

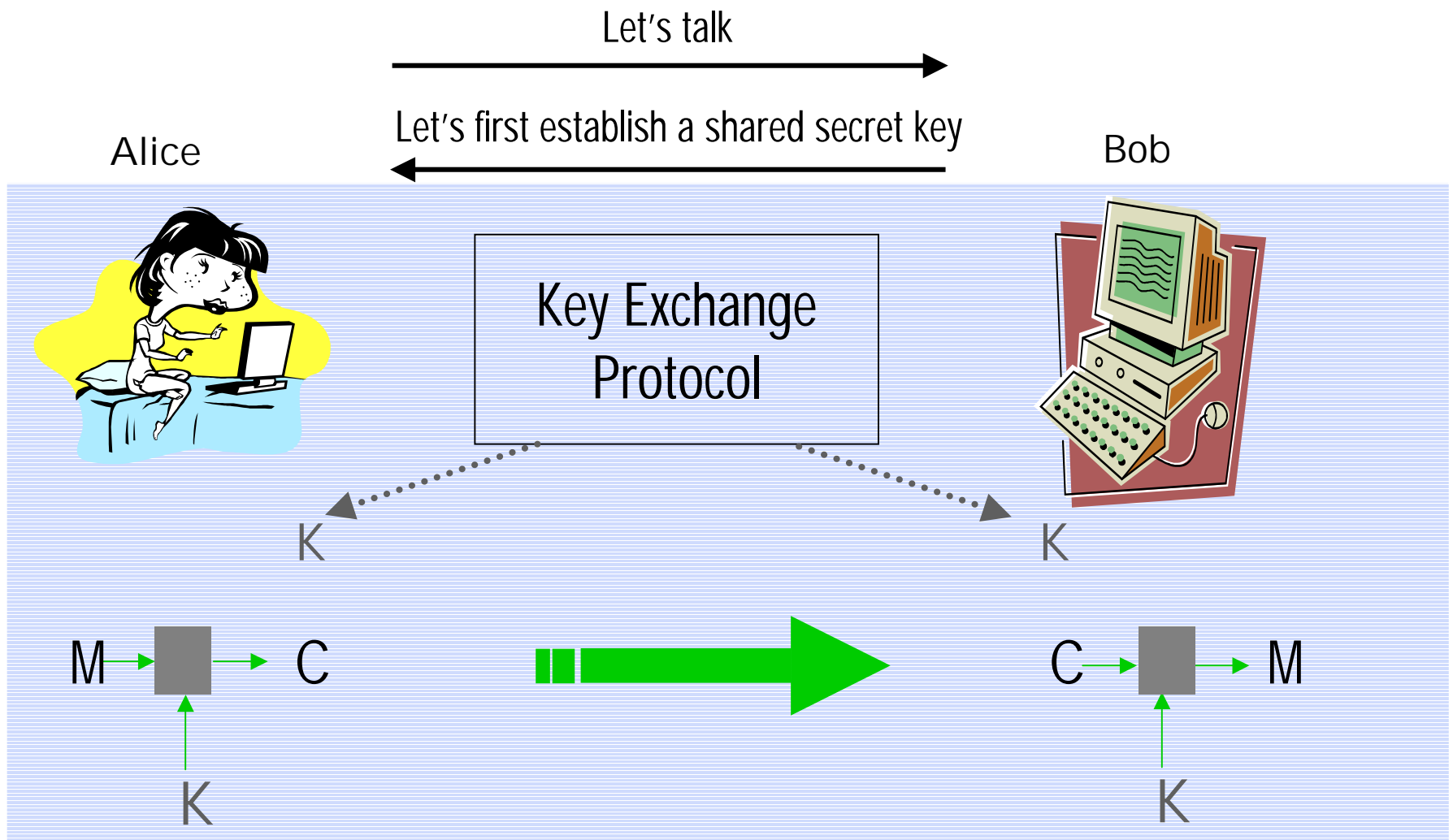
Secure Channels based on Authenticated Encryption Schemes: A Simple Characterization

Chanathip Namprempre ([aka Meaw](#))

University of California, San Diego

[Work to appear in Asiacrypt 2002.]

A Common Way to Communicate over Insecure Networks



Secure Channel? [CK01]

Security Model for Secure Channels per Canetti and Krawczyk

- **Ideal World**
 - Secure communication happens magically the way we want them to.
 - Adversaries **deliver** messages but cannot inject or modify messages.
- **Real World**
 - Run the protocol to communicate.
 - Adversaries **deliver** messages and can **inject** and **modify** messages.

If the protocol is secure, the two worlds should be “indistinguishable.”

Secure Channels per Canetti and Krawczyk

A network channel protocol is a secure channel protocol if it is both

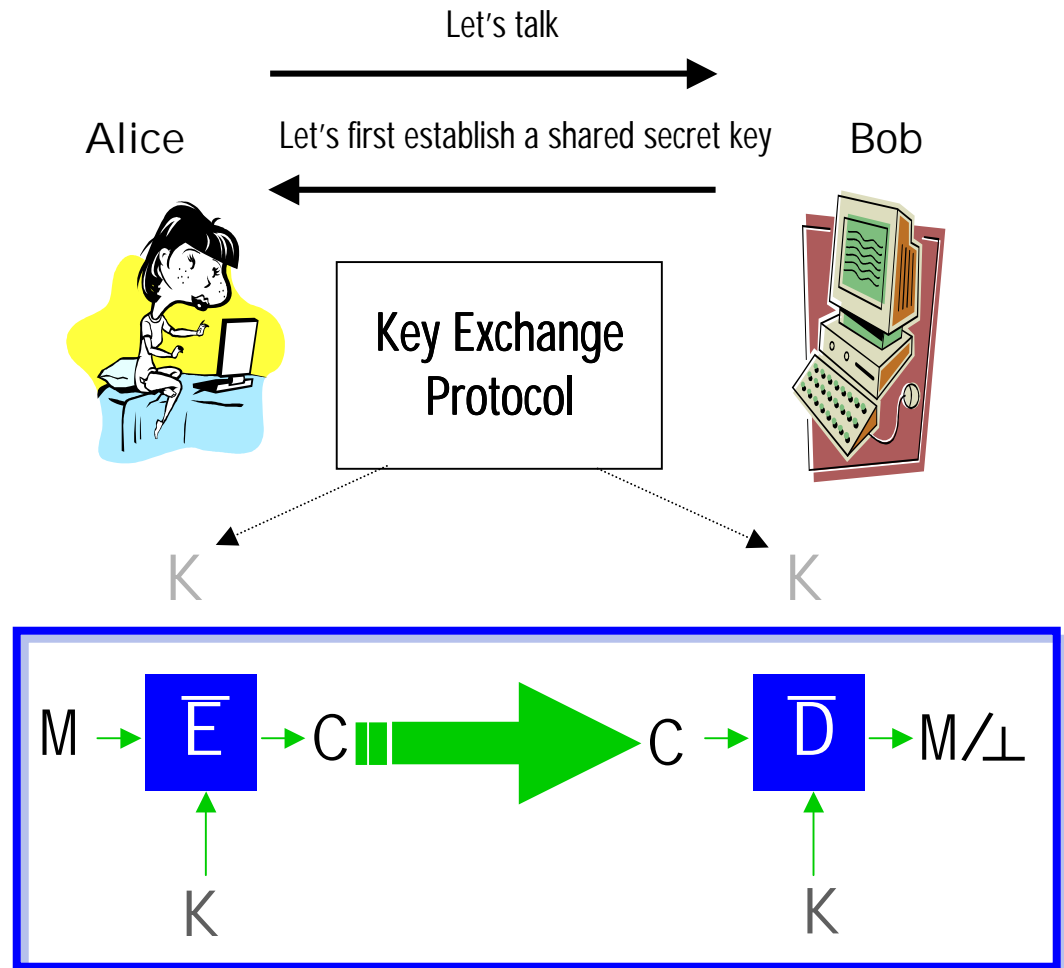
- a secure authentication protocol and
- a secure encryption protocol.

Statistical closeness between the distributions generated by the system running the protocol against adversaries in the **two worlds**.

“Find-then-guess” style **indistinguishability** [GM84,BDJR97] where the adversary runs in the **real world**.

Characterizing Secure Channels

- Assume “secure” KE
- Focus on protocols based on authenticated encryption schemes

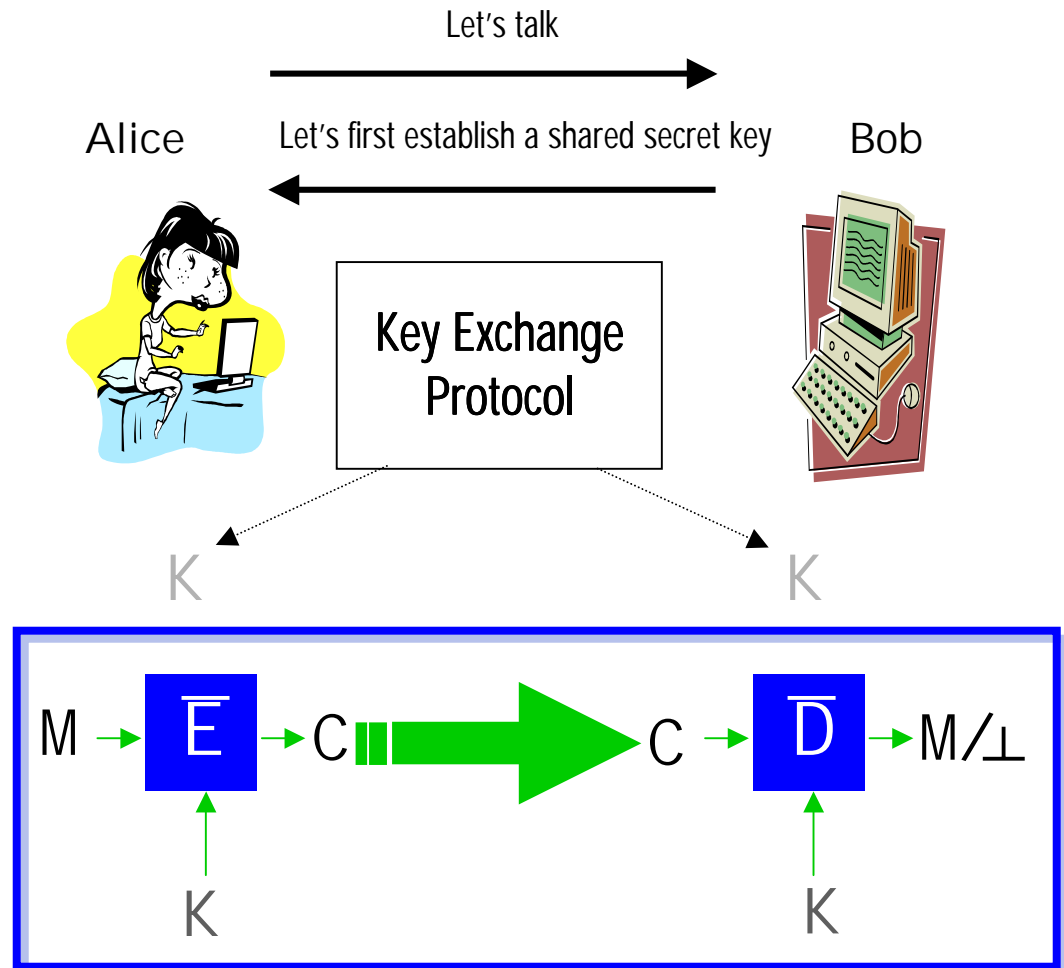


Simple Characterization of Secure Channels

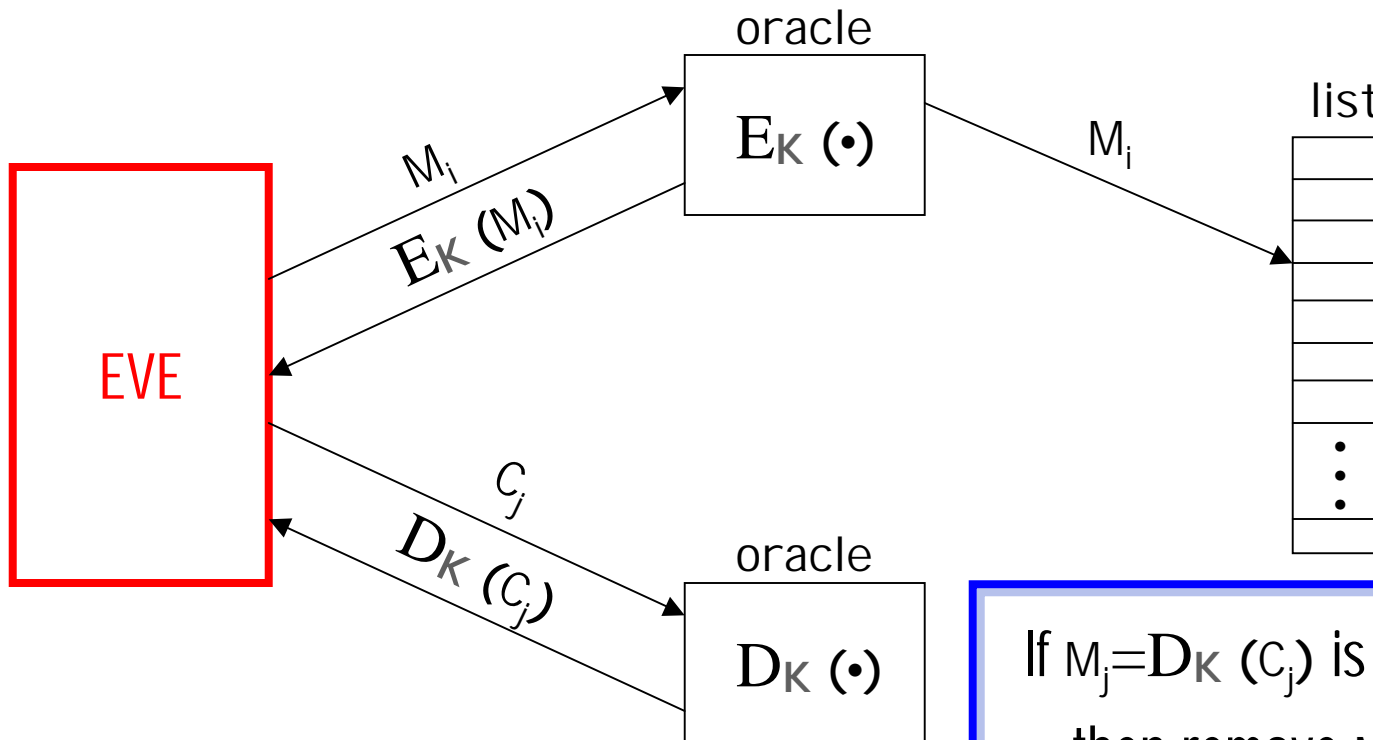
Assuming "secure" KE

The channel protocol is a **secure channel** *if and only if* the underlying **authenticated encryption scheme** is secure under the notions

SINT-PTXT and IND-CCVA



Capturing Secure Authentication Protocol: SINT-PTXT (Strong Integrity of Plaintexts)

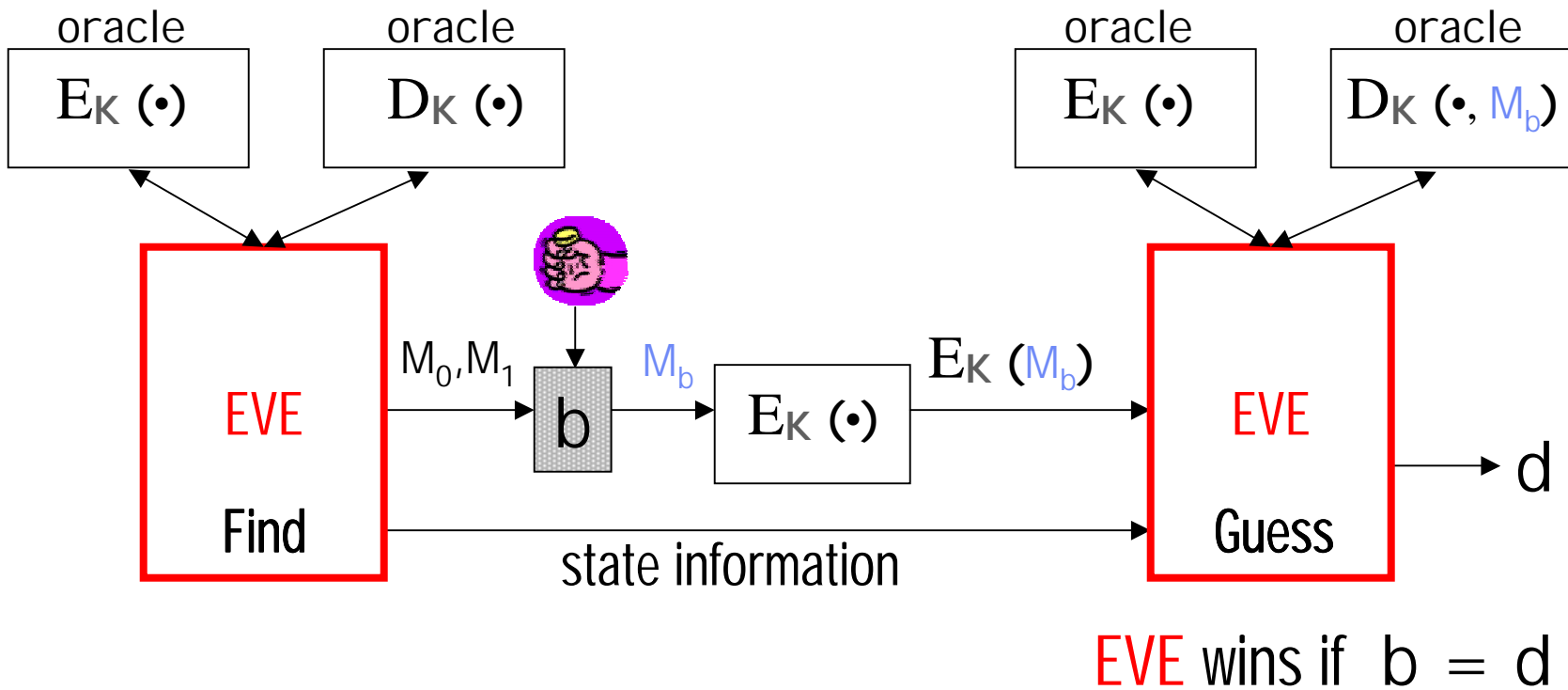


Model replays and forgeries

i.e. if **EVE** can replay or forge valid ciphertexts, then she wins.

- If $M_j = D_K(C_j)$ is in the list,
- then remove M_j from the list
 - else **EVE** wins.

Capturing Secure Encryption Protocol: IND-CCVA (indistinguishability against CCA with verification)



- The oracles are stateful.
- The oracle $D_K(\cdot, M_b)$ returns a special symbol if the decryption is equal to M_b .
- **EVE** cannot query $E_K(\cdot)$ on M_0 or M_1 .
- **EVE** cannot query $E_K(\cdot)$ on a particular message more than once.

Results

Assuming that the KE protocol is secure,

- the channel protocol is a **secure authentication protocol**
if and only if
the authenticated encryption scheme is **SINT-PTXT** secure.
- the channel protocol is a **secure encryption protocol**
if and only if
the authenticated encryption scheme is **IND-CCVA** secure.

Benefits

- Protocols can be analyzed in a **modular** fashion.
- The two notions provide a **simple characterization** of secure channels, assuming that the underlying KE protocol is secure.
- The two notions follow the traditional approach of defining security notions, and thus is **easy to use** in analysis.