Certificate Transparency

Andrew Ayer, SSLMate

https://agwa.name
https://sslmate.com
@__agwa

Slides at https://agwa.name/talks/ct.pdf

Certificate Authority Blunders

- Symantec – test.com, example.com, O=Test
- GoDaddy – Domain validation vulnerability
- Comodo – Domain validation vulnerabilities (x2)
- Comodo – Misissued certificate for .sb TLD
- Trustis – SHA-1
- Quo Vadis – SHA-1
- Symantec – SHA-1
- Symantec – Non-random serial number
- Verizon/DigiCert – Unknown/Unaudited Sub CAs
- WoSign/StartCom – Too many to list...

Certificate Authority Blunders
(not just last year's)

- Symantec – test.com, example.com, O=Test
- GoDaddy – Domain validation vulnerability
- Comodo – Domain validation vulnerabilities (x2)
- Comodo – Misissued certificate for .sb TLD
- Trustis – SHA-1
- Quo Vadis – SHA-1
- Symantec – SHA-1
- Symantec – Non-random serial number
- Verizon/DigiCert – Unknown/Unaudited Sub CAs
- WoSign/StartCom – Too many to list...
- GlobalSign – test.com
- Let's Encrypt – CAA checking bug (CPS violation)
- Symantec – DV vulnerability (bad email regex)
- GlobalSign – DNS name containing whitespace
- Symantec – “Test” certificates, inc. google.com
- Comodo – internal host names
- India CCA – compromised, google.com
- TurkTrust – accidental sub CAs
- ANSSI – Issued Sub CA for MitM device
- Trustwave – Issued Sub CA for MitM device
- DigiNotar – Total compromise
- StartCom – Webapp vulnerability
- Comodo – RAs compromised, google.com
- IpsCA – null prefix attack
- Comodo – RA not performing domain validation
- Thawte – sslcertificates@live.com
- VeriSign – Unauthorized MSFT code signing cert
- Countless encoding bugs and RFC violations...

“Sunlight is said to be the best of disinfectants”

– Justice Louis Brandeis

Why Certificate Transparency?

- Remediation of incidents
  - Including CA distrust!
- Encourages better CA behavior
- Data informs security improvements
- Builds on top of the existing Web PKI

Signed Certificate Timestamps (SCTs)

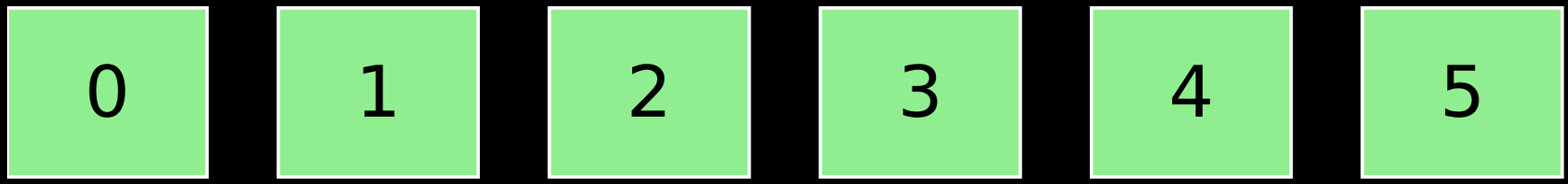
- Signed promise by log to publish certificate within defined Maximum Merge Delay (MMD)
  - 24 hours for all current logs
- Certificates only trusted if accompanied by SCT(s)

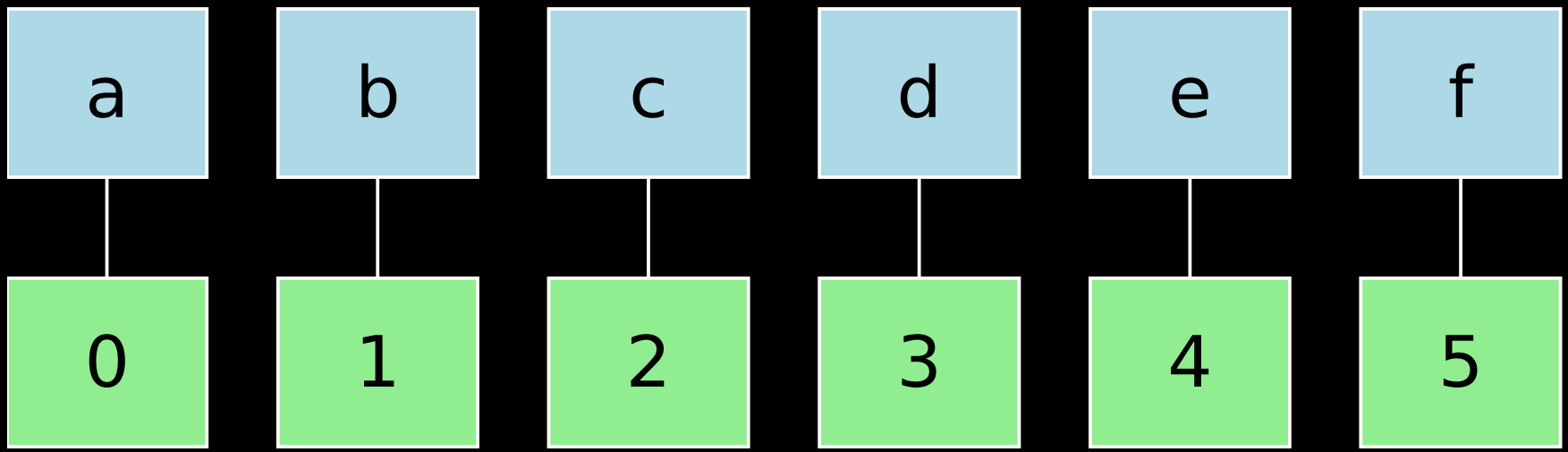
How to Deliver SCTs to Clients

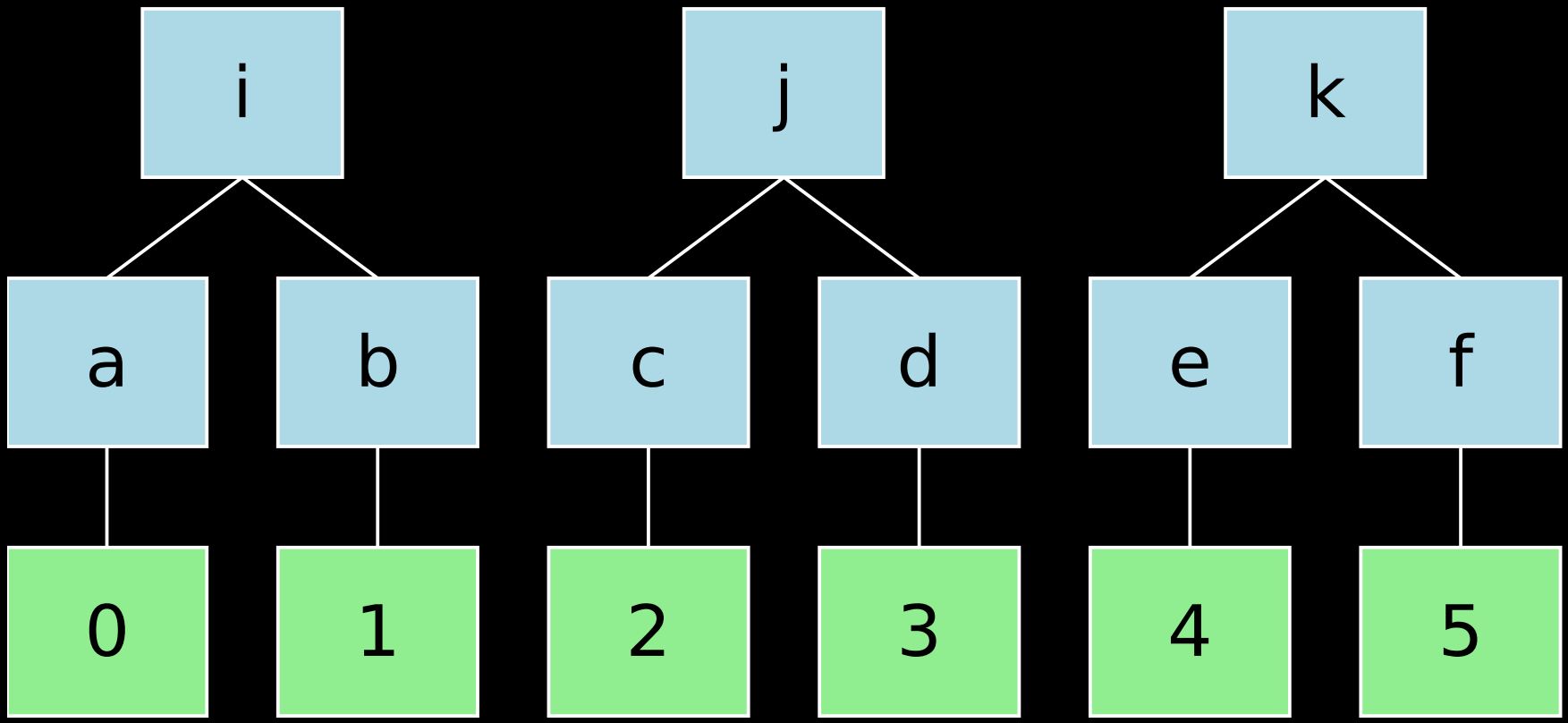
- TLS Extension
  - Server operator's responsibility
  - Requires server support
- OCSP Extension
  - CA's responsibility
  - Requires OCSP Stapling
- Certificate Extension
  - CA's responsibility
  - Works everywhere
  - But if CT log becomes distrusted, cert may become invalid

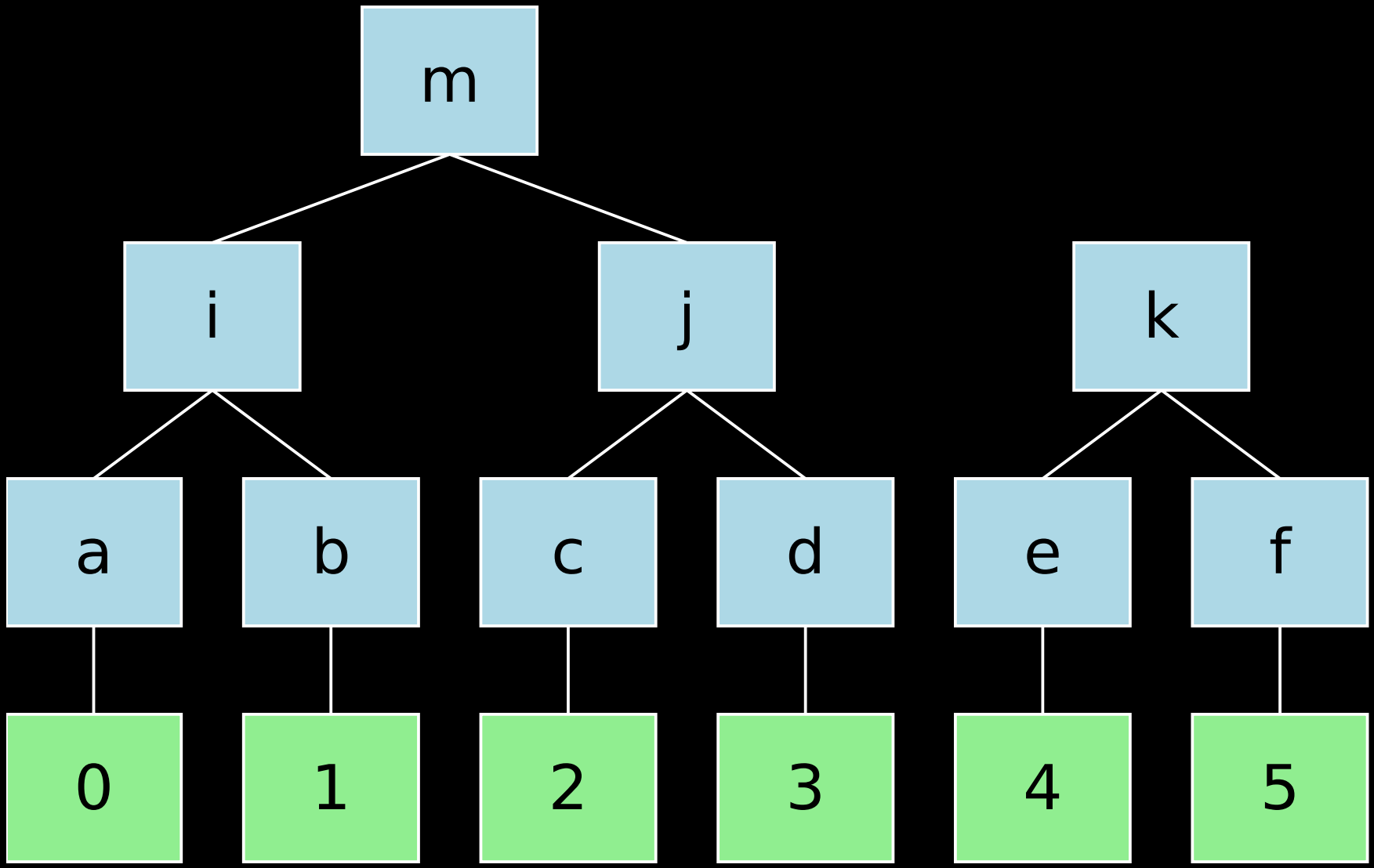
No Trusted Third Parties!

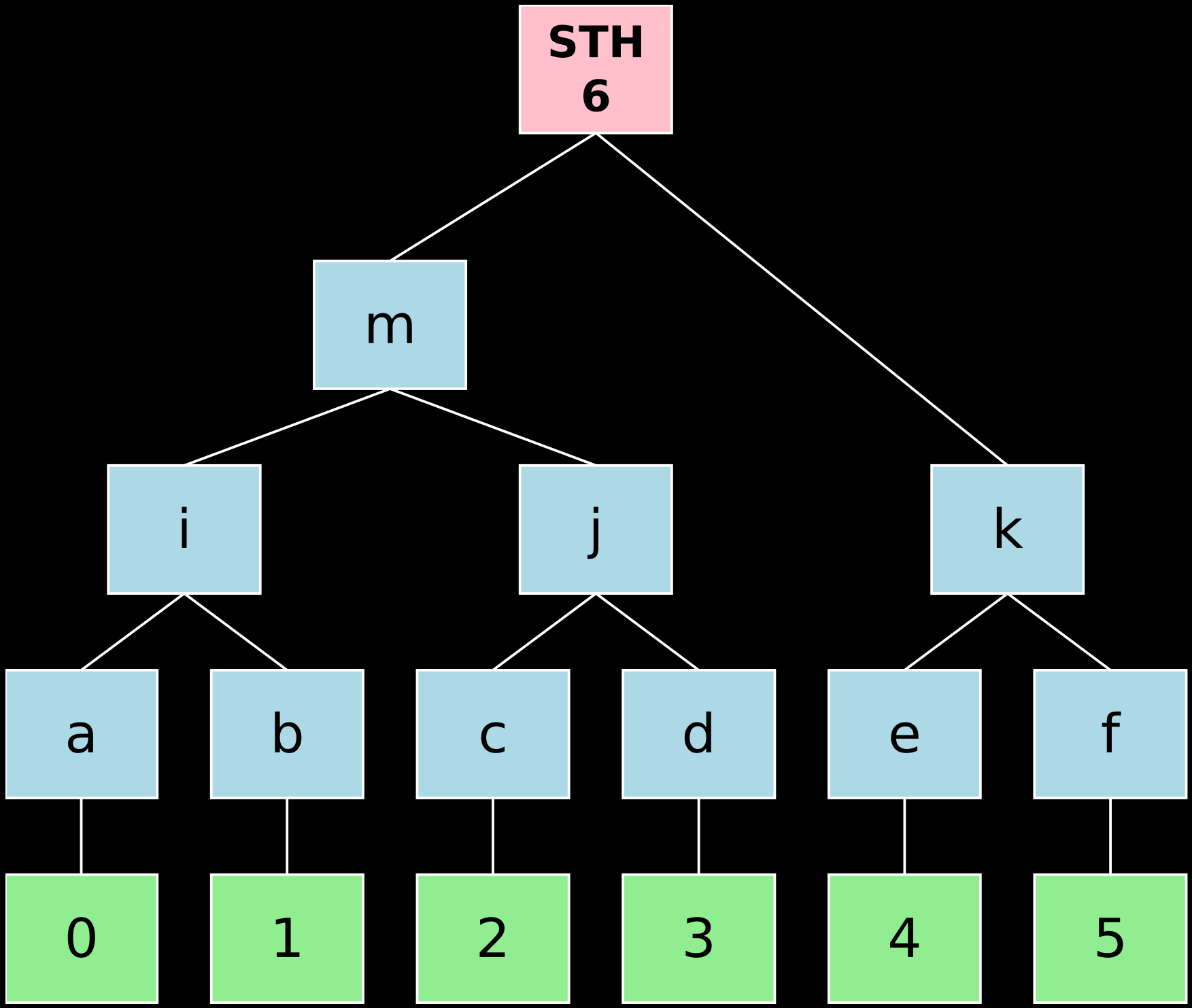
- Ways a CT log could misbehave:
  - Issue an SCT but never log the certificate
  - Remove a certificate from the log
  - Present different versions of log to different people

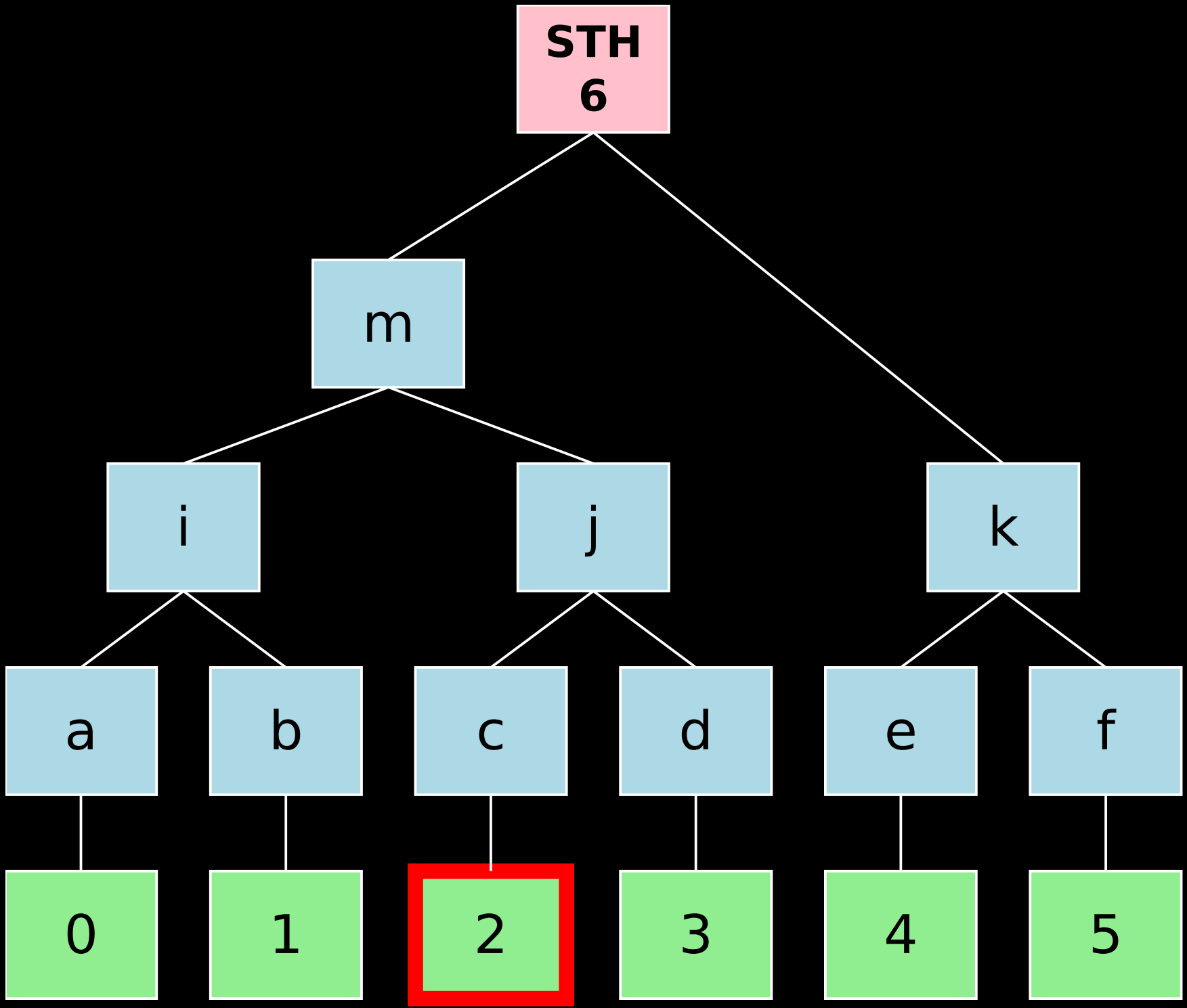

0
1
2
3
4
5

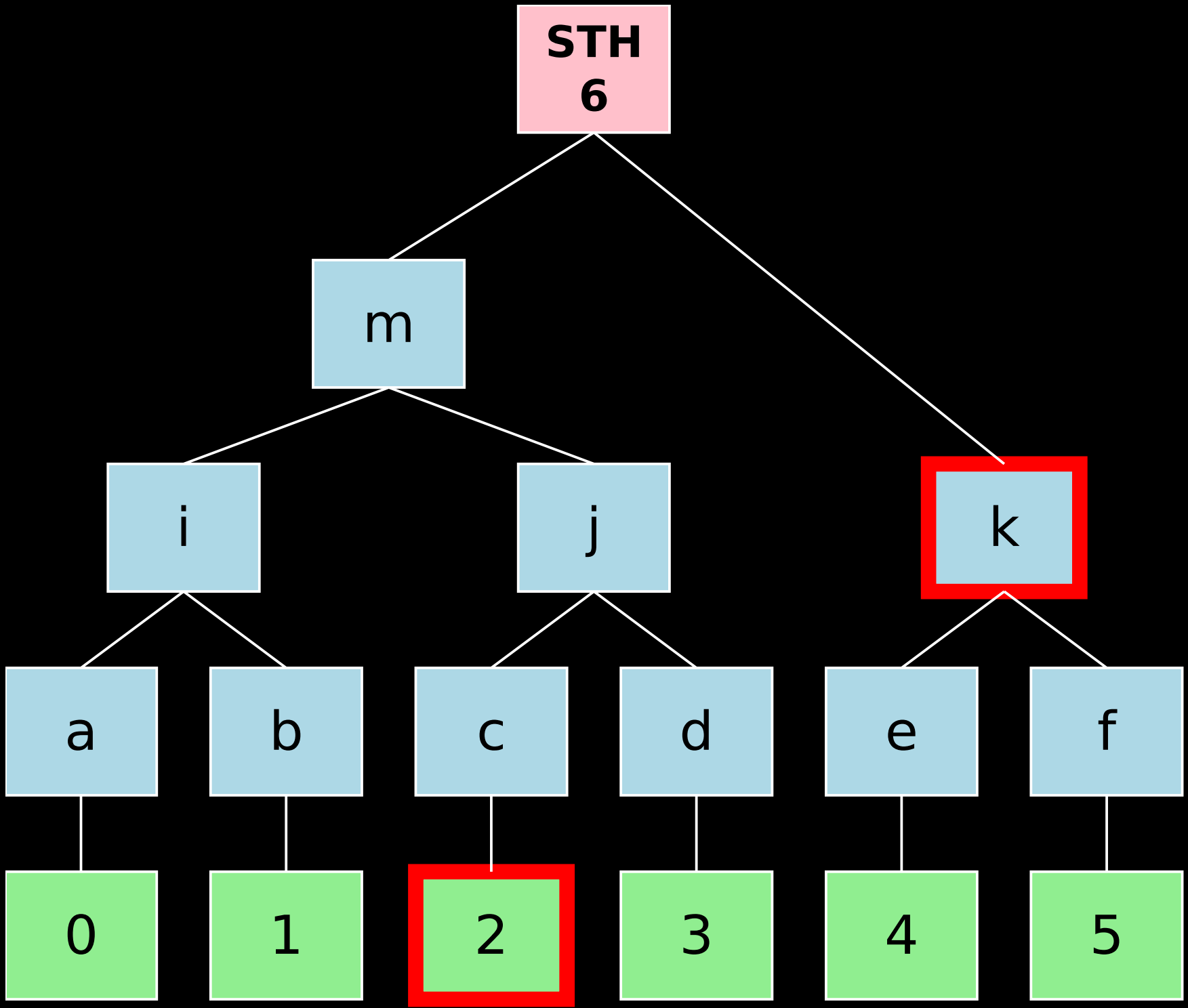

a
b
c
d
e
f
0
1
2
3
4
5

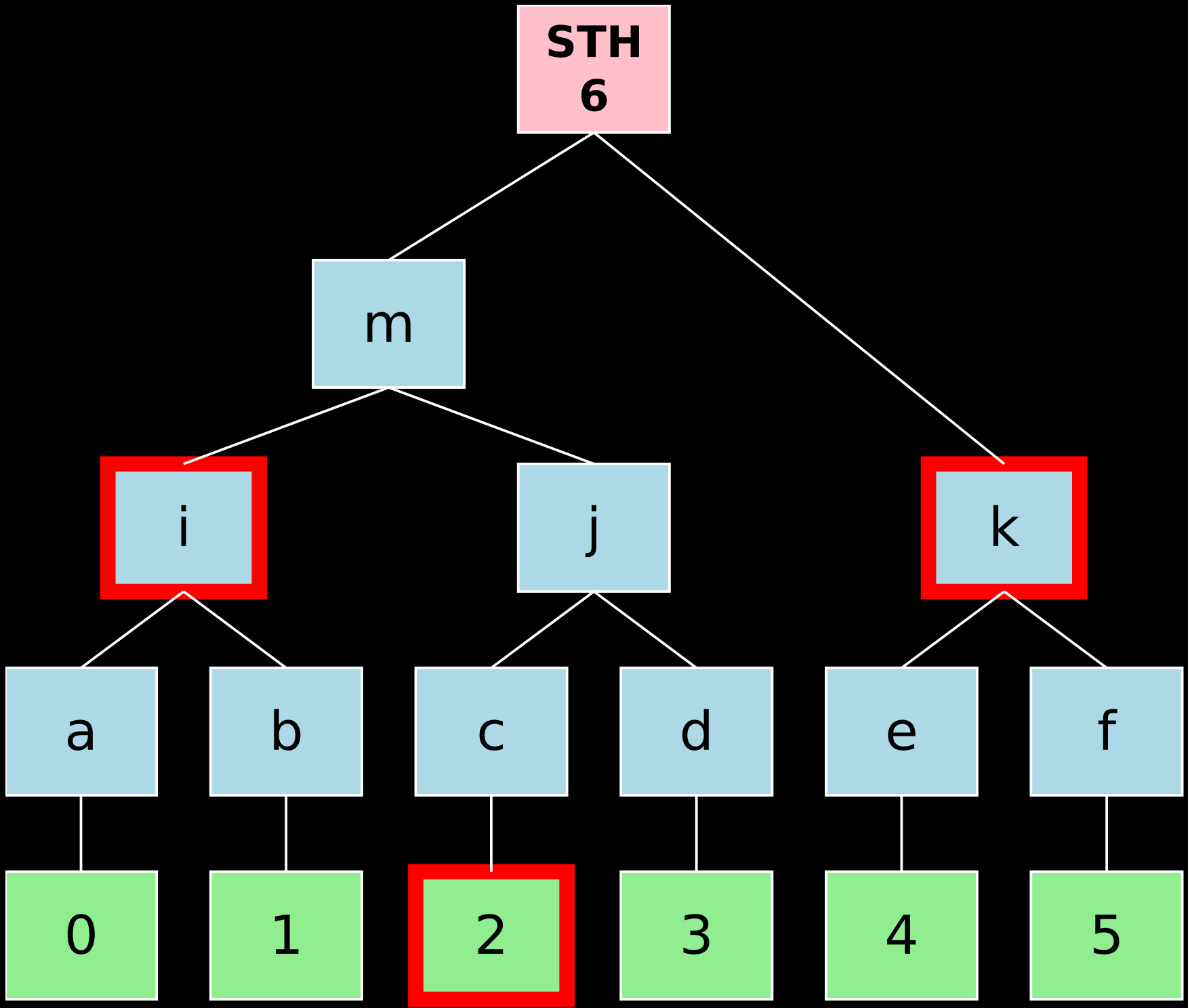

i
j
k
a
b
c
d
e
f
0
1
2
3
4
5

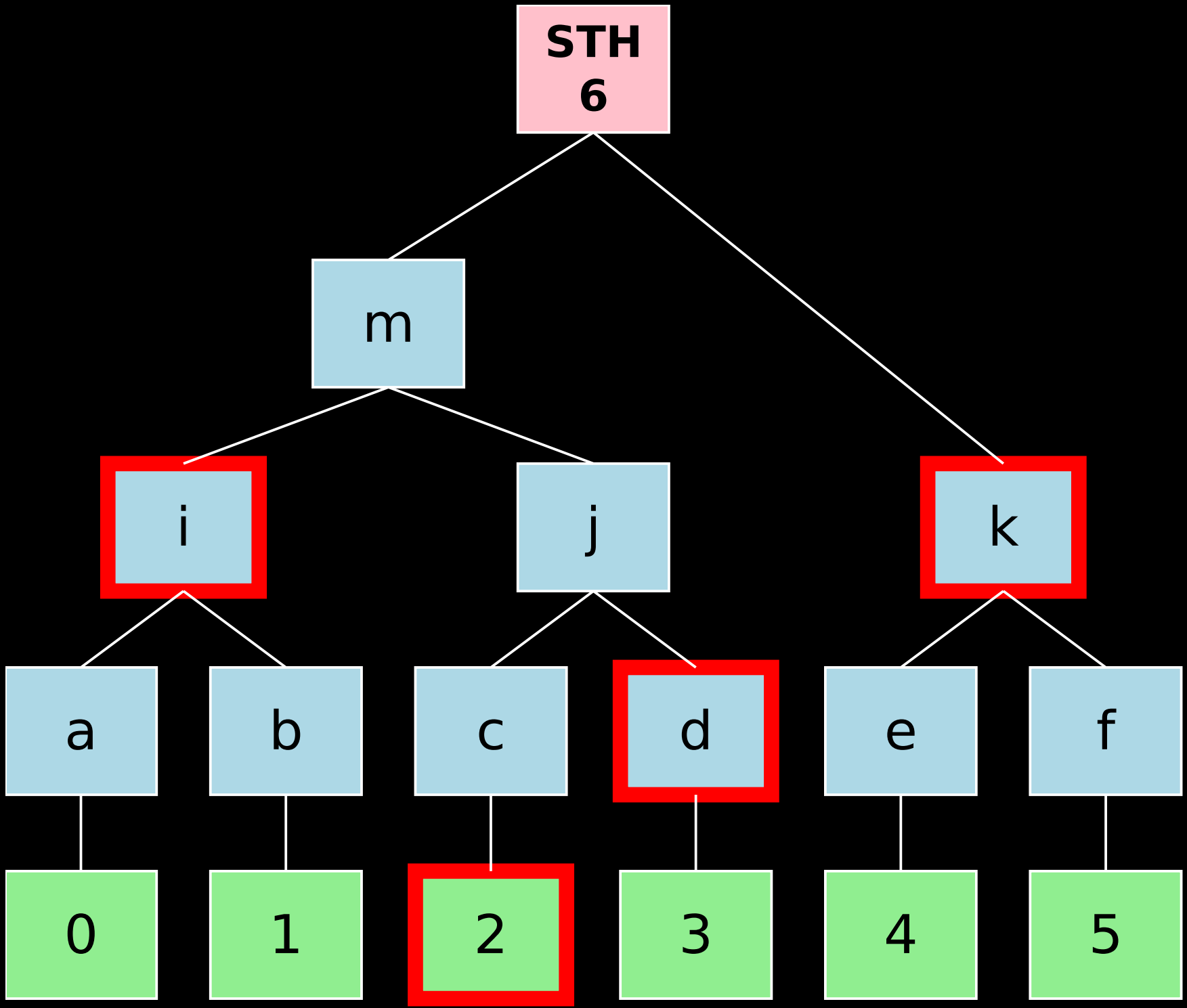

m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5

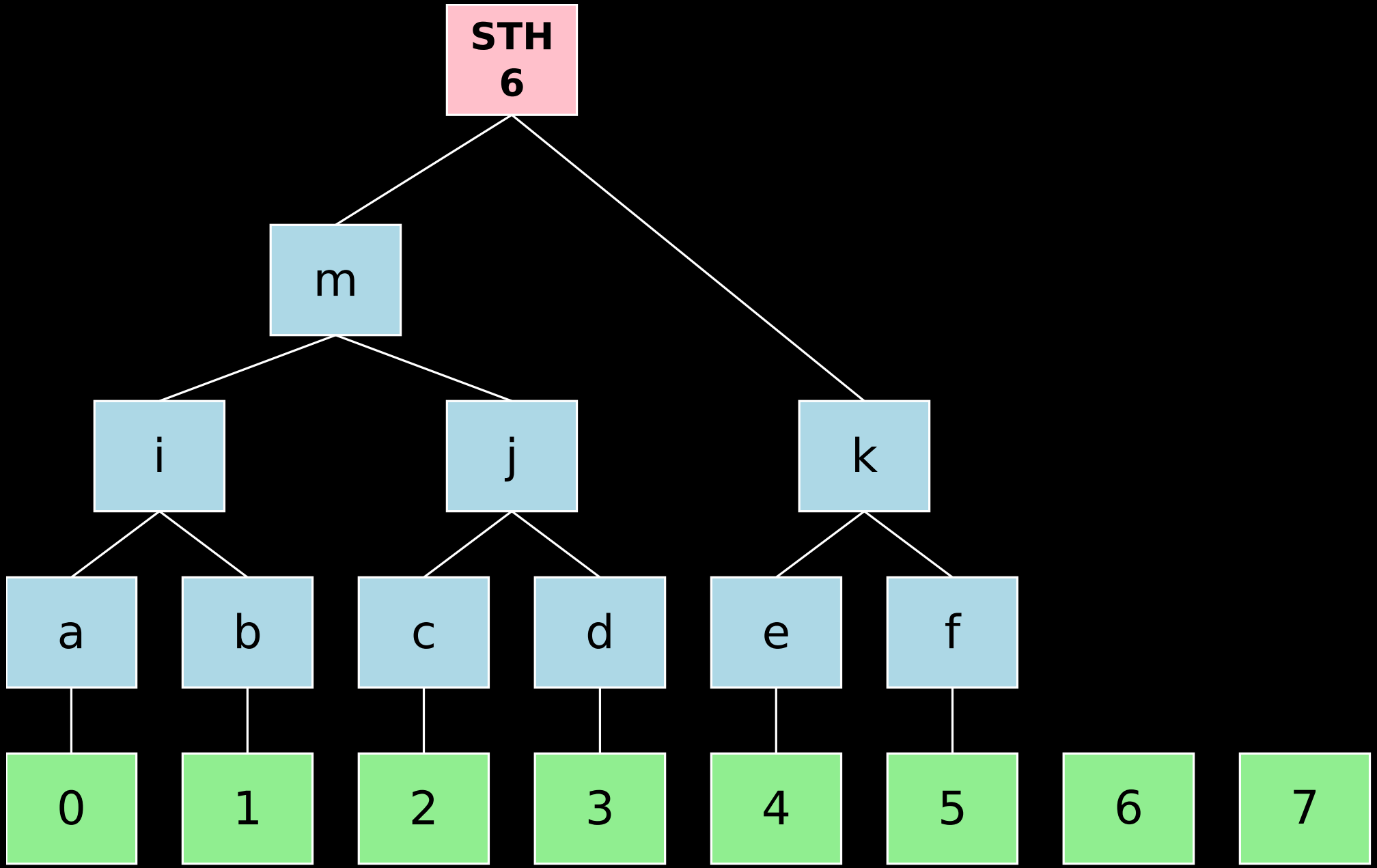

STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5

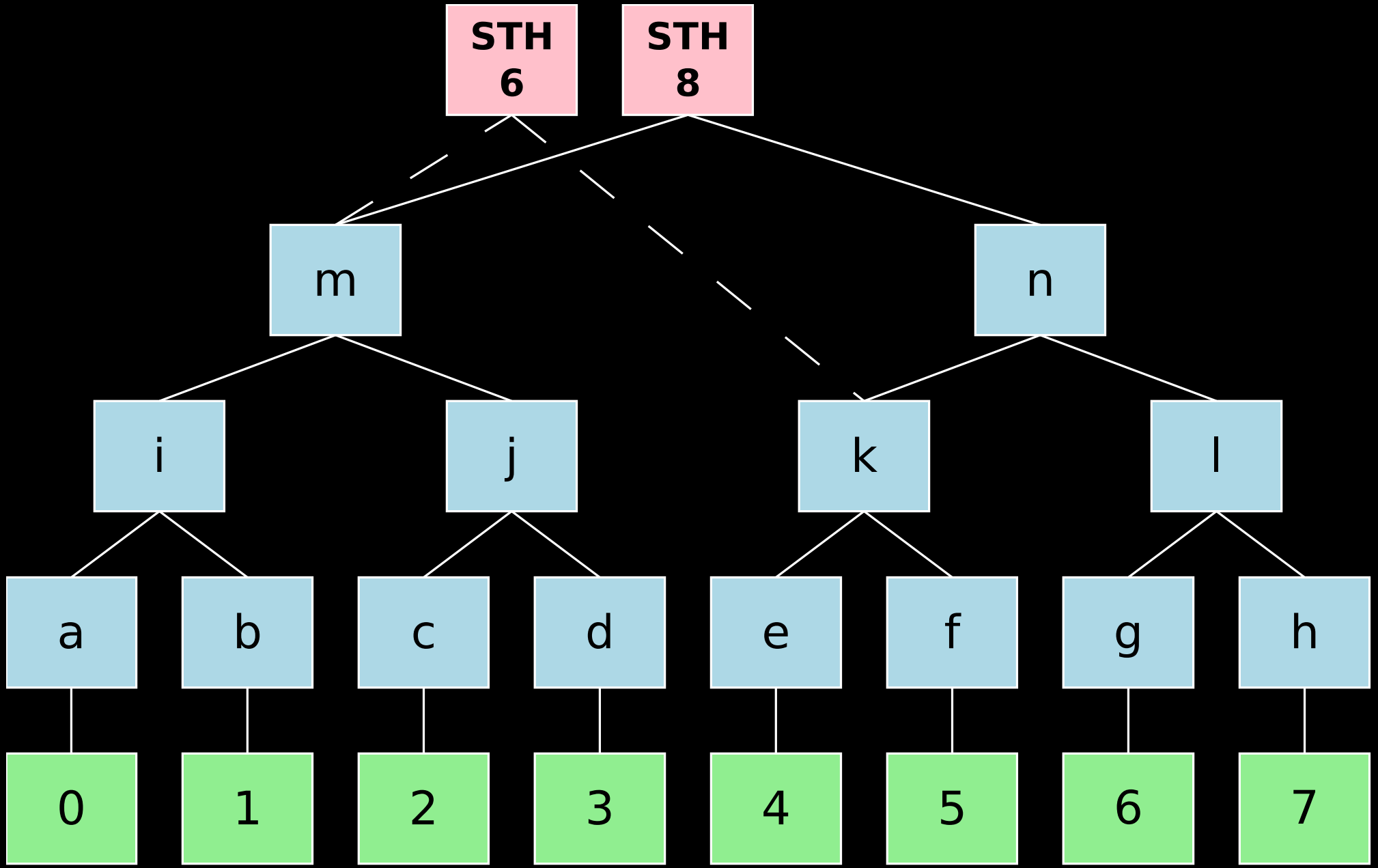

STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5

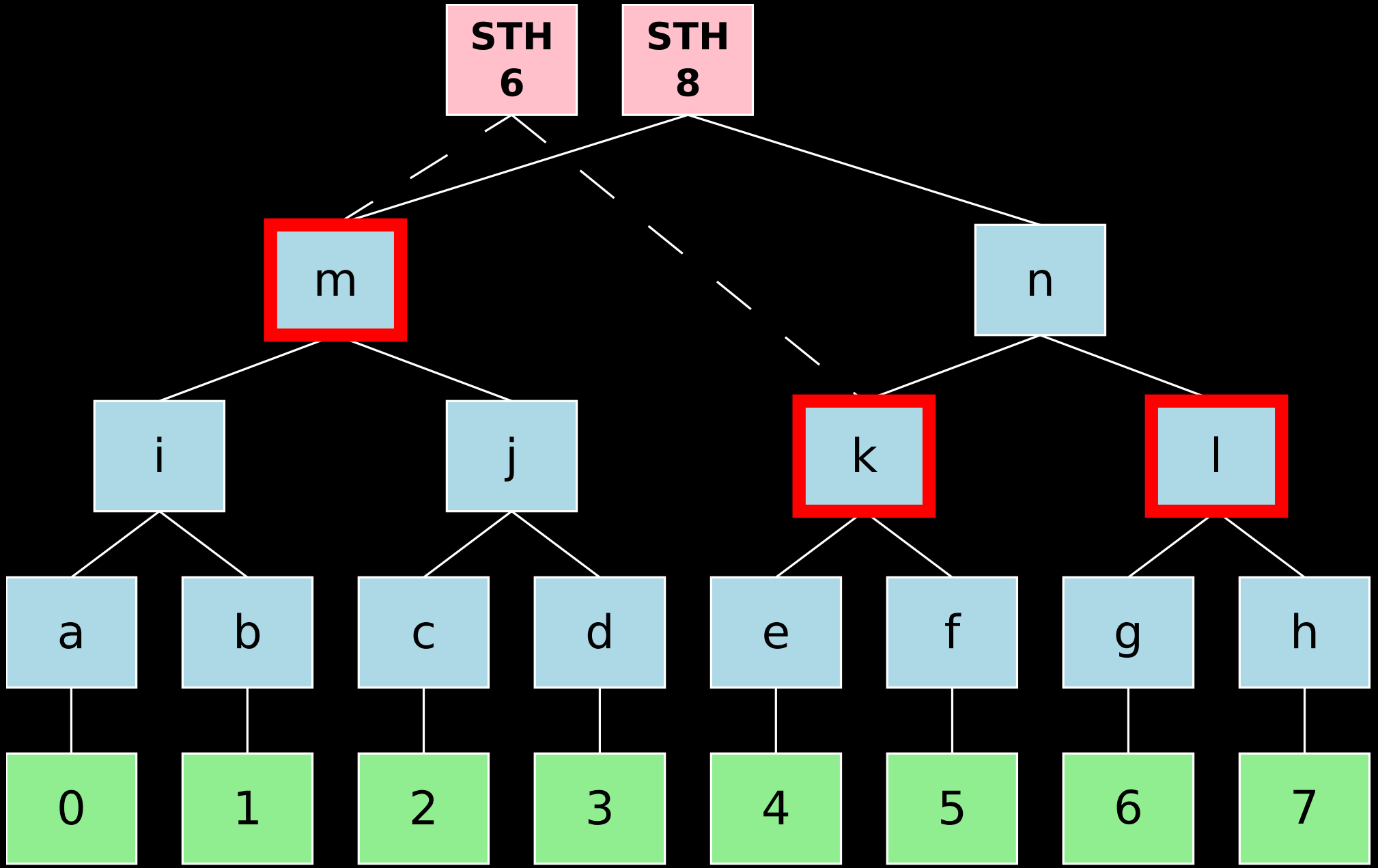

STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5


STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5


STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5


STH
6
m
i
j
k
a
b
c
d
e
f
0
1
2
3
4
5
6
7


STH 6
STH 8
m
n
i
j
k
l
a
b
c
d
e
f
g
h
0
1
2
3
4
5
6
7


STH 6
STH 8
m
n
i
j
k
l
a
b
c
d
e
f
g
h
0
1
2
3
4
5
6
7

Certificate Transparency Today

- RFC 6962 (experimental)
- 24 logs (11 trusted by Chrome)
  - Google (x8), Venafi (x2), PuChuangSiDa, NORDUnet
  - Various CAs
- 91 million unique certs
- Largest log has 75 million certs
  - Growing by 13 million a month
- Log failures: Certly, Izenpe, Aviator, Venafi?

Client/Browser Support

- Chrome
  - Required for EV since 2015
  - Required for new Symantec certs since June 2016
  - Required for all new certs starting October 2017
  - Does not check inclusion proofs yet
    - In-progress: fetch proofs over DNS (for privacy)
    - Interim solution: SCTs required from 1 Google and 1 non-Google log

Client/Browser Support

- Apple
  - App developers can opt-in with App Transport Security
- Mozilla
  - Under discussion
  - Concerns about log auditing
- Microsoft
  - Expressed interest

Monitors

- Cert Spotter (me) – Good for alerting
  - Open source: https://github.com/SSLMate/certspotter
  - Hosted service: https://sslmate.com/certspotter
- crt.sh (Rob Stradling of Comodo) – Good for searching
  - https://crt.sh
- Facebook
- Google
- DigiCert

Certificate Transparency Future

- RFC 6962-bis (Standards Track)
  - Minor improvements to RFC 6962
- Gossip Internet Draft
  - Helps with auditing
- Threat analysis Internet Draft
- Log monitor API
- Redaction of sensitive DNS labels
  - secretproject.example.com → ?.example.com
- Binary Transparency, Key Transparency