Impossibility Result for Secret Establishment

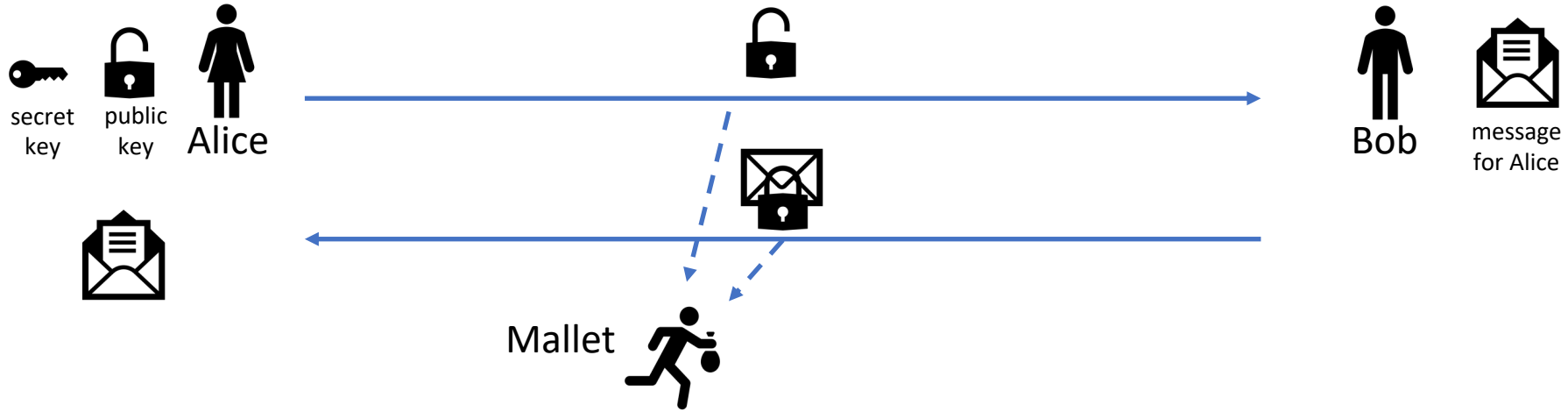
Patrick Schaller

Overview

- Motivation
- “Formal” Model
- Proof
- Summary

Motivation

- In 1976 Whitfield Diffie and Martin Hellman have introduced public key cryptography in their seminal paper “New Directions in Cryptography” [DH76].
- In their work, Diffie and Hellman have showed a way, how authentic communication from Alice to Bob can be turned into secret communication from Bob to Alice.



Motivation

- In [DH76] Diffie and Hellman have proposed a key exchange mechanism/protocol, that allows Alice and Bob to derive a shared secret key over an authentic channel in the presence of an attacker.
  - The security of the protocol is based on the difficulty of the discrete logarithm problem in finite fields.
- In [RSA78] Rivest, Shamir and Adleman propose public key encryption and a digital signature scheme.
  - The scheme is based on the difficulty of factoring natural numbers.

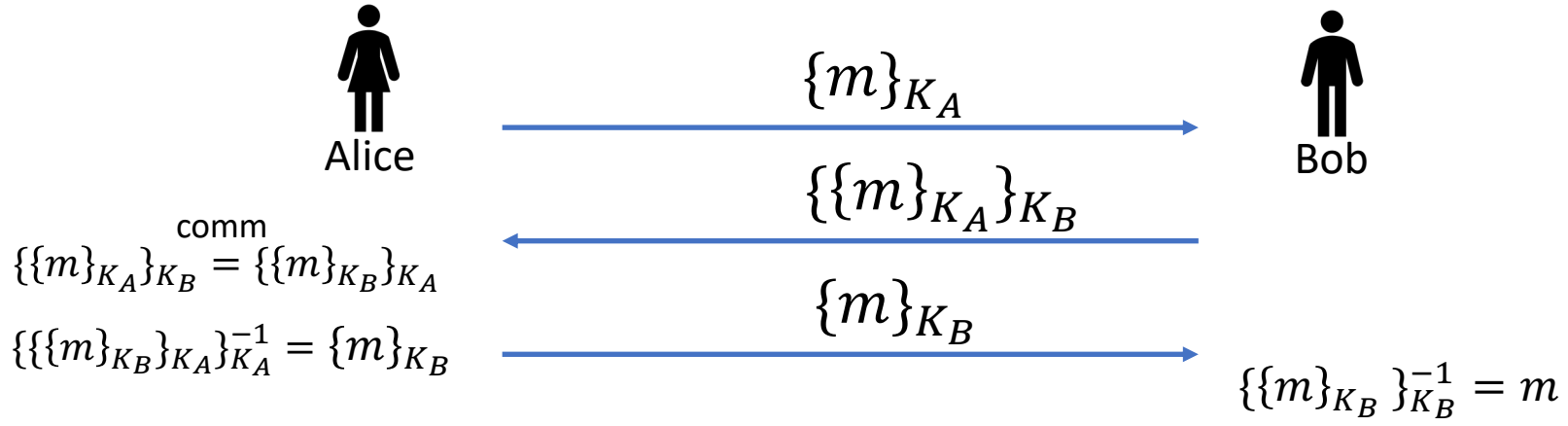
Motivation

- What do we need in terms of “ingredients” to create a public-key encryption (or key exchange) scheme?
- The existing schemes for public-key cryptography are based on advanced algebra (finite fields, elliptic curves).
- On the other hand symmetric cryptographic algorithms, in comparison to their public-key counterpart, use much simpler mathematical operations (cp. RC4, Trivium, DES,...).
  - To be fair, one has to admit that the security guarantees of symmetric algorithms are based on heuristics, whereas in the case of asymmetric algorithms guarantees can be “related” to hard math problems.

Motivation

- How do functions look like that enable us to build public key algorithms/protocols?

Shamir's "Three Pass Protocol" uses a commutative encryption scheme with the property:
$\{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A}$ ($\{m\}_K$ denotes encryption of message m with key K)



- Does this work for $\oplus$ (xor) as it is used for the One-Time Pad?

Motivation

- No, unfortunately it does not work with $\oplus$ (xor).
  - xor has (besides commutativity) the additional property that it is self-inverse, i.e., $K_A \oplus K_A = 0$.
  - In the protocol we use the first $(m \oplus K_A)$ and the second message $((m \oplus K_A) \oplus K_B)$ to build $m \oplus K_A \oplus (m \oplus K_A) \oplus K_B = m \oplus m \oplus K_A \oplus K_A \oplus K_B = K_B$, and thus we can derive the secret message m from the last message $m \oplus K_B$.
- *However, could there exist other, perhaps three, five or seven step protocols that enable Alice and Bob to exchange/create a secret in the presence of a passive attacker?*

Model: Knowledge

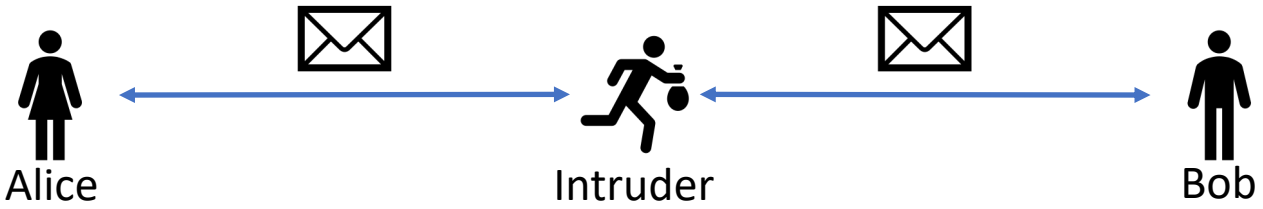
- Consider two honest agents Alice and Bob.
- Alice and Bob both have a knowledge K_{Alice} and K_{Bob}.
- Alice and Bob can create fresh messages (keys, secrets, nonces), but before any run, we assume $K_{Alice} \cap K_{Bob} = \emptyset$.
- For the attacker I, we assume that his knowledge K_I is initially empty.
- We further assume, that honest agents, as well as the attacker, may use $\bigoplus(xor)$ to build new message, i.e., $a, b \in K_x \Rightarrow a \bigoplus b \in \overline{K_x}$.
- By $\overline{K}$ we denote the closure of the knowledge K under $\bigoplus(xor)$

Model: Equational Theory

- In terms of $\oplus$ we consider the following equational theory:
  - Associativity: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
  - Commutativity: $a \oplus b = b \oplus a$
  - Null-String: $0 \oplus a = a \oplus 0 = a$
  - Self-Inverse: $a \oplus a = 0$
- We get a so called *symbolic message* model.
  - We do not take the length of strings into account (could be padded up to a certain length).
  - We do not take probabilities into account (e.g., that a certain string could be guessed).

Model: Communication

- To exchange a message, Alice and Bob hand a message over to the attacker.
- Without loss of generality, we assume that Alice starts the protocol sending message m_1, Bob sending message m_2, etc.
- We thus get the following rules:
  - $K_I^{i+1} = K_I^i \cup \{m_{i+1}\}$
  - $m_{2i+1} \in \overline{K_{Alice} \cup K_I^{2i}}$ and $m_{2i} \in \overline{K_{Bob} \cup K_I^{2i-1}}$



Model: Security Properties

- Alice and Bob manage to create a shared secret, if they exchange a set of messages, such that both can derive a term, that cannot be derived by the attacker.
- In our model: There is a message m_{secret}, where:

$$m_{secret} \in \overline{K_{Alice} \cup K_I^j} \cap \overline{K_{Bob} \cup K_I^j}, \text{ but } m_{secret} \notin \overline{K_I^j}$$

- Alice and Bob can derive m_{secret} after j communication steps, but the attacker cannot derive m_{secret} from the messages exchanged between Alice and Bob.

Impossibility Proof

- **<u>Claim:</u>** There is *no* protocol that would enable Alice and Bob to create a shared secret in the presence of a (passive) attacker, using only $\oplus$ (xor), if they did not share a secret beforehand.
- We will use the symbolic message model and the communication model introduced on the last slides.
- The proof is done in our model by contradiction, i.e., we assume that such a protocol exist and show that this leads to a contradiction.

Proof

- Without loss of generality, we assume $\overline{K_{Alice}} \cap \overline{K_{Bob}} = \emptyset$ and $K_I^0 = \emptyset$.
- Furthermore, we assume that Alice starts communication and that Alice and Bob exchange messages alternatively:
  - every $(2i+1)$-th message is sent by Alice, thus $m_{2i+1} \in \overline{K_{Alice} \cup K_I^{2i}}$,
  - every $2i$-th message is sent by Bob, thus $m_{2i} \in \overline{K_{Bob} \cup K_I^{2i-1}}$.
- Let $l_0 = 2i_0 + 1$ be the step, in which Bob can derive message m_{secret} which Alice already holds, but the attacker cannot reconstruct.
- Then $m_{secret} \in \overline{K_{Alice} \cup K_I^{2i_0}}$, $m_{secret} \in \overline{K_{Bob} \cup K_I^{2i_0+1}}$, but $m_{secret} \notin \overline{K_I^{2i_0+1}}$.

Proof

- Consider the last message sent by Alice m_{2i_0+1}, then we have $\overline{K_I^{2i_0+1}} = K_I^{2i_0} \cup \{m_{2i_0+1}\}$
- Because of the equational properties of $\oplus$, we know that $m_{2i_0+1} = m_A \oplus m_I$, where $m_A \in \overline{K_A}$, but $m_A \notin K_I^{2i_0}$, and $m_I \in K_I^{2i_0}$.
- As a consequence, we know that $m_A \in \overline{K_I^{2i_0+1}}$.
- We also know that $m_{secret} = m_{2i_0+1} \oplus m = m_A \oplus m_I \oplus m$, where $m \in K_B \cup K_I^{2i_0}$ and thus $m \in K_I^{2i_0}$ (else already m would already be a shared secret)
- But then we have $m_{secret} \in \overline{K_I^{2i_0+1}}$ ⚡

Summary

- We have shown that there cannot exist *any* secret establishment protocol in the presence of a passive attacker that uses only $\oplus$ (xor).
- We have have proven our claim that no such protocol exists by first assuming that such a protocol exists and by showing that this leads to a contradiction.
- In our work [SSB10] we have extended the results to more general cases of equational theories and proved the corresponding results with the theorem prover Isabelle/HOL.

References

- [DH76]: “New Directions in Cryptography” W.Diffie, M.Hellman, IEEE Transactions on Information Theory, 1976
- [RSA78]: “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, R.Rivest, A.Shamir, L.Adleman, Communications of the ACM 21, 1978
- [SSB10]: “Impossibility Results for Secret Establishment”, B.Schmidt, P.Schaller, D.Basin, IEEE Computer Security Foundations Symposium (CSF), 2010