Security models and proofs: Insights and examples

Sven Laur

Historical perspective

1981 Dolev and Yao, *On the Security of Public Key Protocols.*

1984 Simmons, *Authentication Theory/Coding Theory.*

1993 Bellare and Rogaway, *Entity Authentication and Key Distribution.*

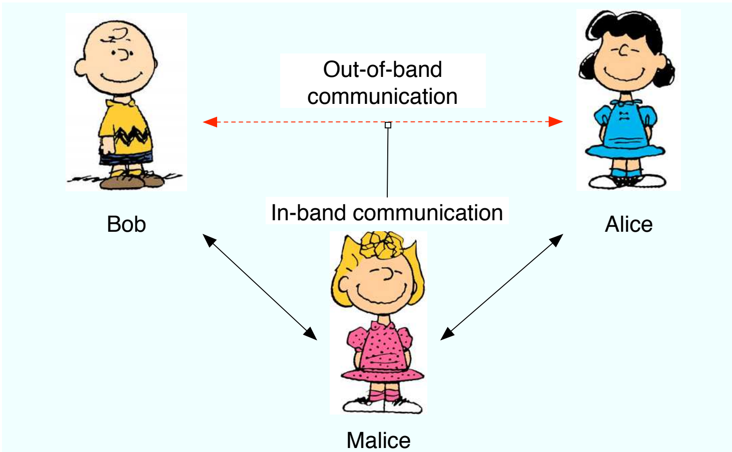
2000 Pfitzmann, Schunter, Waidner
Cryptographic Security of Reactive Systems.

2002 Canetti, Lindell, Ostrovsky, Sahai,
Universally composable two-party and multi-party secure computation.

2003 Lindell, *General Composition and Universal Composability in Secure Multi-Party Computation.* (Security in arbitrary comp. context.)

2005 Serge Vaudenay, *Secure Communications over Insecure Channels Based on Short Authenticated Strings.*

Authentication: stand-alone security model



In-band communication is routed via malicious adversary, Malice, who can read, insert, drop and modify messages.

Out-of-band communication is authentic and sometimes secret. Malice can only read, delay and reorder messages.

Malice succeeds in deception if Alice and Bob accept different outputs.

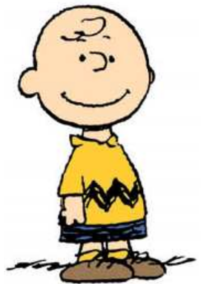
Classical message authentication

Alice

Send $k \leftarrow \mathcal{K}$ over a confidential channel. $\longrightarrow$

Send m and a tag $\texttt{tag} = h(m, k)$. $\longrightarrow$

Bob accepts m iff $\texttt{tag} = h(m, k)$.



Bob

As Malice does not know the secret key k there are two attack types:

- Impersonation attacks. Malice tries to inject a message $\widehat{m}$ when Alice has not sent any messages.
- Substitution attacks. Malice tries to change a message m into $\widehat{m}$ by choosing a proper $\widehat{\texttt{tag}}$.

Necessary properties of the hash functions

Impersonation attacks. For every message m, the tag distribution

$$\mathcal{D}_m = \{h(m, k) : k \leftarrow \mathcal{K}\}$$

must be (computationally) close to uniform distribution.

Substitution attacks. The tag $h(m, k)$ should reveal minimal amount of information about the key and tag, i.e., a (computational) conditional entropy $H(h(\widehat{m}, k)|h(m, k)),\ m \neq \widehat{m}$ must be maximal.

There are hash-functions (*perfect hash functions*) that provide optimal information-theoretic security for a single protocol run. Many fast and computationally secure message authentication codes are built on top of information-theoretic counterparts using pseudorandom generators.

Towards Bellare-Rogaway model

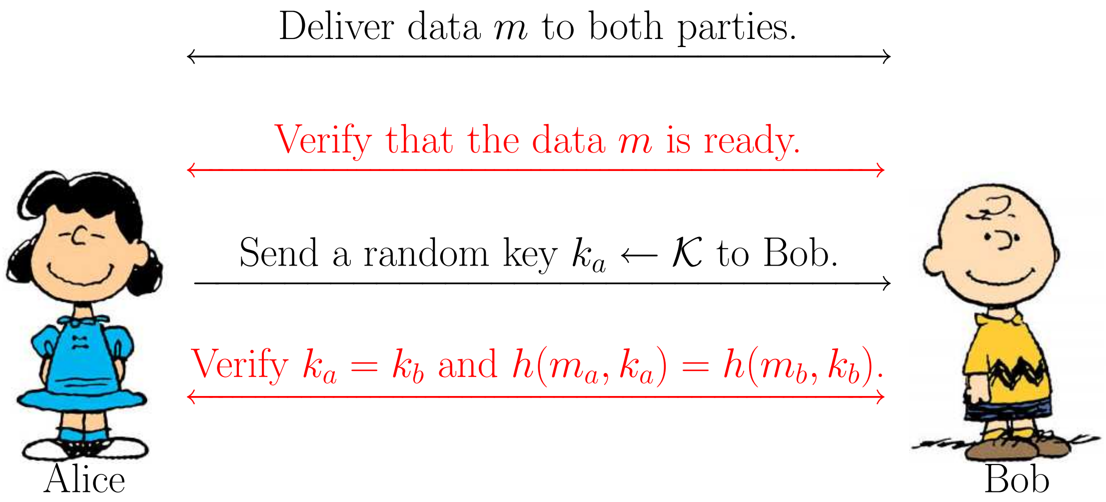
Add to the stand-alone model

- Man-in-the-middle attack
- Interleaving attack
- Random timing
- Worst possible scenario

Security in Bellare-Rogaway model

- Is the classical message authentication protocol secure in BR-model?
- If not under which restrictions this protocol is secure?
- How to construct a corresponding mutual authentication protocol?

MANA II protocol



Security proof

- What happens if Malice does not deliver data before synchronisation?
- What happens if Malice changes k to $\widehat{k}$?
- How is the remaining attack called? Which properties must h satisfy?

Security in Bellare-Rogaway model

Let the final check value of MANA II be 2ℓ bits long (i.e. $2^{-\ell}$-secure). Let q be the maximal number of protocols run in parallel.

- Show that MANA II is not secure in BR-model?
- Give a simple lower bound on security w.r.t. q and ℓ?
- Is the lower bound w.r.t. q and ℓ also the upper bound?
- If not under which restrictions this protocol is secure?

Rewinding is incompatible with parallel runs

Example: Blum's coin flipping protocol run in parallel.

Alice sends a commitment Com(x) for $x \leftarrow \{0,1\}$ to Bob.

Bob sends $y \leftarrow \{0,1\}$ to Alice who opens Com(x) and both output $x \oplus y$.

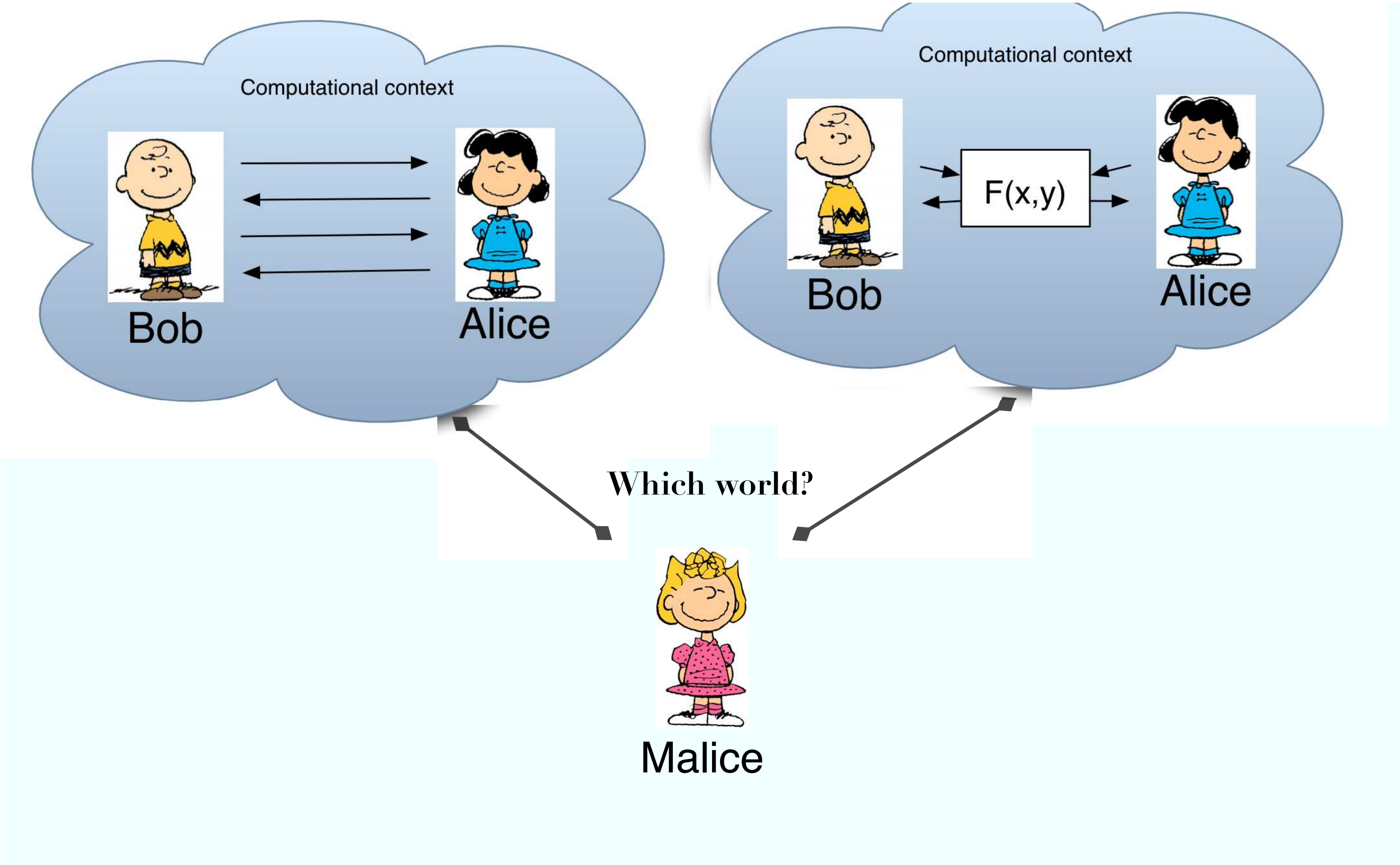
Task 1: Force the output $x \oplus y = 0$ by sending different Com(x) values.

Task 2: Force the output $x_i \oplus y_i = 0,\ i = 0,1$ by sending:

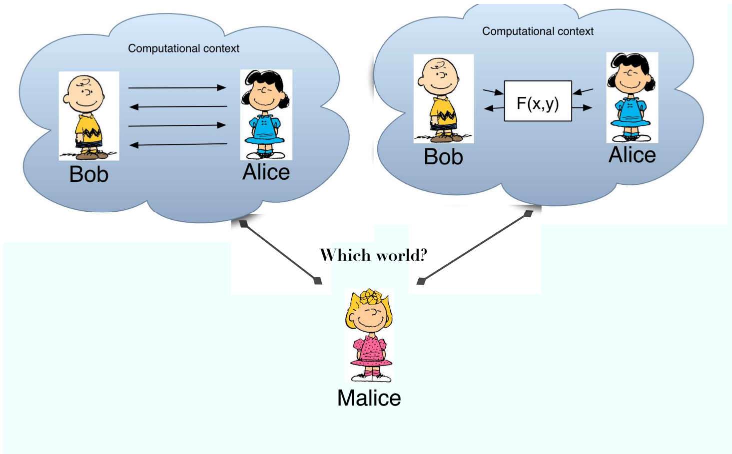
- different Com(x) values sequentially to Bob;
- different Com(x) values concurrently to Bob.

Where is the catch? Why there is a state space explosion?

Security in any computational context



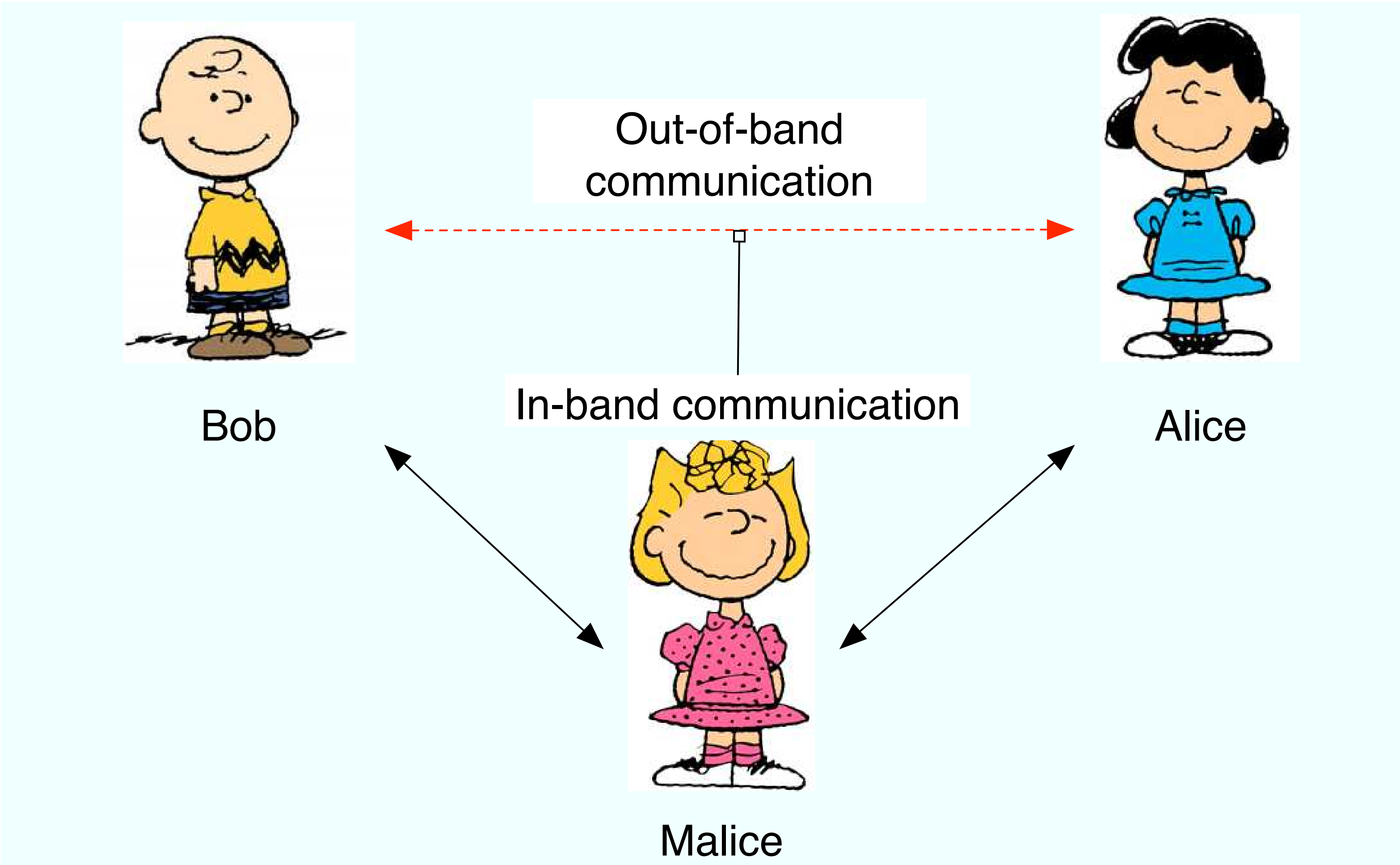
Security in any computational context



A protocol is secure in any computational context if:

- The protocol is secure in the stand-alone model.
- There is no rewinding arguments in the proof.
- Simulators used in the proofs are black-box and universal.
- Protocol messages can be separated from other messages

What is the biggest challenge in stand-alone model?



Classification of authentication protocols

- Based on long pre-shared values:
  (a) Classical message authentication (*pre-shared secrets*)
    - HMAC
    - CBC-MAC.

  (b) Public key infrastructure (*pre-shared certificates*)
    - X.509 certificates and authentication

- Based on interactive authentic communication:
  (a) Password-based authentication (*short confidential messages*)
    - WPA-PSK, WEP-TKIP
    - EKE, EKE2, SPEKE

  (b) Manual authentication (*short authentic test tags*)
    - MANA II
    - MANA IV

Manually authenticated key exchange

- Classical key exchange + Manual authentication
  – MA–DH (*specially optimised*)
- Hybrid encryption + Manual authentication
  – manually authenticated hybrid encryption
- ???

Known upper bounds and corresponding attacks

- Guessing attack with success $2^{-\ell}$ affects
  - classical authentication
  - password-protected key exchange

- Simple collision attack with success $2^{-\ell}$ affects
  - manual authentication