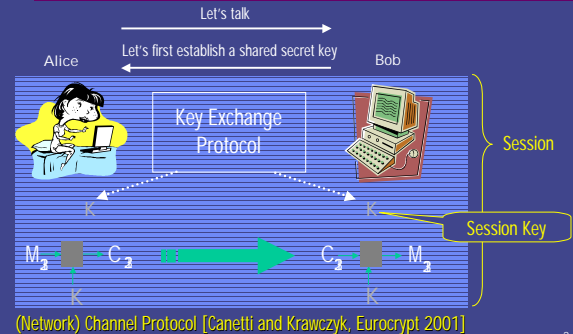


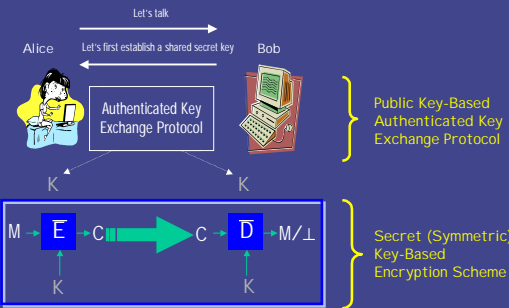
Secure Channels based on Authenticated Encryption Schemes: A Simple Characterization

Chanathip Nampremre (aka **Meaw**)
Thammasat University, Thailand
ASIACRYPT 2002.

A Common Way to Communicate over Insecure Networks



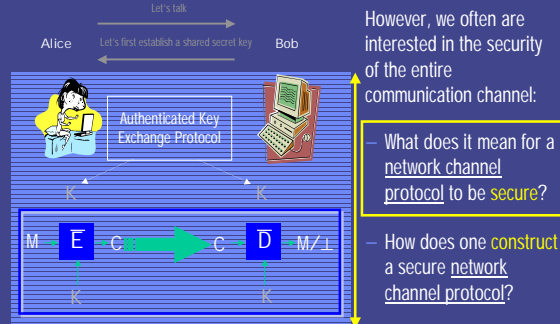
Relevant Cryptographic Primitives



Often, the two cryptographic primitives are designed and analyzed **separately**.

- **Authenticated Key Exchange (KE) Protocol:**
 - **Constructions:** Variants of Diffie-Hellman, protocols based on public-key encryption and signature schemes, ...
 - **Security Notions:** Entity authentication and key exchange security by BR93, BCK98, S99, CK01, ...
- **Secret Key-Based Encryption Scheme:**
 - **Constructions:** CBC-mode encryption, CTR-mode encryption, ...
 - **Security Notions:** Indistinguishability, Non-Malleability, Integrity, ...

But what about the **entire** channel?



What do we expect from a "secure channel"?

- Key exchange portion "works"
 - Session keys are secret.
 - Sessions are independent: Successfully recovering keys for some sessions does not help in breaking other sessions.
 - Perfect Forward Secrecy: Exposure of long-term keys does not lead to exposure of data communicated in the past.
 - ...
- Data communication portion "works"
 - Privacy of data: It is hard to obtain any information about the data being communicated.
 - Authenticity of data: It is hard to modify, forge, replay data, etc.
 - It should not expose the session key being used.
 - ...

Secure Channel [CK01]

Q: What does it mean for a network channel protocol to be **secure**?

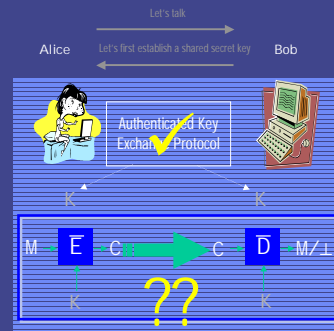
- Canetti and Krawczyk [CK01] provide a **definition** of **secure channels** in a **secure multi-party computation model**.

Q: How does one **construct** a secure network channel protocol?

- Canetti and Krawczyk [CK01] provide a **construction** of a class of encryption schemes that, once combined with a “secure” key exchange protocol, yield secure channels.
- Krawczyk [K01] also provides **necessary condition** under which this class of encryption schemes yield secure channels.

7

We ask the following question:



Suppose that the underlying key exchange protocol is “secure,”

- What are the **necessary and sufficient conditions** for **any** encryption scheme to yield a secure channel per [CK01]?

8

Results

Assuming that the underlying key exchange protocol is secure,

A channel protocol is a **secure channel** *if and only if* the underlying encryption scheme provides

- Strong integrity of plaintexts: **SINT-PTXT**
- Indistinguishability against chosen-ciphertext attacks with verification: **IND-CCVA**

9

Benefits

The **necessary and sufficient conditions** that we found

- **distill the security properties** of the underlying encryption schemes needed to obtain secure channels
- provide a **simple characterization** of secure channels, assuming that the underlying key exchange protocol is “secure”
- allow one to analyze network channel protocols in a **modular** fashion
- follow the traditional approach of defining security notions, and thus are **easy to use** in analysis of channel protocols

10

Definition of Secure Channels per [CK01]

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

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

11

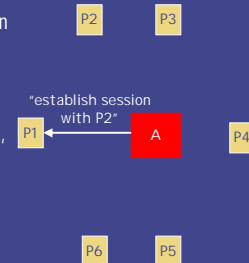
Security Model of [CK01]

– Each party goes through the setup phase of the protocol then waits for **activations** from adversary.

– **Possible activations:** establish session, send msg, receive msg, etc.

– **Message delivery** is completely controlled by adversary.

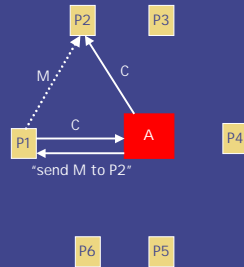
– The **protocol output** is the concatenation of the outputs of the parties and of the adversary.



12

Security Model of [CK01]

- Each party goes through the setup phase of the protocol then waits for **activations** from adversary.
- Possible **activations**: establish session, send msg, receive msg, etc.
- **Message delivery** is completely controlled by adversary.
- The **protocol output** is the concatenation of the outputs of the parties and of the adversary.

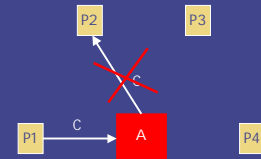


13

Security Model of [CK01]: AM and UM

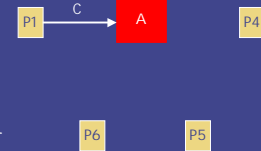
Authenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order



Unauthenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order
 - inject messages
 - modify messages

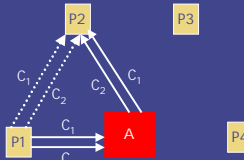


14

Security Model of [CK01]: AM and UM

Authenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order



Unauthenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order
 - inject messages
 - modify messages

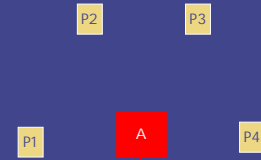


15

Security Model of [CK01]: AM and UM

Authenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order



Unauthenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order
 - inject messages
 - modify messages

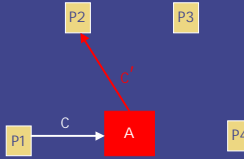


16

Security Model of [CK01]: AM and UM

Authenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order



Unauthenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order
 - inject messages
 - modify messages



17

Security Model of [CK01]: AM and UM

Authenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order

These requirements model asynchronous and unreliable, but otherwise ideal communication networks.

Unauthenticated-link Model

- Adversary can
 - drop messages
 - deliver messages out of order
 - inject messages
 - modify messages

These requirements model adversarially-controlled, asynchronous, unreliable communication networks.

18

Notion 1: Security of Authentication Protocols

Ideal World

- [AM]: Adversary controls message delivery but **cannot** inject or modify messages.
- Secure communication happens "magically."

Real World

- [UM]: Adversary controls message delivery and **can** inject or modify messages.
- Parties run the protocol to communicate.

A network channel protocol provides **secure authentication** **IF AND ONLY IF** the protocol outputs generated in the two worlds are "indistinguishable."

19

Notion 1: Security of Authentication Protocols

Observations

- The **only difference** in the power of an adversary running in the real world and the ideal world is the following:
 - In contrast to the real world, the adversary cannot inject or modify messages in the ideal world.
- Therefore,

IF a channel protocol prevents replays and forges of messages,
THEN the protocol outputs in the two worlds will be indistinguishable.

20

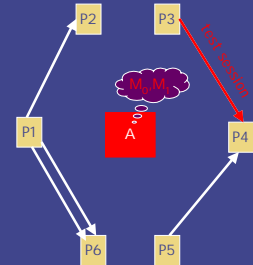
Notion 2: Security of Encryption Protocols

- Adversary and parties run in the **real world**.
 - **UM**: Adversary control message delivery and **can** inject or modify messages.
 - Parties run the protocol to communicate.
- During the run, adversary chooses a session whose privacy it wishes to break.
- Adversary plays a game similar to the "find-then-guess" definition for adaptive chosen-ciphertext security of encryption schemes (IND-CCA) with a few important exceptions.

21

Notion 2: Security of Encryption Protocols

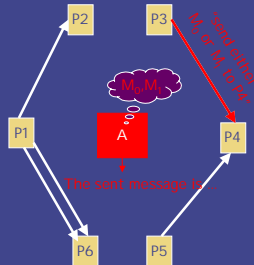
[CK01]'s notion of secure encryption is similar to the "find-then-guess" indistinguishability for adaptive chosen-ciphertext security (IND-CCA).



22

Notion 2: Security of Encryption Protocols

[CK01]'s notion of secure encryption is similar to the "find-then-guess" indistinguishability for adaptive chosen-ciphertext security (IND-CCA).



23

Secure Channels per [CK01]

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**.

24

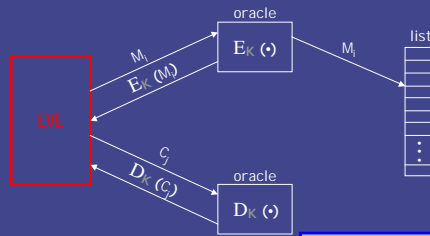
Result: Secure Authentication

Assuming that the KE protocol is secure,

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

25

Capturing Secure Authentication: SINT-PTXT



This models replays and forgeries.

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.

26

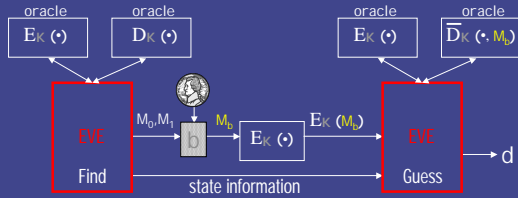
Result: Secure Encryption

Assuming that the KE protocol is secure,

the channel protocol is a **secure encryption protocol** if and only if the underlying encryption scheme is **IND-CCVA** secure.

27

Capturing Secure Encryption: IND-CCVA



EVE wins if $b = d$

- The oracle $\overline{D}_K(\cdot, M_b)$ returns a special symbol if the decryption is equal to M_b .
- The oracles are stateful.
- **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.

28

Conclusion

We have provided **necessary and sufficient conditions** for any encryption scheme to yield a **secure channel** per [CK01], assuming that the underlying key exchange protocol is secure.

Full version of the paper is on eprint:
<http://eprint.iacr.org/2002/065/>

29