MATSUURA LAB.

[Cryptography and Information Security]

Department of Informatics and Electronics

Information Security

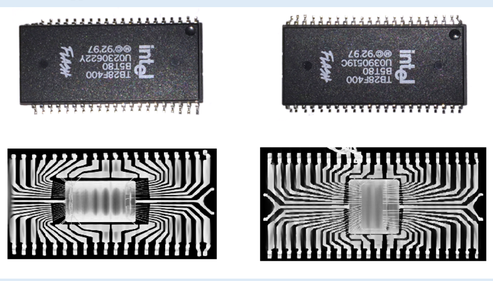
Department of Information and Communication Engineering,

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

- Signature for Objects

  The product you bought could be counterfeit...

  - e.g.)



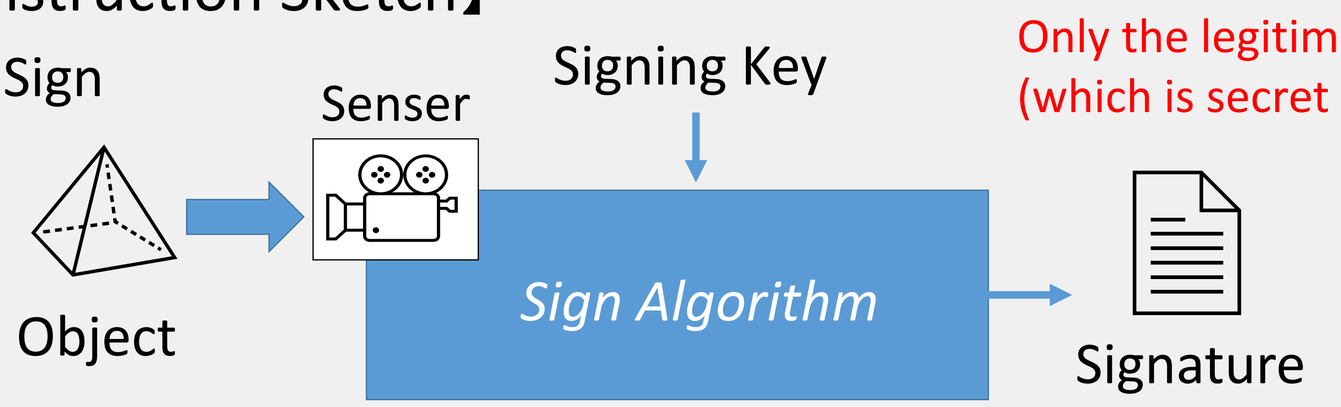
An authentic flash memory IC and its counterfeit replica.
Referenced from KiarashKevin86 [CC BY-SA 4.0], Wikimedia Commons.

Even experts cannot distinguish the authentic one from its counterfeit.

⇒ Using “Unforgeability” which digital signature schemes satisfy [1],
we aim to *create a scheme in which we can detect counterfeits*.

【Construction Sketch】

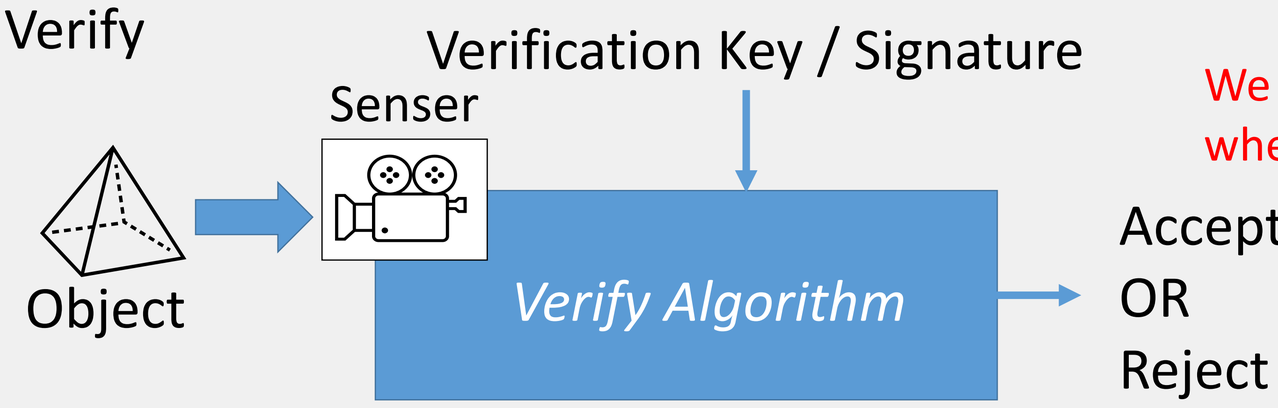
- Sign



Only the legitimate user who has the signing key (which is secret information) can sign objects.

Sign the object (Create a signature for the input object)

- Verify



We can detect counterfeits when the verify algorithm returns reject.

Verify the pair of the object and the signature.

Applying a digital signature scheme, we suggest a provably secure "Signature for Object" scheme which satisfies unforgeability if the based scheme satisfies it. [2]

- Non-trivial Questions
  - Though cryptography is a theory that is closed within cyberspace, how can we formalize physical actions, like sensing objects?
  - Outputs of the sensers is not always constant. So, how to realize a signature scheme for fuzzy messages?
  - To what extent is it possible to achieve advanced functionality? [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．