MATSUURA LAB.

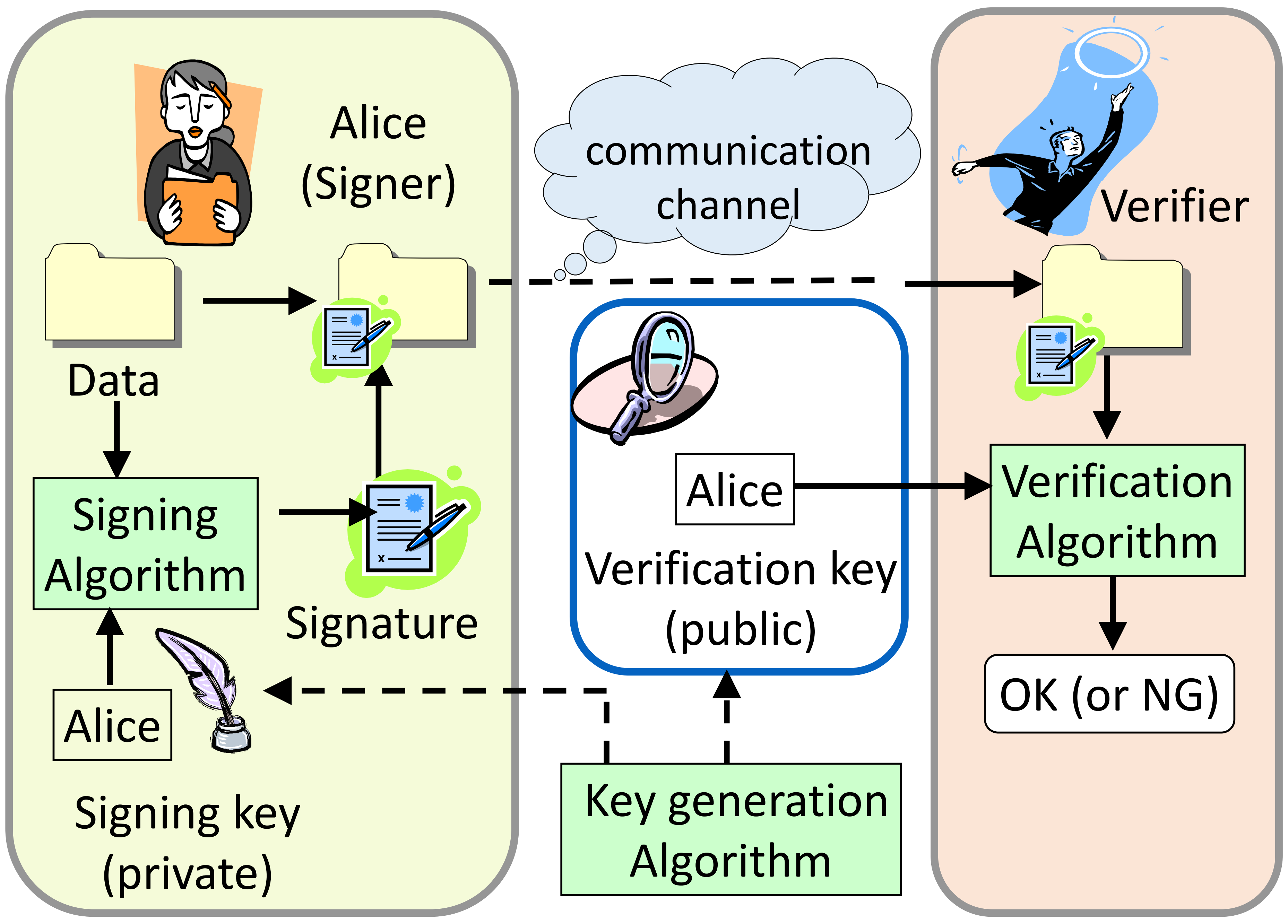
[Cryptography and Information Security]

Department of Informatics and Electronics

Information Security

Information and Communication Engineering Department

http://kmlab.iis.u-tokyo.ac.jp/



Digital Signature

- Cryptographic technology to ensure the integrity of electronic data.
  - Tampering Verification.
  - Spoofing Detection.

Aggregate Signature

- Signature scheme that aggregates many signatures into one and verifies it.

[Merit] : Efficient signature verification.

[Problem] : The inclusion of even one invalid signature invalidates all.

Fault-tolerant Aggregate Signature

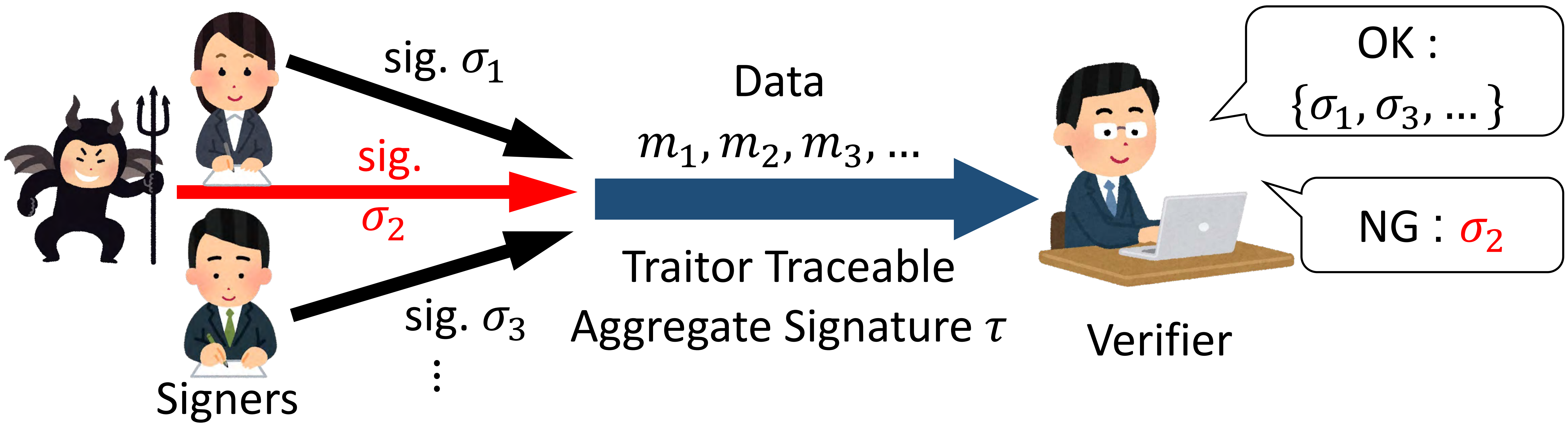
- Some partially aggregated signatures verify valid signatures.

Traitor Traceable Aggregate Signature

- Aggregate signature scheme that makes use of traitor tracing.

[Feature] : Tracks and eliminates invalid signatures in aggregate signature.

[Merit] : Enables efficient verification of aggregate signature even if it contains invalid signatures.


sig. σ_1
sig. σ_2
sig. σ_3
⋮
Signers
Data
$m_1, m_2, m_3, \dots$
Traitor Traceable Aggregate Signature τ
Verifier
OK : $\{\sigma_1, \sigma_3, \dots\}$
NG : σ_2