Quotable Signatures for Authenticating Shared Quotes

Joan Boyar[1] **Simon Erfurth**[1]
Kim S. Larsen[1] Ruben Niederhagen[1,2]

[1]University of Southern Denmark, Denmark

[2]Academia Sinica, Taiwan

Latincrypt 2023

✉ simon@serfurth.dk 🌐 www.serfurth.dk 🐦 @SimonErfurth

DDC
digital democracy centre

Motivating Example: Mitigating Fake News

Motivating Example: Mitigating Fake News

Problem

- More and more news are consumed on social media.
- Readers don't know source of news on social media.
- News media's reputation is an important heuristic.

Motivating Example: Mitigating Fake News

Problem

- More and more news are consumed on social media.
- Readers don't know source of news on social media.
- News media's reputation is an important heuristic.

We can use cryptography to fight this!

Motivating Example: Mitigating Fake News

Problem

- More and more news are consumed on social media.
- Readers don't know source of news on social media.
- News media's reputation is an important heuristic.

We can use cryptography to fight this!

Our idea: Add signatures to quotes.

Motivating Example: Mitigating Fake News

kilometer lang
26 stop underv
(Foto: © Tim Kil
Jensen, Ritzau S

LÆS OP ORDBOG TEKST

AF
Mona Aaberg

I GÅR KL. 12:00

Letbanen i Odense blev indviet tninger. Den skulle gøre det lettere at bruge offentlig trafik og binde b Share with signature en.

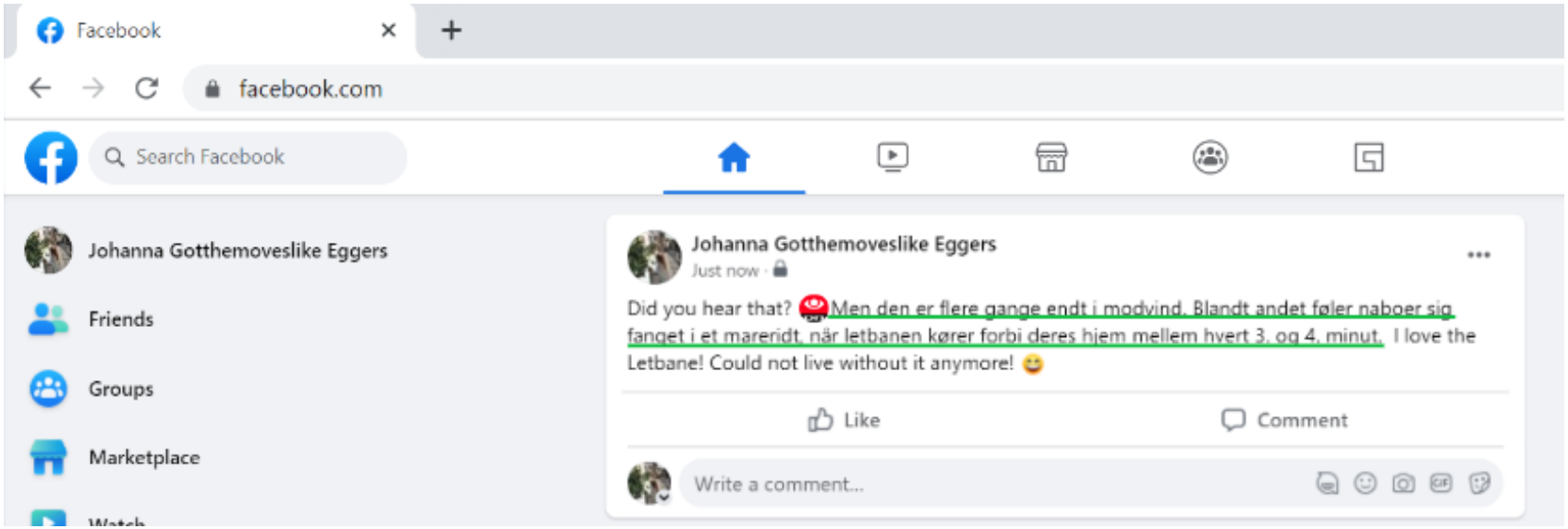
Men den er flere gange endt i modvind. Blandt andet føler naboer sig fanget i et mareridt, når letbanen kører forbi deres hjem mellem hvert 3. og 4. minut.

- Det er det, jeg kalder jetjageren, siger Gitte Hermansen.

I halvandet år har hun boet i et nyt boligkompleks med letbanen som nabo. Da hun og manden valgte den lejlighed, fik de fik at vide, at letbanen ville være næsten lydløs - en støj der blev beskrevet som lyden fra en elbil.

Men seks måneder efter det første tog kørte ud på skinnerne, er virkeligheden er en helt anden for naboerne til letbanen.

Motivating Example: Mitigating Fake News



Motivating Example: Mitigating Fake News

"German Institute claims there was fraud in the Brazilian election"

Motivating Example: Mitigating Fake News

"German Institute claims there was fraud in the Brazilian election"

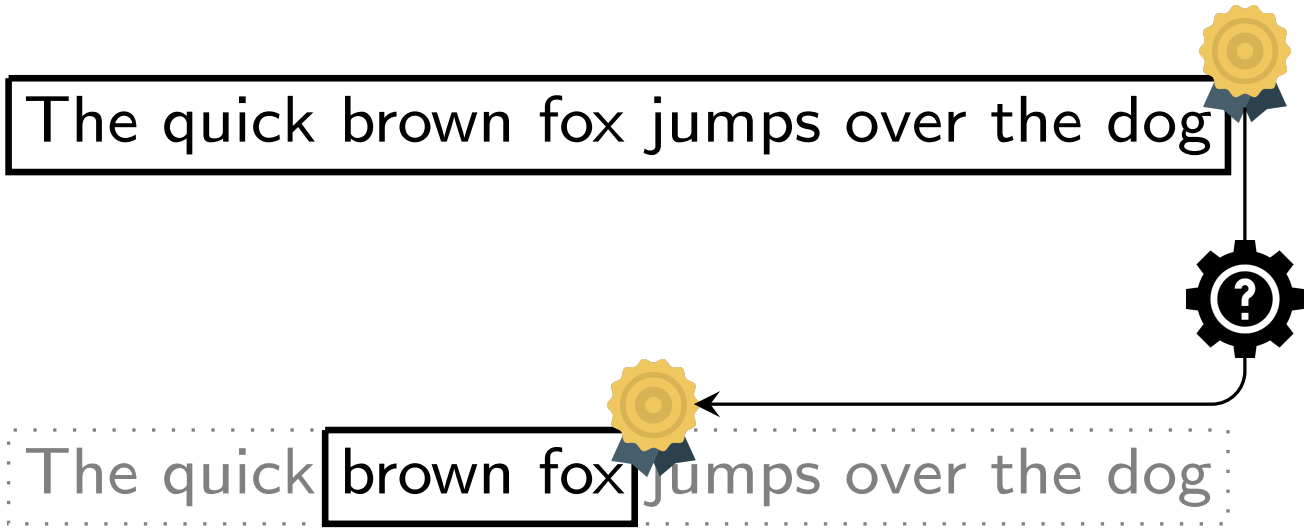
"Dr. Alter Mann mit Brille"

Quotable Signatures

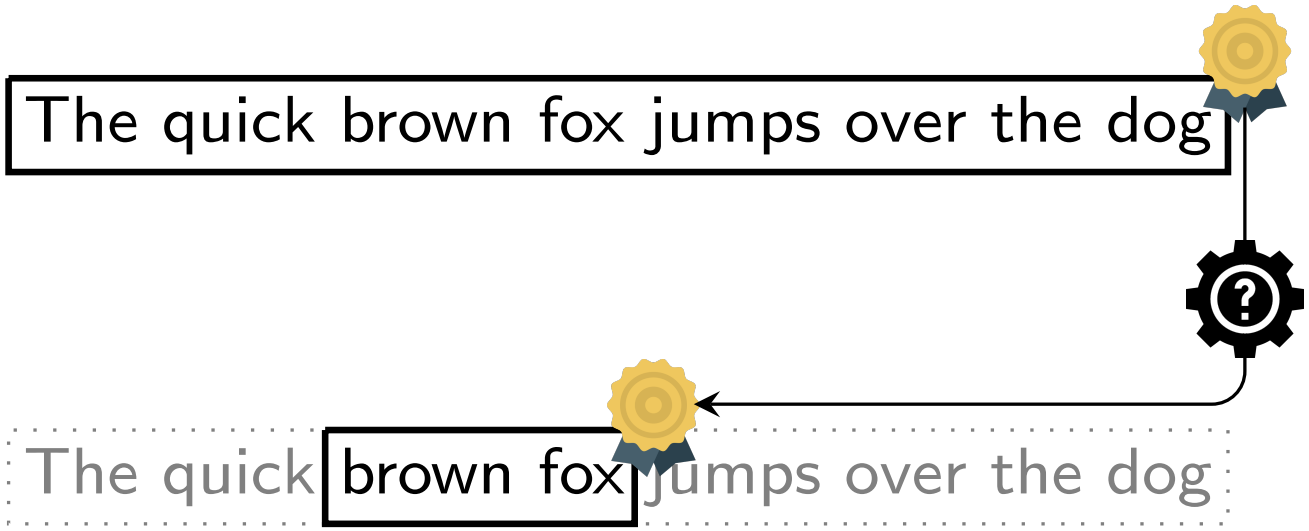
Quotable Signatures

Quotable Signatures

Quotable Signatures



Quotable Signatures



Goal

Create a quotable signature scheme (QSS) allowing extraction of signatures for quotes, *without knowing the secret key or interacting with the signer*.

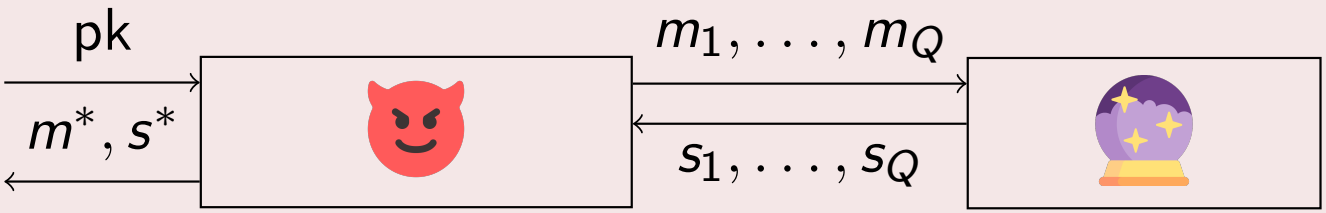
Security

QSS Unforgeability

A QSS is existentially unforgeable if no (PPT) adversary $(\mathsf{Adv}^{\mathcal{O}_{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}}(\mathsf{pk}))$, wins the QSS unforgeability game with non-negligible probability.

QSS Unforgeability Game

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}()$



if $(\mathsf{Ver}_{\mathsf{pk}}(m^*, s^*) = \top)$ and $(\forall k \in \{1, 2, \ldots, Q\} : m^* \not\preceq m_k)$

$\mathsf{Adv}^{\mathcal{O}_{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}}(\mathsf{pk})$ wins

Note: $m^* \preceq m$ means m^* is contained as a quote in m.

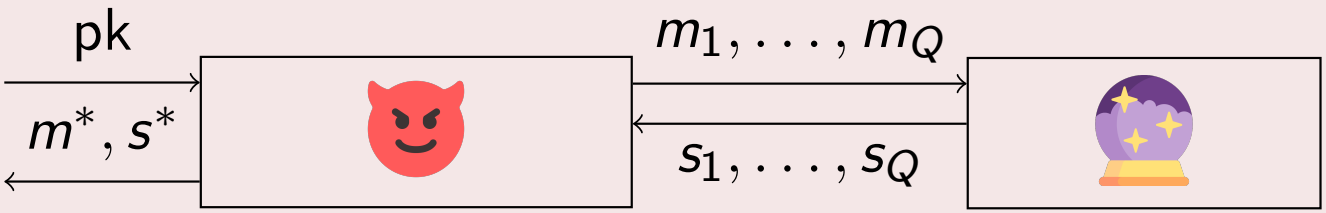
Security

QSS Unforgeability

A QSS is existentially unforgeable if no (PPT) adversary $(\mathsf{Adv}^{\mathcal{O}_{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}}(\mathsf{pk}))$, wins the QSS unforgeability game with non-negligible probability.

QSS Unforgeability Game

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}()$



if $(\mathsf{Ver}_{\mathsf{pk}}(m^*, s^*) = \top)$ and $(\forall k \in \{1, 2, \ldots, Q\} : m^* \not\preceq m_k)$

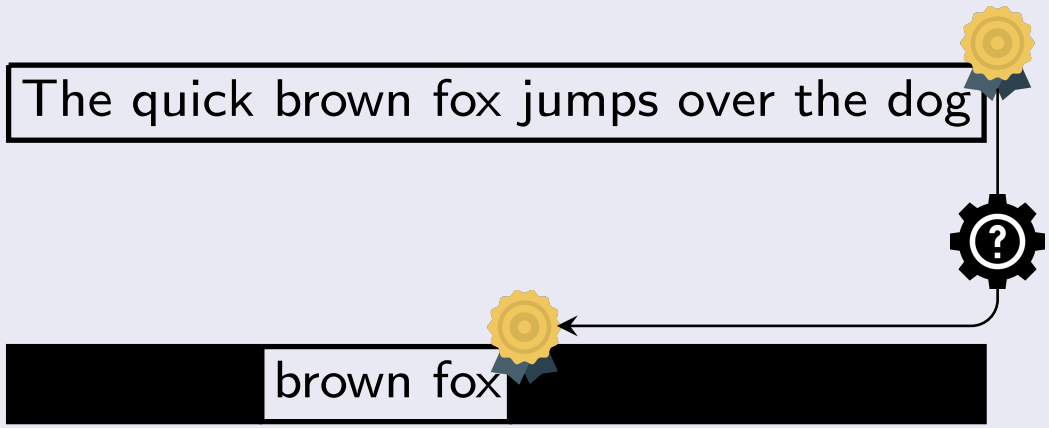
$\mathsf{Adv}^{\mathcal{O}_{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}}(\mathsf{pk})$ wins

Note: $m^* \preceq m$ means m^* is contained as a quote in m.

Related Work

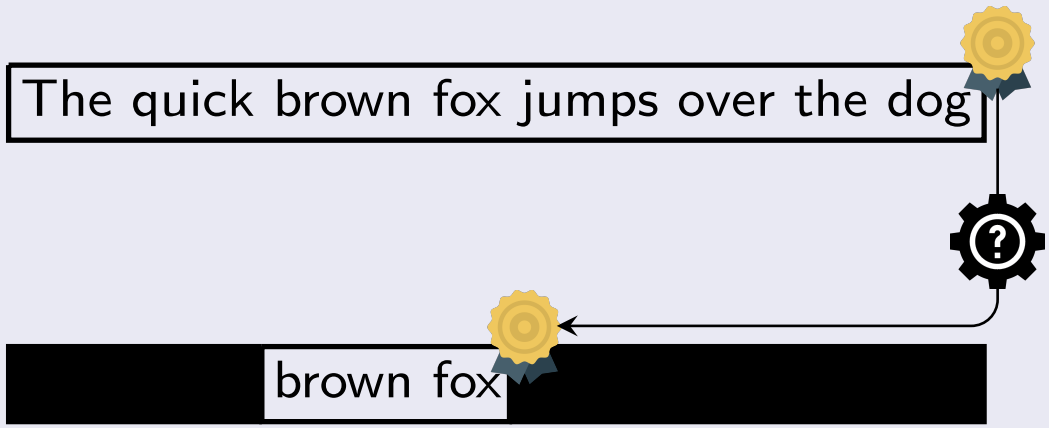
Related Work

Redactable Signature Schemes



Related Work

Redactable Signature Schemes

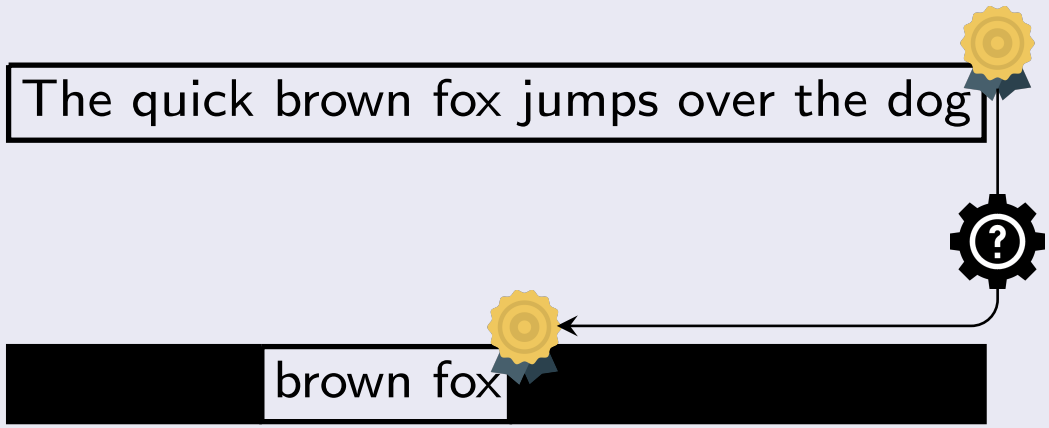


Kreutzer, Niederhagen, Shrishak, and Simo Fhom [KNSS19]

Introduces the idea of QSSs and for our construction.

Related Work

Redactable Signature Schemes



Kreutzer, Niederhagen, Shrishak, and Simo Fhom [KNSS19]

Introduces the idea of QSSs and for our construction.

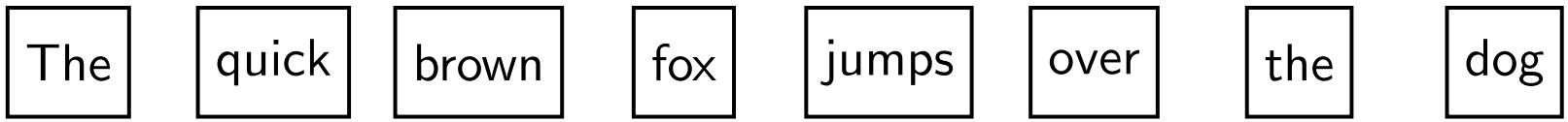
Our contributions

(1) Security notion, (2) Prove security and analyze complexity, (3) More efficient than RSSs, (4) Concrete algorithms.

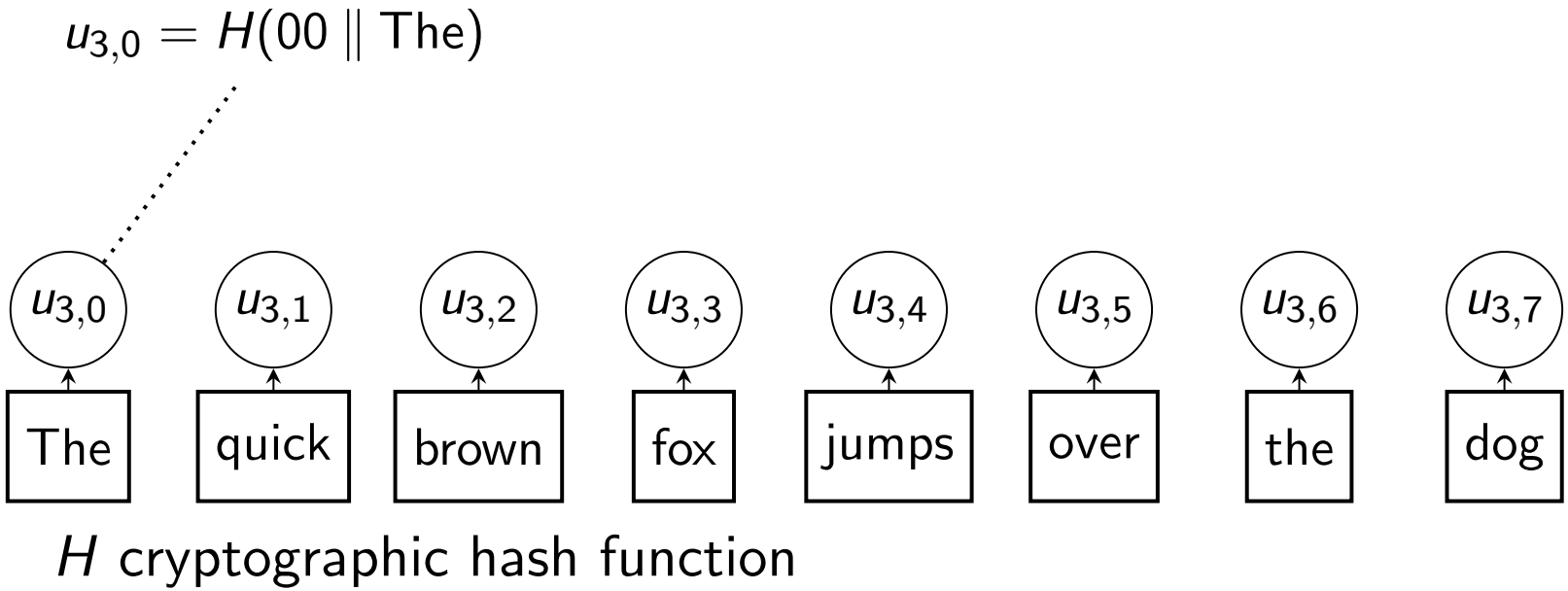
Construction

The quick brown fox jumps over the dog

Construction

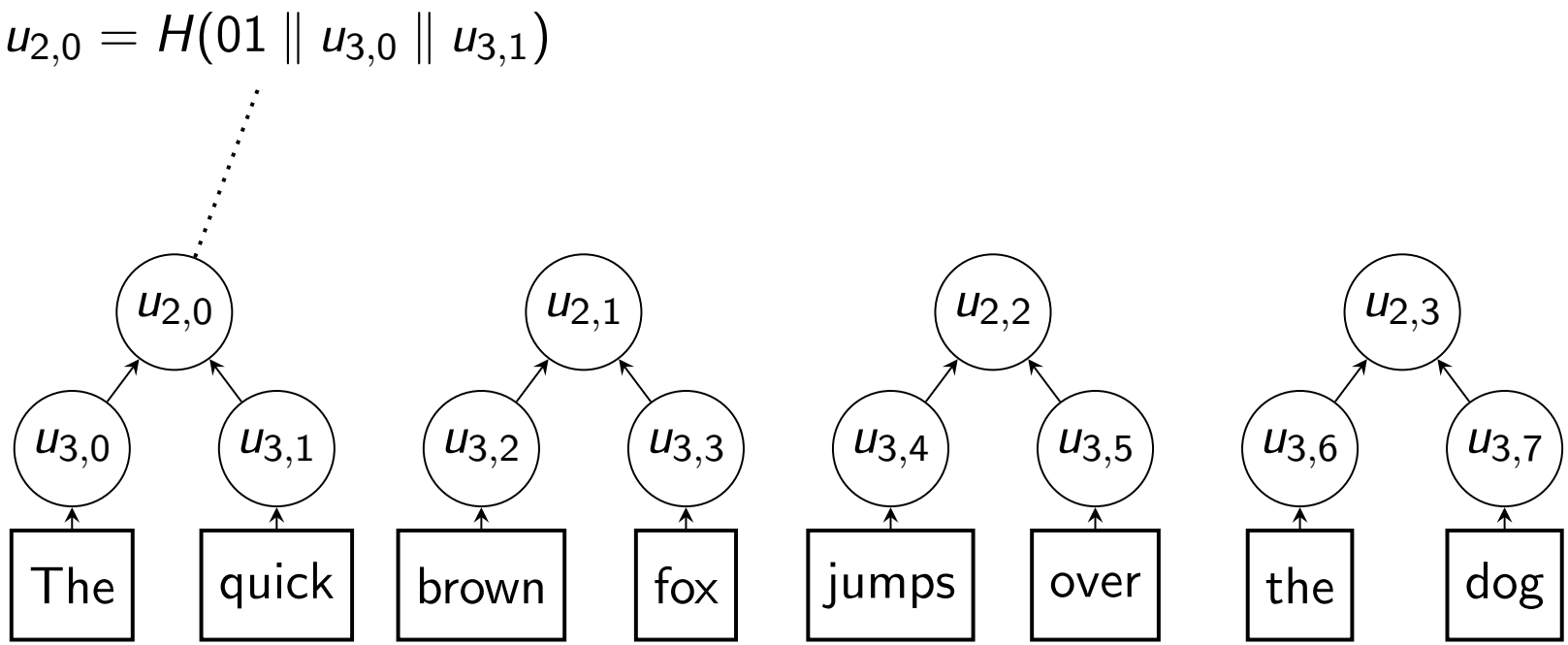


Construction



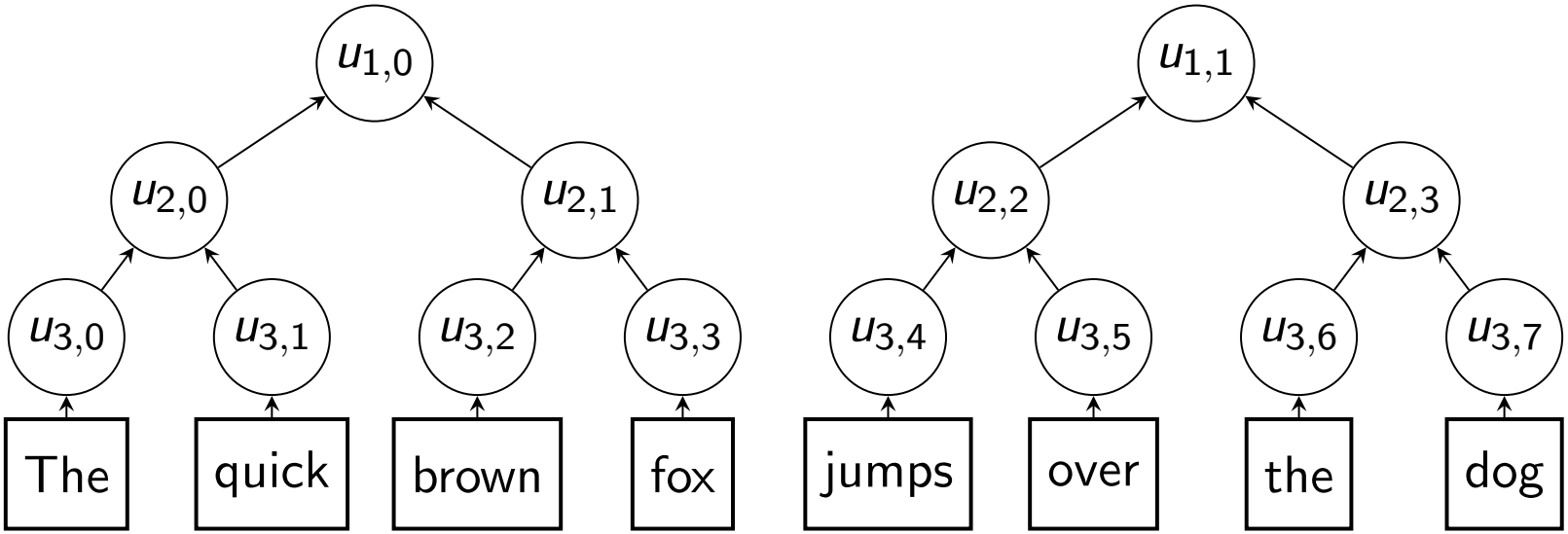
H cryptographic hash function

Construction



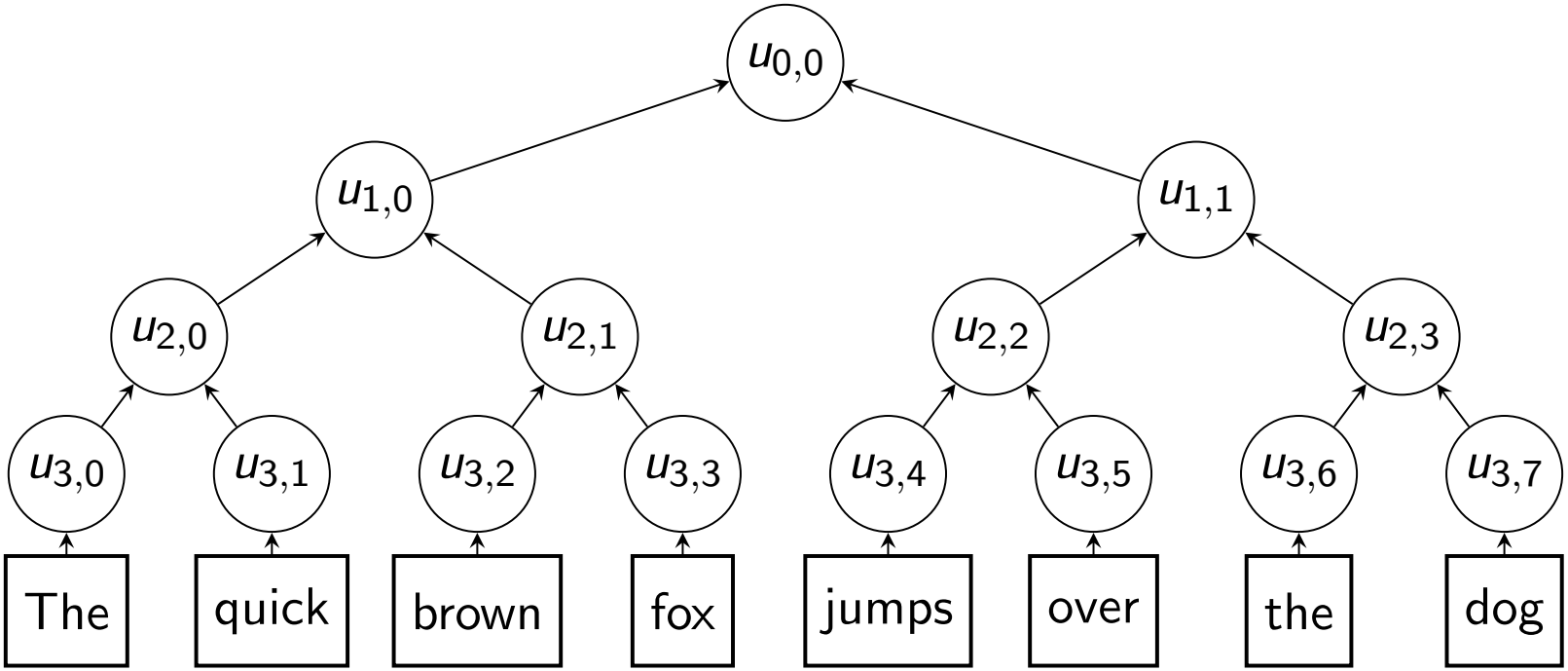
H cryptographic hash function

Construction



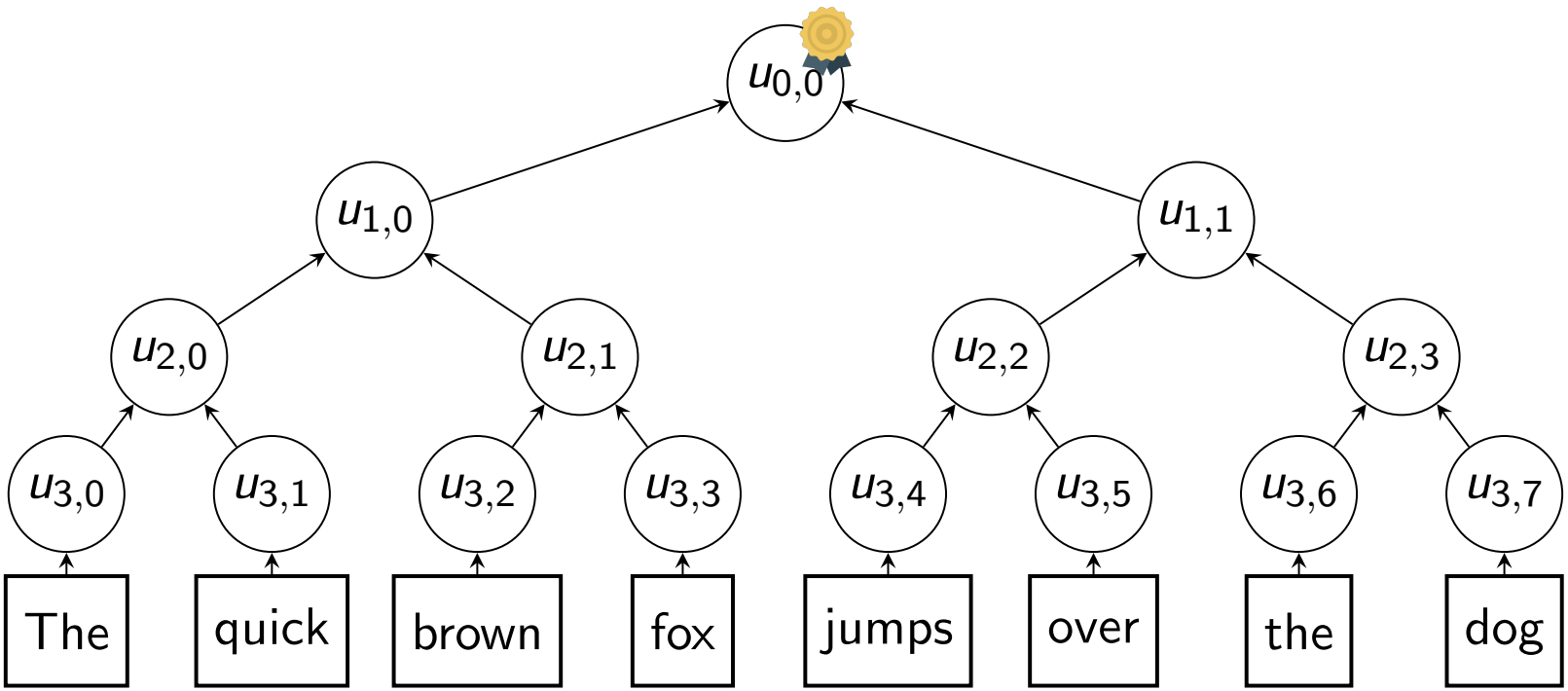
H cryptographic hash function

Construction



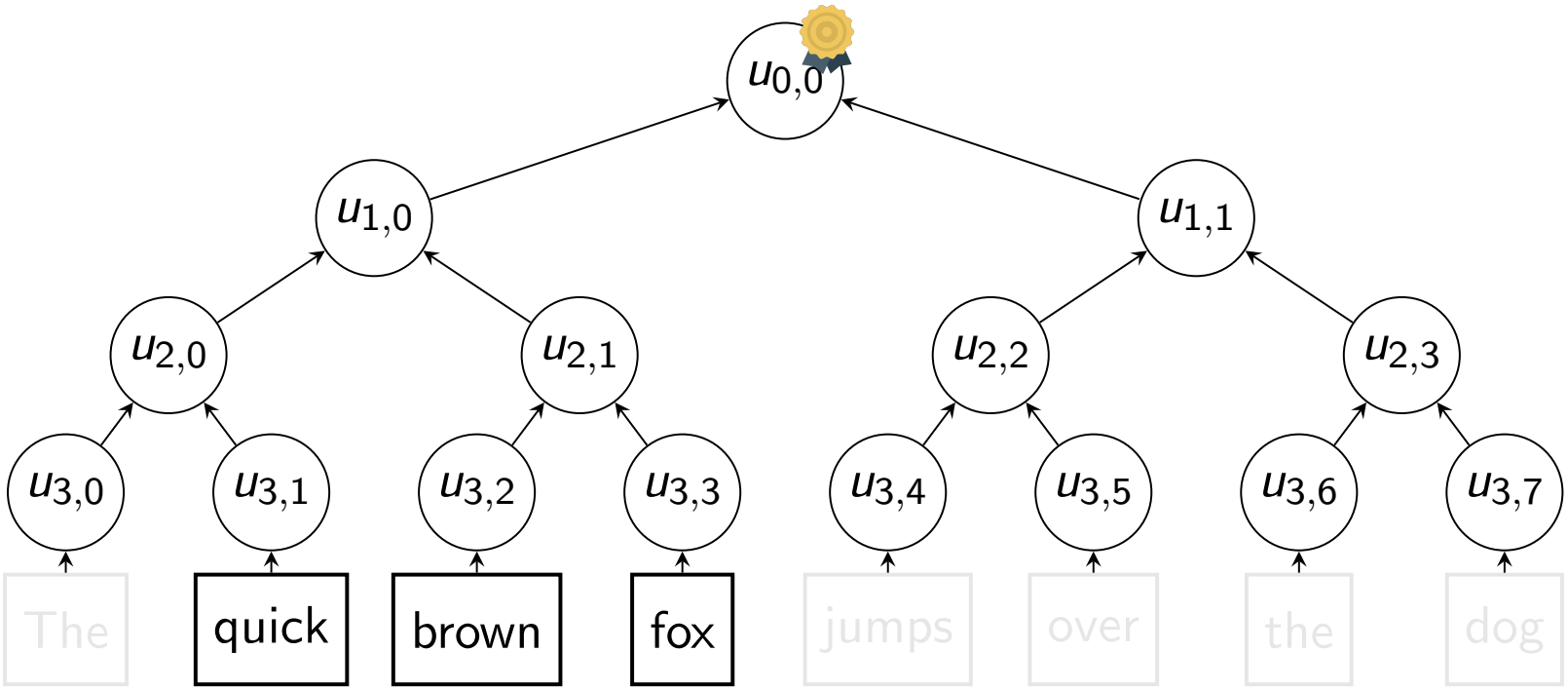
H cryptographic hash function

Construction

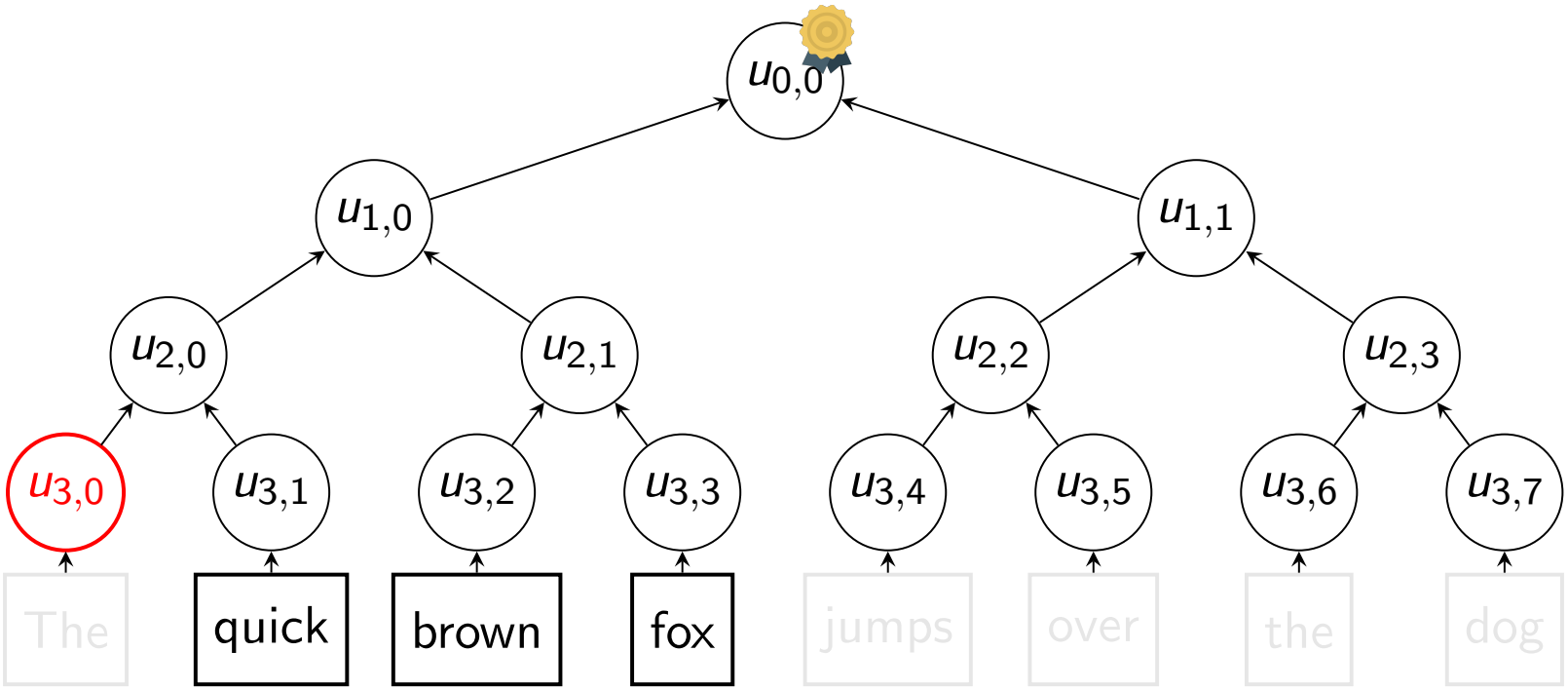


H cryptographic hash function, classic digital signature.

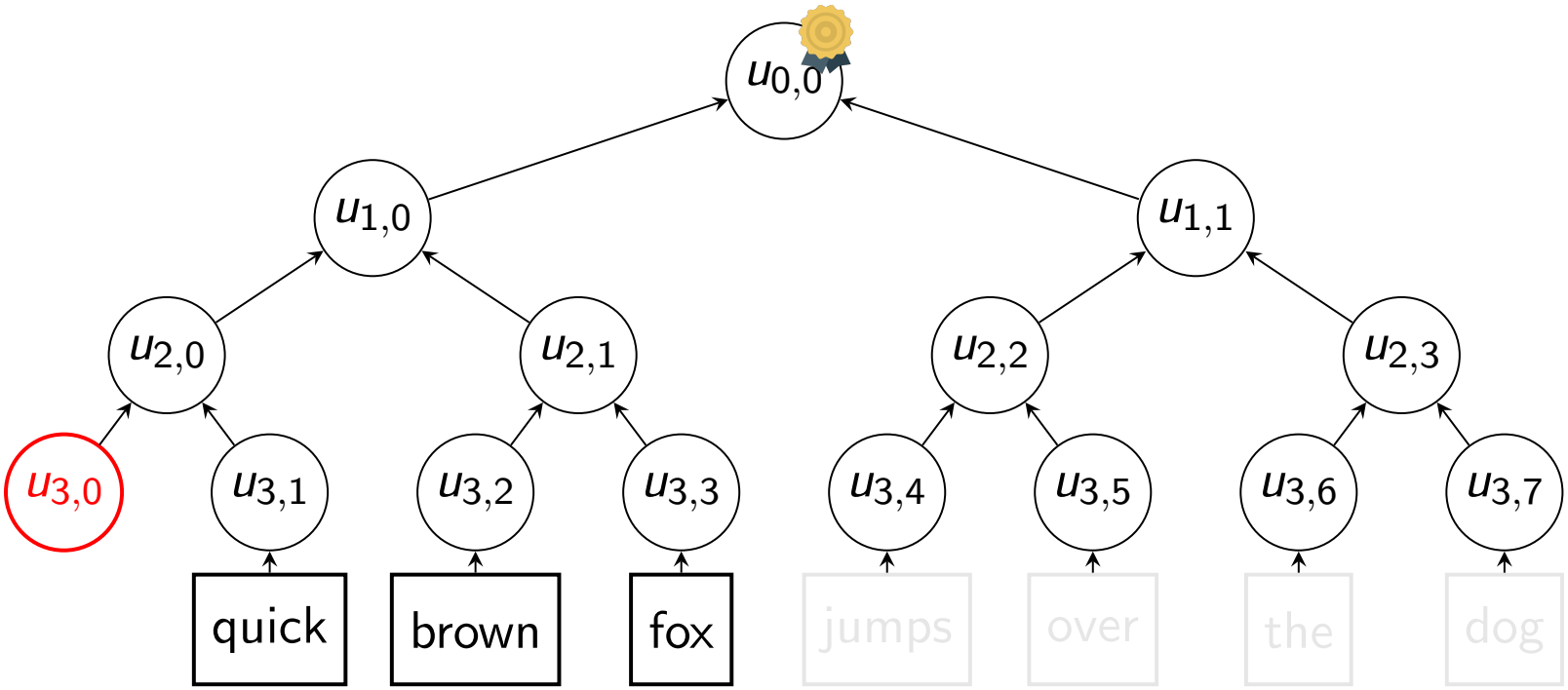
Quoting


$u_{0,0}$
$u_{1,0}$
$u_{1,1}$
$u_{2,0}$
$u_{2,1}$
$u_{2,2}$
$u_{2,3}$
$u_{3,0}$
$u_{3,1}$
$u_{3,2}$
$u_{3,3}$
$u_{3,4}$
$u_{3,5}$
$u_{3,6}$
$u_{3,7}$
The
quick
brown
fox
jumps
over
the
dog

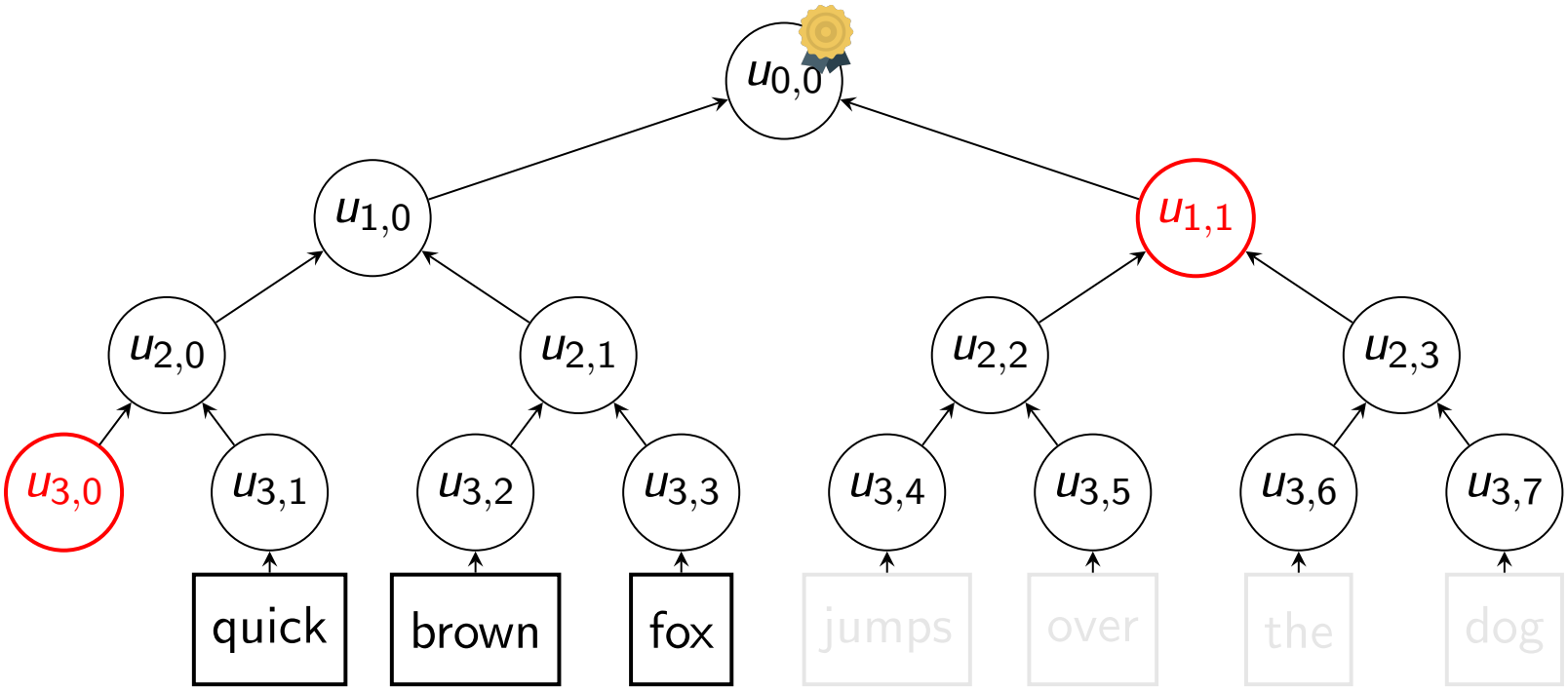
Quoting


$u_{0,0}$
$u_{1,0}$
$u_{1,1}$
$u_{2,0}$
$u_{2,1}$
$u_{2,2}$
$u_{2,3}$
$u_{3,0}$
$u_{3,1}$
$u_{3,2}$
$u_{3,3}$
$u_{3,4}$
$u_{3,5}$
$u_{3,6}$
$u_{3,7}$
The
quick
brown
fox
jumps
over
the
dog

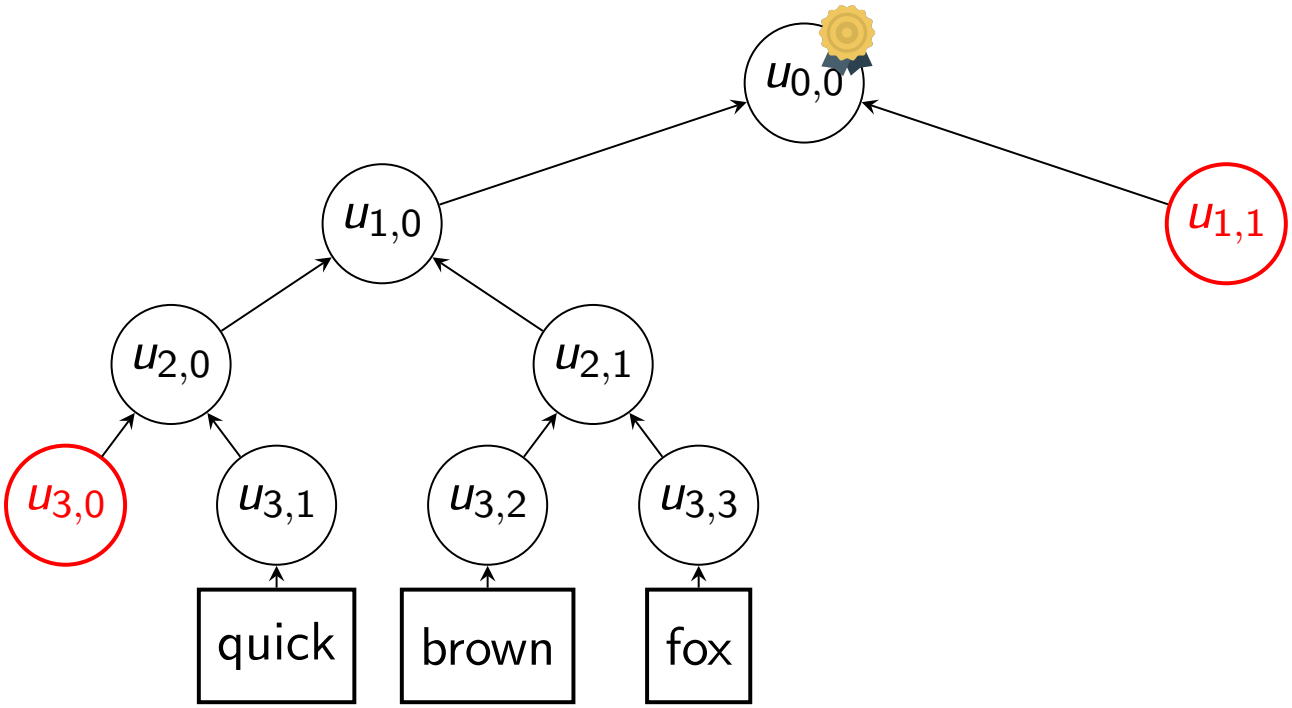
Quoting


$u_{0,0}$
$u_{1,0}$
$u_{1,1}$
$u_{2,0}$
$u_{2,1}$
$u_{2,2}$
$u_{2,3}$
$u_{3,0}$
$u_{3,1}$
$u_{3,2}$
$u_{3,3}$
$u_{3,4}$
$u_{3,5}$
$u_{3,6}$
$u_{3,7}$
quick
brown
fox
jumps
over
the
dog

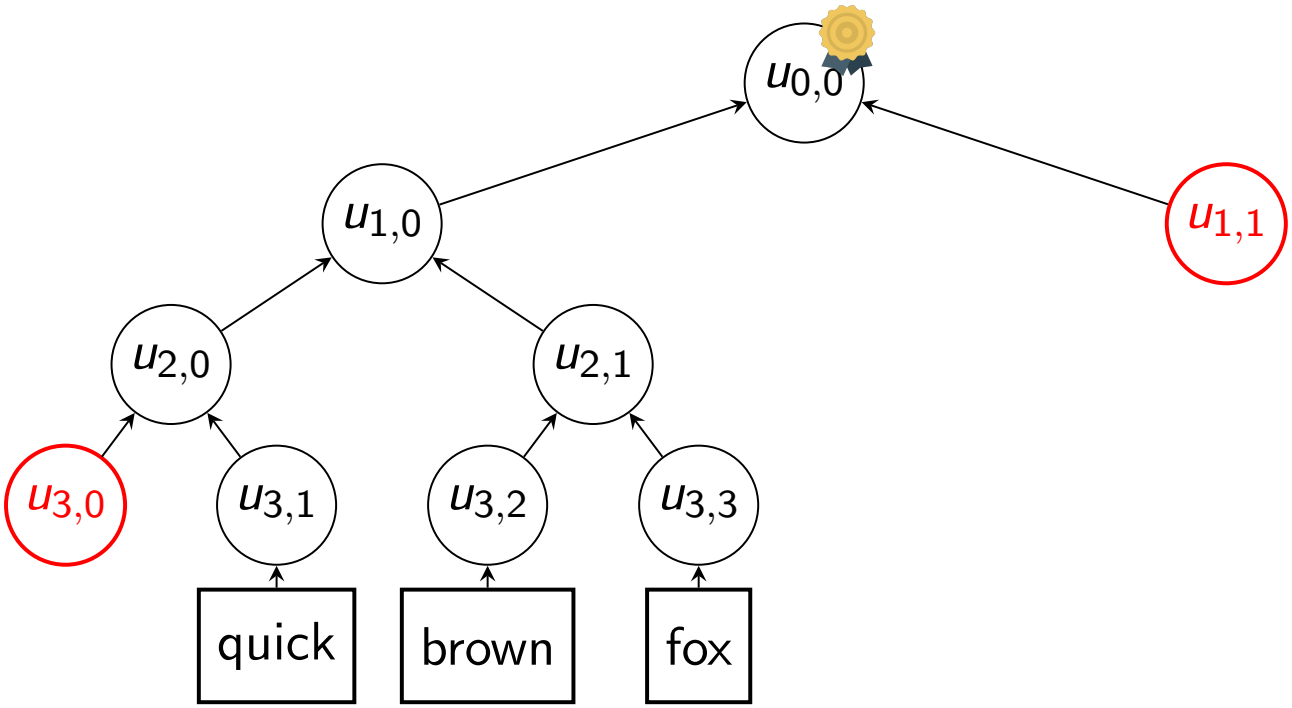
Quoting


$u_{0,0}$
$u_{1,0}$
$u_{1,1}$
$u_{2,0}$
$u_{2,1}$
$u_{2,2}$
$u_{2,3}$
$u_{3,0}$
$u_{3,1}$
$u_{3,2}$
$u_{3,3}$
$u_{3,4}$
$u_{3,5}$
$u_{3,6}$
$u_{3,7}$
quick
brown
fox
jumps
over
the
dog

Quoting



Quoting



A signature for "quick brown fox" is $\{\mathrm{Sig}_{\mathsf{sk}}(u_{0,0}), u_{3,0}, u_{1,1}, \ldots\}$.

Summarizing

Summarizing

KeyGen

As in underlying “normal” digital signature scheme (DS).

Summarizing

KeyGen

As in underlying “normal” digital signature scheme (DS).

Sign

Find root hash, sign with DS.
Signature: DS signature for root hash.

Summarizing

KeyGen

As in underlying “normal” digital signature scheme (DS).

Sign

Find root hash, sign with DS.
Signature: DS signature for root hash.

Quote

Find verification path for quote.
Signature: Verification path and DS signature for root hash.

Summarizing

KeyGen

As in underlying "normal" digital signature scheme (DS).

Sign

Find root hash, sign with DS.
Signature: DS signature for root hash.

Quote

Find verification path for quote.
Signature: Verification path and DS signature for root hash.

Verify

Find root hash (using verification path), use DS to verify.

Security

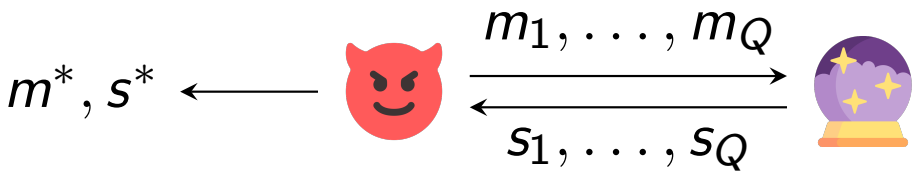
General idea

Show that an adversary against the scheme implies either an adversary against the DS or the used family of hash functions.

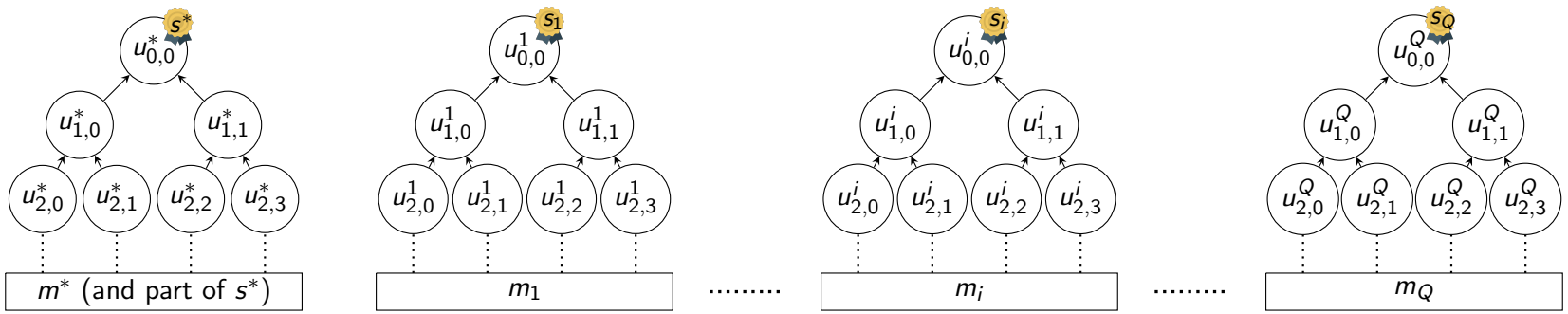
Security

General idea

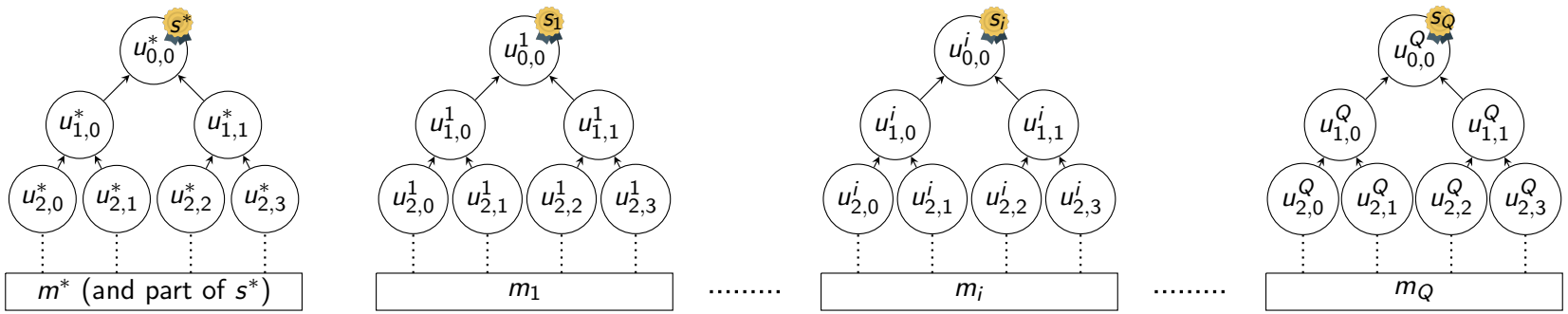
Show that an adversary against the scheme implies either an adversary against the DS or the used family of hash functions.



Security


s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
s_1
$u^1_{0,0}$
$u^1_{1,0}$
$u^1_{1,1}$
$u^1_{2,0}$
$u^1_{2,1}$
$u^1_{2,2}$
$u^1_{2,3}$
m_1
.....
s_i
$u^i_{0,0}$
$u^i_{1,0}$
$u^i_{1,1}$
$u^i_{2,0}$
$u^i_{2,1}$
$u^i_{2,2}$
$u^i_{2,3}$
m_i
.....
s_Q
$u^Q_{0,0}$
$u^Q_{1,0}$
$u^Q_{1,1}$
$u^Q_{2,0}$
$u^Q_{2,1}$
$u^Q_{2,2}$
$u^Q_{2,3}$
m_Q

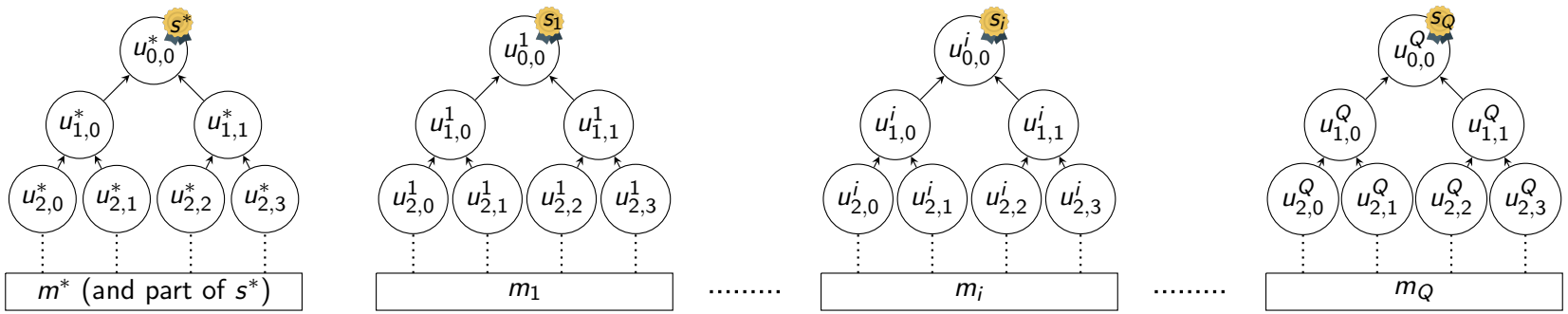
Security



No matching roots

$\Longrightarrow (u^*_{0,0}, s^*)$ is a forgery against DS.

Security



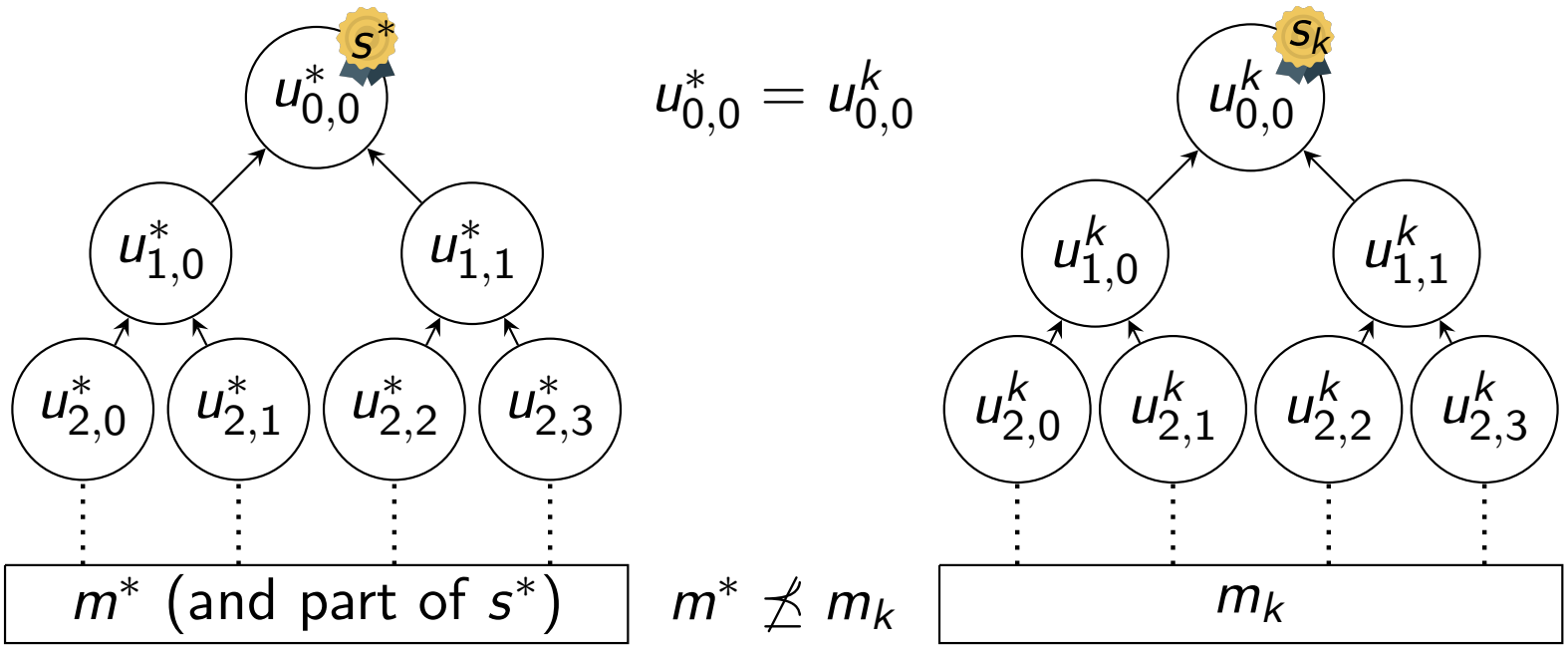
No matching roots

$\Longrightarrow (u^*_{0,0}, s^*)$ is a forgery against DS.

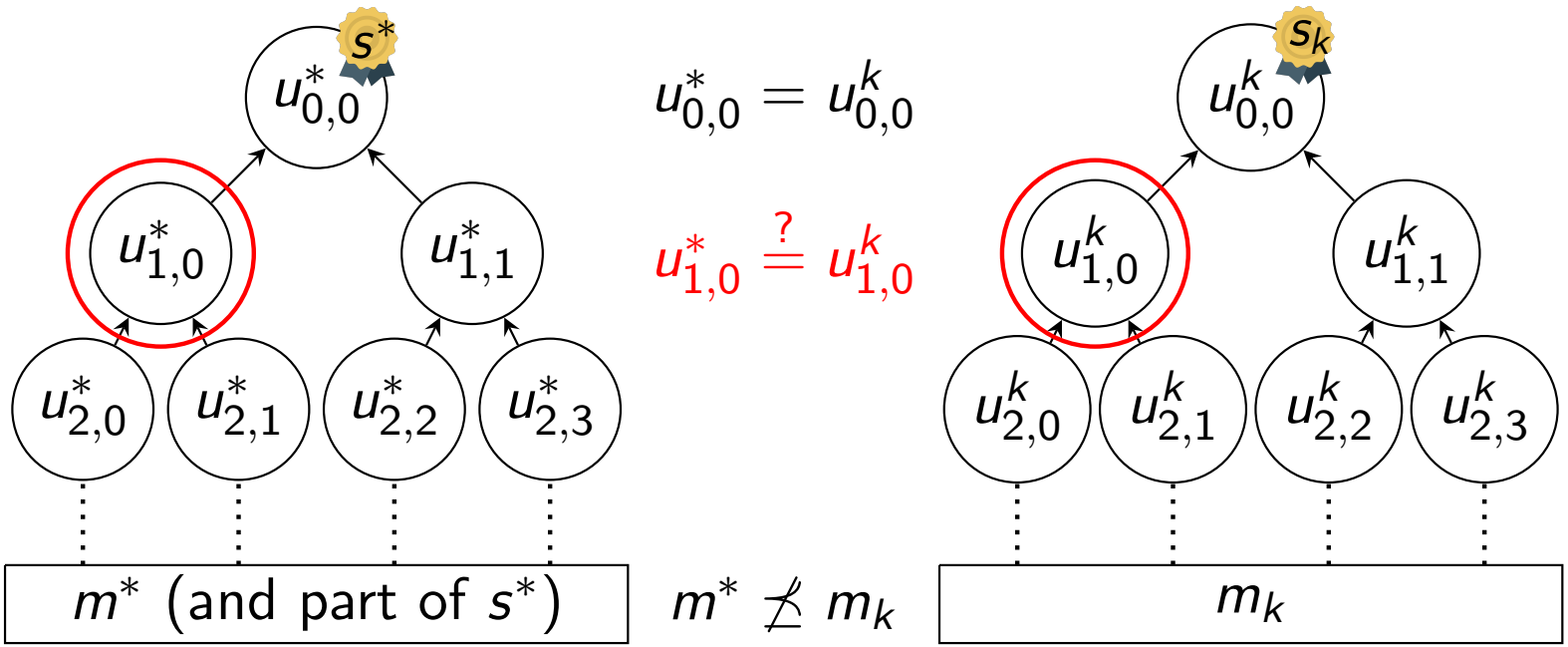
Matching roots

$\exists k\colon u^*_{0,0} = u^k_{0,0}$ but $m^* \not\preceq m_k$.

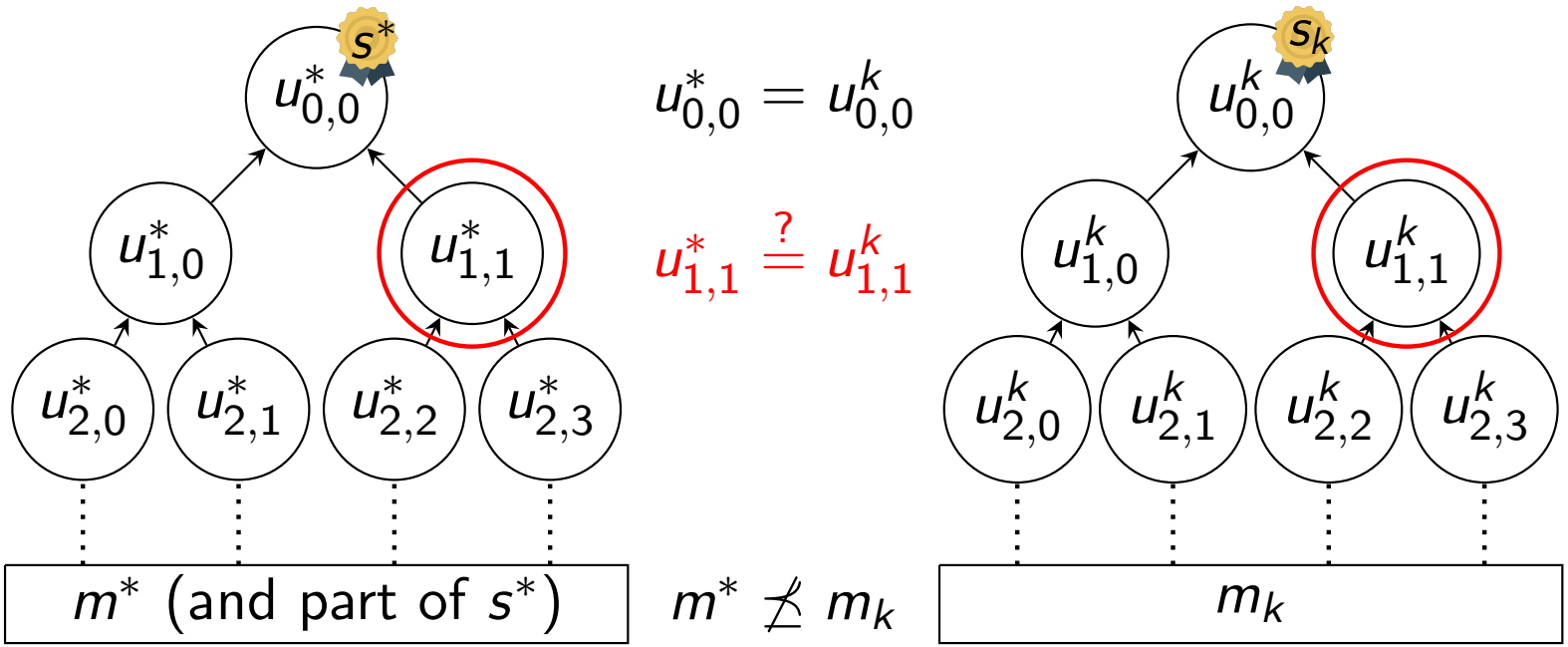
Security


s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
$u^*_{0,0} = u^k_{0,0}$
$m^* \not\preceq m_k$
s_k
$u^k_{0,0}$
$u^k_{1,0}$
$u^k_{1,1}$
$u^k_{2,0}$
$u^k_{2,1}$
$u^k_{2,2}$
$u^k_{2,3}$
m_k

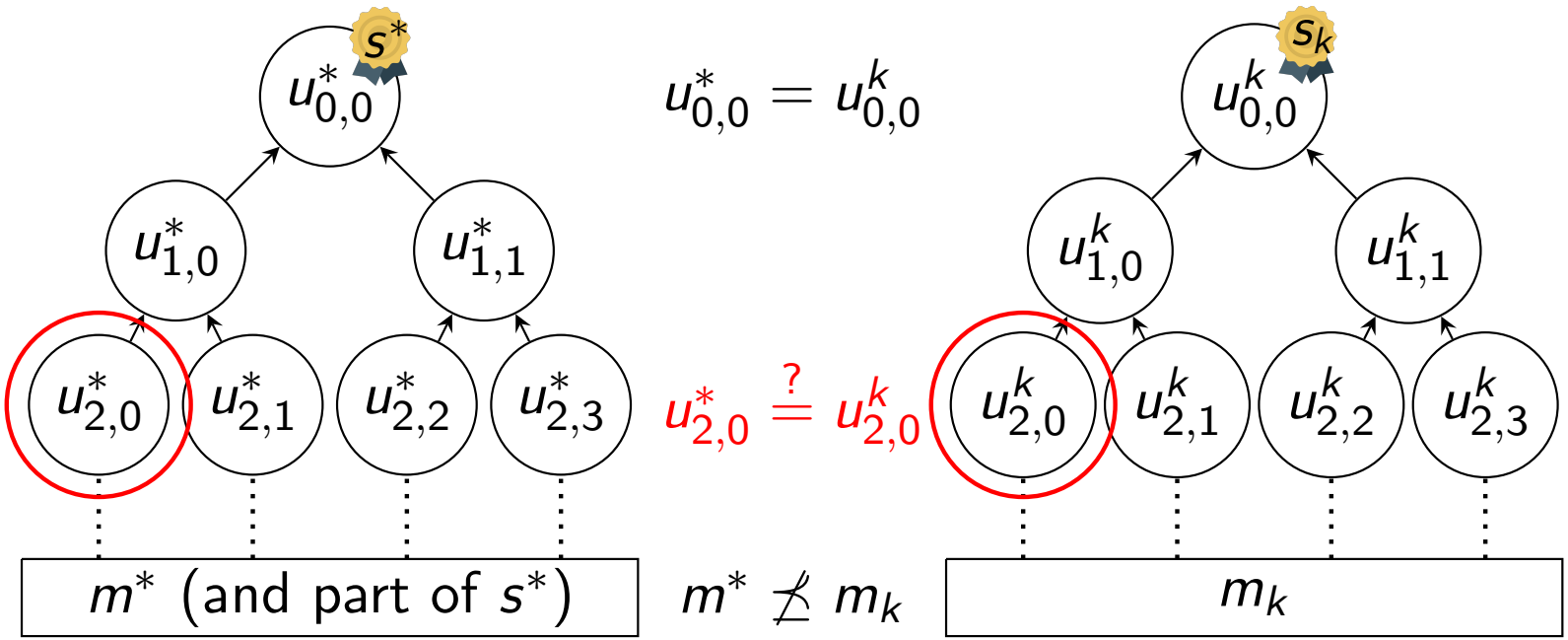
Security


s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
$u^*_{0,0} = u^k_{0,0}$
$u^*_{1,0} \stackrel{?}{=} u^k_{1,0}$
$m^* \not\preceq m_k$
s_k
$u^k_{0,0}$
$u^k_{1,0}$
$u^k_{1,1}$
$u^k_{2,0}$
$u^k_{2,1}$
$u^k_{2,2}$
$u^k_{2,3}$
m_k

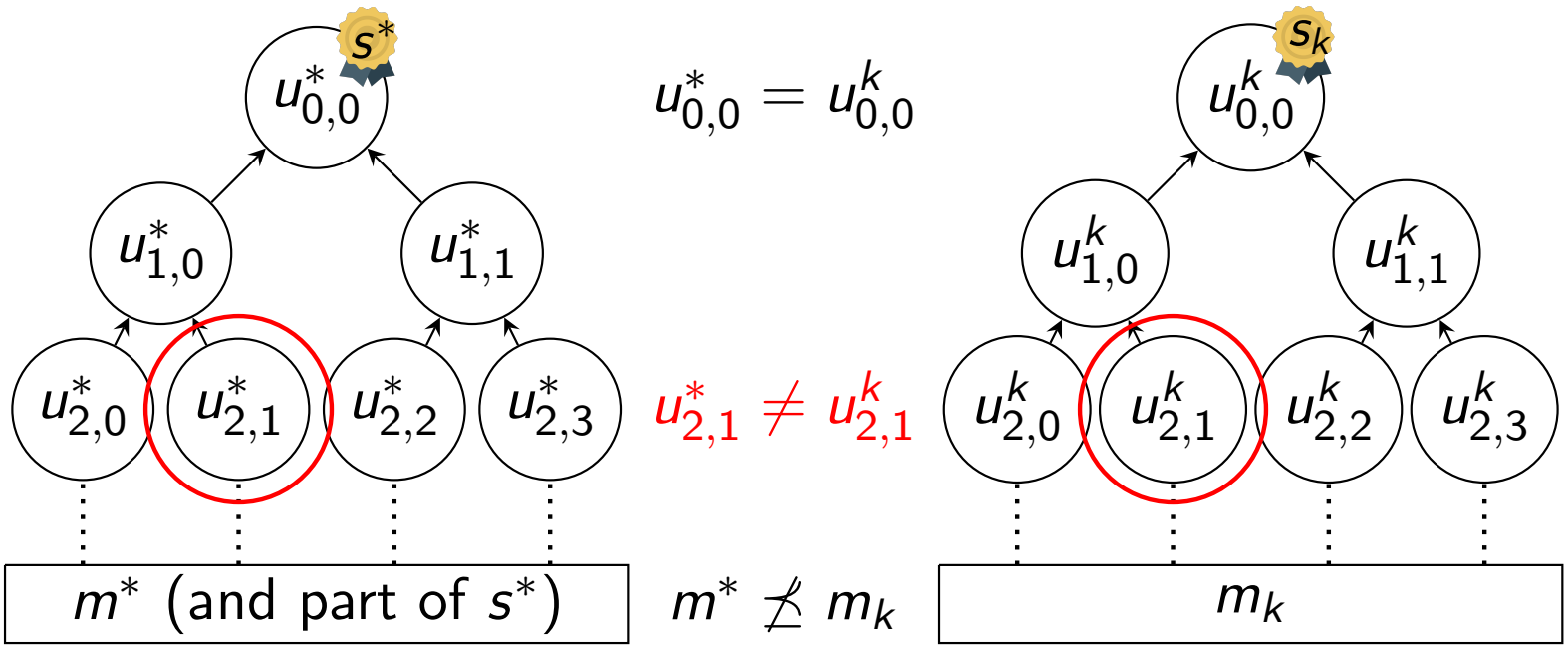
Security


s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
$u^*_{0,0} = u^k_{0,0}$
$u^*_{1,1} \stackrel{?}{=} u^k_{1,1}$
$m^* \not\preceq m_k$
s_k
$u^k_{0,0}$
$u^k_{1,0}$
$u^k_{1,1}$
$u^k_{2,0}$
$u^k_{2,1}$
$u^k_{2,2}$
$u^k_{2,3}$
m_k

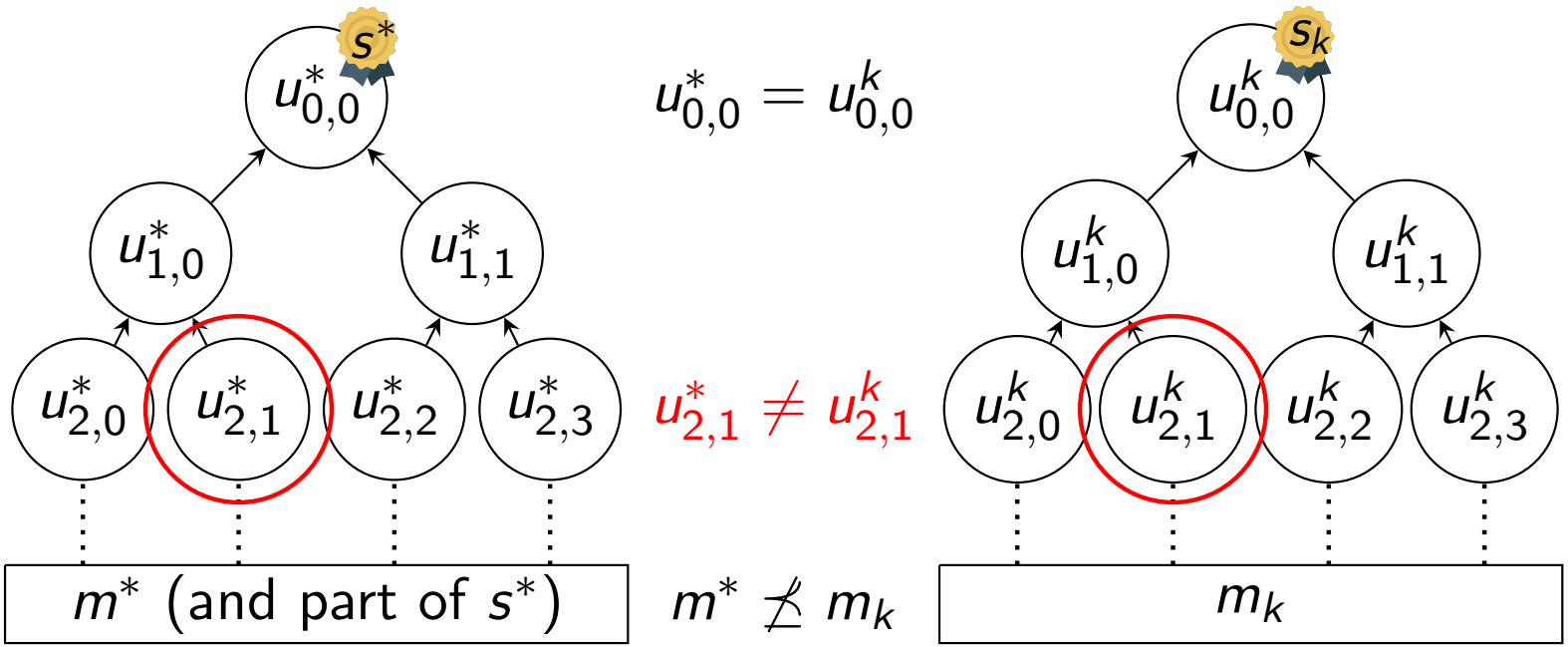
Security


s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
$u^*_{0,0} = u^k_{0,0}$
$u^*_{2,0} \stackrel{?}{=} u^k_{2,0}$
$m^* \not\preceq m_k$
s_k
$u^k_{0,0}$
$u^k_{1,0}$
$u^k_{1,1}$
$u^k_{2,0}$
$u^k_{2,1}$
$u^k_{2,2}$
$u^k_{2,3}$
m_k

Security

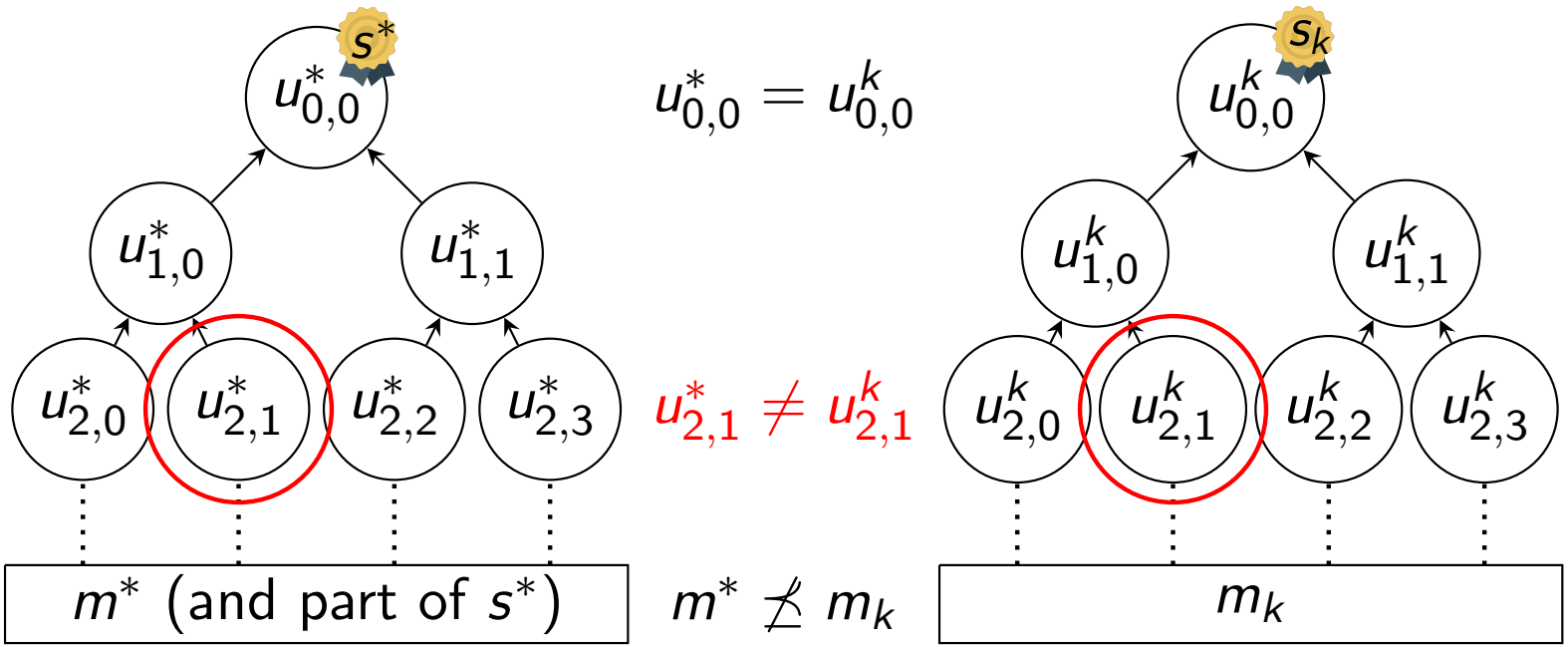

s^*
$u^*_{0,0}$
$u^*_{1,0}$
$u^*_{1,1}$
$u^*_{2,0}$
$u^*_{2,1}$
$u^*_{2,2}$
$u^*_{2,3}$
m^* (and part of s^*)
$u^*_{0,0} = u^k_{0,0}$
$u^*_{2,1} \neq u^k_{2,1}$
$m^* \not\preceq m_k$
s_k
$u^k_{0,0}$
$u^k_{1,0}$
$u^k_{1,1}$
$u^k_{2,0}$
$u^k_{2,1}$
$u^k_{2,2}$
$u^k_{2,3}$
m_k

Security



$$H(01 \parallel u^*_{2,0} \parallel u^*_{2,1}) = u^*_{1,0} = u^k_{1,0} = H(01 \parallel u^k_{2,0} \parallel u^k_{2,1})$$

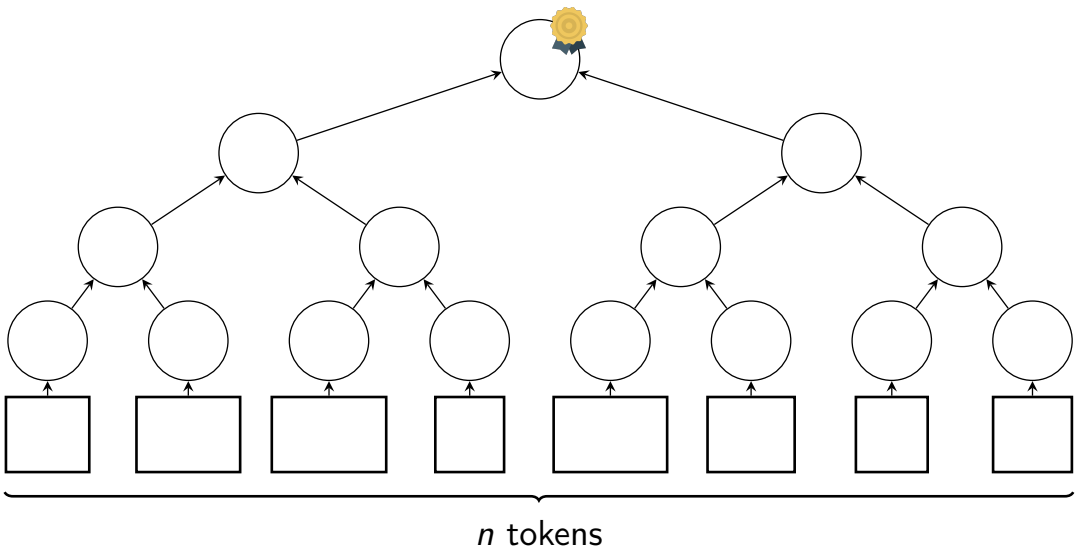
Security



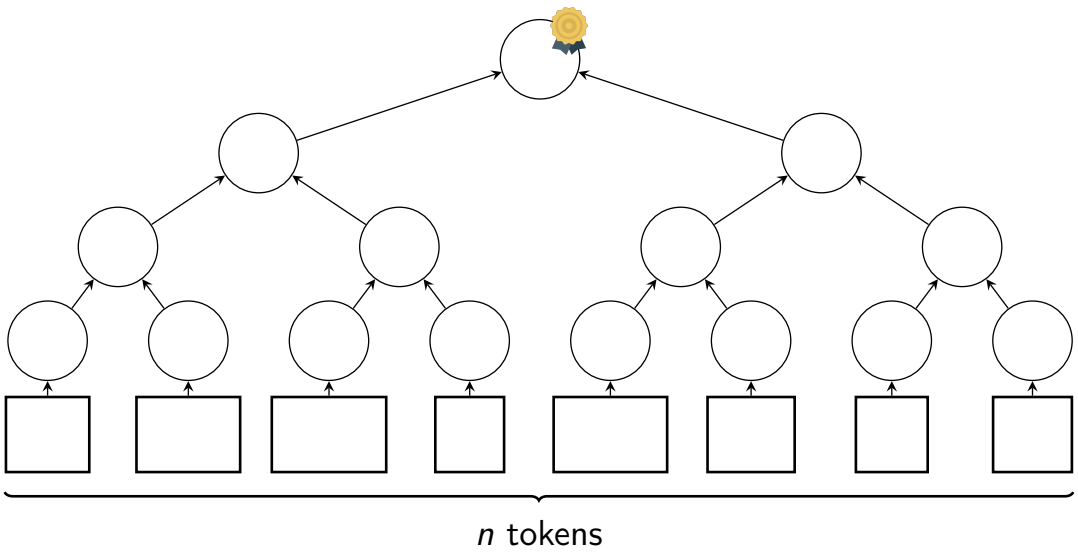
$$H(01 \parallel u^*_{2,0} \parallel u^*_{2,1}) = u^*_{1,0} = u^k_{1,0} = H(01 \parallel u^k_{2,0} \parallel u^k_{2,1})$$

Since $u^*_{2,1} \neq u^k_{2,1}$ this is a collision for H.

Performance



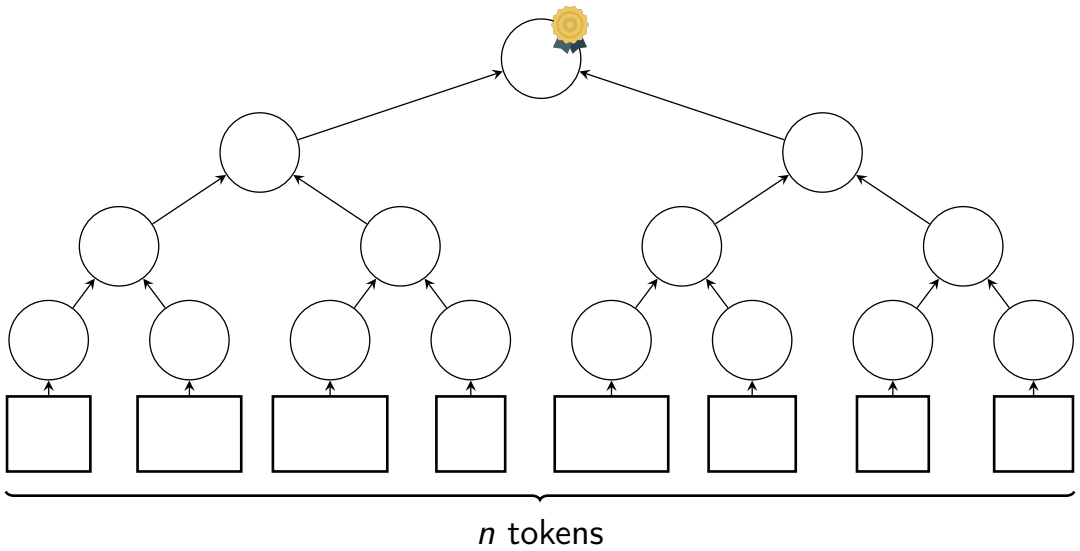
Performance



Computation time

(Up to) $2n - 1$ hashes and one classical signature operation.

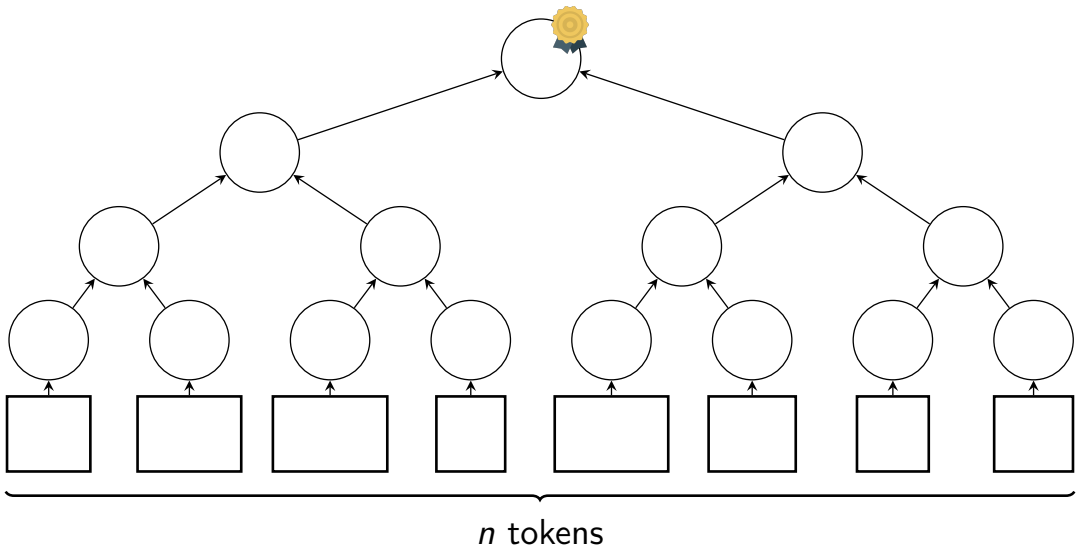
Performance



Initial signature size

One DS signature.

Performance



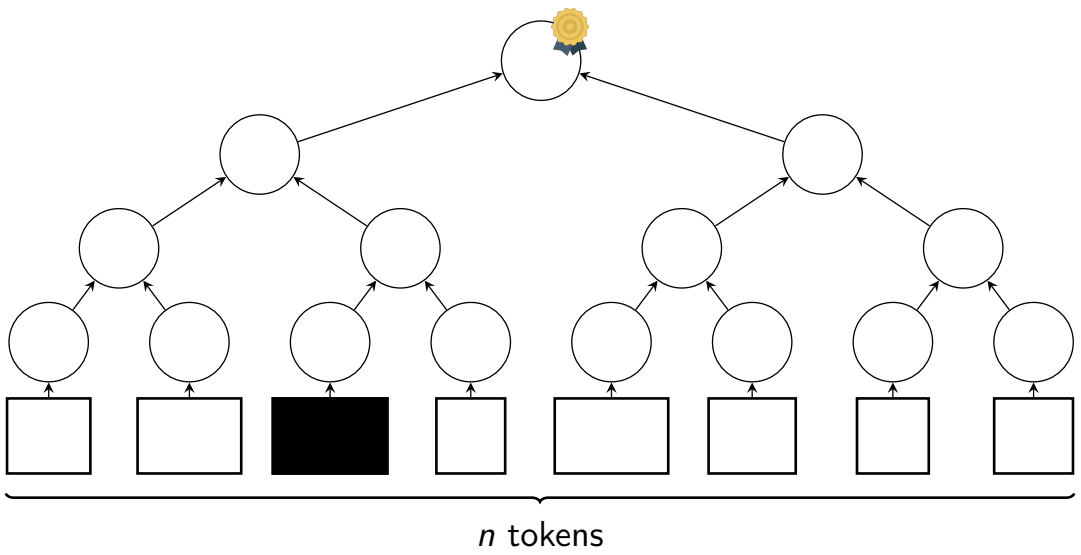
Initial signature size

One DS signature.

Quoted signature size

One DS signature +

Performance



Initial signature size

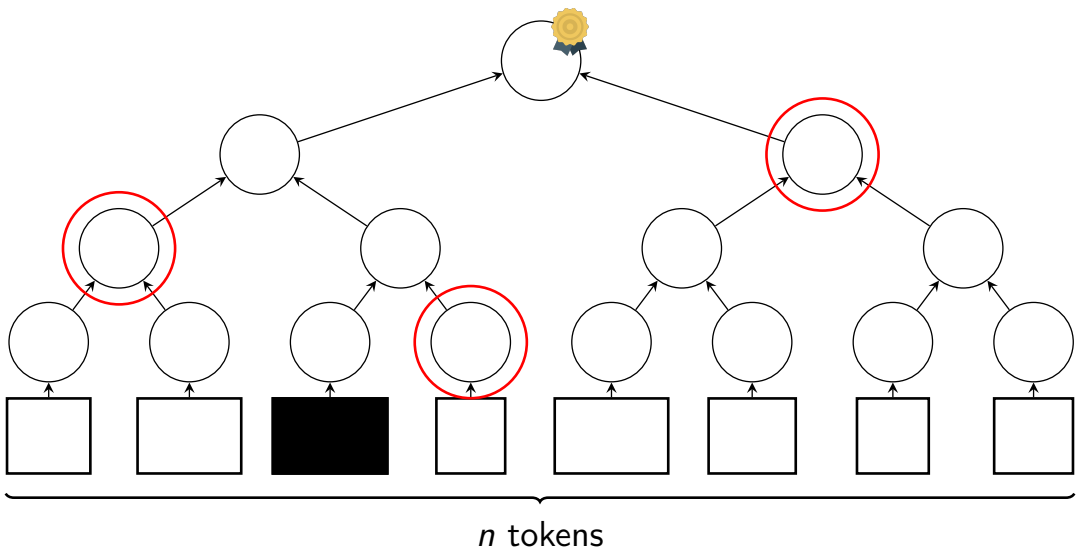
One DS signature.

Quoted signature size

One DS signature +

- One token quoted:

Performance



Initial signature size

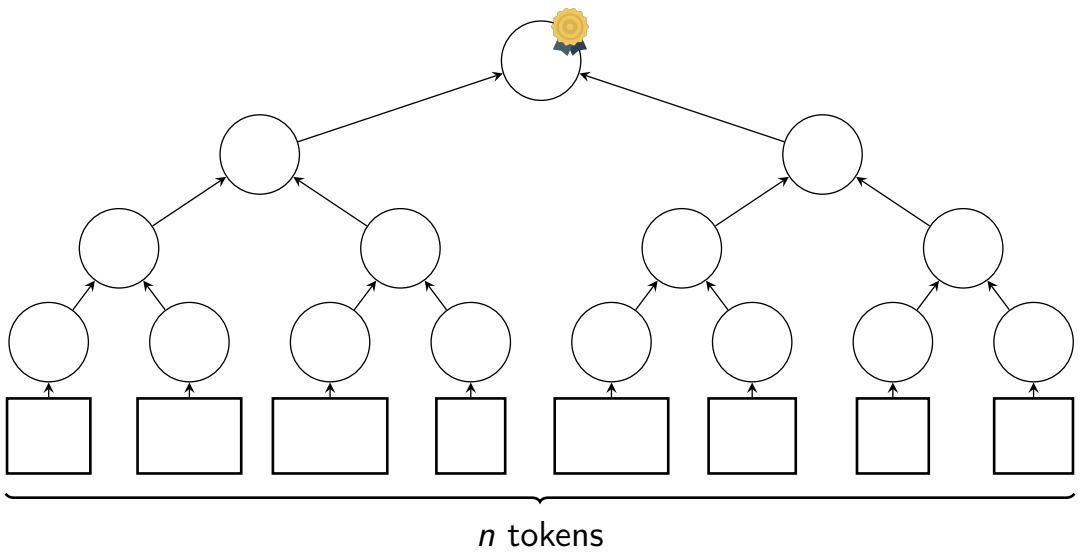
One DS signature.

Quoted signature size

One DS signature +

- One token quoted: $O(\log n)$ hashes

Performance



Initial signature size

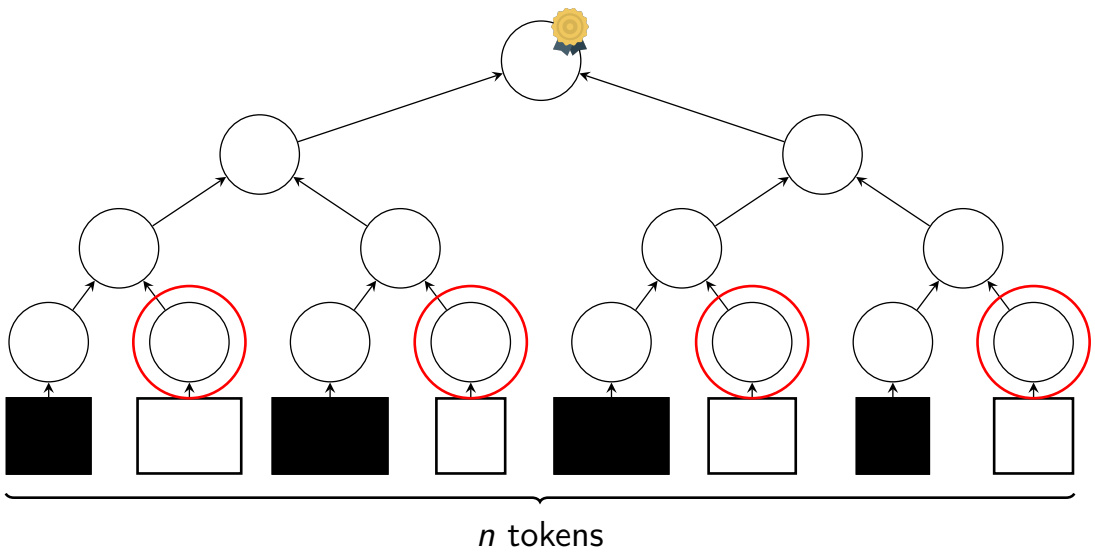
One DS signature.

Quoted signature size

One DS signature +

- One token quoted: $O(\log n)$ hashes
- Arbitrary quotation:

Performance



Initial signature size

One DS signature.

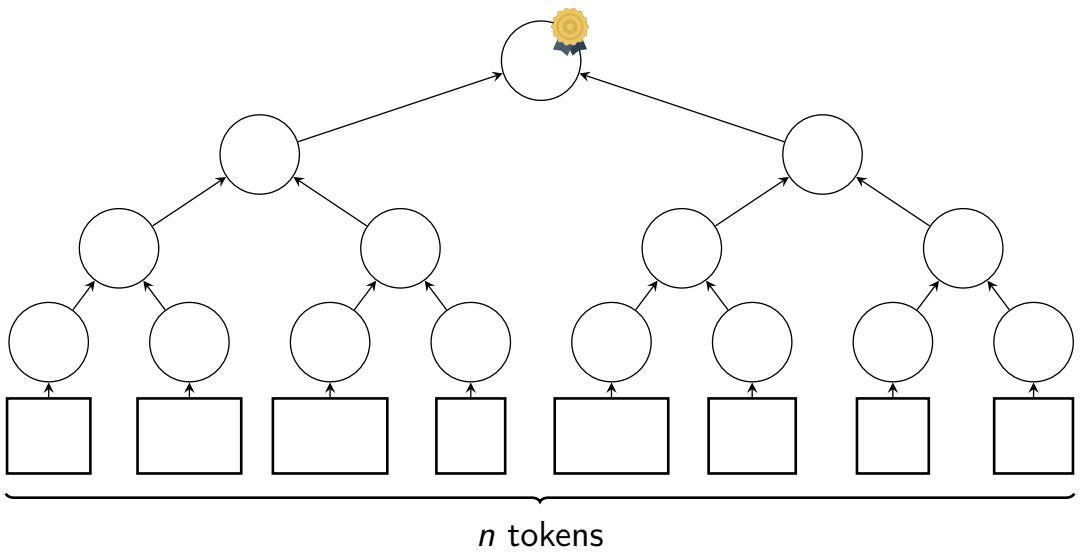
Quoted signature size

One DS signature +

- One token quoted: $O(\log n)$ hashes
- Arbitrary quotation: $O(n)$ hashes

(Exact sizes in paper)

Performance



Initial signature size

One DS signature.

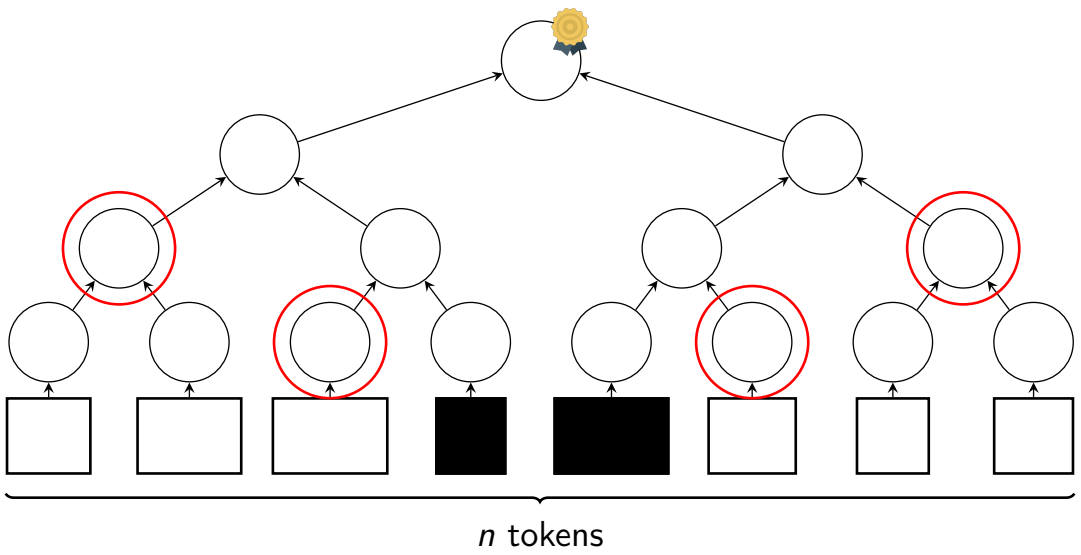
Quoted signature size

One DS signature +

- One token quoted: $O(\log n)$ hashes
- Arbitrary quotation: $O(n)$ hashes
- Contiguous quotation:

(Exact sizes in paper)

Performance



Initial signature size

One DS signature.

Quoted signature size

One DS signature +

- One token quoted: $O(\log n)$ hashes
- Arbitrary quotation: $O(n)$ hashes
- Contiguous quotation: $O(\log n)$ hashes

(Exact sizes in paper)

Open questions

Open questions

Quote signature size independent of message size

Efficient scheme where the size of a signature does not depend on the size of the original message?

Open questions

Quote signature size independent of message size

Efficient scheme where the size of a signature does not depend on the size of the original message?

Linguistic aspects

- How to tokenize; dog. or dog .?

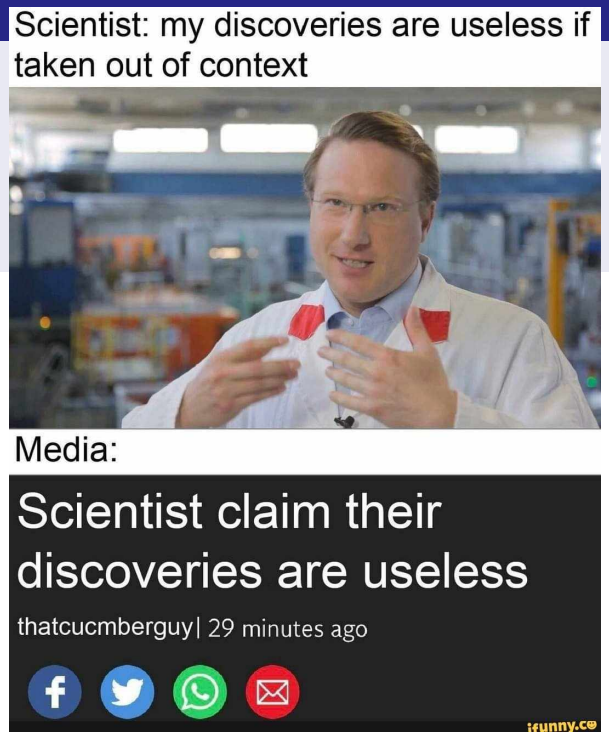
Open questions

Quote signature size independent of message size

Efficient scheme where the size of a signature does not depend on the size of the original message?

Linguistic aspects

- How to tokenize; dog. or dog . ?
- Quoting out of context?



Open questions

Quote signature size independent of message size

Efficient scheme where the size of a signature does not depend on the size of the original message?

Linguistic aspects

- How to tokenize; dog. or dog . ?
- Quoting out of context?

Real-world test

Will it help? Can we get "big players" on board?

Thank you for listening.

full version on arXiv

[BELN23]

References

[BELN23] Joan Boyar, Simon Erfurth, Kim S. Larsen, and Ruben Niederhagen. *Quotable signatures for authenticating shared quotes*. 2023. URL: https://arxiv.org/abs/2212.10963v2.

[KNSS19] Michael Kreutzer, Ruben Niederhagen, Kris Shrishak, and Hervais Simo Fhom. "Quotable Signatures using Merkle Trees". In: *INFORMATIK 2019*. Vol. P-294. Lecture Notes in Informatik. 2019, pp. 473–477.

Acknowledgments

Thanks to Johanna Eggers (@joh_eggers) for the mock-up illustrations.
These slides have been designed using images from Flaticon.com.