松浦研究室

[暗号と情報セキュリティ]

生産技術研究所　情報・エレクトロニクス系部門

Department of Informatics and Electronics

情報理工学系研究科

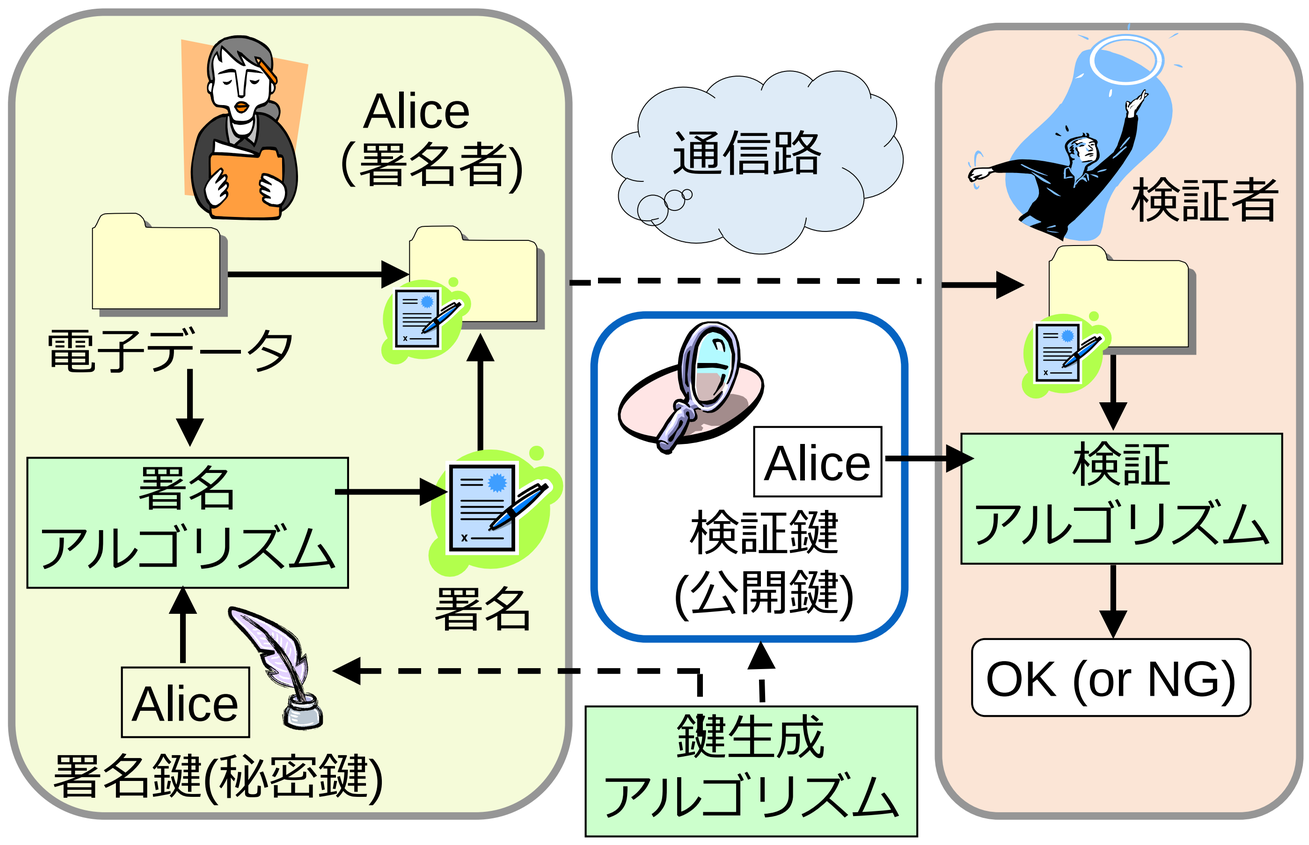
電子情報学専攻

情報セキュリティ

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

電子署名

- 電子データの完全性を保証する暗号技術。
  - 電子データの署名後に改ざんの有無を検証。
  - 署名者のなりすましの存在を検出。



集約署名

- 多数の電子署名を1つに集約して検証する署名方式。

[利点]：効率の良い署名検証。

[問題]：無効署名が1つでも含まれると全署名が無効。

フォールトトレラント集約署名

- 複数の部分的な集約署名から有効署名を検証。

不正署名を追跡可能な集約署名

- 不正者追跡方式を用いて集約署名を作成。

[特徴]：集約署名に含まれる不正署名を追跡し排除。

[利点]：不正署名を含む集約署名でも効率的な署名検証が可能。