CWI

Secure Authentication from a Weak Key, Without Leaking Information

Niek Bouman
joint work with Serge Fehr

FRIDAY MAY, 27 - CWI SCIENTIFIC MEETING

Please Enter Your PIN Code

Please Enter Your PIN Code

What if the machine is fake ?!

“Secure Identification”

Two parties, user and server, share a password *W*

- Honest server is protected against fake user
- Honest user is protected against fake server
- User and server protected against a “Man-in-the-Middle”

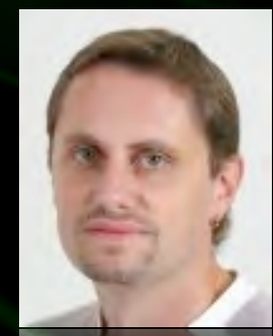
Secure Identification with Laser Light?

Secure Identification with Laser Light?

Why?

To avoid complexity-theory assumptions

Secure Identification with Laser Light?



Serge Fehr, Chris Schaffner *et al.* "Secure Identification and QKD in the Bounded Quantum Storage Model" (CRYPTO 2007)

Motivation for our Work / Talk

- Identification scheme of DFSS'07 requires not only a shared password (e.g. pincode) but also an additional shared secret key
- Goal: Modify the scheme such that a shared password suffices

Identification Scheme DFSS'07

Message
Authentication

Message Authentication

Message Authentication

Eve

Alice

Bob

Message Authentication

Eve

Alice

Bob

Message Authentication

Eve

Alice

Bob

Secret Key *X*

Tag = MAC(*X*, )

Message Authentication

Alice

Eve

, Tag

Bob

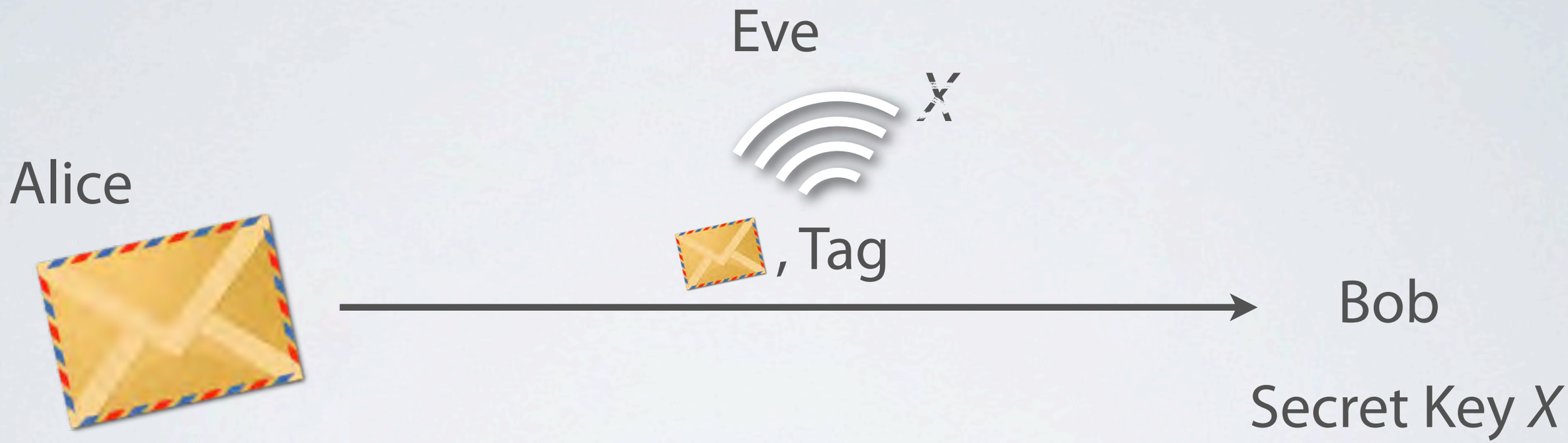
Secret Key *X*

Secret Key *X*

Tag = MAC(*X*, )

Tag allows Bob to check whether Eve modified the message

Message Authentication



Where does *X* come from?

Eve

Alice

Bob

w

w

Z

Where does *X* come from?

Eve

Alice

Bob

W

W

X

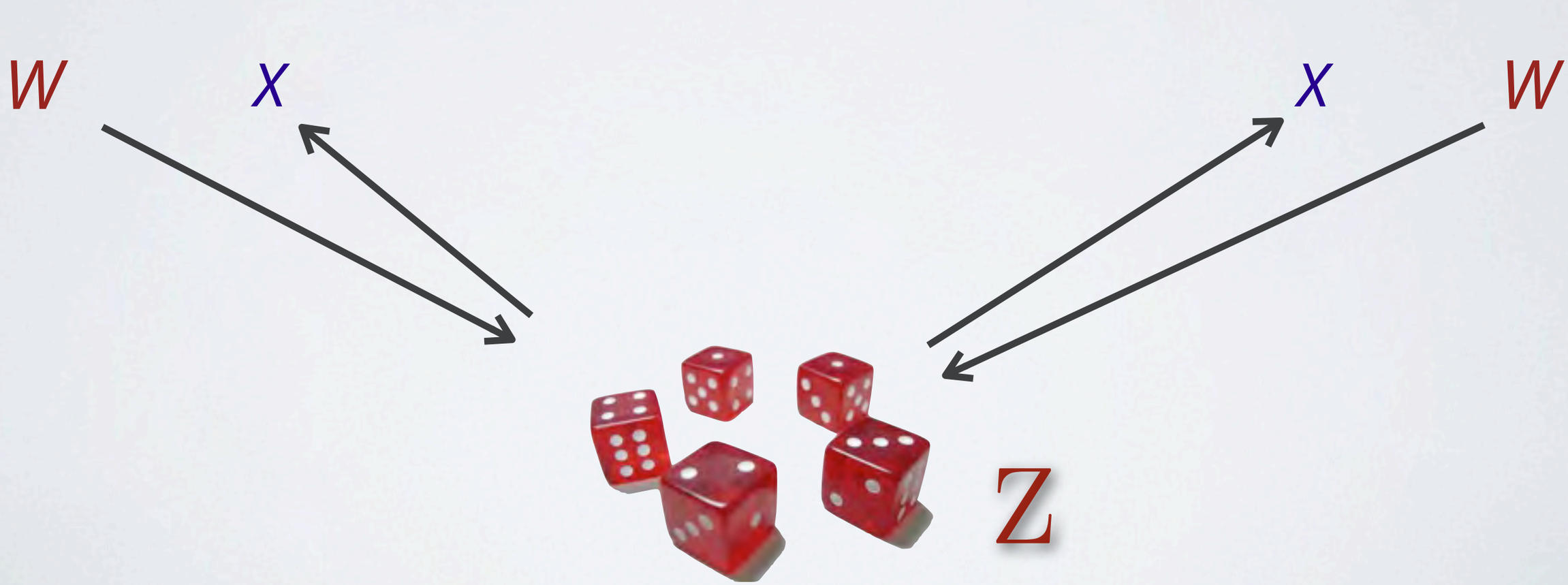
Z

Where does *X* come from?

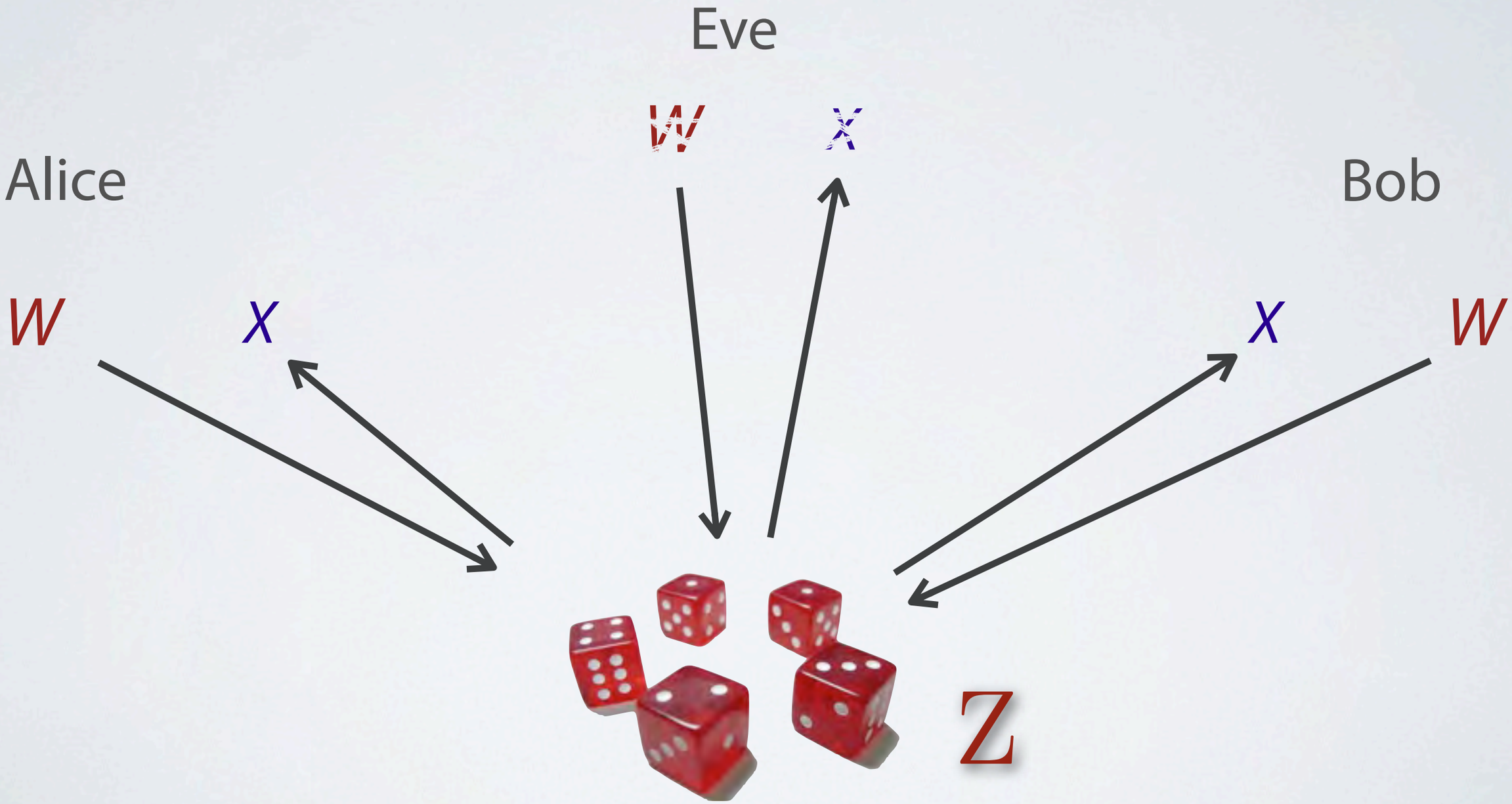
Eve

Alice

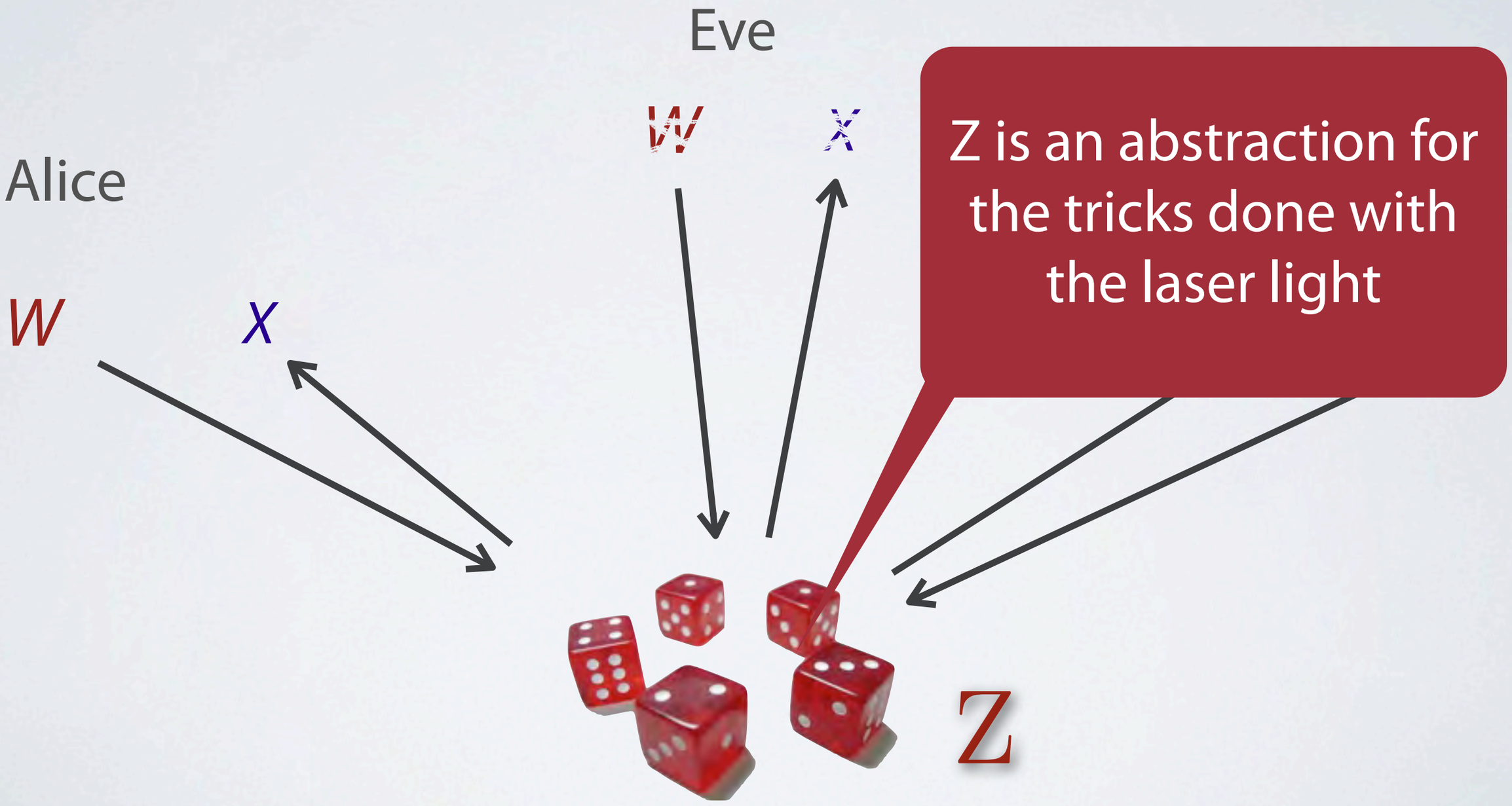
Bob



Where does *X* come from?



Where does *X* come from?

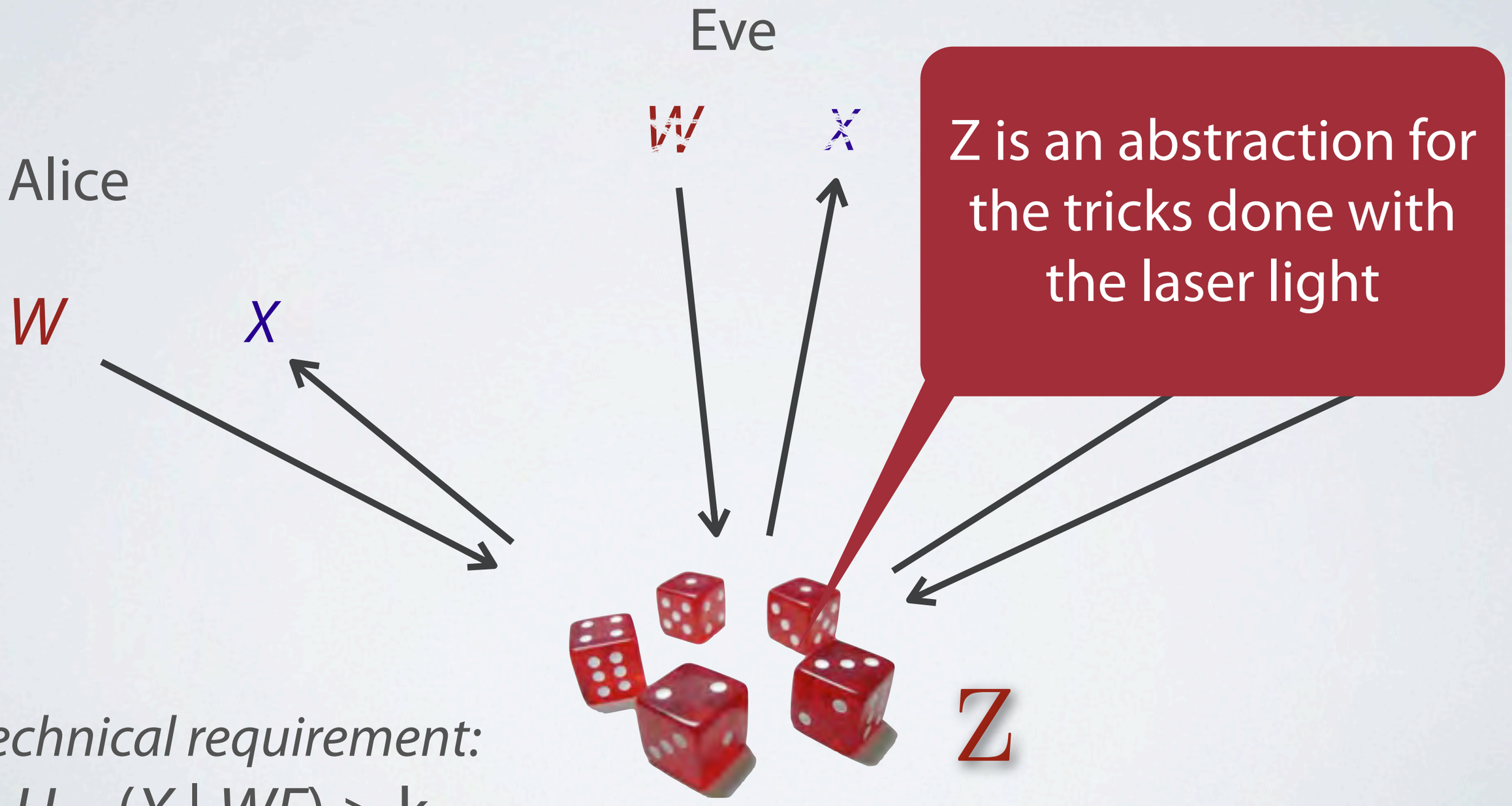


Z is an abstraction for the tricks done with the laser light

Where does *X* come from?

Alice

Eve



Z is an abstraction for the tricks done with the laser light

Technical requirement:

$H_{\min}(X \mid WE) > k$

Problem Statement

Problem Statement

- Alice (user) and Bob (server) want to reuse the identification password *W*

Problem Statement

- Alice (user) and Bob (server) want to reuse the identification password *W*
- Authentication key *X* is derived from Z using *W*
  => *statistical dependence* between *X* and *W*

Problem Statement

- Alice (user) and Bob (server) want to reuse the identification password *W*
- Authentication key *X* is derived from Z using *W*
  => *statistical dependence* between *X* and *W*
- When *X* is used, information about it leaks to Eve
  => *potential leakage about W as well*

Problem Statement

- Alice (user) and Bob (server) want to reuse the identification password *W*
- Authentication key *X* is derived from Z using *W*
  => *statistical dependence* between *X* and *W*
- When *X* is used, information about it leaks to Eve
  => *potential leakage about W as well*

Problem:

Problem Statement

- Alice (user) and Bob (server) want to reuse the identification password *W*
- Authentication key *X* is derived from Z using *W*
  => *statistical dependence* between *X* and *W*
- When *X* is used, information about it leaks to Eve
  => *potential leakage about W as well*

Problem:

- *W* cannot be reused

Solution / Contribution

- Authentication Protocol with "*W*-Privacy":
  does (provably) not significantly leak information about *W*

- Overcomes the need for the additional key in the quantum identification scheme from DFSS'07

Solution / Contribution

- Authentication Protocol with "*W*-Privacy":
  does (provably) not significantly leak information about *W*

- Overcomes the need for the additional key in the quantum identification scheme from DFSS'07

Thank You!