

Constructing Confidential Channels from Authenticated Channels—Public-Key Encryption Revisited

Sandro Coretti Ueli Maurer Björn Tackmann

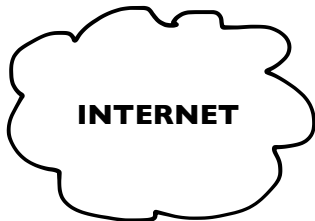
Department of Computer Science
ETH Zürich

ASIACRYPT 2013

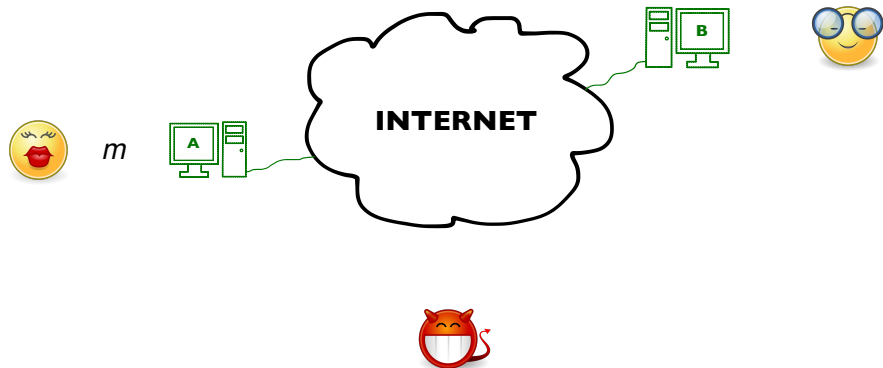
Confidential Communication with PKE



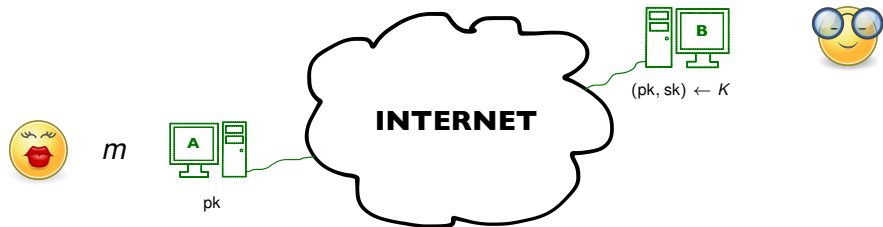
m



Confidential Communication with PKE



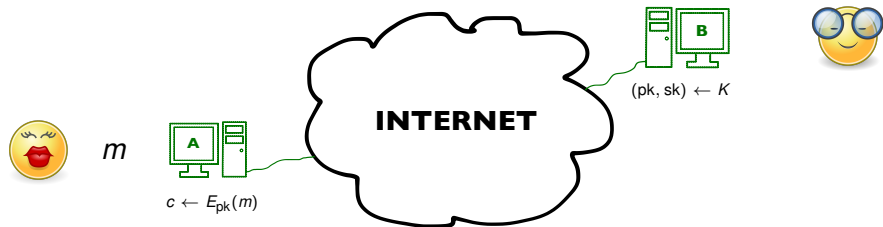
Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

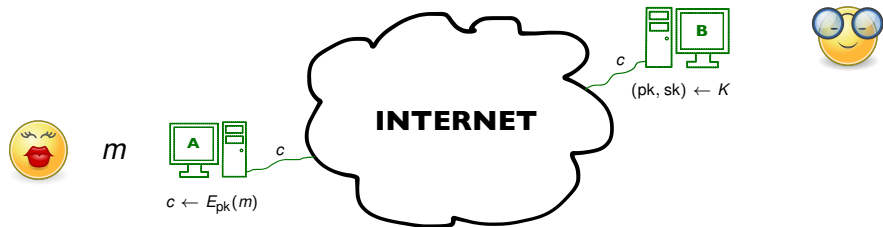
Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

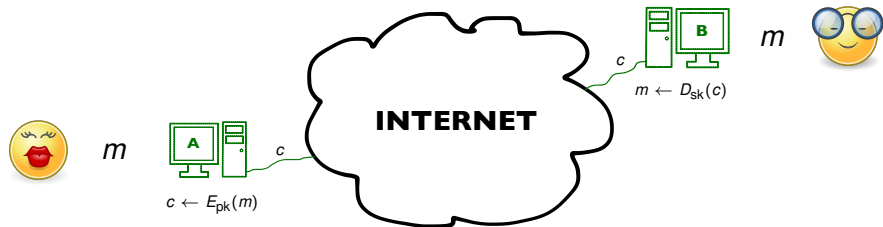
Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

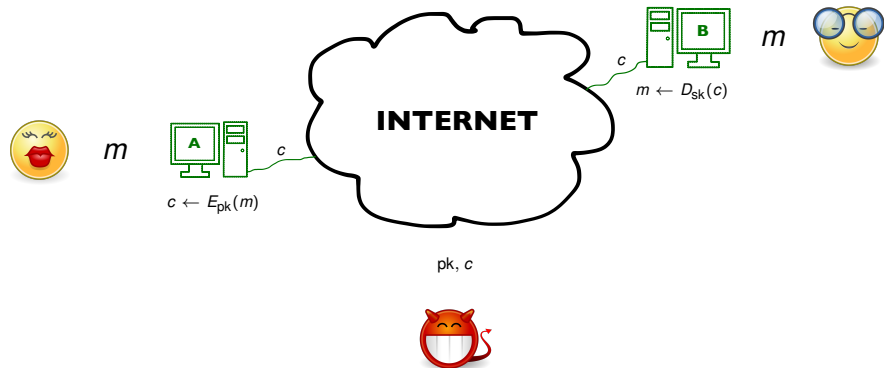
Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

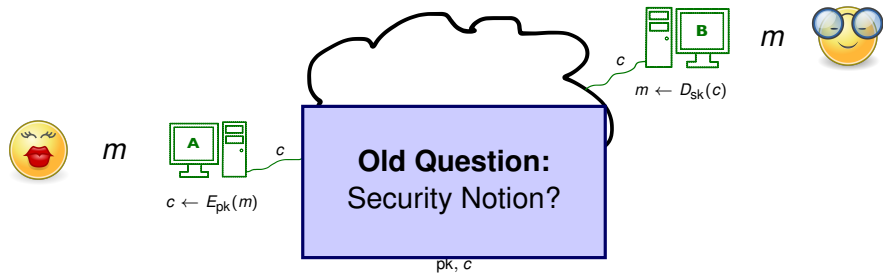
Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

Confidential Communication with PKE



PKE Scheme:

$$\Pi = (K, E, D)$$

PKE Security Notions



PKE Security Notions

- ▶ Semantic Security and Indistinguishability
[GM84, Yao82, Gol89]



PKE Security Notions

- ▶ Semantic Security and Indistinguishability [GM84, Yao82, Gol89]
- ▶ Non-Malleability [DDN91, BDPR98, BS99]



PKE Security Notions

- ▶ Semantic Security and Indistinguishability [GM84, Yao82, Gol89]
- ▶ Non-Malleability [DDN91, BDPR98, BS99]
- ▶ Extended by non-adaptive and adaptive chosen-ciphertext attacks (CCA) [NY90, ZS92]



PKE Security Notions

- ▶ Semantic Security and Indistinguishability [GM84, Yao82, Gol89]
- ▶ Non-Malleability [DDN91, BDPR98, BS99]
- ▶ Extended by non-adaptive and adaptive chosen-ciphertext attacks (CCA) [NY90, ZS92]
- ▶ Replayable CCA security [CKN03]



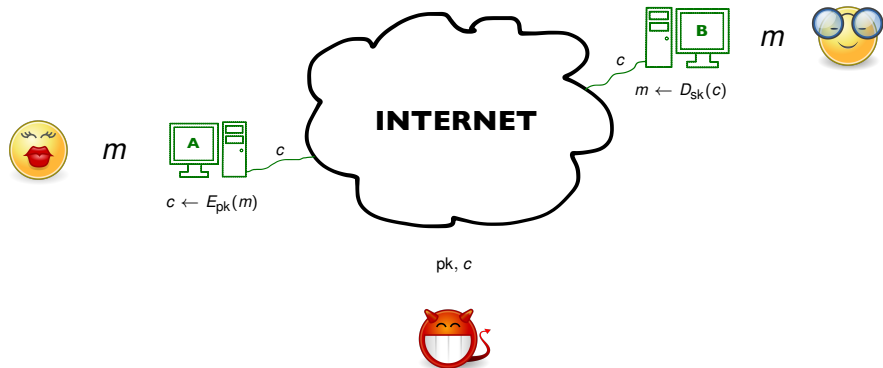
PKE Security Notions

- ▶ Semantic security [GM84, Yao87]
- ▶ Non-Malleability [GM84, BS99]
- ▶ Extended by non-adaptive and adaptive chosen-ciphertext attacks (CCA) [NY90, ZS92]
- ▶ Replayable CCA security [CKN03]

Which one to use?

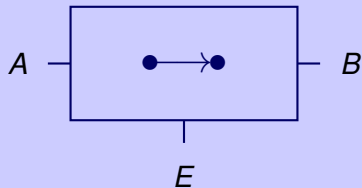


Confidential Communication with PKE



Confidential Communication with PKE

Goal: Secure Channel Resource



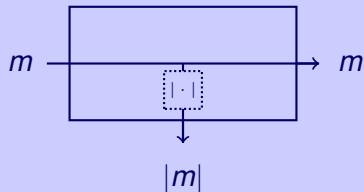
Confidential Communication with PKE

Goal: Secure Channel Resource



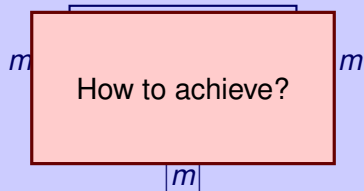
Confidential Communication with PKE

Goal: Secure Channel Resource

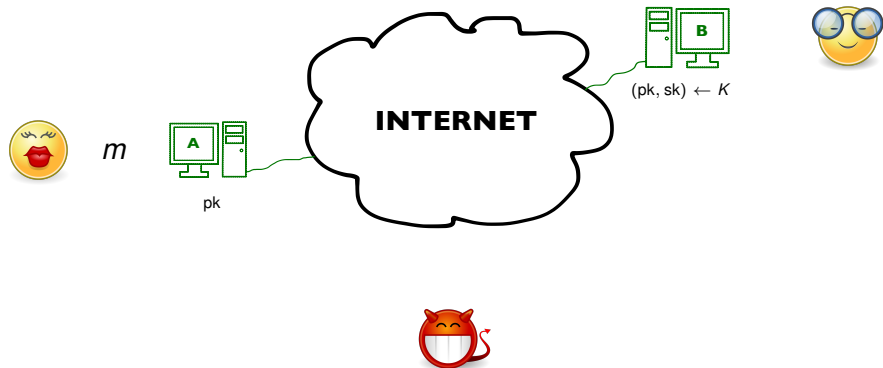


Confidential Communication with PKE

Goal: Secure Channel Resource

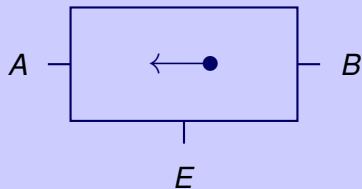


Confidential Communication with PKE



Confidential Communication with PKE

Assumption: Public key transmitted **authentically**.



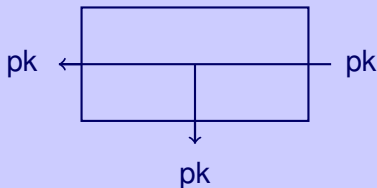
Confidential Communication with PKE

Assumption: Public key transmitted **authentically**.

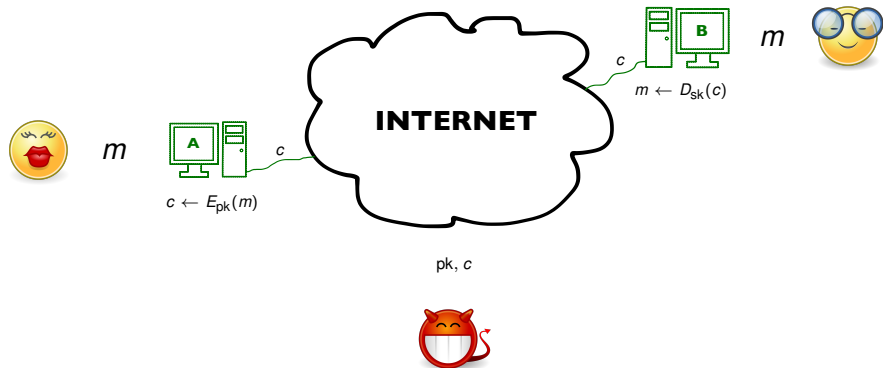


Confidential Communication with PKE

Assumption: Public key transmitted **authentically**.

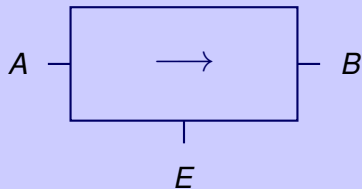


Confidential Communication with PKE



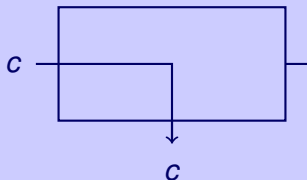
Confidential Communication with PKE

Internet: **Insecure** communication only.



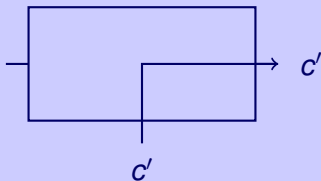
Confidential Communication with PKE

Internet: Insecure communication only.



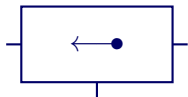
Confidential Communication with PKE

Internet: **Insecure** communication only.

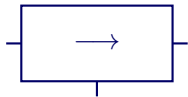


The Goal

Assumed



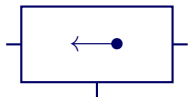
authenticated channel



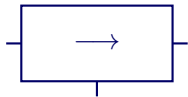
insecure channel

The Goal

Assumed

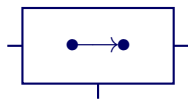


authenticated channel



insecure channel

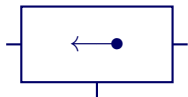
To Be Constructed



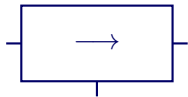
secure channel

The Goal

Assumed



authenticated channel

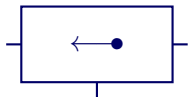


insecure channel

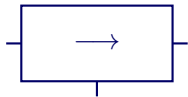
E has all the
capabilities of A .

The Goal

Assumed

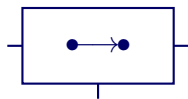


authenticated channel



insecure channel

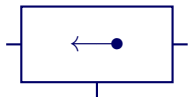
To Be Constructed



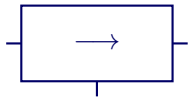
secure channel

The Goal

Assumed

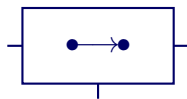
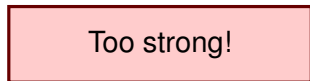


authenticated channel



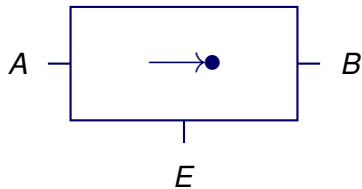
insecure channel

To Be Constructed

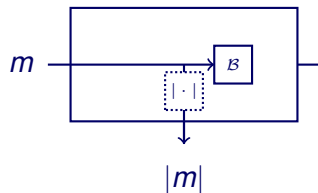


secure channel

New Goal: Confidential Channel



New Goal: Confidential Channel



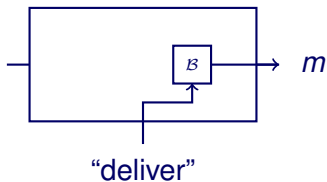
- ▶ Messages stored in **buffer**.

New Goal: Confidential Channel



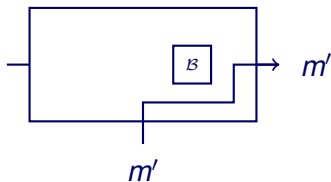
- ▶ Messages stored in **buffer**.
- ▶ Eve's choices:

New Goal: Confidential Channel



- ▶ Messages stored in **buffer**.
- ▶ Eve's choices:
 - ▶ **deliver** messages

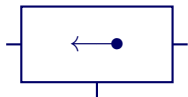
New Goal: Confidential Channel



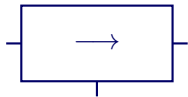
- ▶ Messages stored in **buffer**.
- ▶ Eve's choices:
 - ▶ **deliver** messages
 - ▶ **inject** messages

The Goal

Assumed

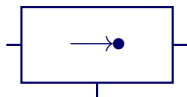


authenticated channel



insecure channel

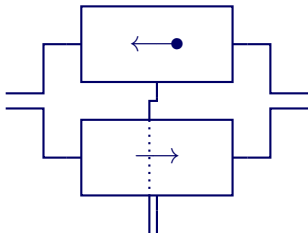
To Be Constructed



confidential channel

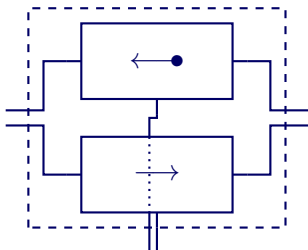
The Goal

Assumed



The Goal

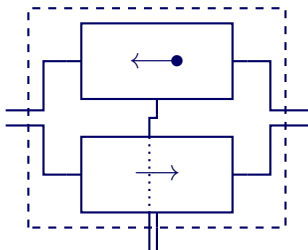
Assumed



**Parallel
Composition:**
Again a resource.

The Goal

Assumed

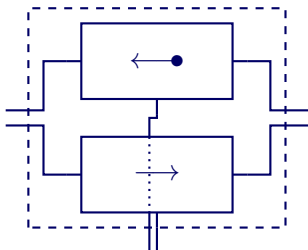


**Parallel
Composition:**
Again a resource.

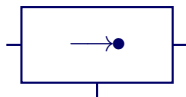
Notation: $[\leftarrow \bullet, \rightarrow]$

The Goal

Assumed

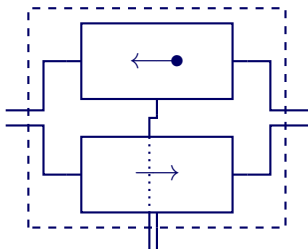


To Be Constructed

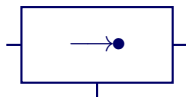


The Goal

Assumed

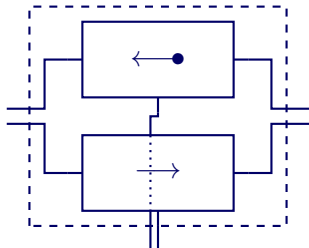


To Be Constructed

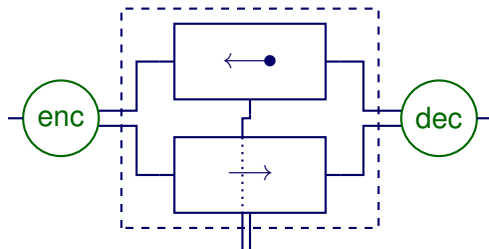


Goal: Construct $\rightarrow \bullet$ from $[\leftarrow \bullet, \rightarrow]$.

PKE Protocol

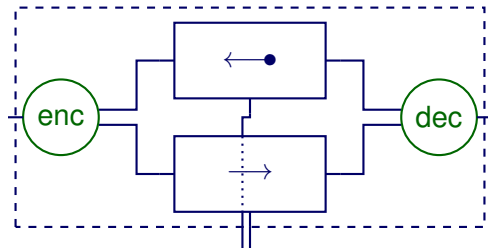


PKE Protocol



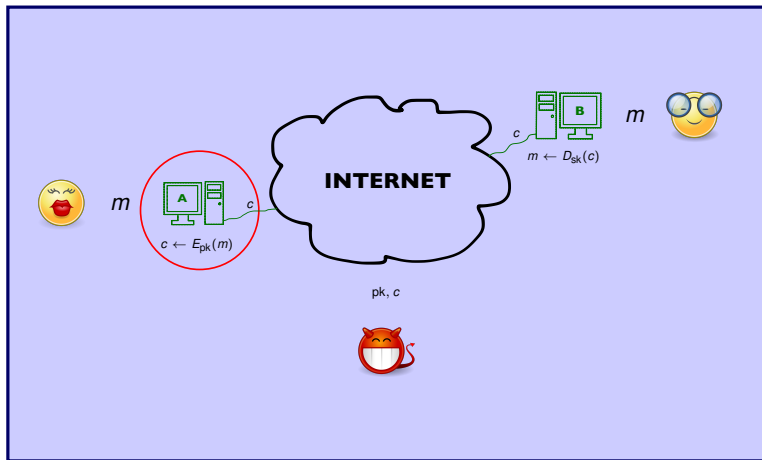
A and B attach protocol **converters**.

PKE Protocol

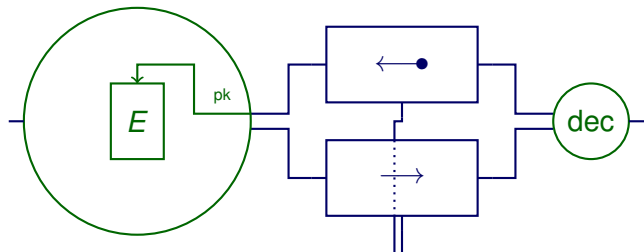


Notation: $enc^A dec^B [\leftarrow \bullet, \rightarrow]$

PKE Protocol



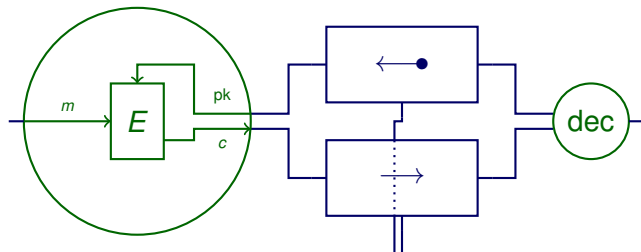
PKE Protocol



PKE Scheme:

$\Pi = (K, E, D)$

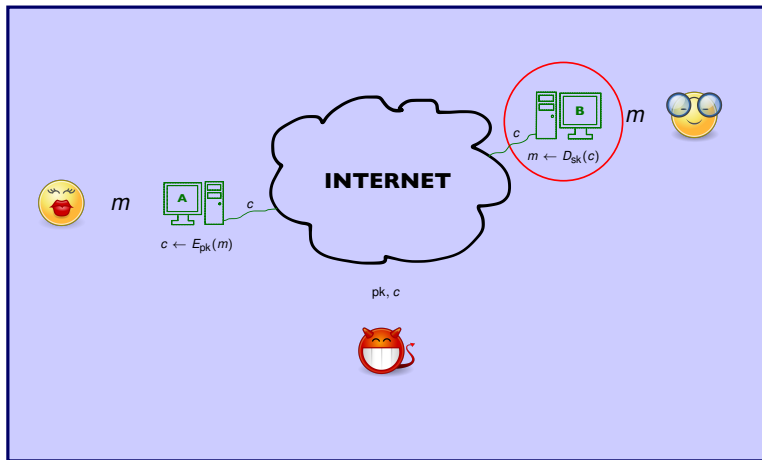
PKE Protocol



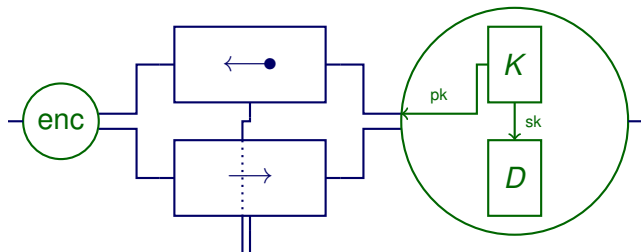
PKE Scheme:

$\Pi = (K, E, D)$

PKE Protocol



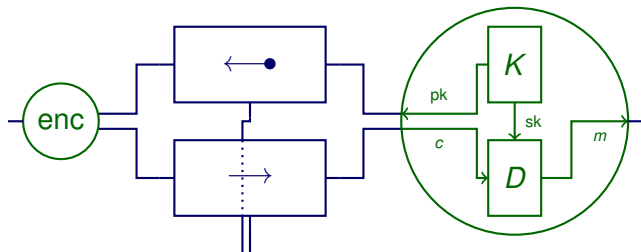
PKE Protocol



PKE Scheme:

$\Pi = (K, E, D)$

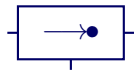
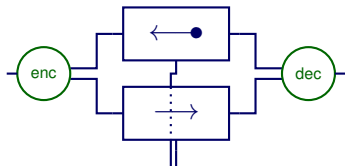
PKE Protocol



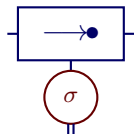
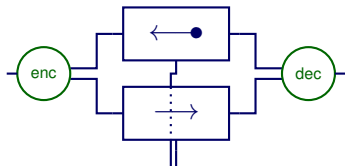
PKE Scheme:

$\Pi = (K, E, D)$

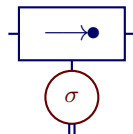
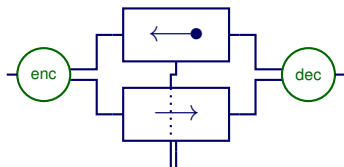
Security Notion



Security Notion

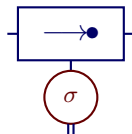
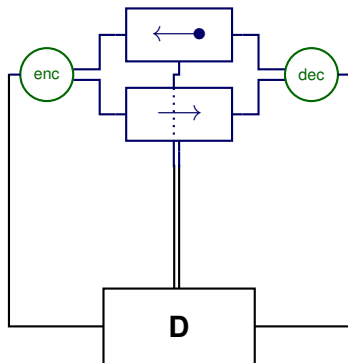


Security Notion

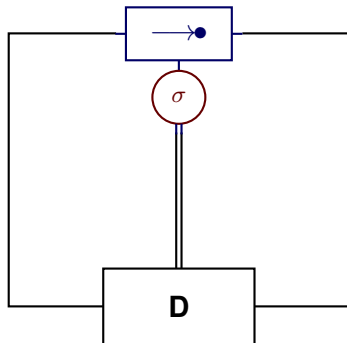
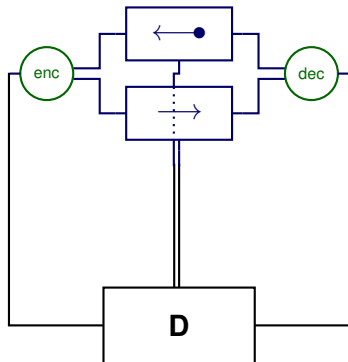


Translates attacks onto $\text{enc}^A \text{dec}^B [\leftarrow \bullet, \rightarrow]$ into attacks onto $\rightarrow \bullet$.

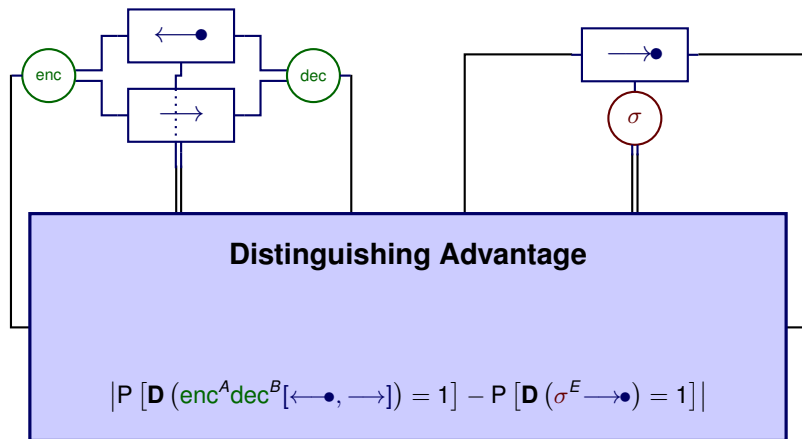
Security Notion



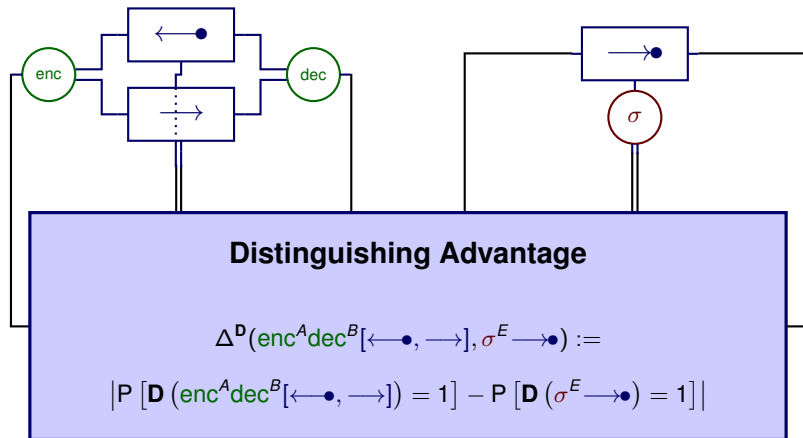
Security Notion



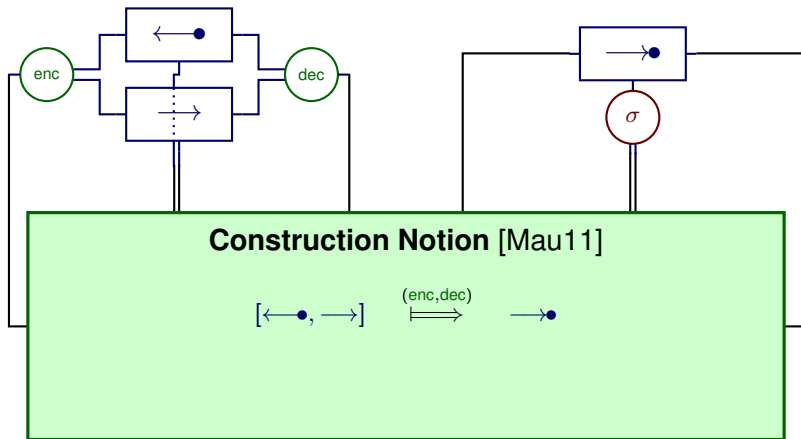
Security Notion



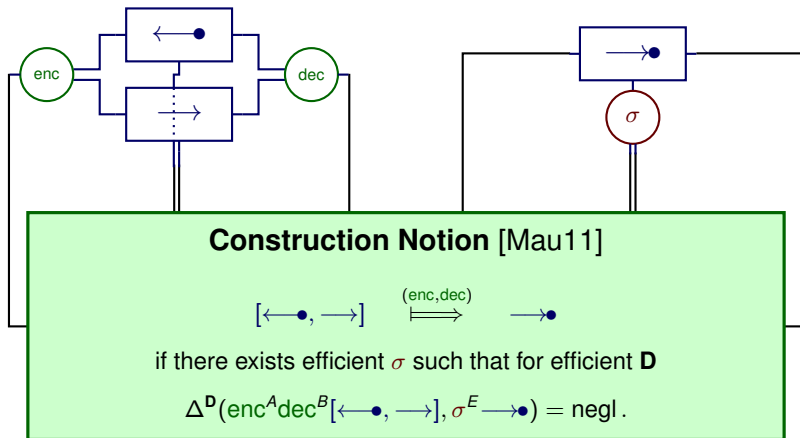
Security Notion



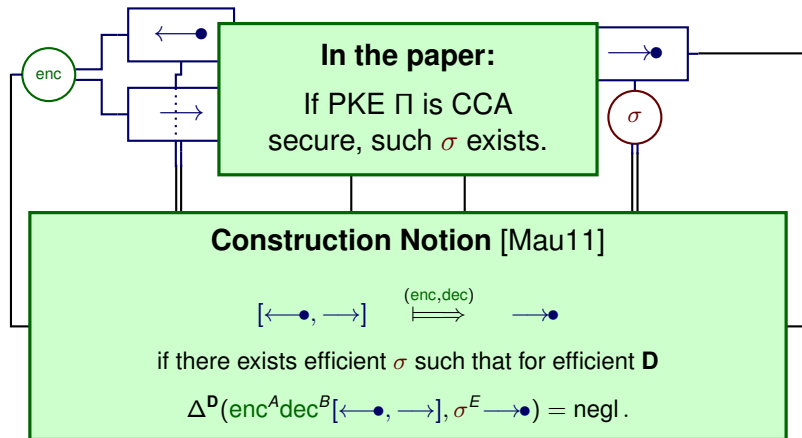
Security Notion



Security Notion



Security Notion



Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.

Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment

Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment

Assumed Resource

$[\leftarrow \bullet, \rightarrow]$

Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment
 - ▶ security **guarantees**

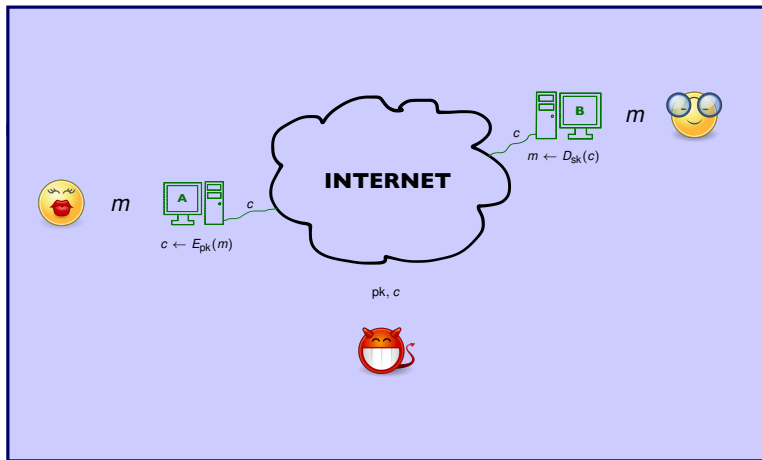
Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment
 - ▶ security **guarantees**

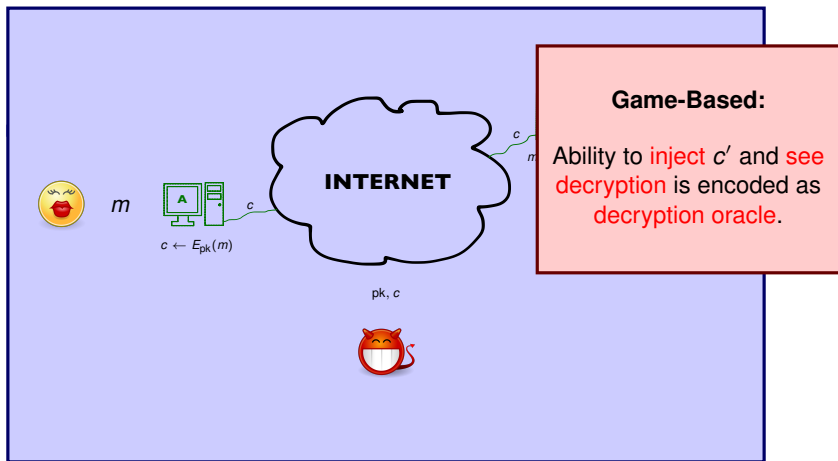
Constructed Resource



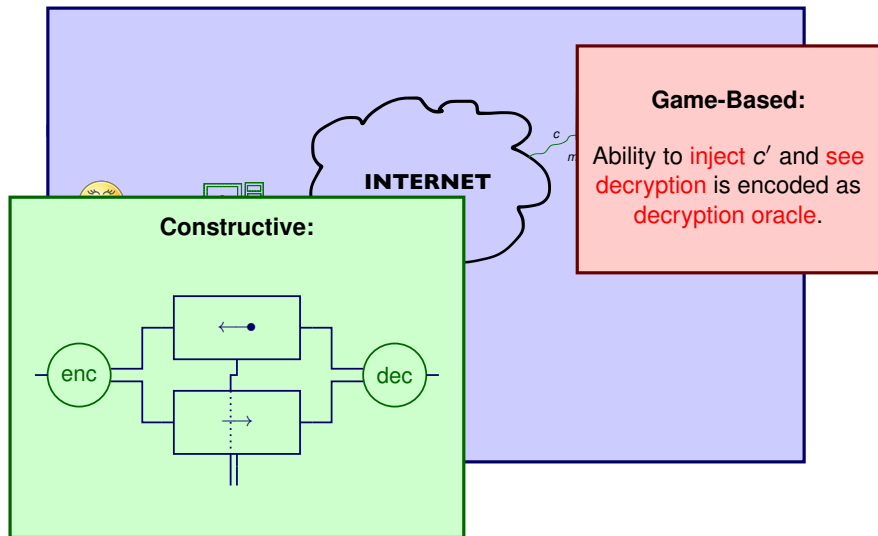
Benefits of the Constructive Approach [Mau11]



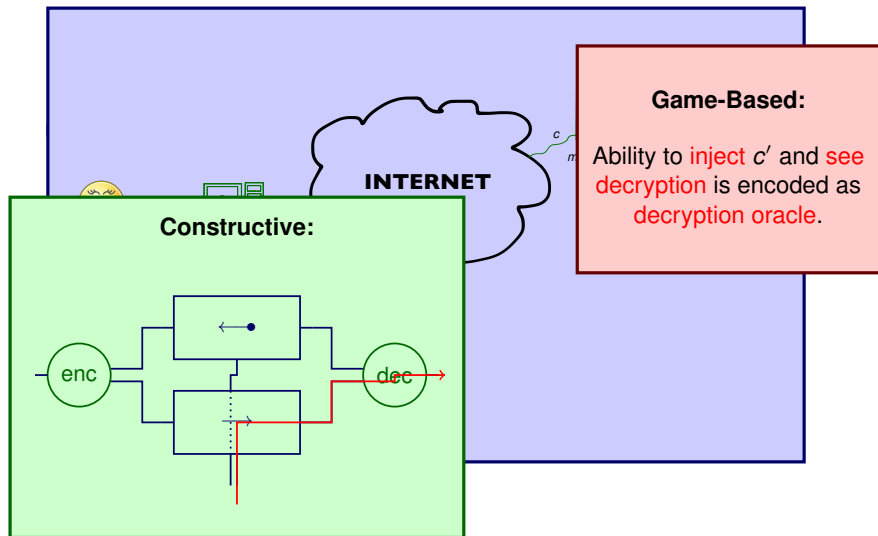
Benefits of the Constructive Approach [Mau11]



Benefits of the Constructive Approach [Mau11]



Benefits of the Constructive Approach [Mau11]



Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment
 - ▶ security **guarantees**
- ▶ Composition theorem

Benefits of the Constructive Approach [Mau11]

▶ **Cle**

▶

▶

▶ **Cor**

Assume $R \stackrel{\pi}{\iff} S$ and $S \stackrel{\pi'}{\iff} T$. Then:

Benefits of the Constructive Approach [Mau11]

► **Cle**

►

►

► **Cor**

Assume $R \xrightarrow{\pi} S$ and $S \xrightarrow{\pi'} T$. Then:

$$R \xrightarrow{\pi' \circ \pi} T$$

Benefits of the Constructive Approach [Mau11]

► Cle



► Cor

Assume $R \xrightarrow{\pi} S$ and $S \xrightarrow{\pi'} T$. Then:

$$R \xrightarrow{\pi' \circ \pi} T$$

$$[R, U] \xrightarrow{[\pi, \text{id}]} [S, U]$$

$$[U, R] \xrightarrow{[\text{id}, \pi]} [U, S]$$

Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment
 - ▶ security **guarantees**
- ▶ Composition theorem
 - ▶ Enables **modular** protocol design.

Benefits of the Constructive Approach [Mau11]

- ▶ **Clear semantics:** Everything is explicit.
 - ▶ **assumptions** about execution environment
 - ▶ security **guarantees**
- ▶ Composition theorem
 - ▶ Enables **modular** protocol design.
 - ▶ Applicable to the design of **real-world protocols**.

Unilaterally Authenticated Key Exchange

▶ Cle



▶ Cor



Benefits of the Constructive Approach [Mau11]

Unilaterally Authenticated Key Exchange

▶ Cle



▶ Cor



- ▶ One **authenticated** server
- ▶ Many **unauthenticated** clients
- ▶ **Goal:** Key exchange between any client and server.

▶ Cle



▶ Cor



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]

- ▶ **Cle**



- ▶ **Cor**



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:

- ▶ Cle



- ▶ Cor



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:
 - ▶ Digital Signatures

- ▶ Cle



- ▶ Cor



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:
 - ▶ Digital Signatures
 - ▶ Nonces

- ▶ Cle



- ▶ Cor



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:
 - ▶ Digital Signatures
 - ▶ Nonces
 - ▶ KEMs

- ▶ Cle



- ▶ Cor



Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:
 - ▶ Digital Signatures
 - ▶ Nonces
 - ▶ KEMs
- ▶ **Two** rounds

▶ Cle

▶

▶

▶ Cor

▶

▶

Unilaterally Authenticated Key Exchange

- ▶ Simple **modular** protocol [MTC13]
- ▶ Construction steps for cryptographic techniques:
 - ▶ Digital Signatures
 - ▶ Nonces
 - ▶ KEMs
- ▶ **Two** rounds
- ▶ KEM: Only **CPA** required

Contributions

In the paper...

Contributions

In the paper...

- ▶ CCA-security of Π suffices for

$$[\leftarrow \bullet, \rightarrow] \stackrel{(\text{enc}, \text{dec})}{\iff} \rightarrow \bullet.$$

Contributions

In the paper...

- ▶ CCA-security of Π suffices for

$$[\leftarrow \bullet, \rightarrow] \stackrel{(enc, dec)}{\iff} \rightarrow \bullet.$$

RCCA [CKN03] security
of Π is necessary
and sufficient.

Contributions

In the paper...

- ▶ CCA-security of Π suffices for

$$[\leftarrow \bullet, \rightarrow] \stackrel{(\text{enc}, \text{dec})}{\iff} \rightarrow \bullet.$$

- ▶ CPA-security of Π suffices for

$$[\leftarrow \bullet, \bullet \rightarrow] \stackrel{(\text{enc}, \text{dec})}{\iff} \bullet \rightarrow \bullet.$$

Contributions

In the paper...

- ▶ CCA-security of Π suffices for

$$[\leftarrow \bullet, \rightarrow] \stackrel{(enc, dec)}{\iff} \rightarrow \bullet.$$

- ▶ CPA-security of Π suffices for

CPA security of Π is
also necessary.

Contributions

In the paper...

- ▶ CCA-security of Π suffices for

$$[\leftarrow \bullet, \rightarrow] \stackrel{(\text{enc}, \text{dec})}{\iff} \rightarrow \bullet.$$

- ▶ CPA-security of Π suffices for

$$[\leftarrow \bullet, \bullet \rightarrow] \stackrel{(\text{enc}, \text{dec})}{\iff} \bullet \rightarrow \bullet.$$

- ▶ Constructive semantics of other security notions (IND-CCA1, NM-CPA).



Thank you!



References I



Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway.

Relations Among Notions of Security for Public-Key Encryption Schemes.

In Hugo Krawczyk, editor, *CRYPTO 1998*, volume 1462 of *LNCS*, pages 26–45, Heidelberg, 1998. Springer.







Mihir Bellare and Amit Sahai.

Non-malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization.

In Michael Wiener, editor, *CRYPTO 1999*, volume 1666 of *LNCS*, pages 519–536, Heidelberg, 1999. Springer.

References II

-  Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen.
Relaxing Chosen-Ciphertext Security.
In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 565–582, Heidelberg, 2003. Springer.
-  Danny Dolev, Cynthia Dwork, and Moni Naor.
Non-Malleable Cryptography (Extended Abstract).
In *23rd ACM STOC*, pages 542–552, 1991.
-  Shafi Goldwasser and Silvio Micali.
Probabilistic Encryption.
Journal of Computer and System Sciences, 28(2):270–299, 1984.
-  Oded Goldreich.
Foundations of Cryptography.
Class Notes, Spring 1989.
Technion University.

References III



Ueli Maurer.

Constructive Cryptography—A New Paradigm for Security Definitions and Proofs.

In S. Moedersheim and C. Palamidessi, editors, *TOSCA 2011*, volume 6993 of *LNCS*, pages 33–56, Heidelberg, April 2011. Springer.



Ueli Maurer, Björn Tackmann, and Sandro Coretti.

Key Exchange with Unilateral Authentication: Composable Security Definition and Modular Protocol Design.

Cryptology ePrint Archive, Report 2013/555, 2013.



Moni Naor and Moti Yung.

Public-key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks.

In *22nd ACM STOC*, pages 427–437, 1990.



Andrew Chi-Chih Yao.

Theory and Applications of Trapdoor Functions (Extended Abstract).

In *23rd FOCS*, pages 80–91, 1982.



Yuliang Zheng and Jennifer Seberry.

Practical Approaches to Attaining Security Against Adaptively Chosen Ciphertext Attacks (Extended Abstract).

In Ernest F. Brickell, editor, *CRYPTO '92*, volume 740 of *LNCS*, pages 292–304, Heidelberg, 1992. Springer.