CRYPTOGRAPHY

(lecture 8)

Literature:

"To Signal or Not to Signal?.." By Nelson, Pagnin, Askarov (**Section 3**)
"Analysing the Signal Protocol", D. Van Dan (ch 2.1.0-2.1.3)
"Post Quantum Cryptography", by T. Frederiksen
"A Graduate Course in Applied Cryptography" (ch **14.0,14.1.0,8.3**)

Announcements

- Office Hours! **Ivan** from next week (announcement on Canvas later today)
- Lecture on Dec 13th: course recap + info about exam
- Lecture on Dec 9th: by **Victor** on ABC
- All next exercise sessions by **William**
- HA2 deadline: Tuesday **29th** (1st submission)
- Bonus 2 deadline: Friday **2nd**
- HA3 deadline: Tuesday **13th** (1st submission)
- Bonus 3 deadline: Tuesday **20th**
- HARD deadline for final submission: **Jan 8th** (Sunday)
- TAs are supposed to provide feedback within 1 week from the 1st submission deadline; for re-submissions within 1 week from the submission day (timings will be affected by holidays)

Module 2: Agenda

OW(Trapdoor)Functions
DH Key-Exchange
DL, CDH, DHH
Number Theory
RSA, ElGamal Cryptosystems
IND-CPA and IND-CCA
Digital Signatures

Secure Instant Messaging

- Security Notions
- The Signal Protocol
- Session Hijacking Attack

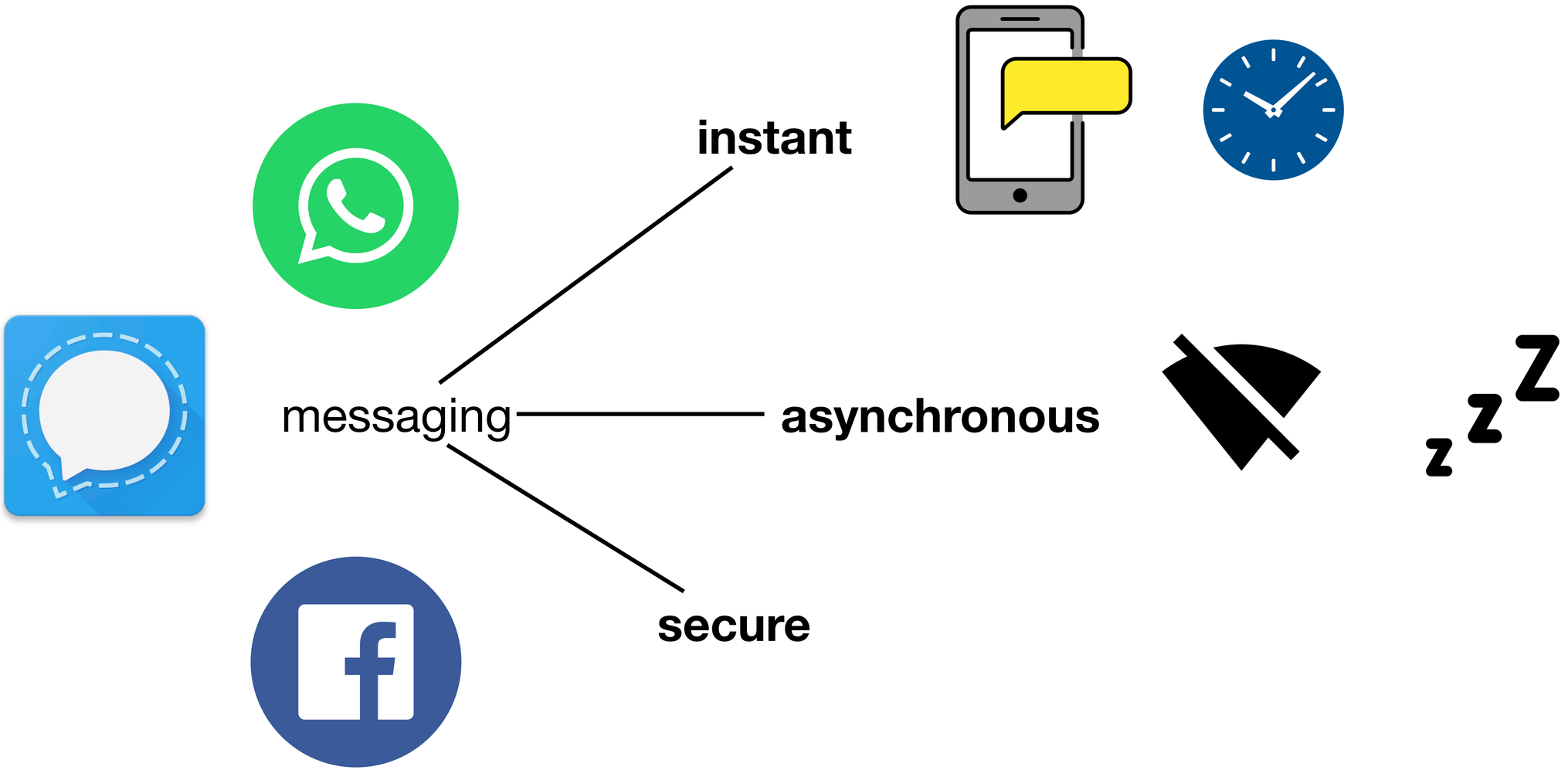
Post Quantum Cryptography

- The Lifespan of a Cryptosystem
- The State of Quantum Computers
- Landscape of PQC

Hash Functions

- Lamport PQ Secure Signature
- The Birthday Paradox - Proof

Signal: Privacy That Fits Your Pockets



Cryptographic Building Blocks

5.2. Recommended cryptographic algorithms

Taken from here

The following choices are recommended for instantiating the cryptographic functions from Section 3.1:

- ***GENERATE_DH()***: This function is recommended to generate a key pair based on the Curve25519 or Curve448 elliptic curves [7].
- ***DH(dh_pair, dh_pub)***: This function is recommended to return the output from the X25519 or X448 function as defined in [7]. There is no need to check for invalid public keys.
- ***KDF_RK(rk, dh_out)***: This function is recommended to be implemented using HKDF [3] with SHA-256 or SHA-512 [8], using *rk* as HKDF *salt*, *dh_out* as HKDF *input key material*, and an application-specific byte sequence as HKDF *info*. The *info* value should be chosen to be distinct from other uses of HKDF in the application.

tiny variation of HMAC

- ***KDF_CK(ck)***: HMAC [2] with SHA-256 or SHA-512 [8] is recommended, using *ck* as the HMAC key and using separate constants as input (e.g. a single byte 0×01 as input to produce the message key, and a single byte 0×02 as input to produce the next chain key).
- ***ENCRYPT(mk, plaintext, associated_data)***: This function is recommended to be implemented with an AEAD encryption scheme based on either SIV or a composition of CBC with HMAC [5], [9]. These schemes provide some misuse-resistance in case a key is mistakenly used multiple times. A concrete recommendation based on

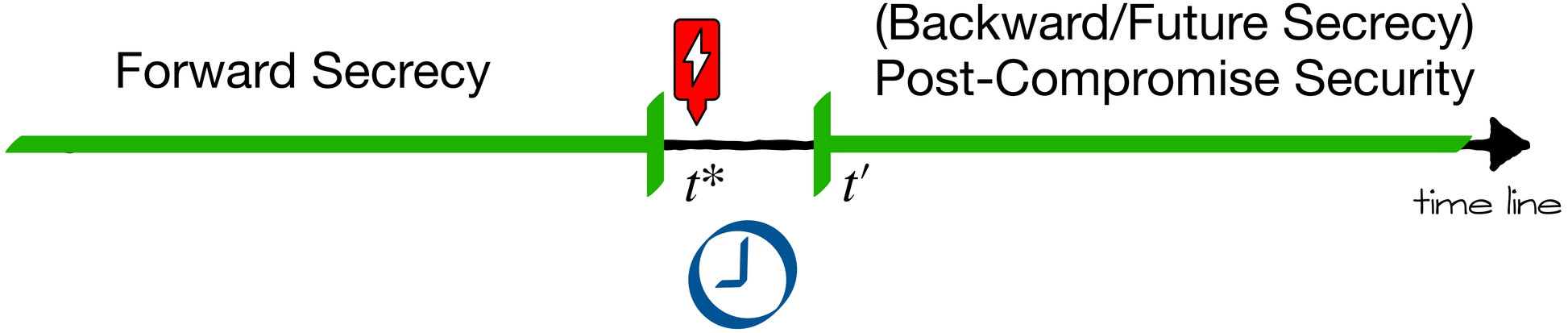
Signal: Privacy That Fits Your Pockets

secure messaging

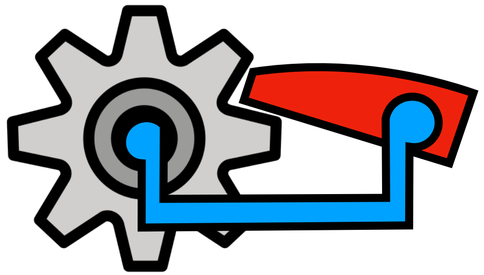
- end-to-end encryption
- interlocutor authentication
- message integrity

Signal: Privacy That Fits Your Pockets

secure messaging

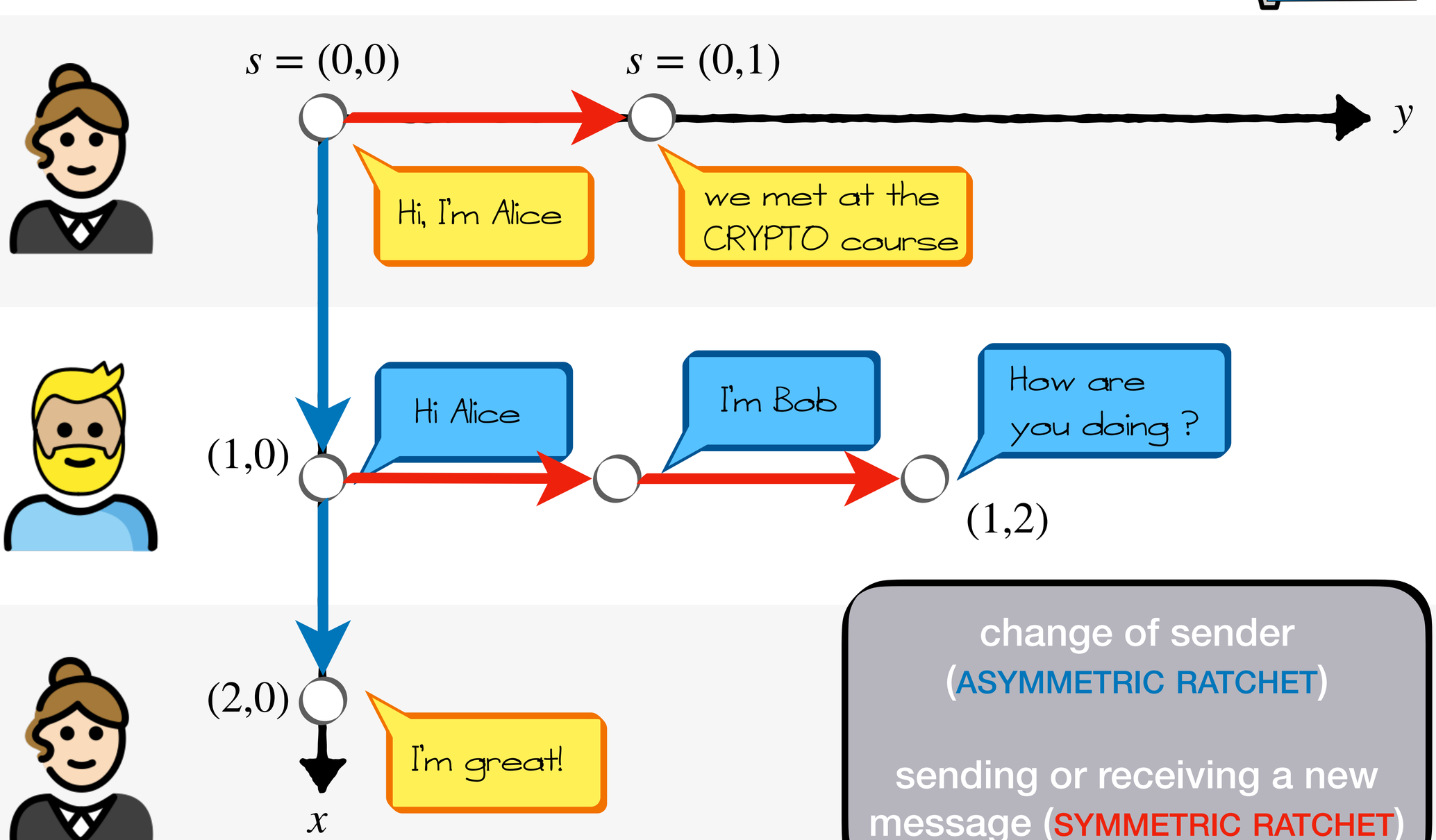


healing window



ratchet

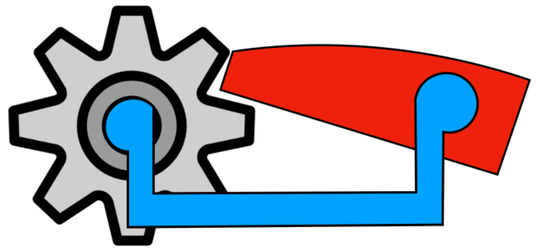
The Time Line of Asynchronous Messaging

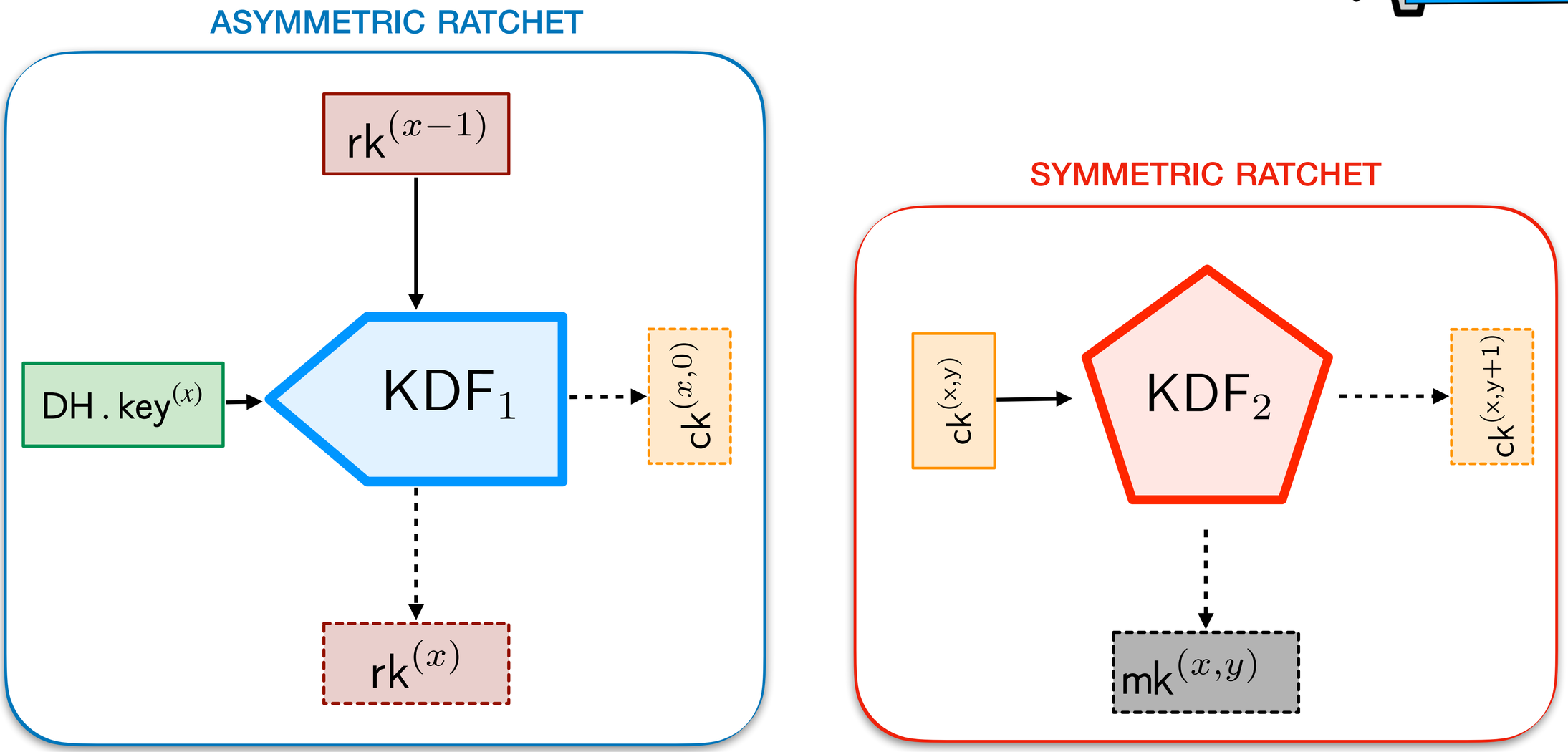


change of sender (ASYMMETRIC RATCHET)

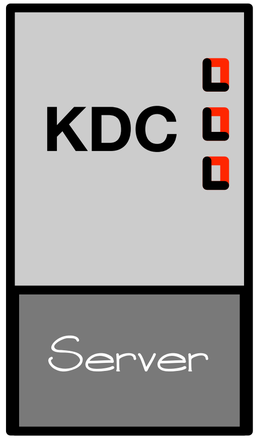
sending or receiving a new message (SYMMETRIC RATCHET)

Asymmetric & Symmetric Ratcheting





Signal: Registration Phase



Bob's key bundle

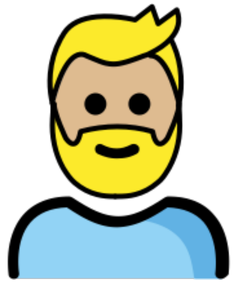
$$\text{Sign}(sk_B, mtpk_B) \rightarrow \begin{pmatrix} pk_B \\ mtpk_B \\ ephpk_B^{(1)} \\ ephpk_B^{(2)} \\ \vdots \\ sgn_B \end{pmatrix}$$

DH keys

$$sk = x \leftarrow \$ - \mathbb{Z}_q$$
$$pk = g^x \in \mathbb{G}$$

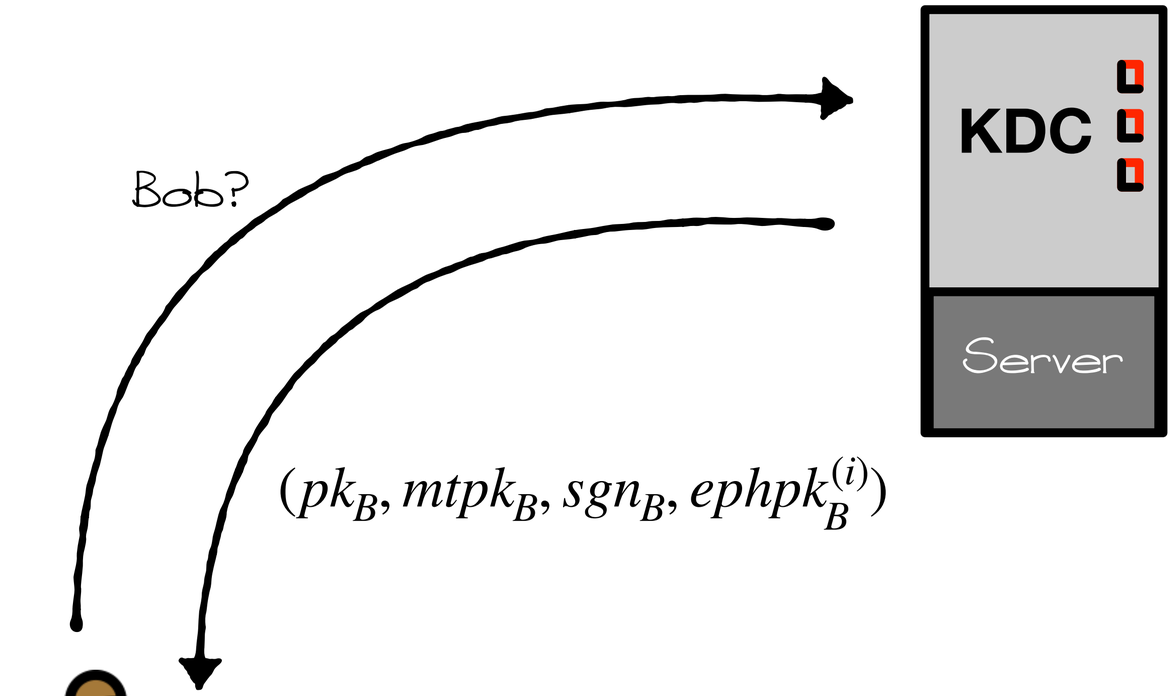
one long term identity key pair (pk_B, sk_B)

one medium term **prekey** pair $(mtpk_B, mtsk_B)$



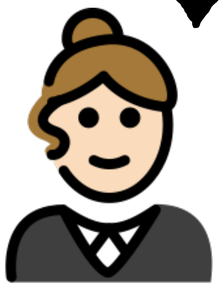
multiple one-time **ephemeral** key pairs $\{(ephpk_B^{(i)}, ephsk_B^{(i)})\}_{i=1}^{N}$

Signal: Session Setup Phase

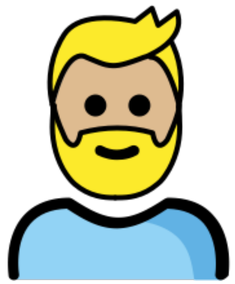


Bob's key bundle

$$\begin{pmatrix} pk_B \\ mtpk_B \\ ephpk_B^{(1)} \\ ephpk_B^{(2)} \\ \vdots \\ sgn_B \end{pmatrix}$$



$\texttt{ms=(}\ (mtpk_B)^{sk_A}\ ||\ (pk_B)^{esk_A}\ ||\ (mtpk_B)^{esk_A}\ ||\ (ephpk_B)^{sk_A}\ \texttt{)}$



sk_A	**identity** key
$mtsk_A$	**prekey**
$\{ephsk_A^{(i)}\}$	**ephemerals**

fresh ephemeral key pair

$esk_A = x \leftarrow \$ - \mathbb{Z}_q$

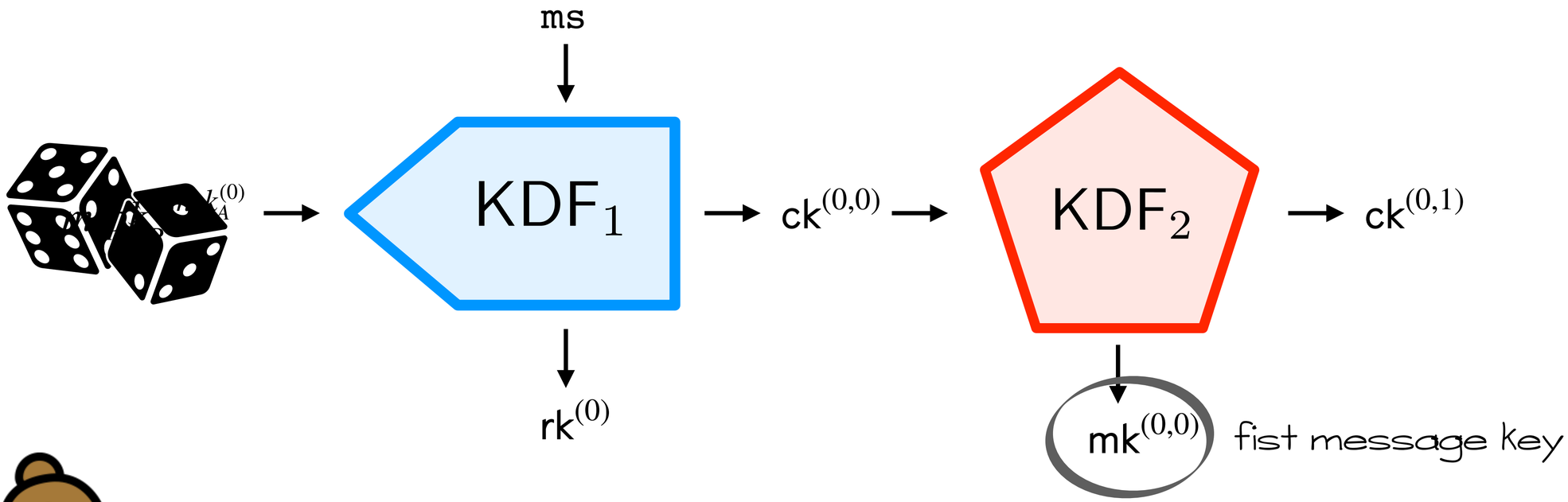
$epk_A = g^x \in \mathbb{G}$

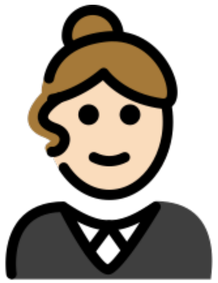
(pk_B, sk_B)

$(mtpk_B, mtsk_B)$

$\{(ephpk_B^{(i)}, ephsk_B^{(i)})\}_{i=1}^{N}$

Signal: Asymmetric Ratchet … And Symmetric Ratchet





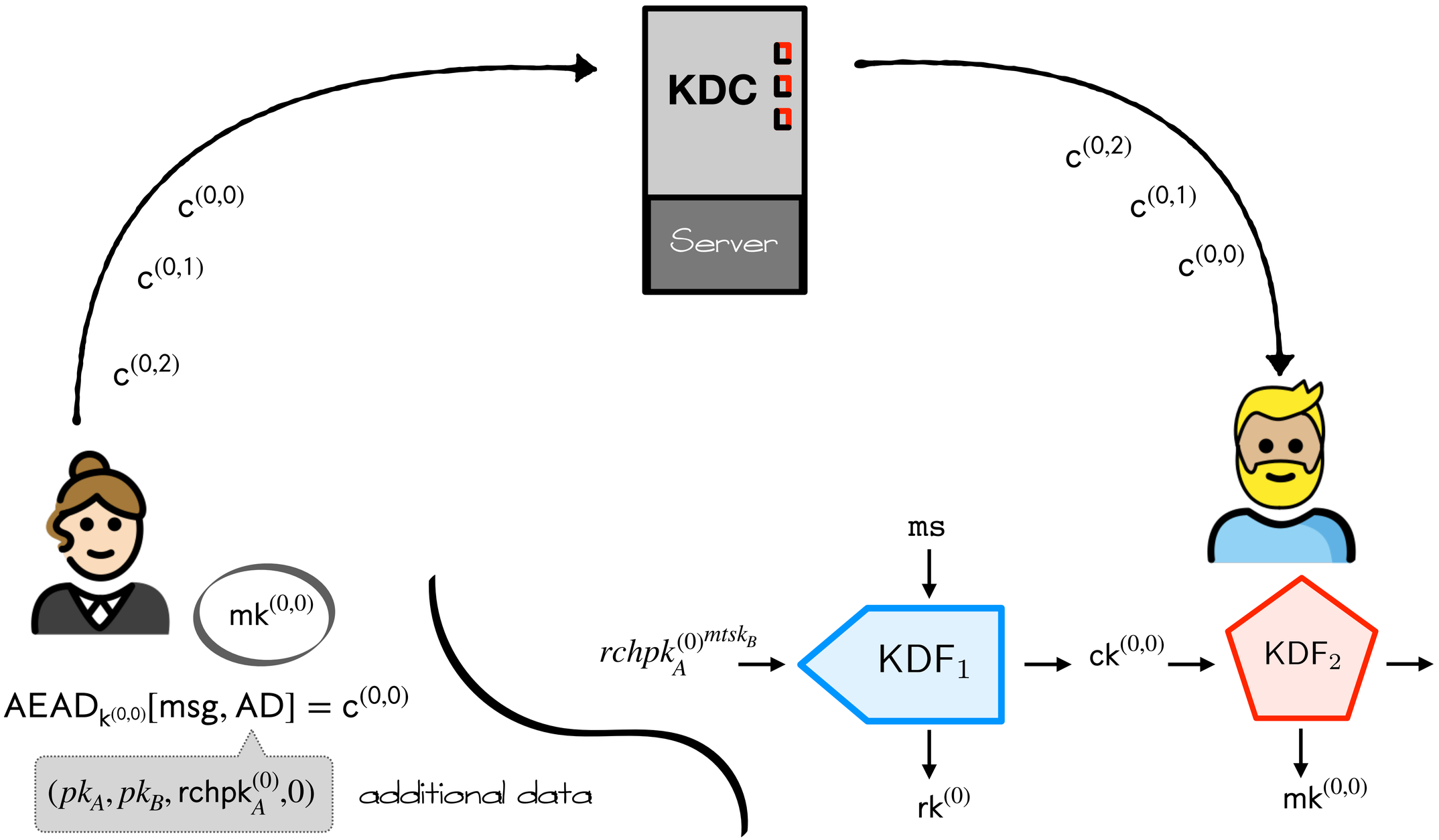
$\texttt{ms=}(\ (mtpk_B)^{sk_A} \ || \ \ (pk_B)^{esk_A} || \ (mtpk_B)^{esk_A} \ || \ (ephpk_B)^{sk_A})$

fresh *ratchet* key pair

$$rchsk_A = x \leftarrow \$ - \mathbb{Z}_q$$

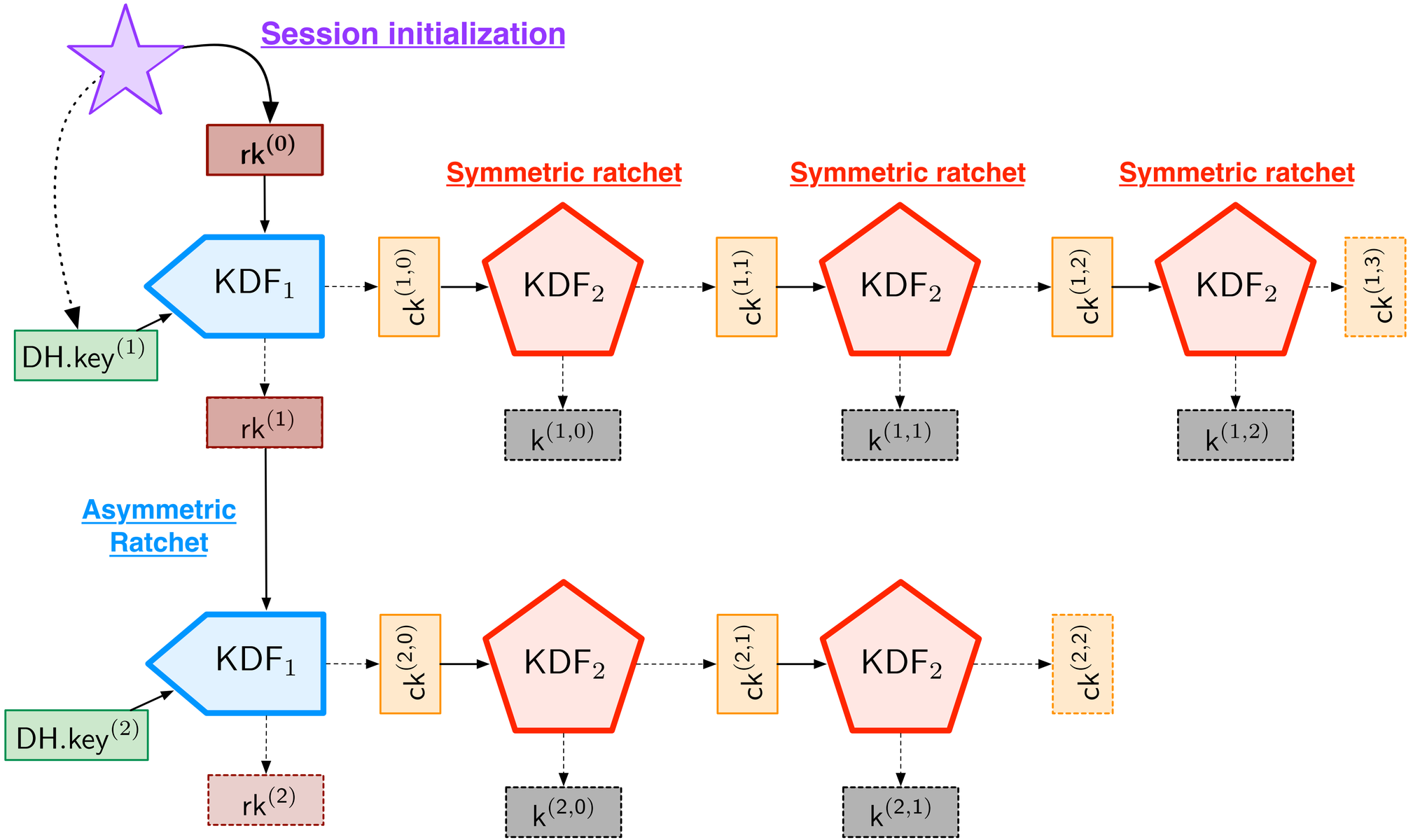
$$rchpk_A = g^x \in \mathbb{G}$$

Signal: Messaging

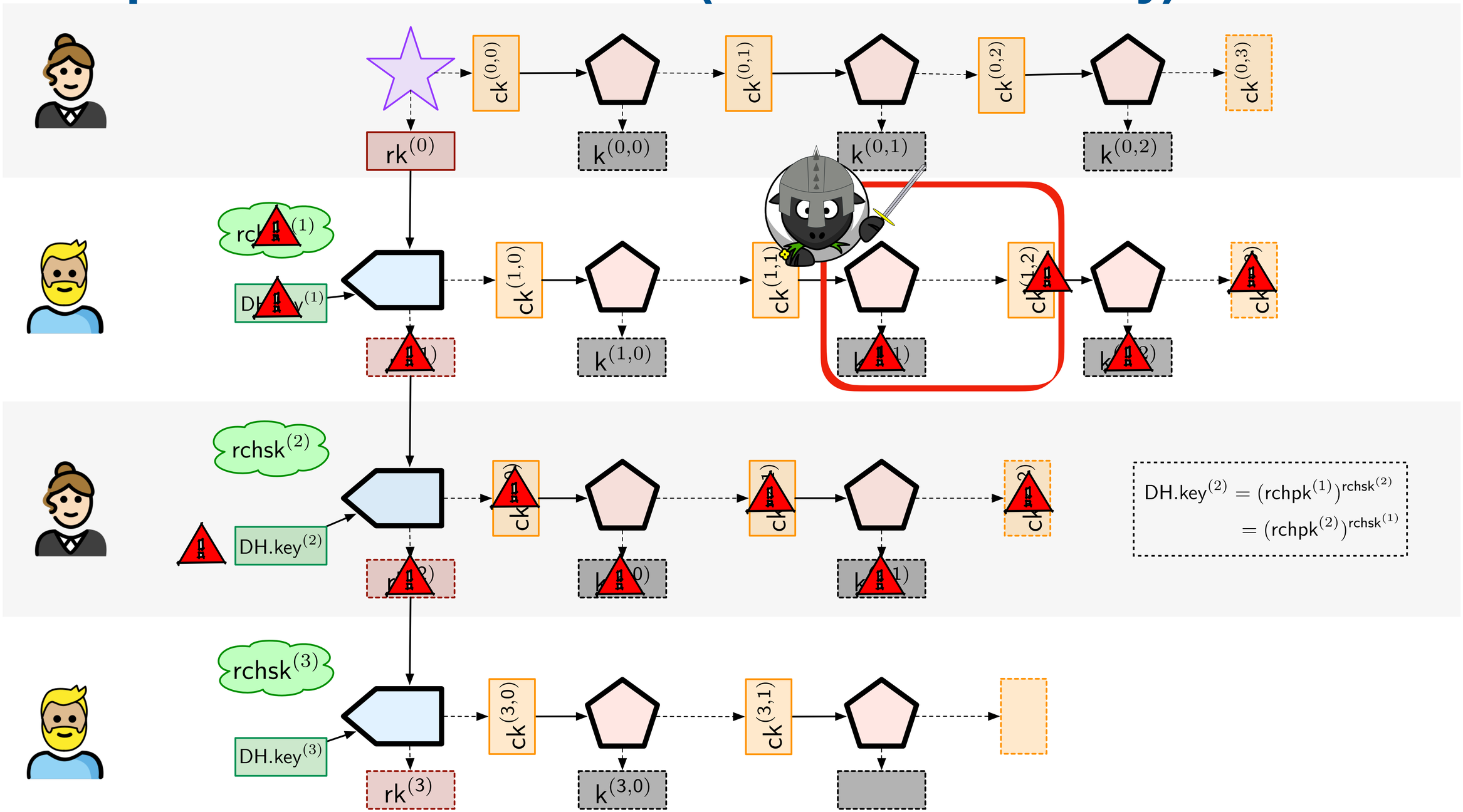


Two Layers of Ratchets

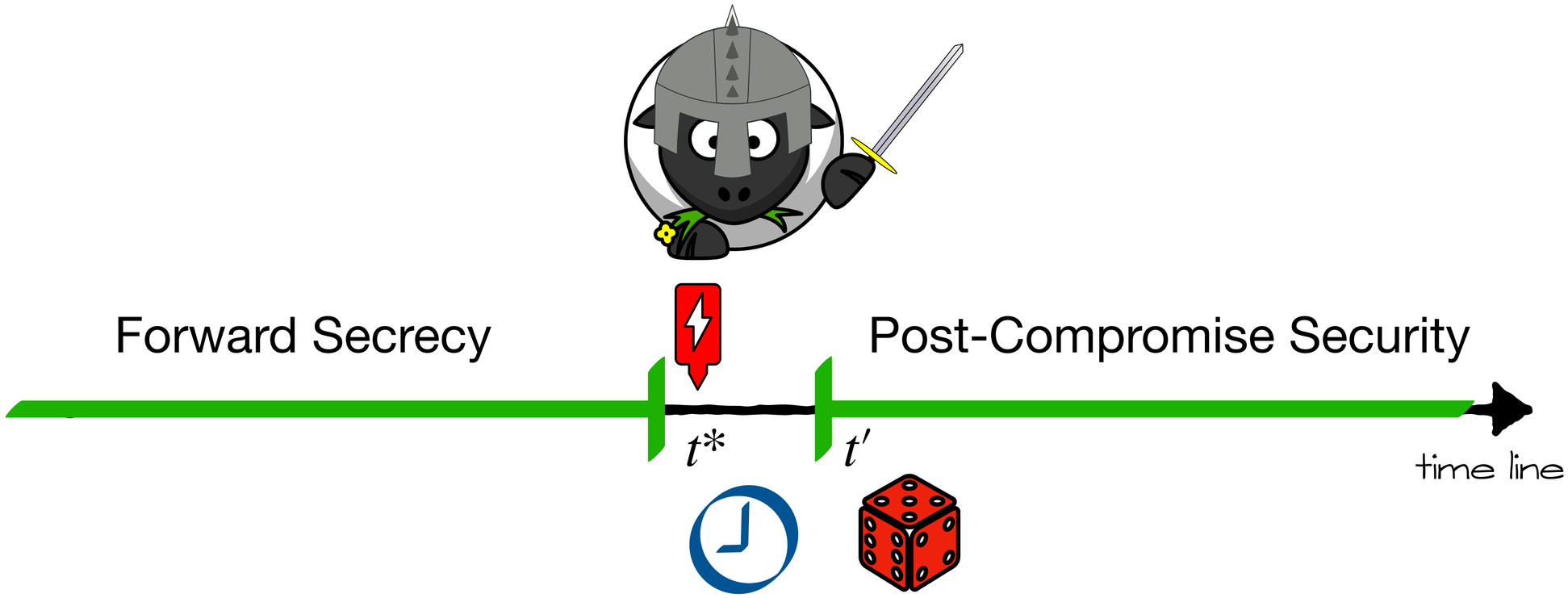
Note: from now on the message key **mk** *is denoted as* **k**



The Impact of Reveal Attacks (Passive Adversary)



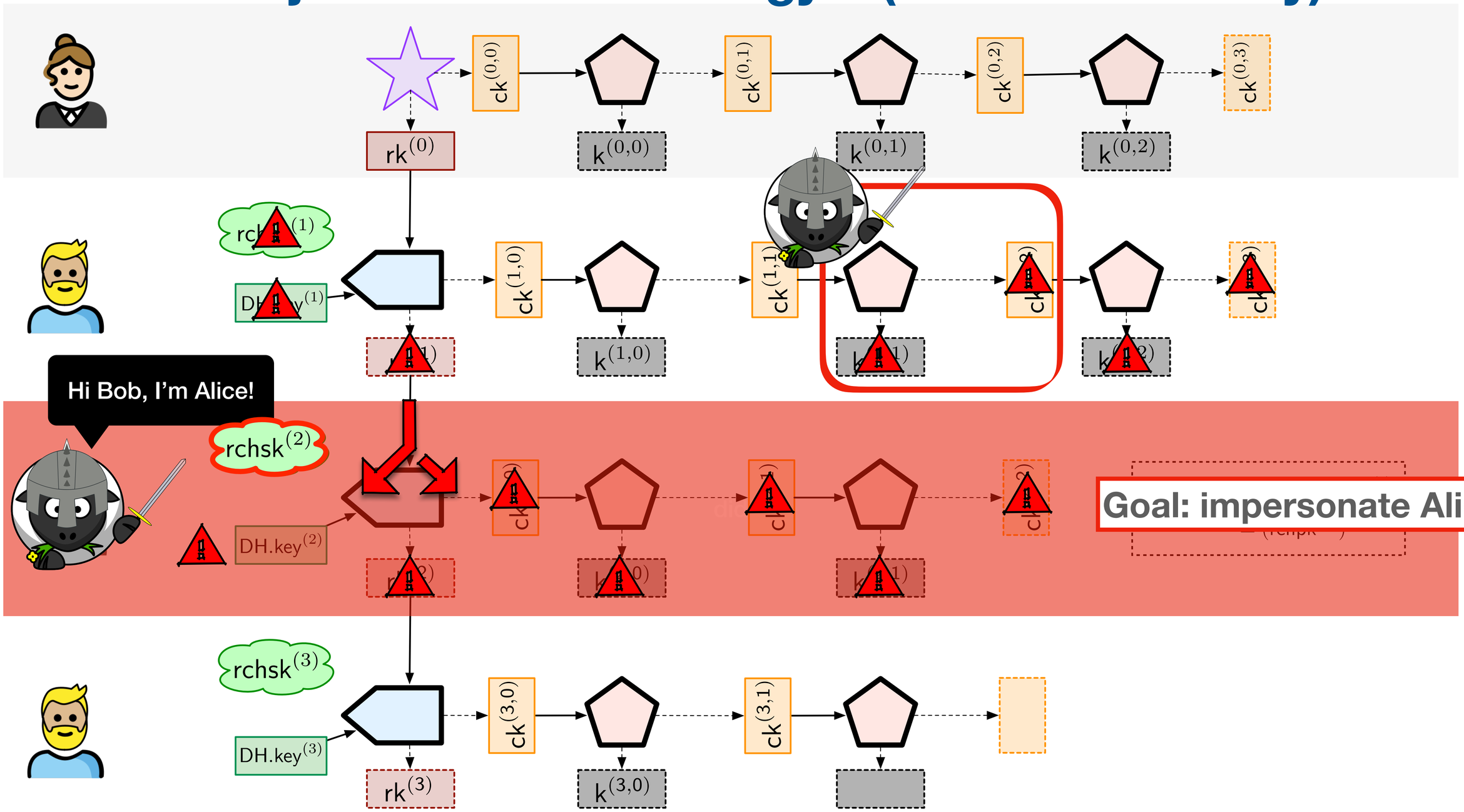
Healing Window for Reveal Attacks



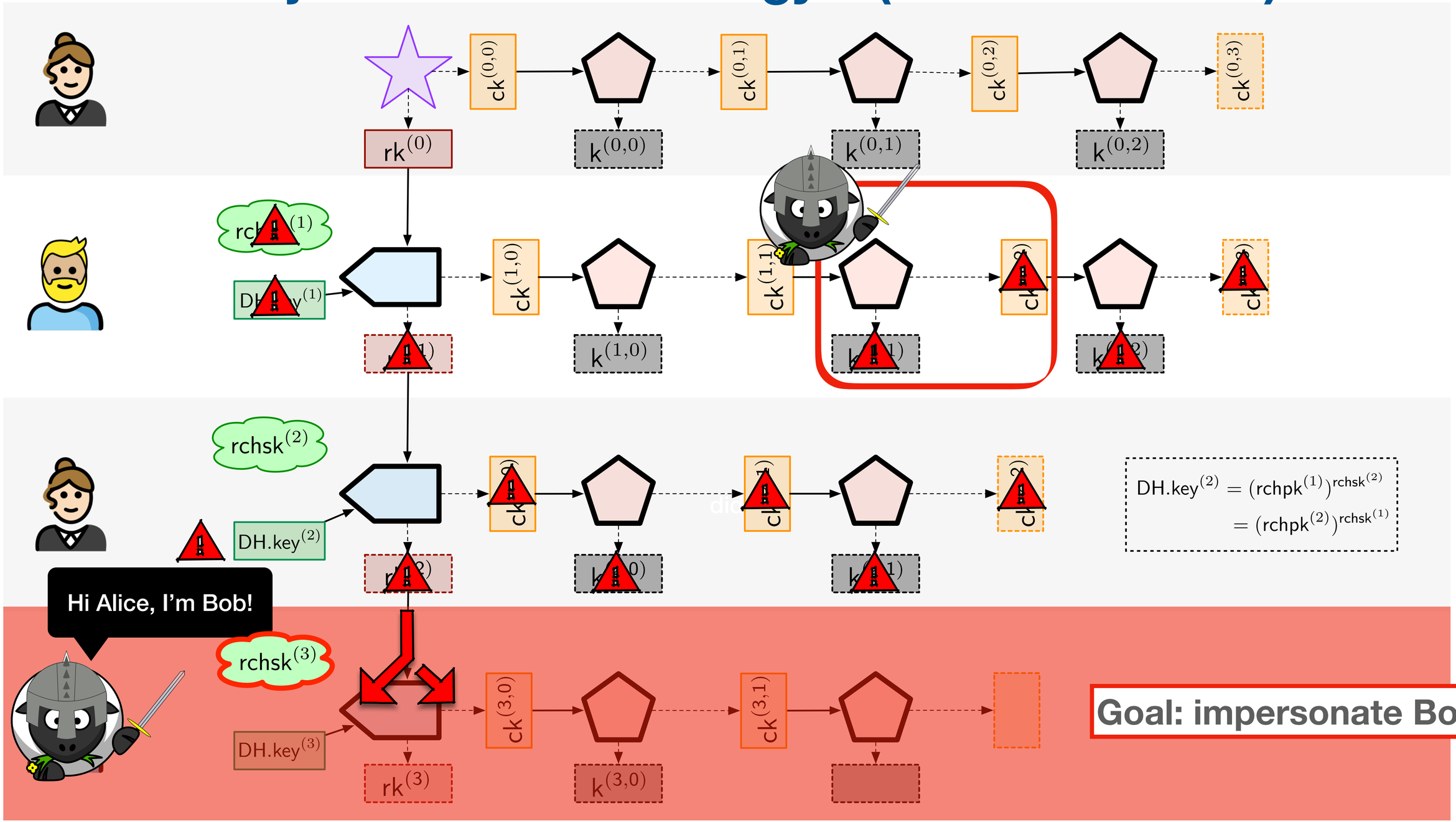
healing window

= 2 asymmetric ratchets

A Reveal & Hijack Attack - Strategy 1 (Active Adversary)



A Reveal & Hijack Attack - Strategy 2 (Active Attacker)



Module 2: Agenda

OW(Trapdoor)Functions
DH Key-Exchange
DL, CDH, DHH
Number Theory
RSA, ElGamal Cryptosystems
IND-CPA and IND-CCA
Digital Signatures

Secure Instant Messaging

- Security Notions
- The Signal Protocol
- Session Hijacking Attack

Post Quantum Cryptography

- The Lifespan of a Cryptosystem
- The State of Quantum Computers
- Landscape of PQC

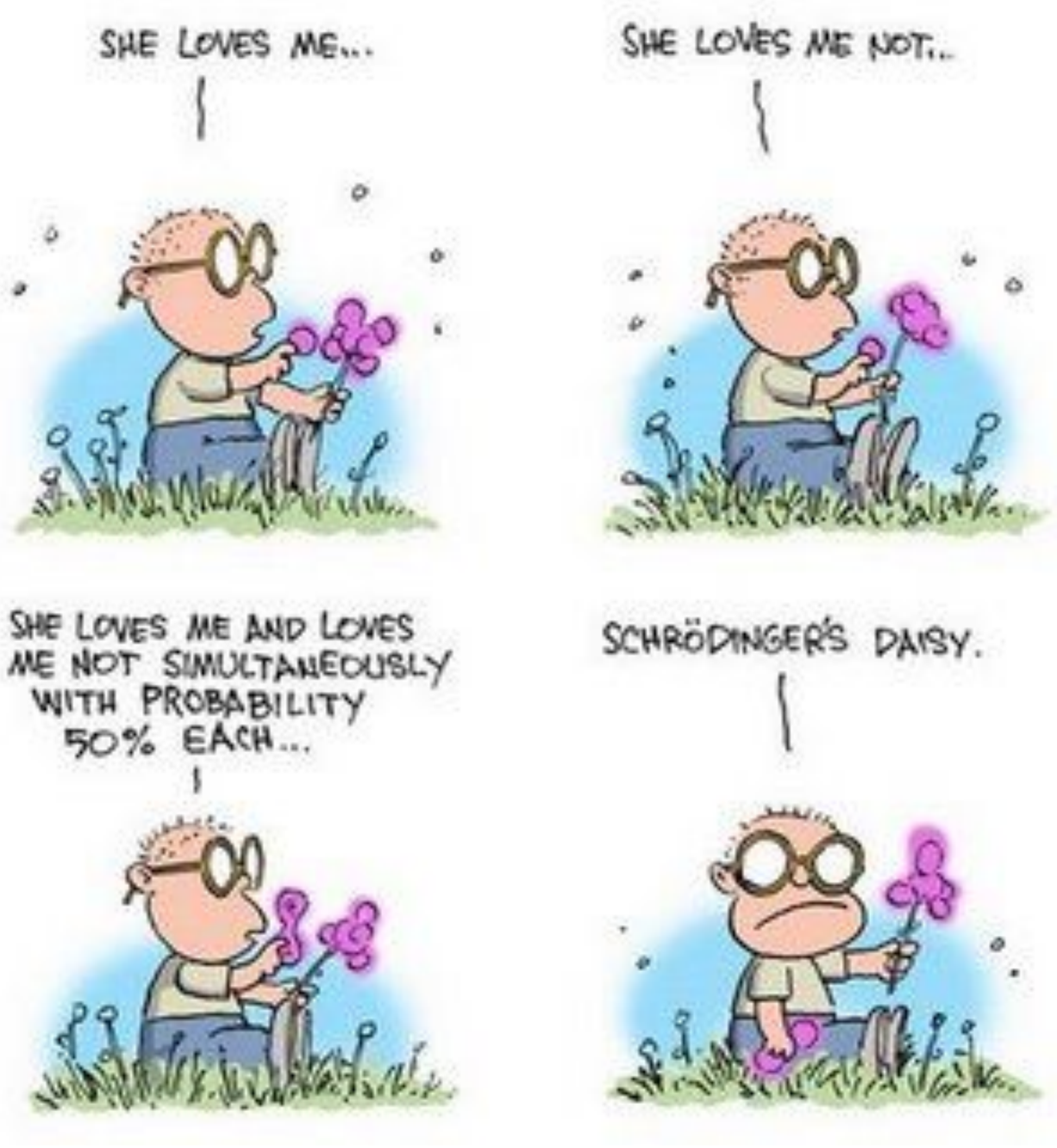
Hash Functions

- Lamport PQ Secure Signature
- The Birthday Paradox - Proof

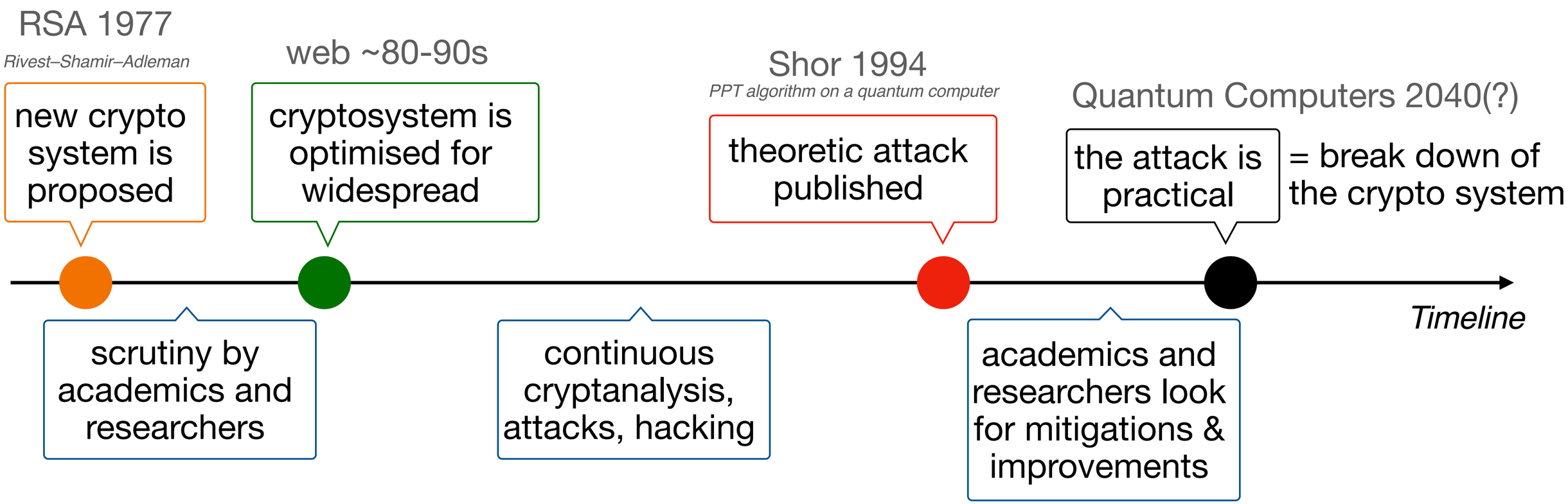
Classical Vs Quantum Computers

The security of ***classical*** crypto relies on the intractability of certain problems using ***modern*** computers.

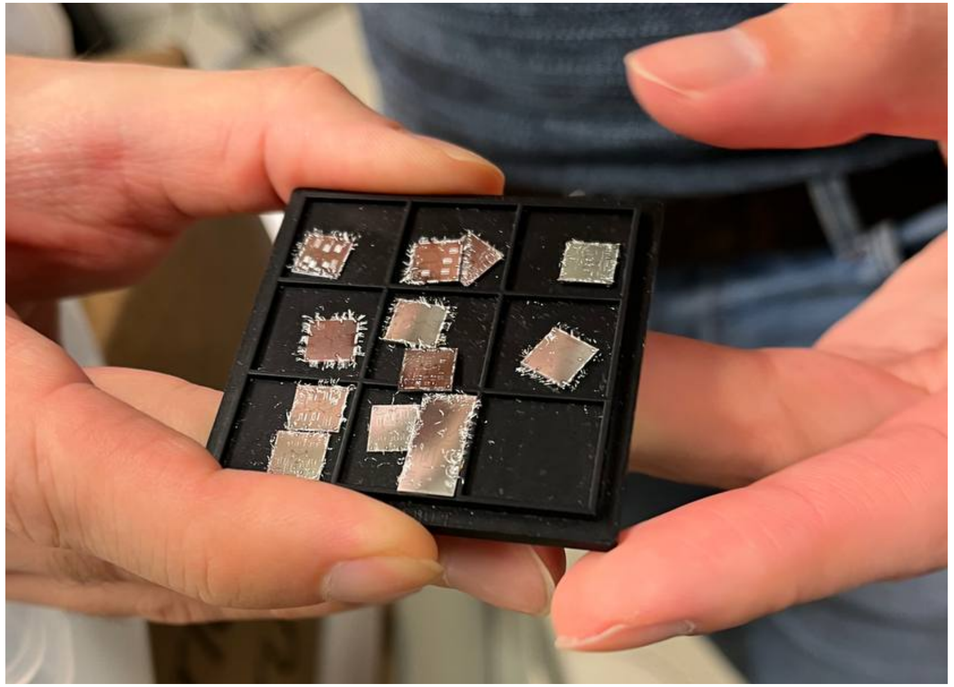
The security of ***post-quantum*** crypto relies on the intractability of certain problems using ***quantum*** computers.



Time Line of ‘Secure’ Cryptographic Algorithms



The State of Quantum Computers



200 seconds QC
=
10,000 years CC

@Chalmers: 25 qubits

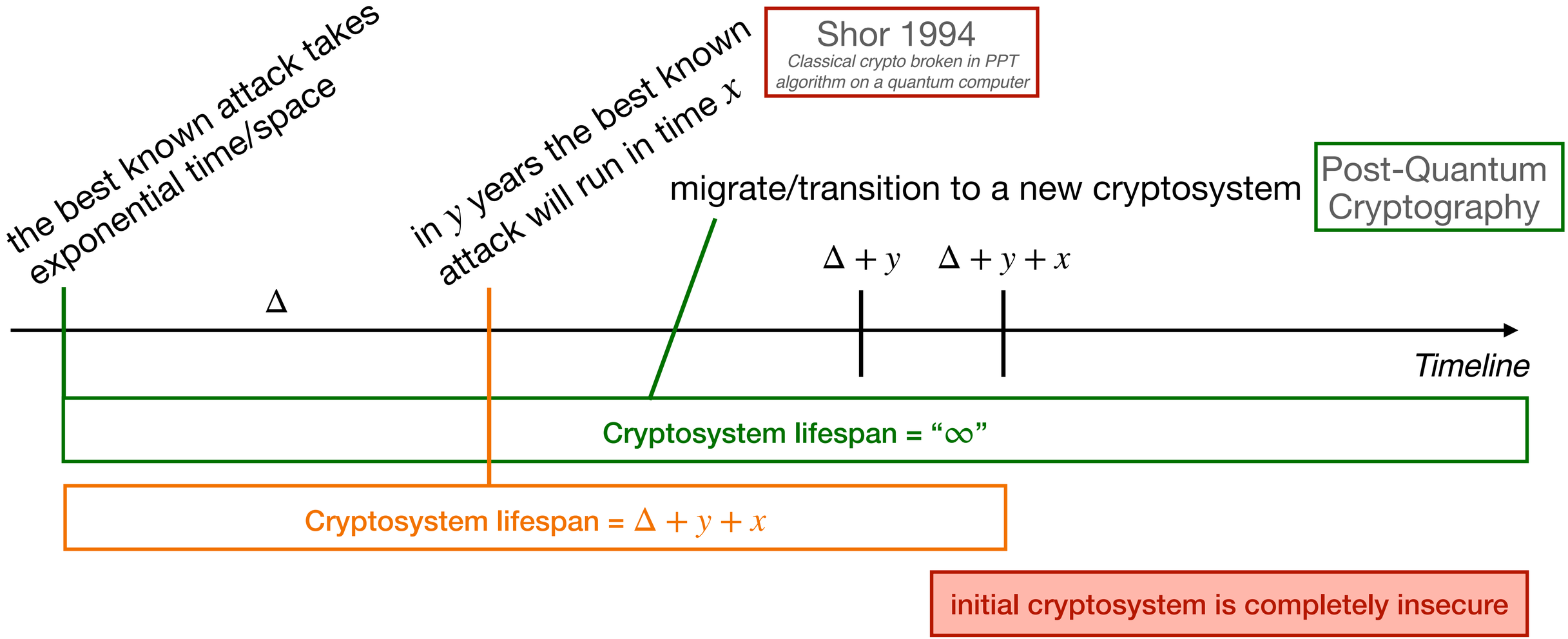
Google: Sycamore chip, 54 qubits

IBM: 433 qubits

NSA: ?

For fun: thequbitgame

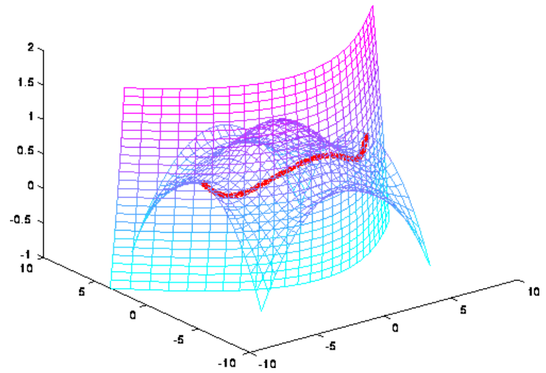
Cryptosystems Lifespan



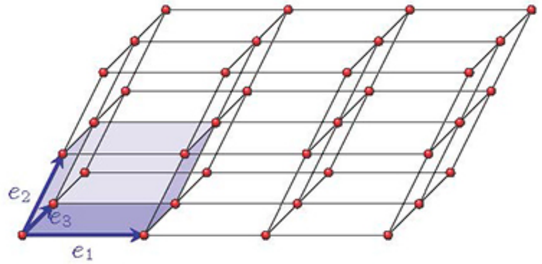
Post Quantum (PQ) Security

For more details check Tanja Lange's lectures

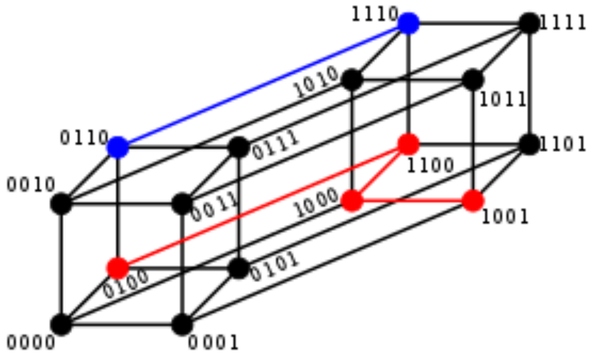
Multi Variate Quadratic Equations



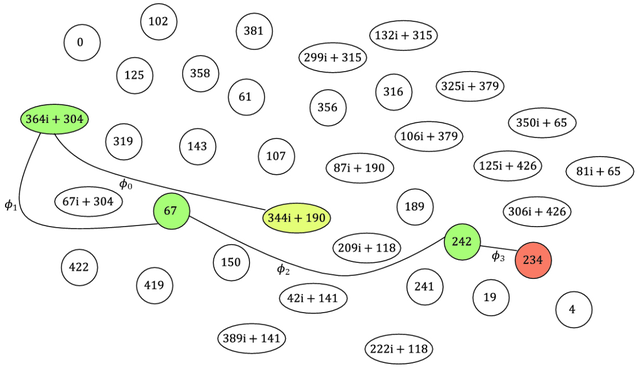
Lattices



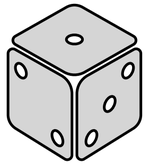
Codes



Isogenies



Hash Functions



Information Theoretic

Module 2: Agenda

OW(Trapdoor)Functions
DH Key-Exchange
DL, CDH, DHH
Number Theory
RSA, ElGamal Cryptosystems
IND-CPA and IND-CCA
Digital Signatures

Secure Instant Messaging

- Security Notions
- The Signal Protocol
- Session Hijacking Attack

Post Quantum Cryptography

- The Lifespan of a Cryptosystem
- The State of Quantum Computers
- Landscape of PQC

Hash Functions

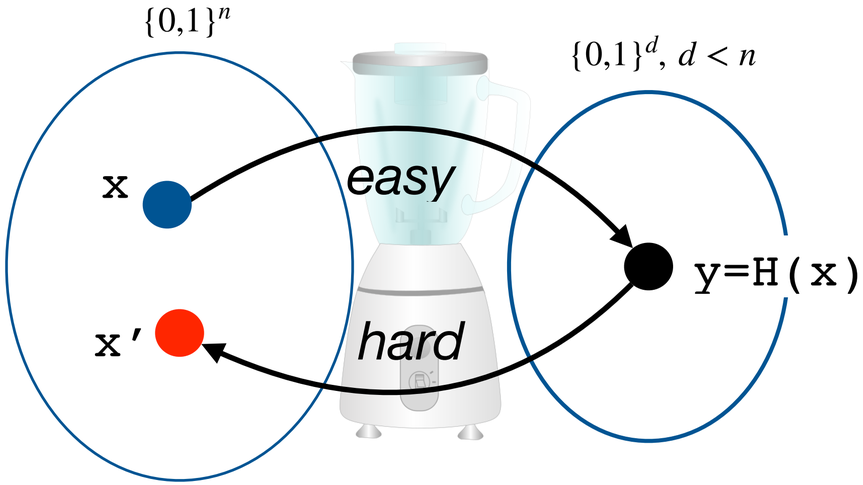
- Lamport PQ Secure Signature
- The Birthday Paradox - Proof

Lamport Signature (Hash-Based PQ)

KeyGen (n) ⇨ (sk, pk)

$$\text{sk} = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{v,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{v,1} \end{pmatrix} \leftarrow \$X^{2v}$$

$$\text{pk} = \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{v,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{v,1} \end{pmatrix} \text{ where } y_{i,b} = f(x_{i,b})$$



Sign (sk, m) ⇨ σ

Take the bit decomposition of m

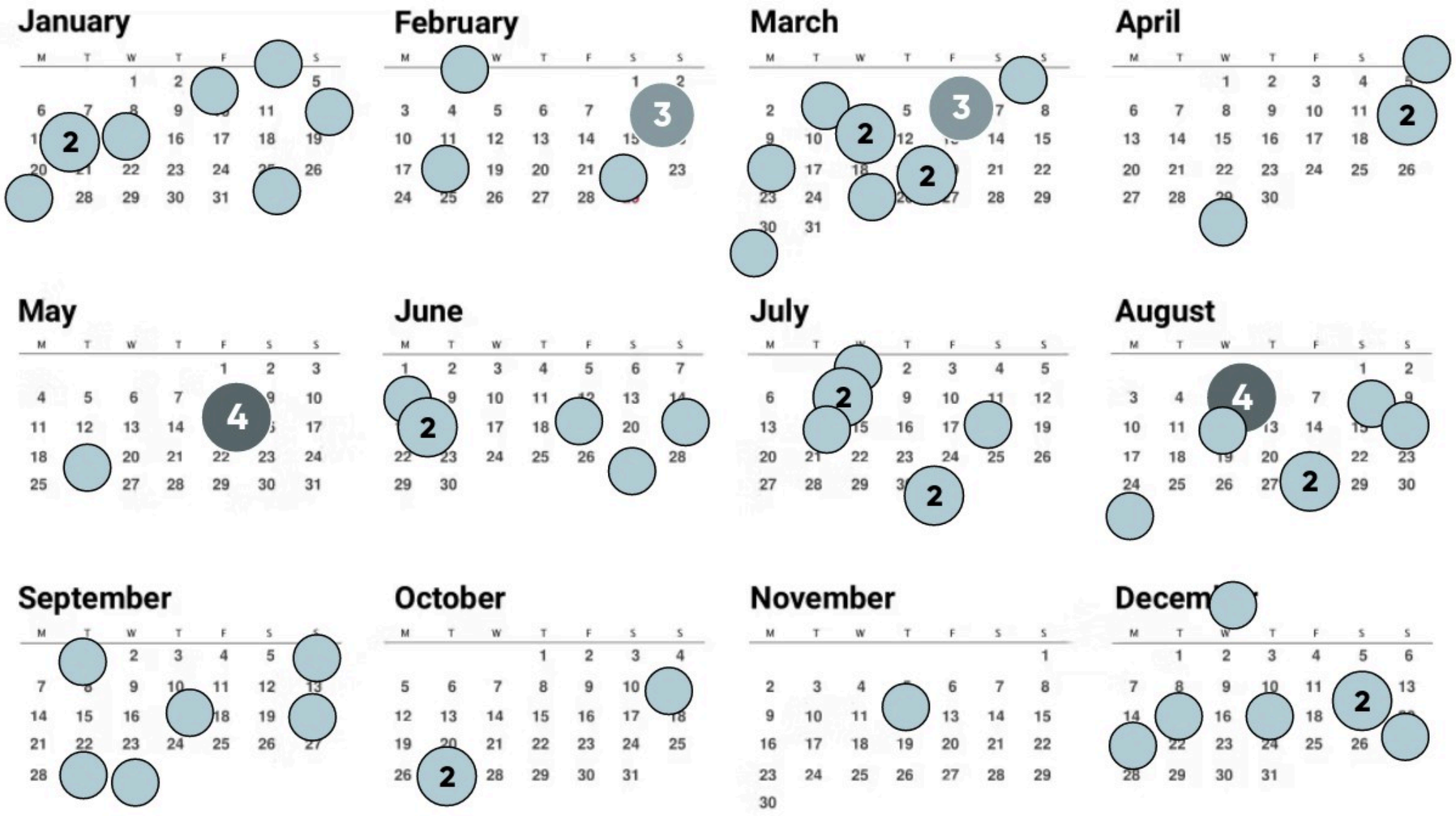
σ = $(x_{1,m[1]}, x_{v,m[v]}, \ldots, x_{v,m[v]})$

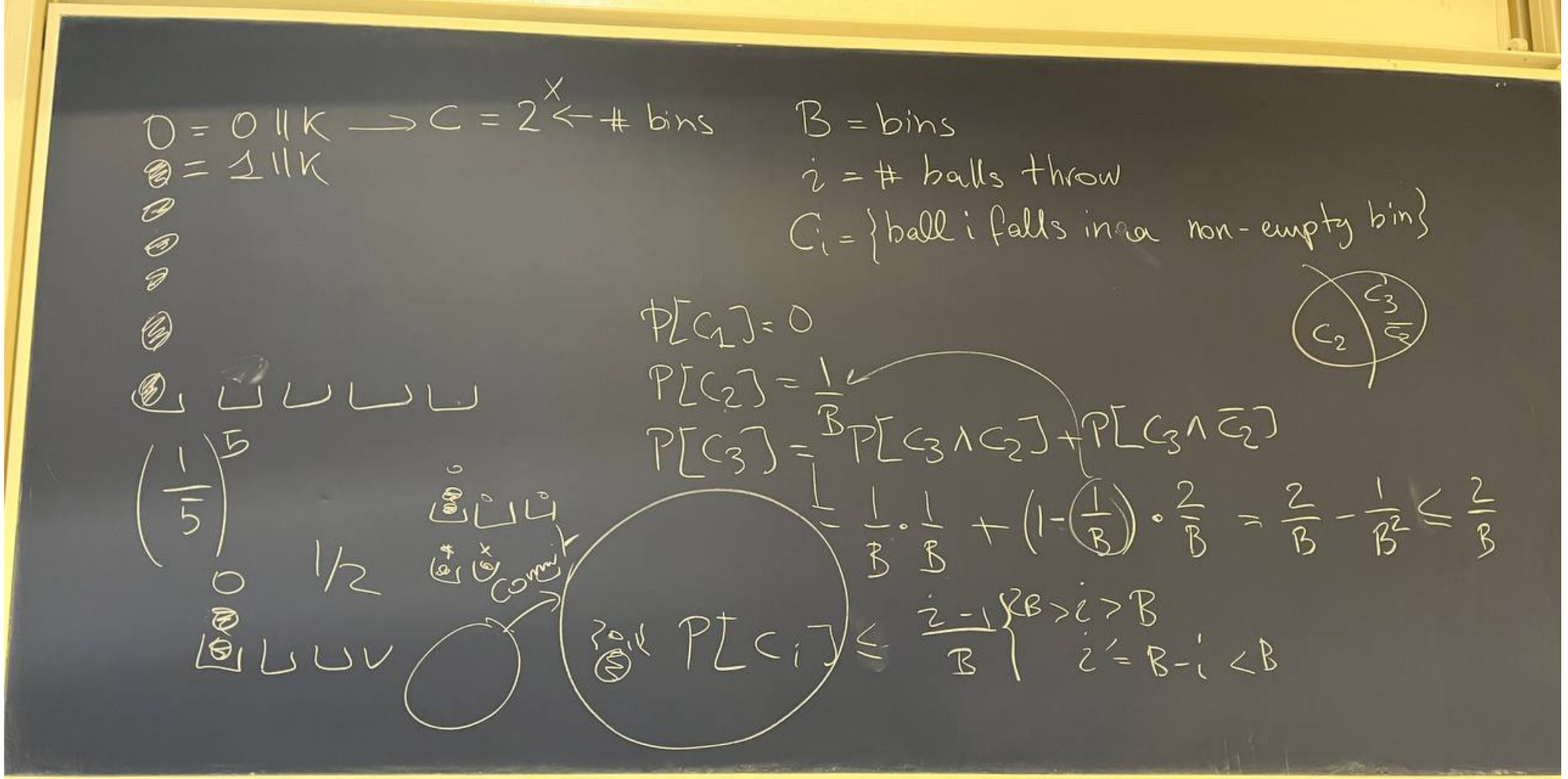
$f : X \rightarrow Y$ is a one-way function and messages are in $m \in \{0,1\}^v$

Ver (pk, m, σ) ⇨ {0, 1}

Accept iff $f(\sigma_{i,m[i]}) = y_{i,m[i]}$ for all $i \in \{1,2,\ldots,v\}$

The Birthday Paradox





reasoning on the blackboard
(useful for HA1)