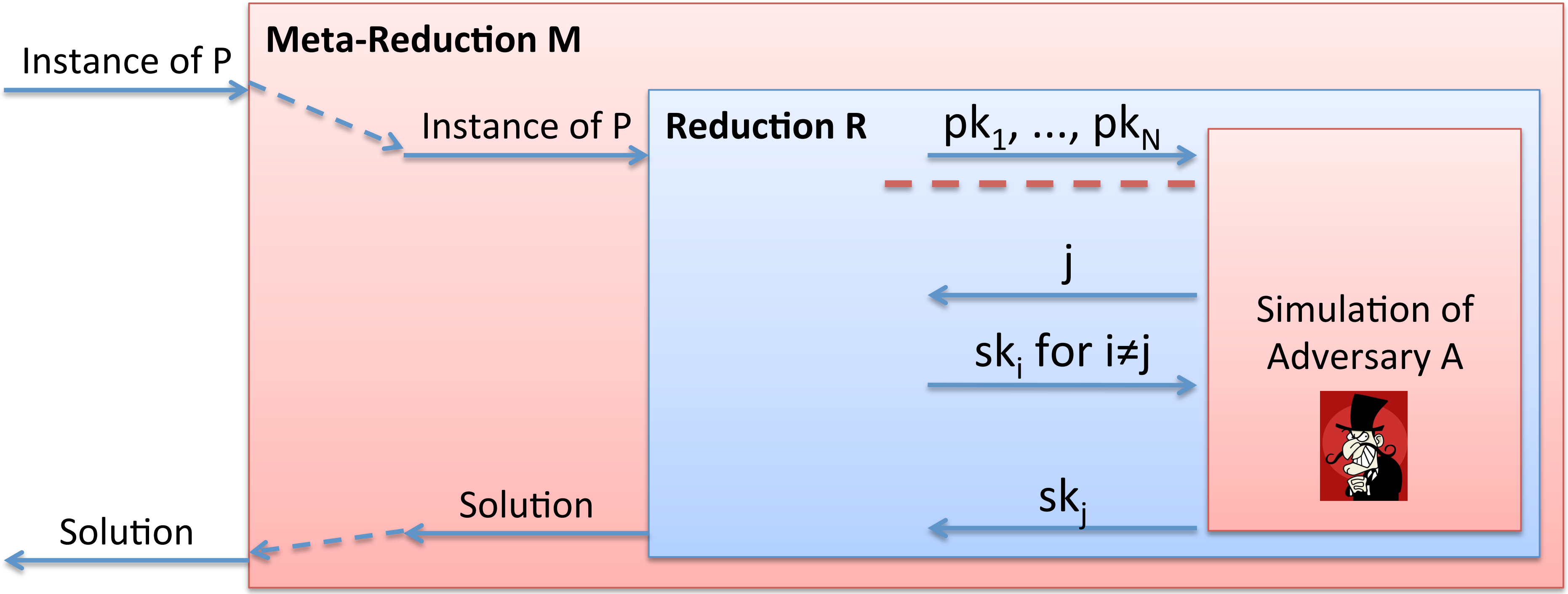
⇒ M learns **all** secret keys

Tightness Bound: Proof Sketch (2/2)



1. Execute R once again, starting from - - - -
2. Simulate A that chooses j uniformly random
3. Output sk_j

Tightness Bound: Proof Sketch (2/2)



1. Execute R once again, starting from - - - -
2. Simulate A that chooses j uniformly random
3. Output sk_j

Perfect simulation of a successful adversary

Requirements on the public-key scheme

- For each pk there is only one **unique** sk (*)
- One can **efficiently verify** that a given sk belongs to a given pk
- Holds for **many** known constructions

(* In the paper: generalized to re-randomizable keys)

Requirements on the public-key scheme

- For each pk there is only one **unique** sk (*)
- One can **efficiently verify** that a given sk belongs to a given pk
- Holds for **many** known constructions

Result:
A public-key scheme that satisfies the above conditions **cannot have a tight security proof** in the multi-user setting with corruptions.

(* In the paper: generalized to re-randomizable keys)

Our approach

<u>Goal:</u> Prove that 1/N-loss is impossible to avoid

1. Define a *weaker* security definition
   - **Counterintuitive:** Should be **more difficult** to prove impossibility of tight reductions!
2. New meta-reduction technique
   - No "annoying term"
   - Weakness of security definitions enables **simple and clean** analysis
3. **Generalize** this technique to other primitives

Goal: easy applicability

Generalized experiment

“Master theorem”

Multi-user security with corruptions

Strengthened versions of [C02, KK12, HJK12]

Security of non-interactive key exchange

Special cases

Generalization to Abstract Relations

$S = \{(x_1, w_1), (x_2, w_2), \ldots, (x_N, w_N)\}$

$x_1, \ldots, x_N$

j

w_i for $i \neq j$

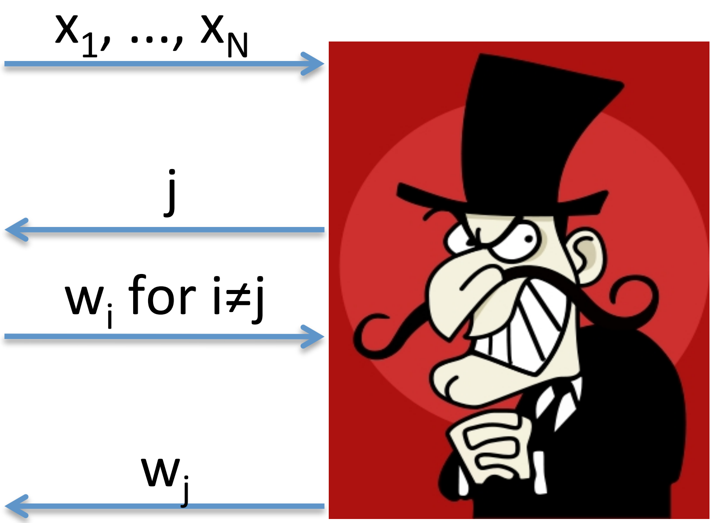
w_j

Requirements on S:

- Efficient **verifiability**
- For each statement x, the witness w is **unique** (or re-randomizable)

Generalization to Abstract Relations

$S = \{(x_1, w_1), (x_2, w_2), \ldots, (x_N, w_N)\}$



Requirements on S:

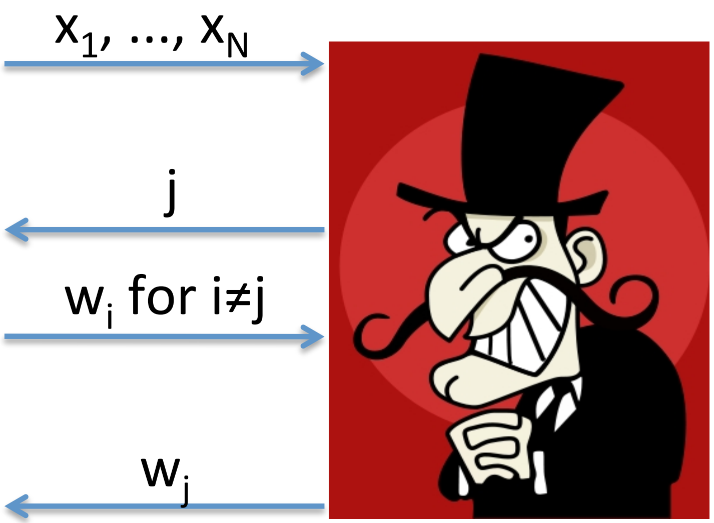
- Efficient **verifiability**
- For each statement x, the witness w is **unique** (or re-randomizable)

For example:

- Public key crypto in the multi-user setting:
  $S = \{(pk_1, sk_1), (pk_2, sk_2), \ldots, (pk_N, sk_N)\}$

Generalization to Abstract Relations

$S = \{(x_1, w_1), (x_2, w_2), \ldots, (x_N, w_N)\}$



Requirements on S:

- Efficient **verifiability**
- For each statement x, the witness w is **unique** (or re-randomizable)

For example:

- Public key crypto in the multi-user setting:
  $S = \{(pk_1, sk_1), (pk_2, sk_2), \ldots, (pk_N, sk_N)\}$
- Signatures in the single-user setting:
  $S = \{(m_1, s_1), (m_2, s_2), \ldots, (m_N, s_N)\}$

Summary

New techniques to prove **inexistence of tight reductions**

- **Stronger results** but **simpler proof**
- More **applications**
- **Easy to check** whether a construction can have a tight security proof
- **Easy to adapt** to other applications via generic "master theorem"

Summary

New techniques to prove **inexistence of tight reductions**

- **Stronger results** but **simpler proof**
- More **applications**
- **Easy to check** whether a construction can have a tight security proof
- **Easy to adapt** to other applications via generic "master theorem"

Thank you!