松浦研究室

[暗号と情報セキュリティ]

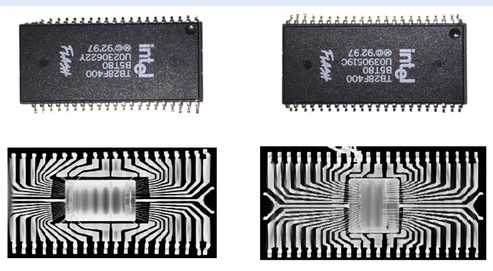
生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics

情報セキュリティ

情報理工学系研究科 電子情報学専攻

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

- モノの電子署名
  購入した製品がもしかしたら偽造品かも？
  - 例）

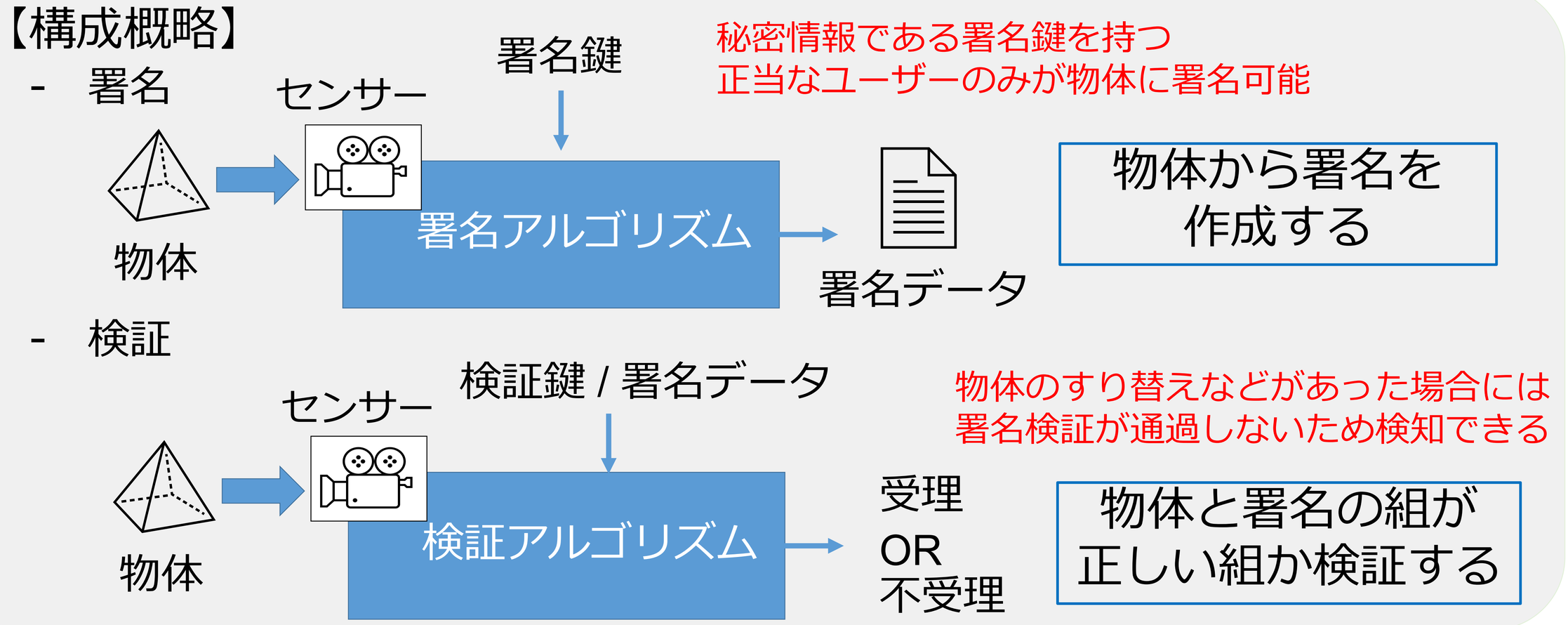


専門家でも本物と偽造品の区別がつかないケースも

フラッシュメモリICの本物とその模造品.
KiarashKevin86 [CC BY-SA 4.0], Wikimedia Commons より引用.

⇒ 電子署名が提供する偽造不可能性 [1] を用いて
理論的に偽造が検知できるような方式の作成を目指す

【構成概略】



従来の電子署名方式を応用することで、基盤とする電子署名方式が偽造不可能であるならば偽造不可能であるような（= 証明可能安全な）モノの電子署名方式を提案 [2]

- 非自明な課題
  - 暗号理論はサイバー空間内で閉じている理論であるが
    「物体をセンサーにかける」操作をどのように記述する？
  - センサーの出力は一定でない可能性が高いが
    ゆらぎのあるデータに対する署名をどのように実現する？
  - 複数の署名を集約して検証するなどの高機能はどこまで実現可能？[3,4]

[1] Goldwasser, S., et al..: A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal on Computing, Vol.17, No.2, pp.281–308 (1988).
[2] 林リウヤほか．“モノの電子署名：物体に署名するための一検討”．2021年コンピュー タセキュリティシンポジウム (CSS2021)，3E-1，オンライン，2021年10月．
[3] 林リウヤほか．“モノの秘匿性を考慮した「モノの電子署名」”．2022年暗号と情報セキュリティシンポジウム (SCIS2022)，3A-2，大阪，2022年1月．
[4] 浅野泰輝ほか．“「モノの電子署名」の複数物体への拡張”．2022年暗号と情報セキュリティシンポジウム (SCIS2022)，3A-6，大阪，2022年1月．