Authentication

Ueli Maurer

ETH Zurich

QCRYPT 2012, Singapore

Authentication

and more ...

Ueli Maurer

ETH Zurich

QCRYPT 2012, Singapore

Three goals of this talk

1. Role of authentication in QKD

Three goals of this talk

1. Role of authentication in QKD

2. Information-theoretically secure authentication

Three goals of this talk

1. Role of authentication in QKD

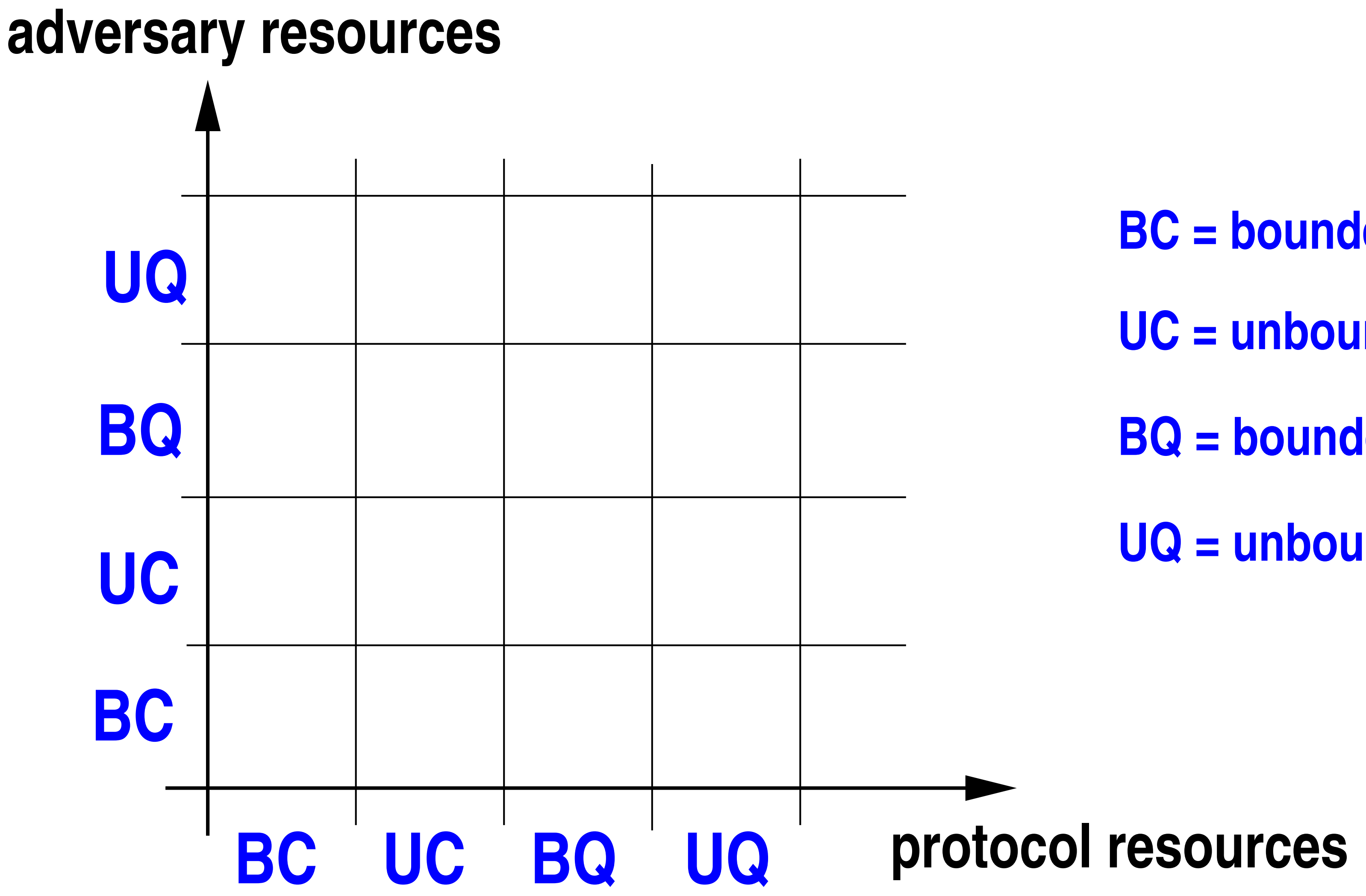
2. Information-theoretically secure authentication

3. Constructive approach to cryptography

Three goals of this talk

1. Role of authentication in QKD
2. Information-theoretically secure authentication
3. Constructive approach to cryptography
   (joint work with Renato Renner)

Security types – a classification



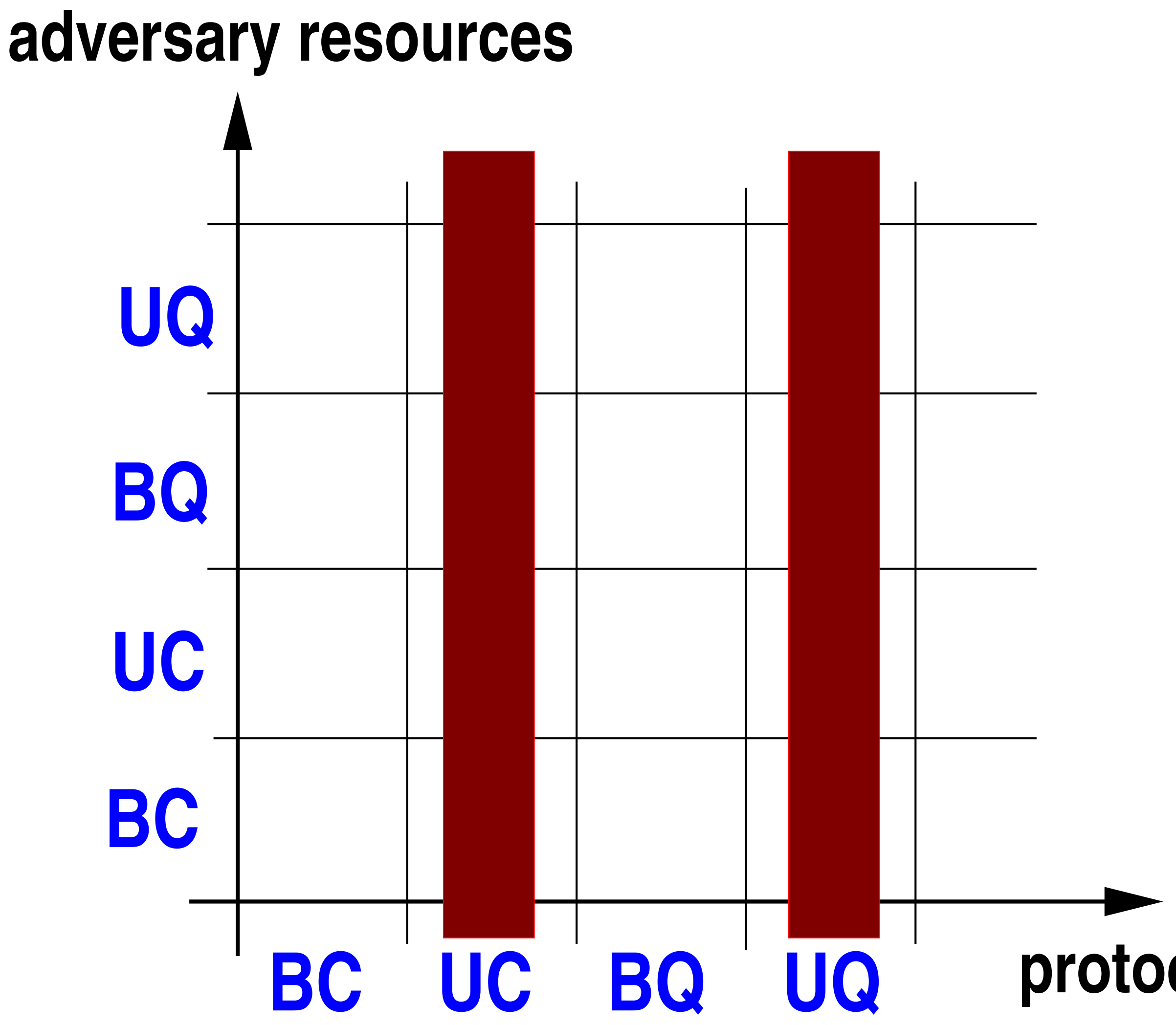
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



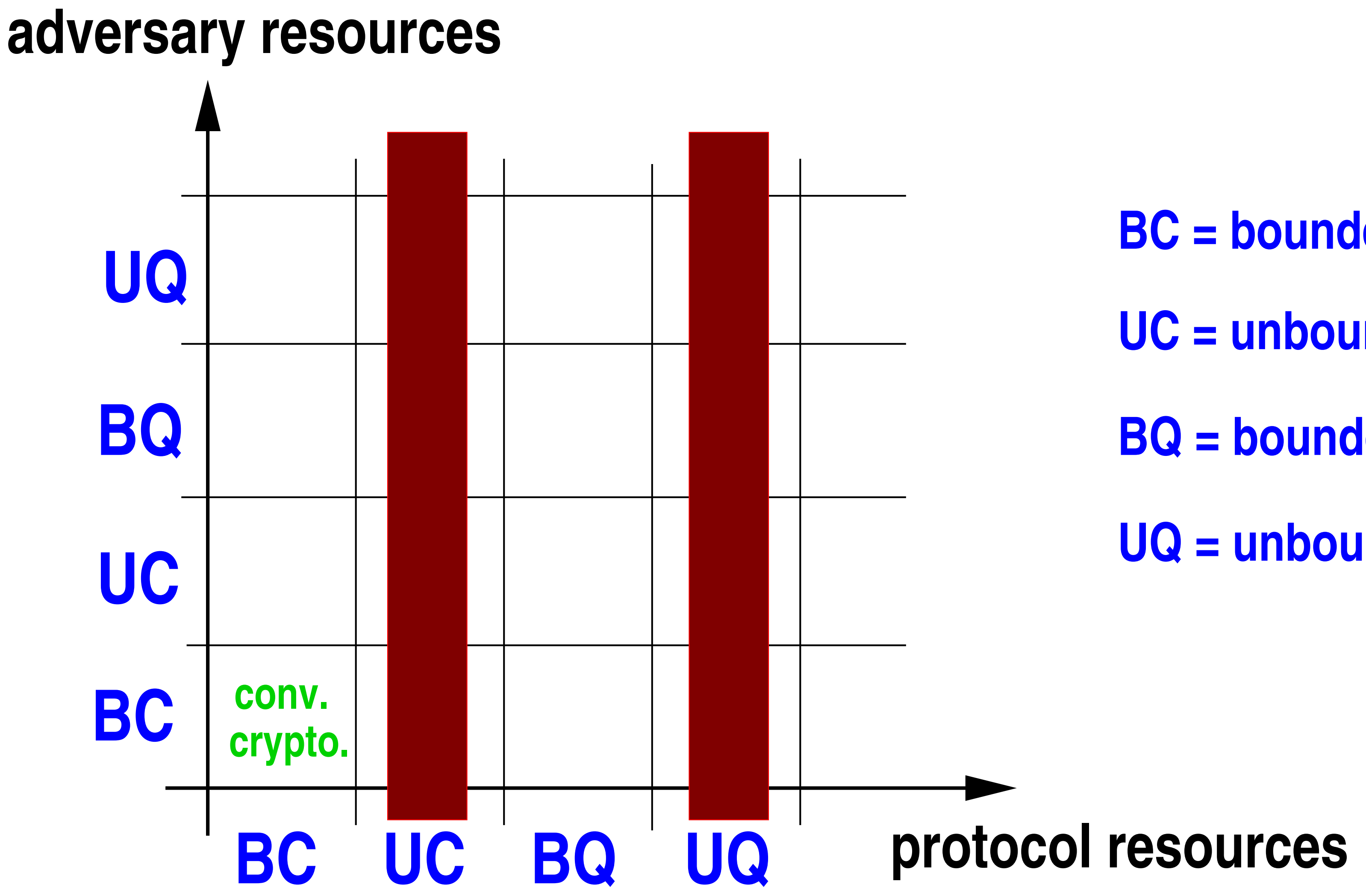
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



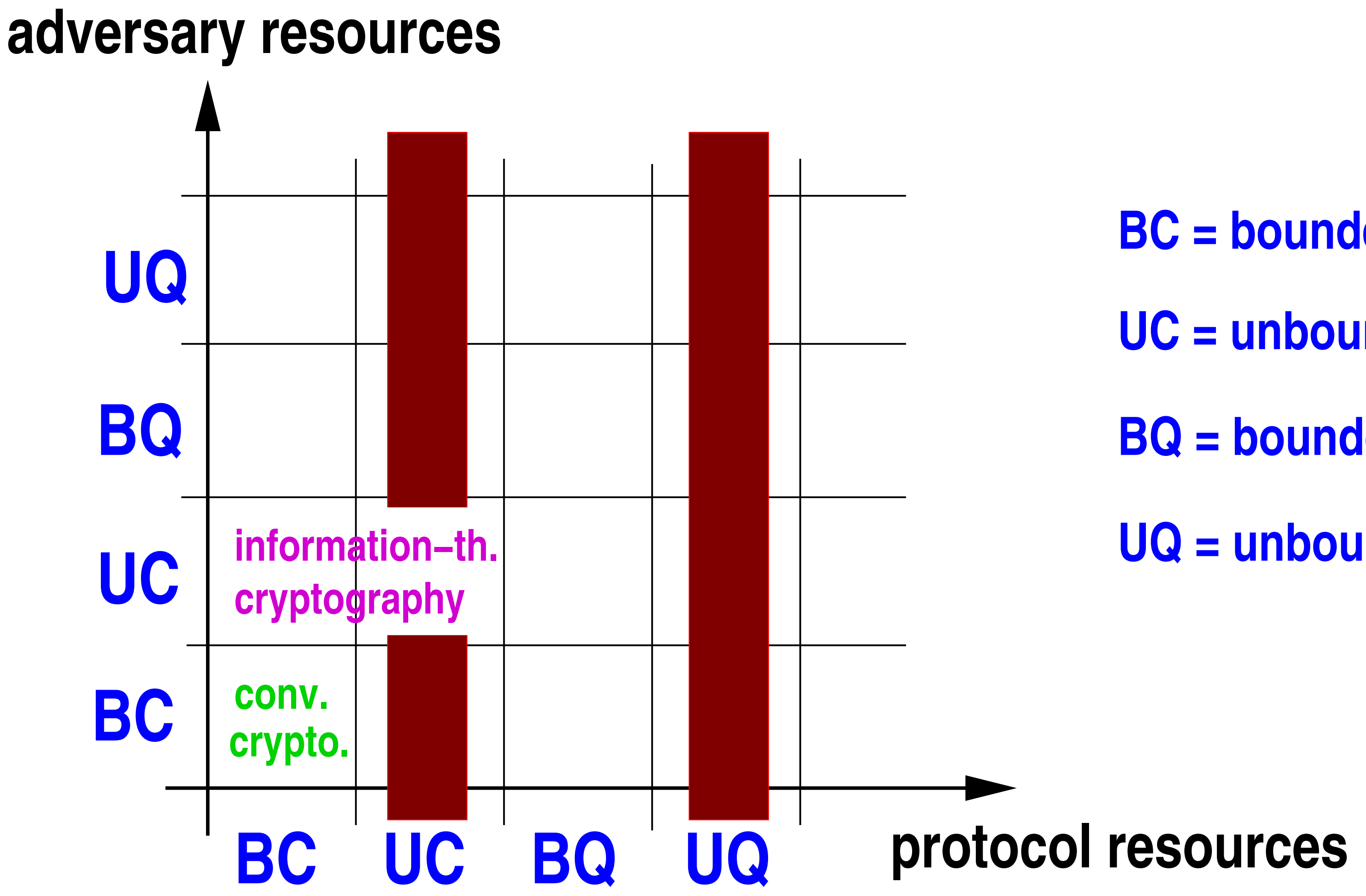
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



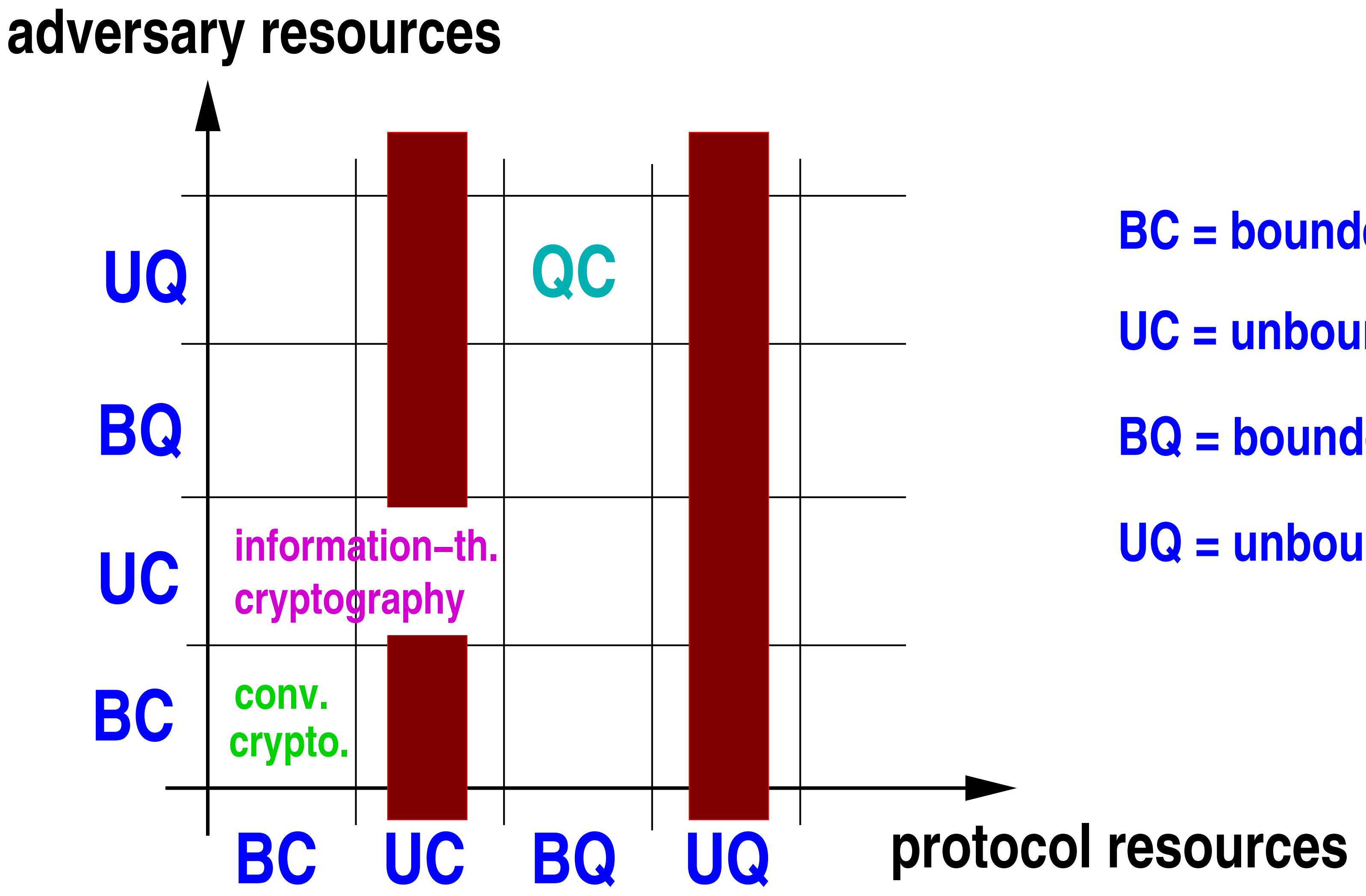
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



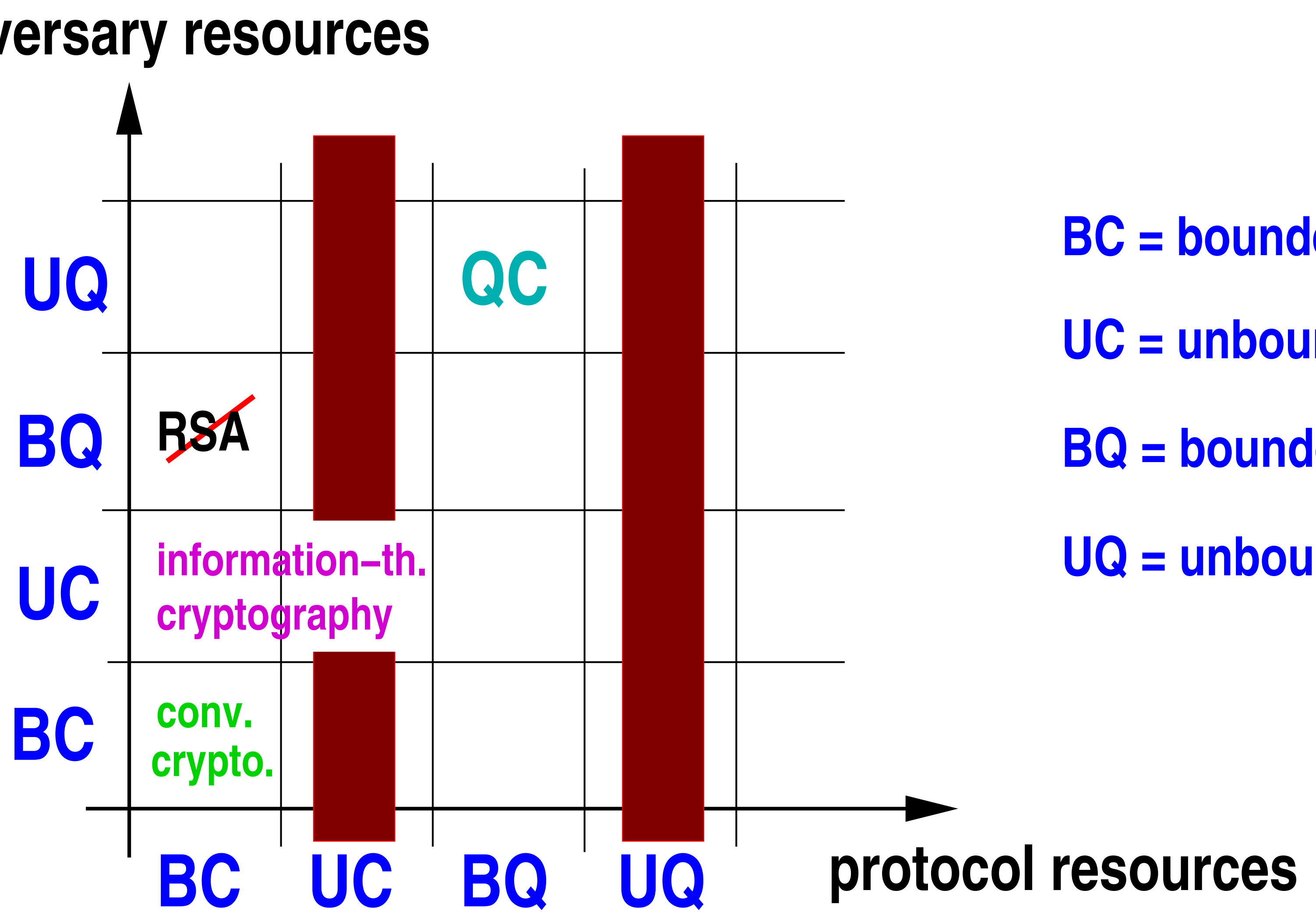
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



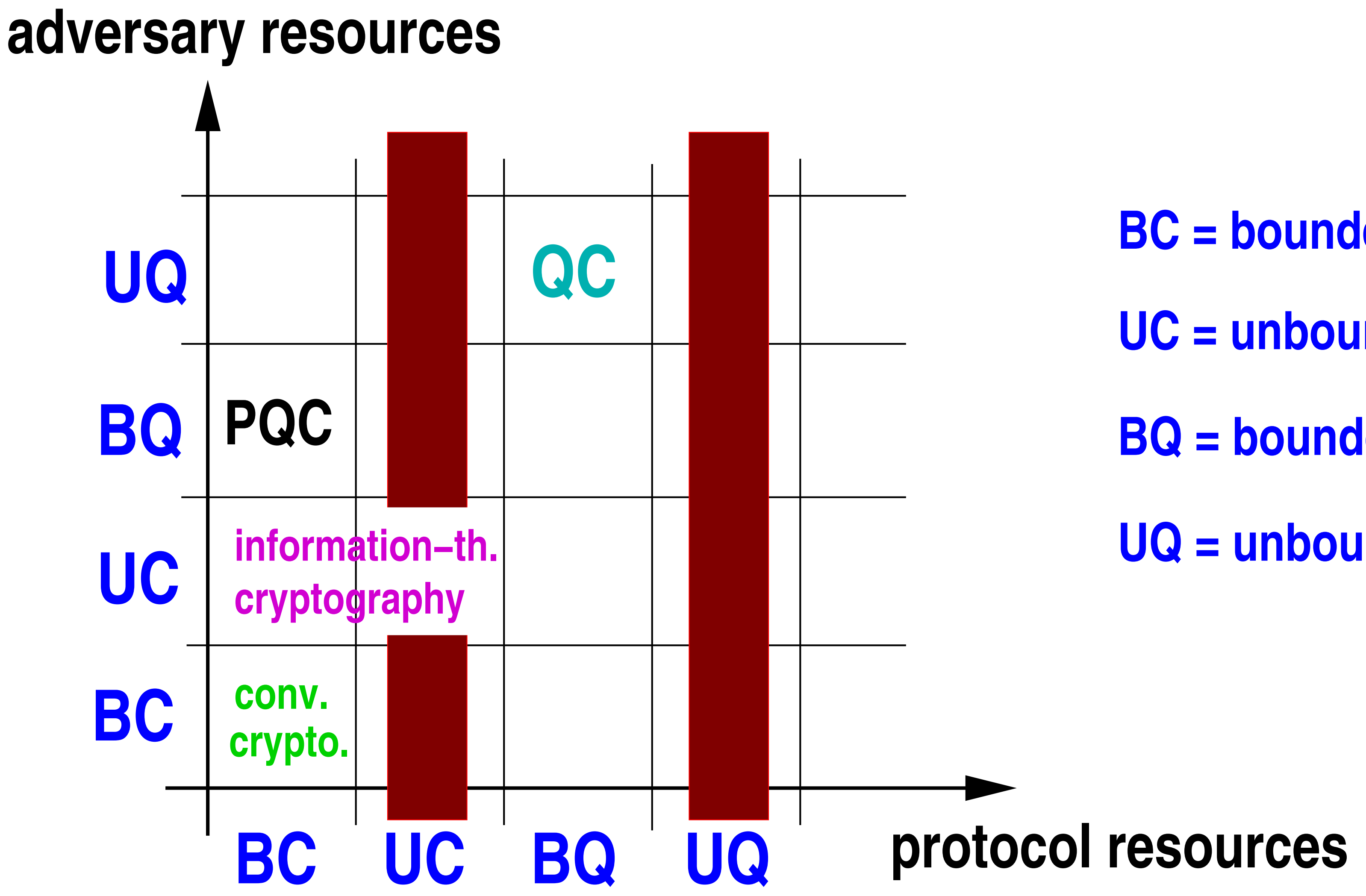
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



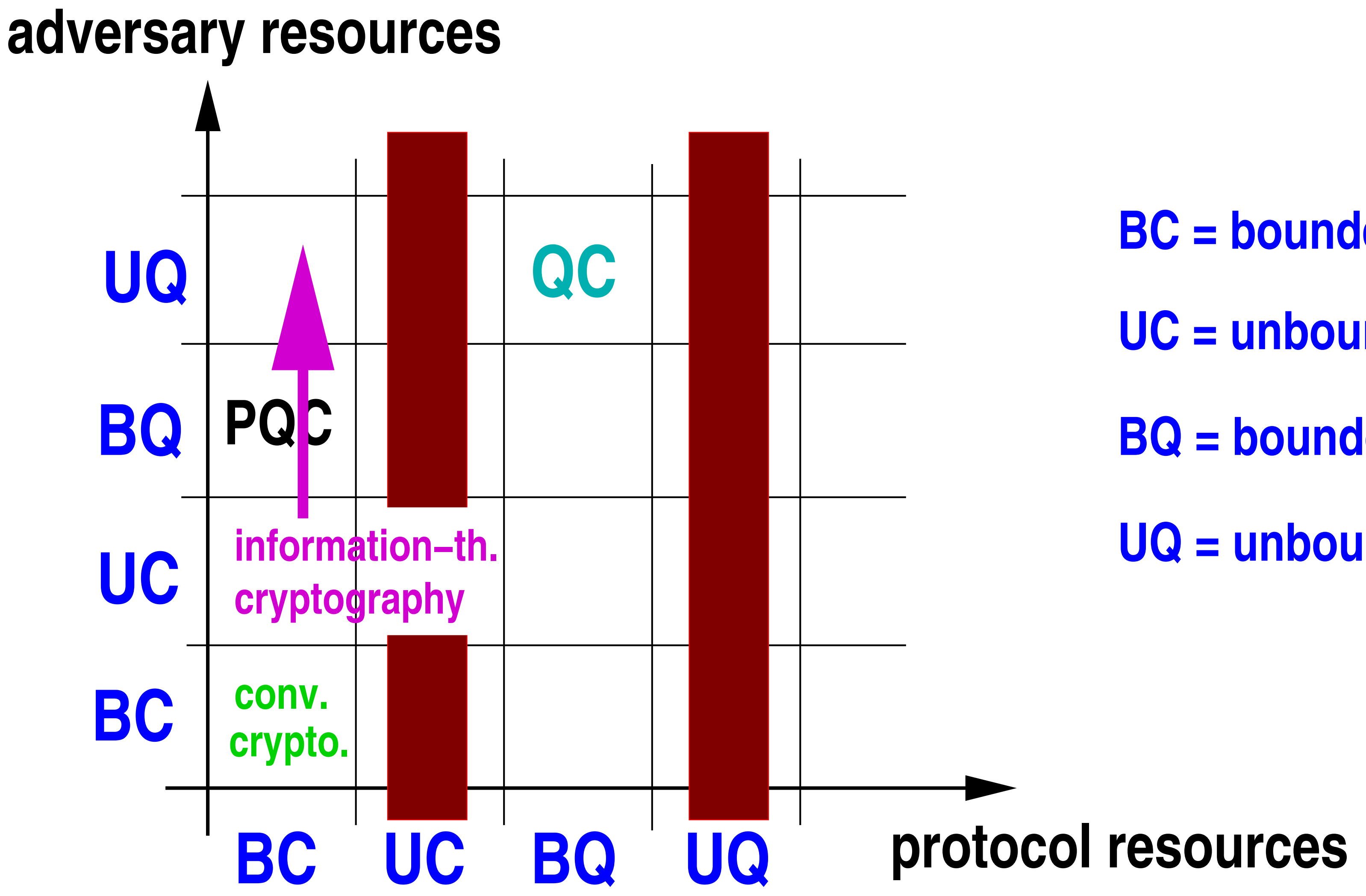
BC = bounded classical

UC = unbounded classical

BQ = bounded quantum

UQ = unbounded quantum

Security types – a classification



BC = bounded classical

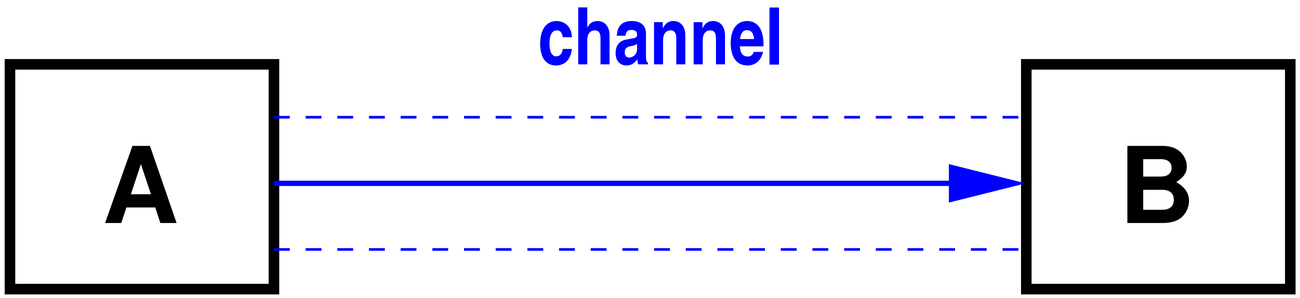
UC = unbounded classical

BQ = bounded quantum

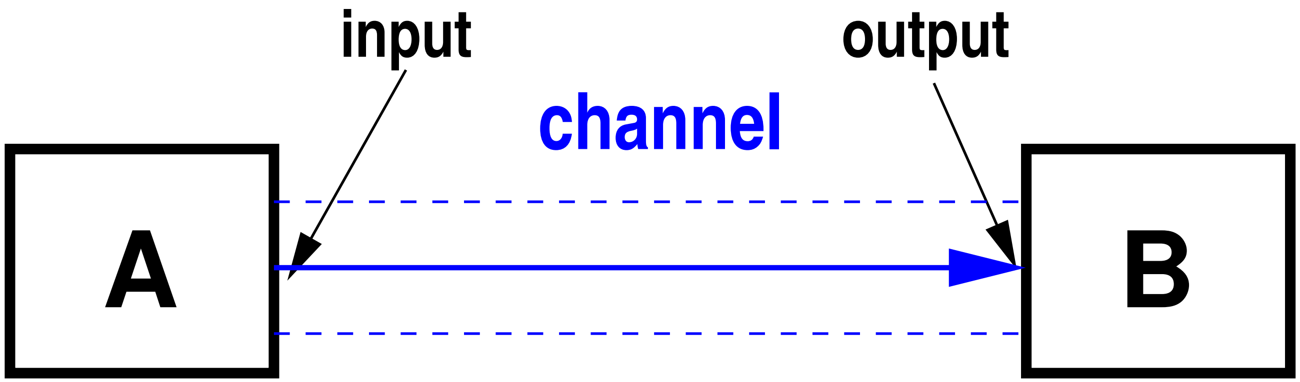
UQ = unbounded quantum

Secrecy and authenticity

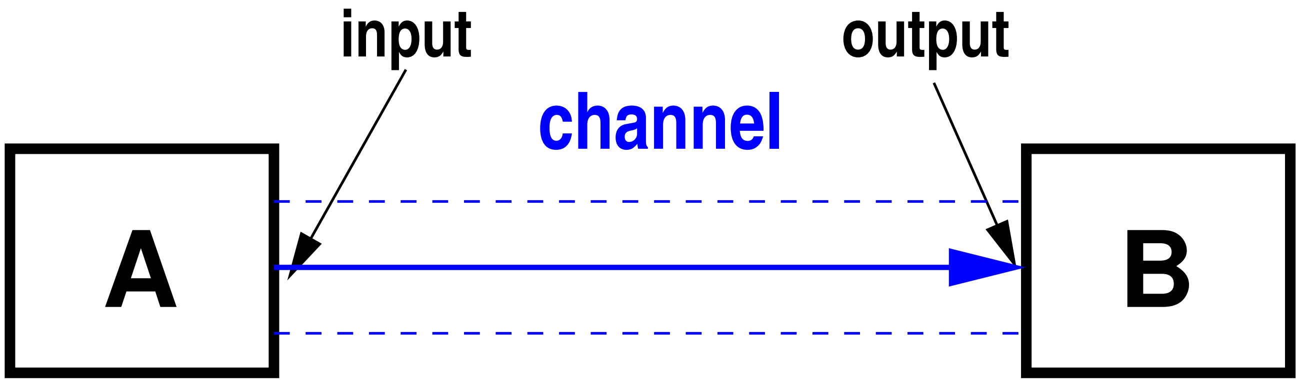
Secrecy and authenticity



Secrecy and authenticity

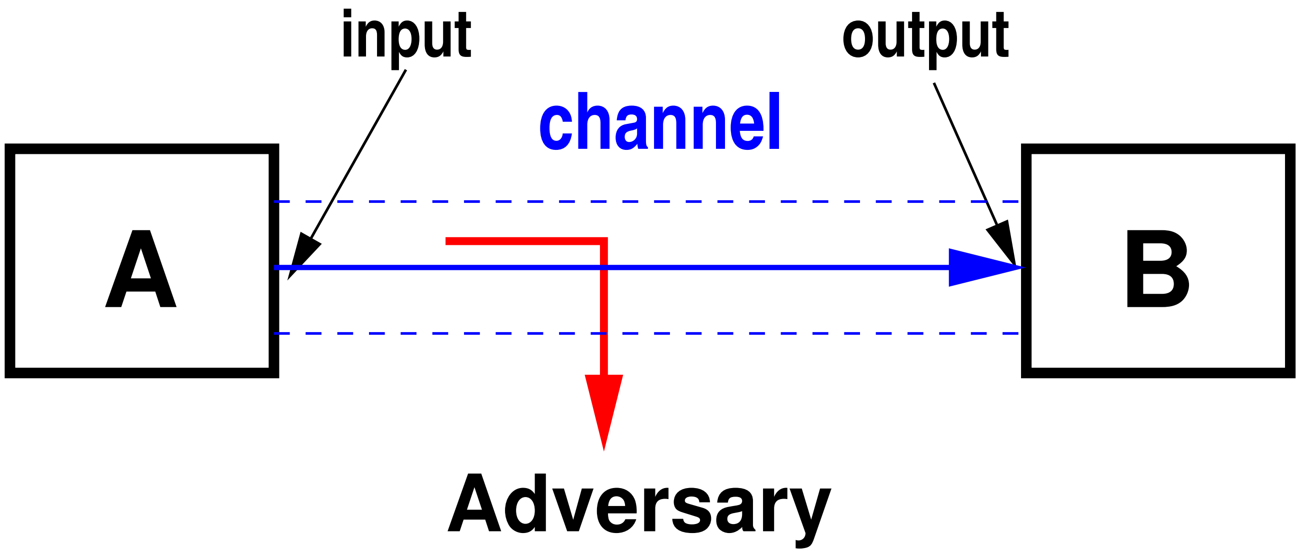


Secrecy and authenticity

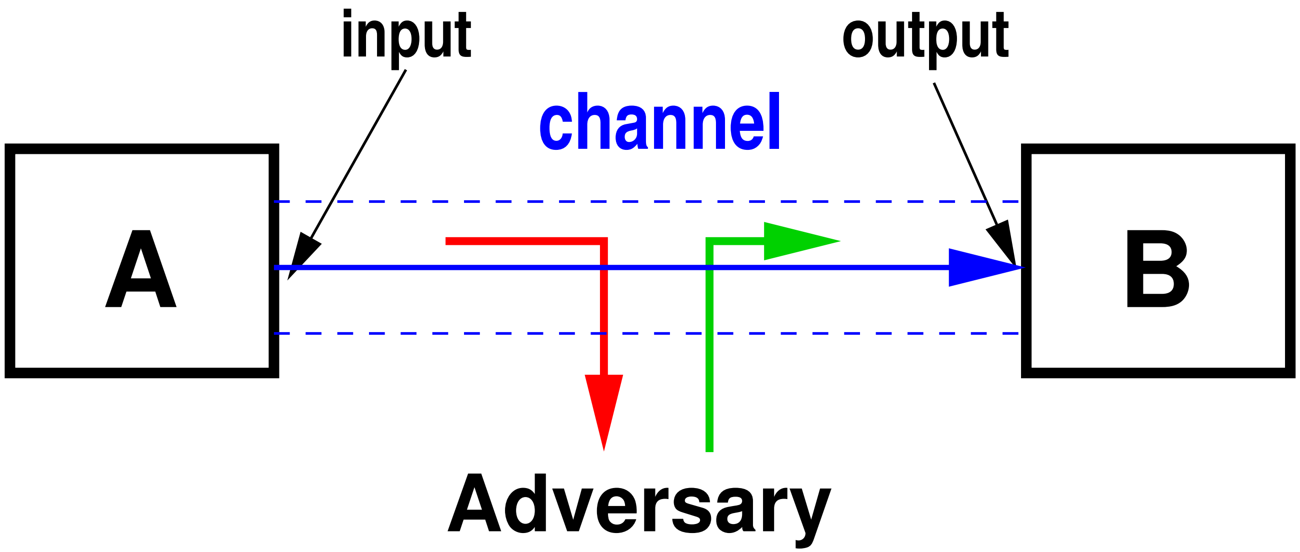


Adversary

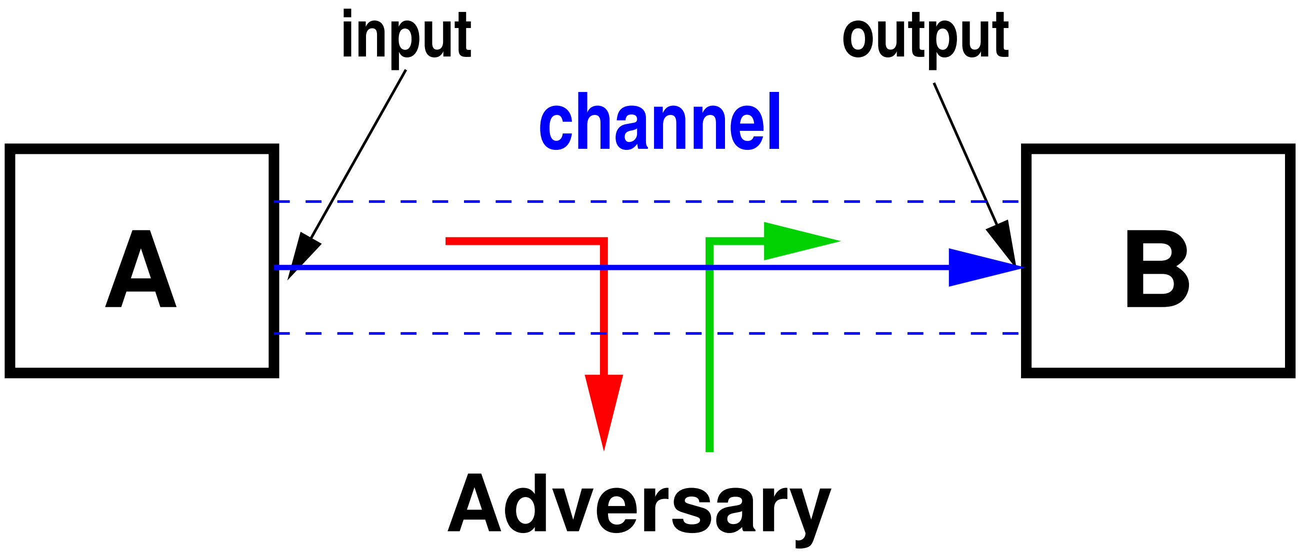
Secrecy and authenticity



Secrecy and authenticity



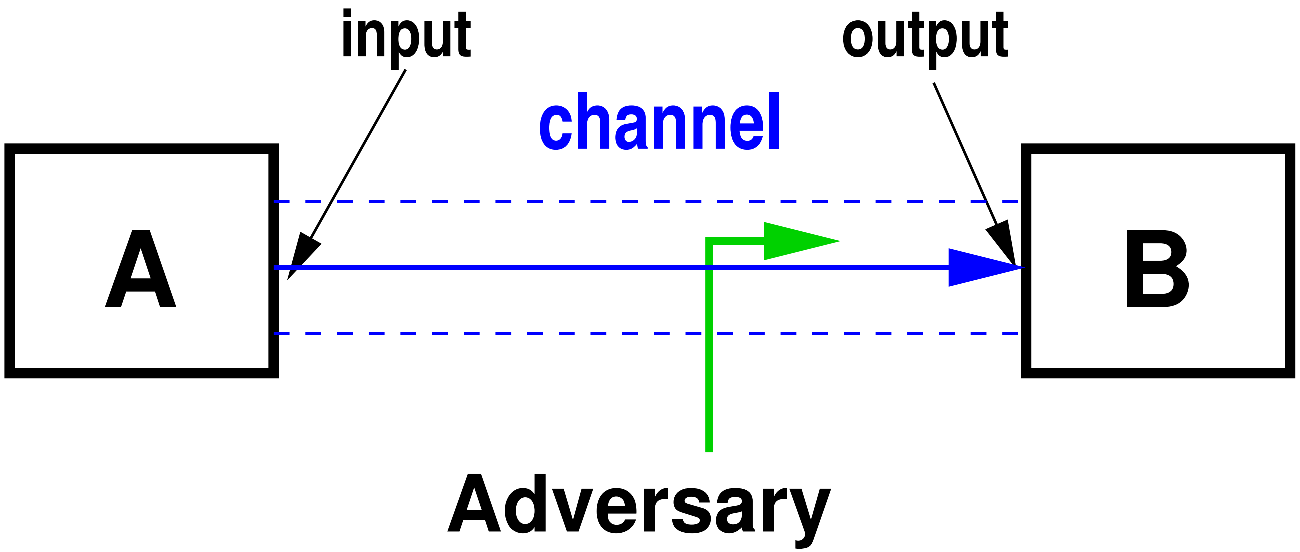
Secrecy and authenticity



Two basic **independent / dual** security properties:

- **secrecy**
- **authenticity**

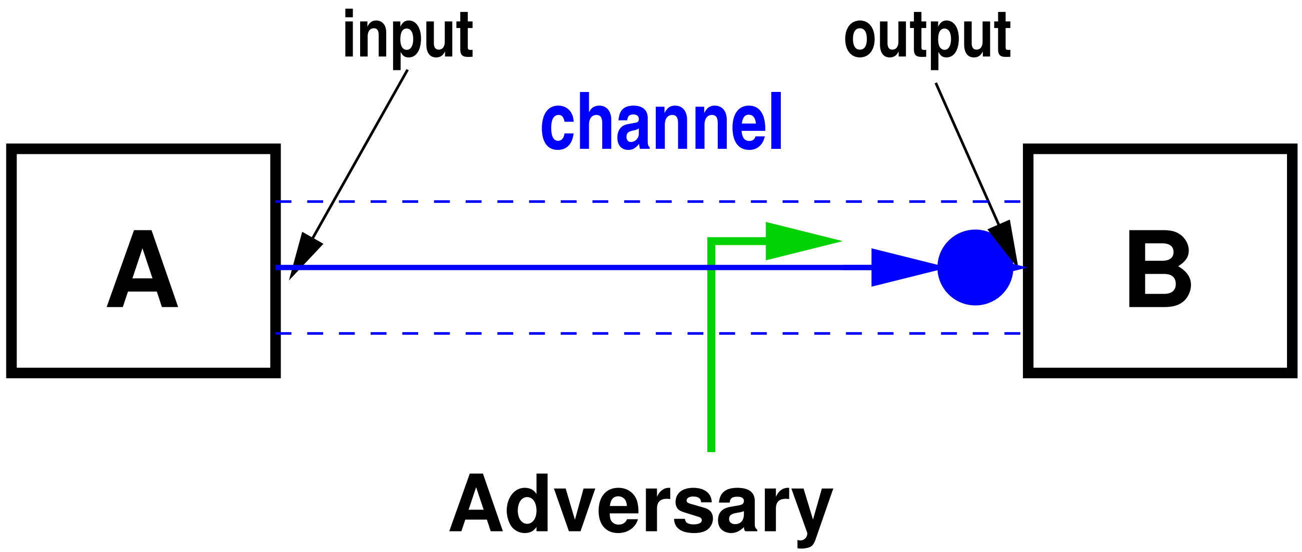
Secrecy and authenticity



Two basic **independent / dual** security properties:

- **secrecy** (output is exclusive)
- **authenticity**

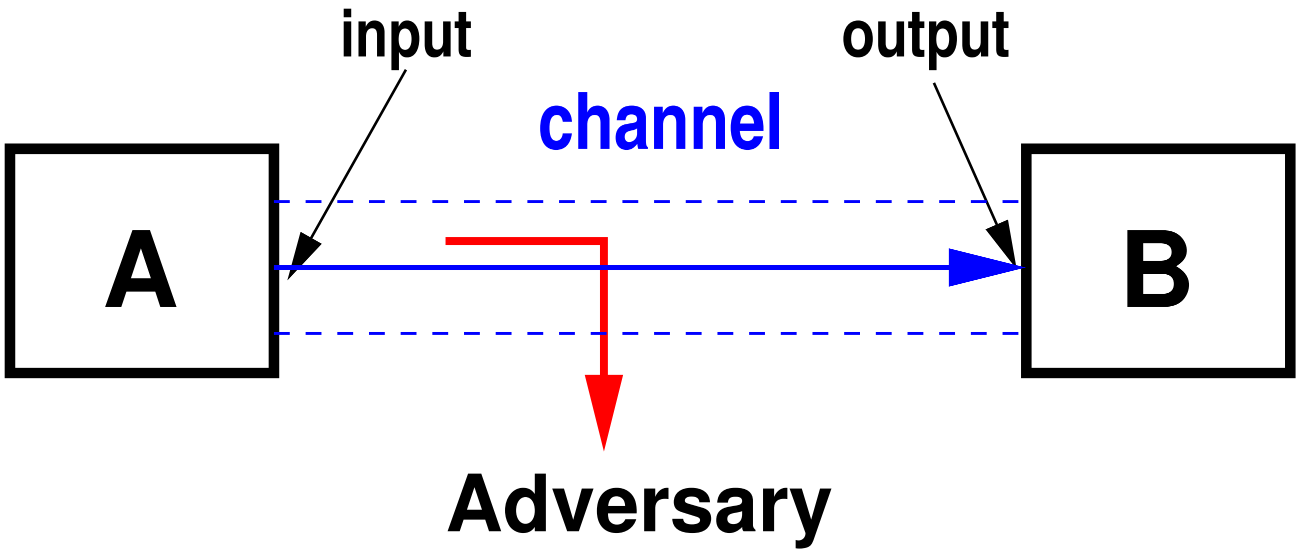
Secrecy and authenticity



Two basic **independent / dual** security properties:

- **secrecy** (output is exclusive)
- **authenticity**

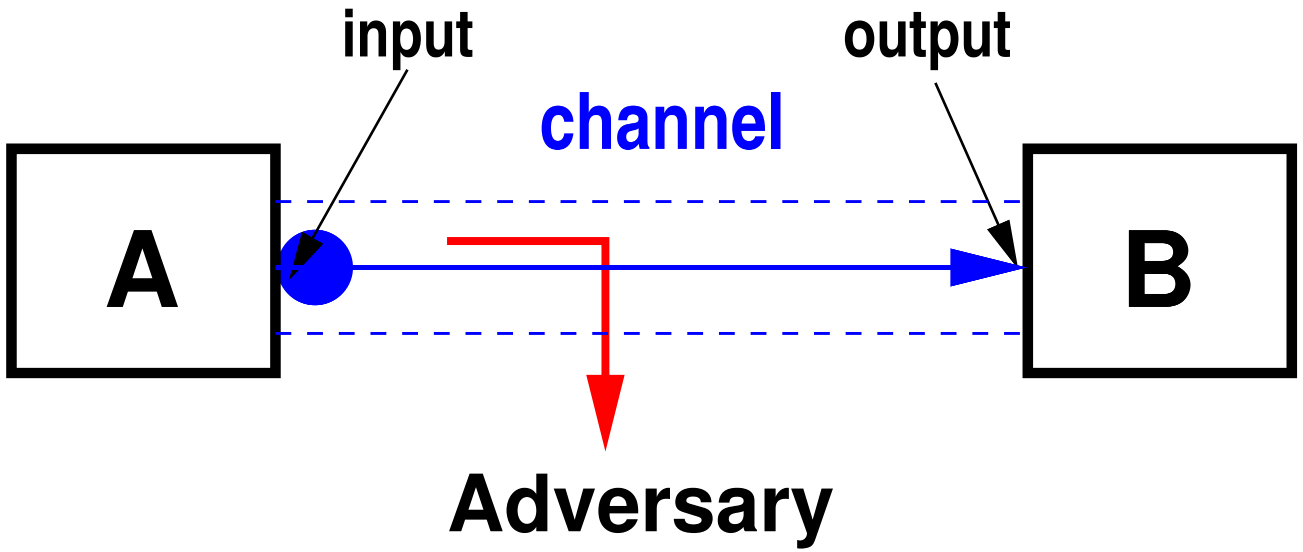
Secrecy and authenticity



Two basic **independent / dual** security properties:

- **secrecy** (output is exclusive)
- **authenticity** (input is exclusive)

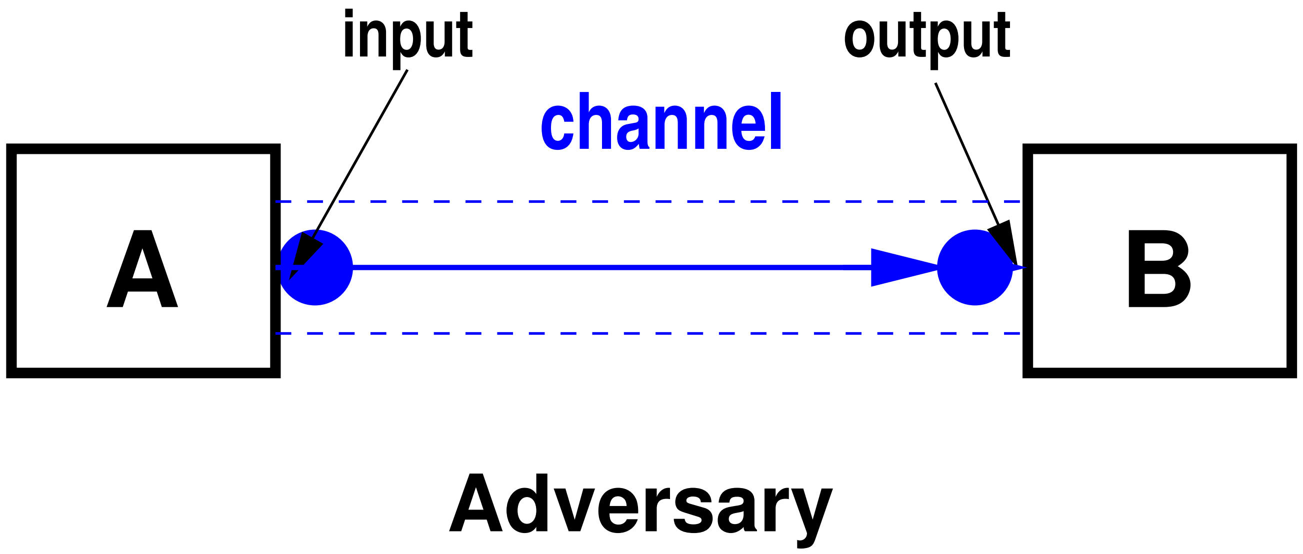
Secrecy and authenticity



Two basic **independent / dual** security properties:

- **secrecy** (output is exclusive)
- **authenticity** (input is exclusive)

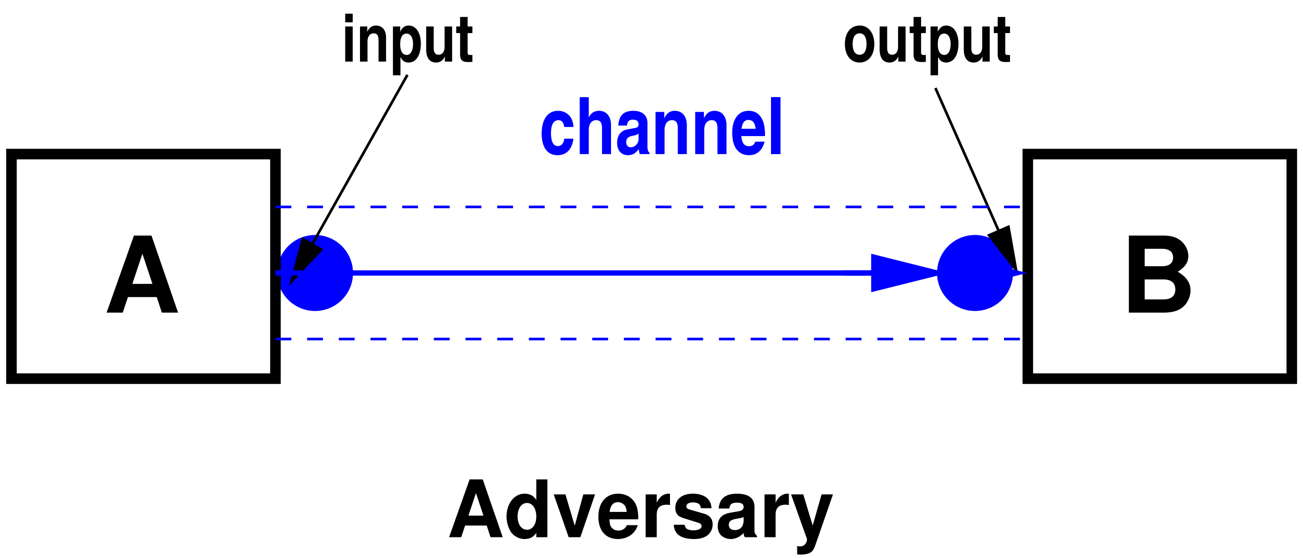
Secrecy and authenticity



Two basic **independent / dual** security properties:

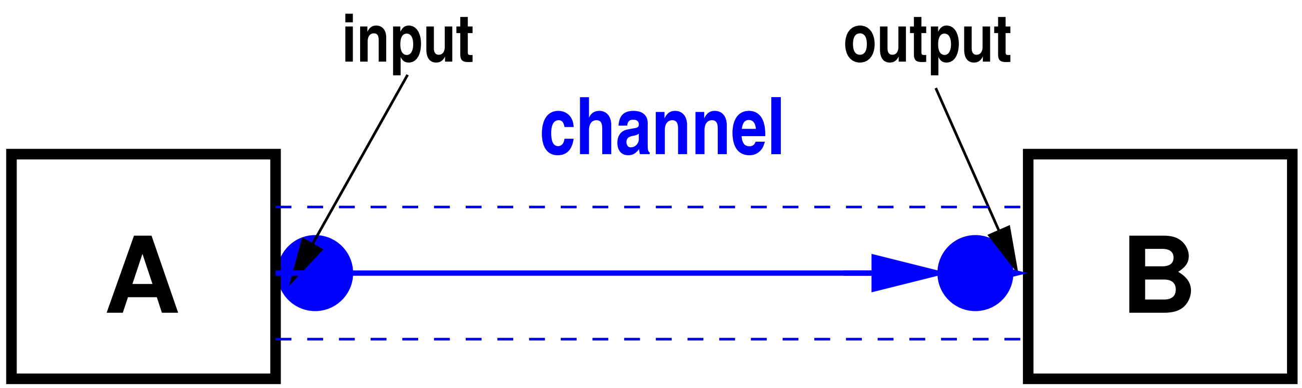
- **secrecy** (output is exclusive)
- **authenticity** (input is exclusive)

Secrecy and authenticity



$A \longrightarrow B$	(insecure) channel from A to B
$A \longrightarrow\!\bullet\ B$	secret channel from A to B
$A \bullet\!\!\longrightarrow B$	authentic channel from A to B
$A \bullet\!\!\longrightarrow\!\bullet\ B$	secure channel from A to B (secret and authentic)

Secrecy and authenticity



Adversary

$A \longrightarrow B$	(insecure) channel from A to B
$A \longrightarrow\!\!\bullet\ B$	secret channel from A to B
$A \bullet\!\!\longrightarrow B$	authentic channel from A to B
$A \bullet\!\!\longrightarrow\!\!\bullet\ B$	secure channel from A to B (secret and authentic)
$A \quad \bullet\!\!=\!\!=\!\!=\!\!\bullet \quad B$	secret key shared by A and B
$A \quad =\!\!=\!\!=\!\!\bullet \quad B$	one-sided key: A knows that at most B knows the key, but B does not know who holds the key.

The •-calculus (for channels and keys)

Calculus

- for the design and analysis of cryptographic protocols
- cryptographic scheme = security transformation
- precise semantics (later)
- security proof by composition

The •-calculus (for channels and keys)

Calculus

- for the design and analysis of cryptographic protocols
- cryptographic scheme = security transformation
- precise semantics (later)
- security proof by composition

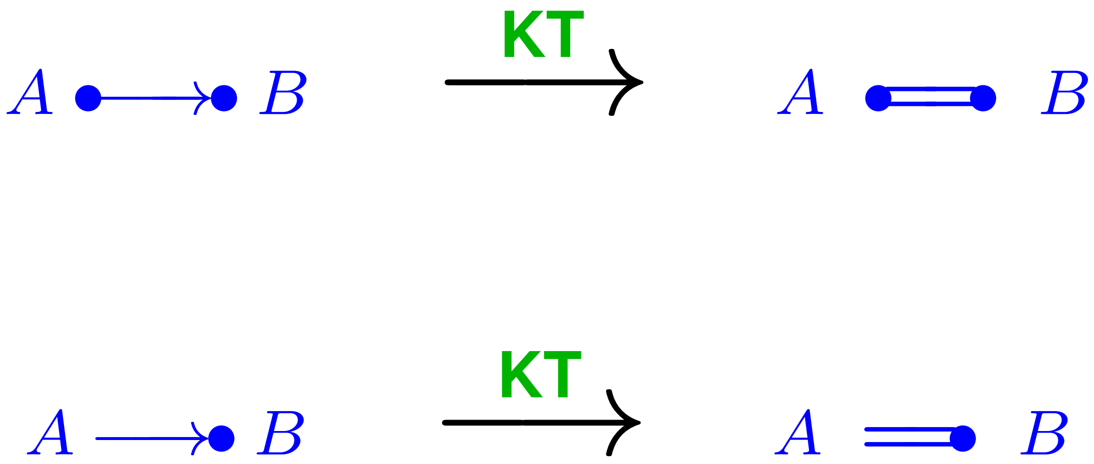
Illustrates:

- the relevant properties of various cryptographic systems
- limitations of cryptography
- role of protocols such as public-key certification
- role of trust
- necessary and sufficient conditions for key management in distributed systems

Key transport in •-calculus

$$A \bullet\!\!\longrightarrow\!\!\bullet\, B \qquad \xrightarrow{\textbf{KT}} \qquad A \bullet\!\!=\!\!=\!\!\bullet\, B$$

Key transport in •-calculus



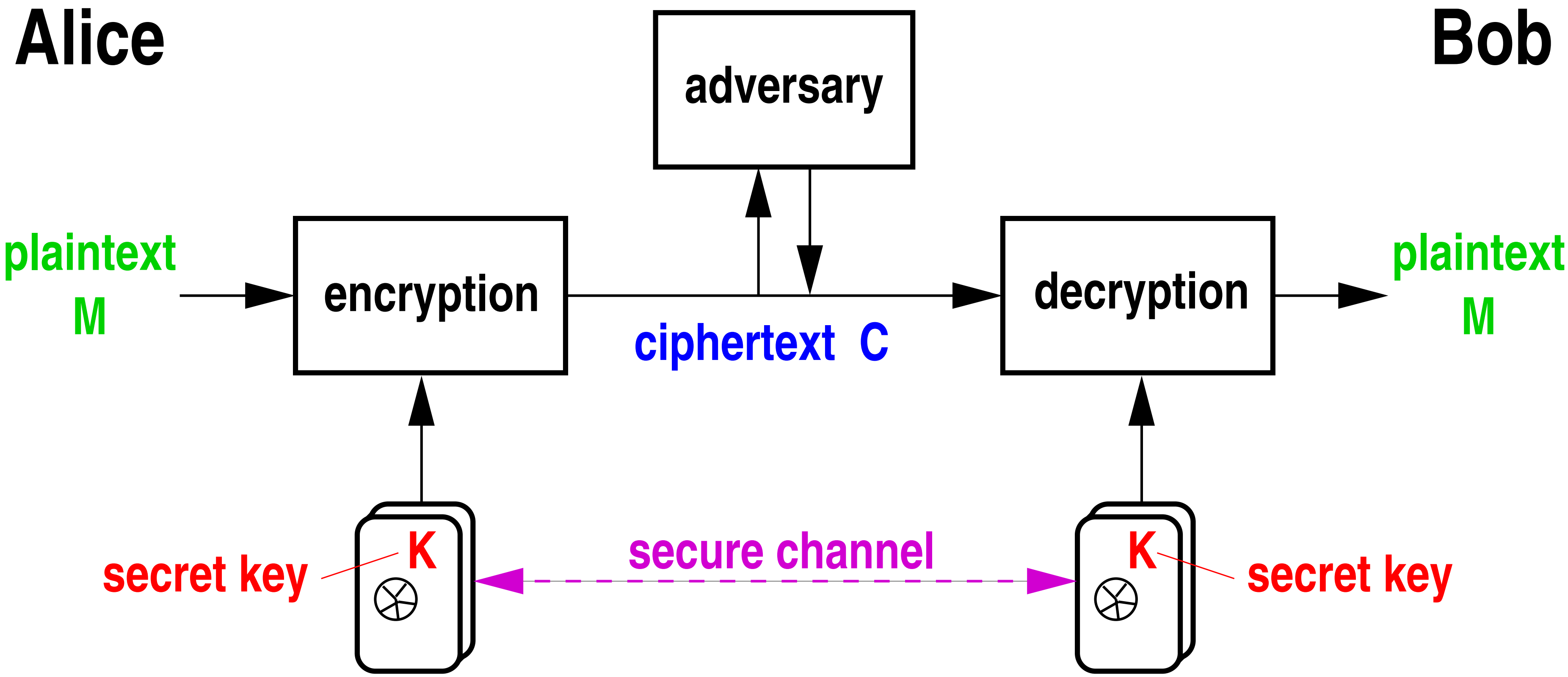
Key transport in •-calculus

$$A \bullet\!\!\longrightarrow\!\!\bullet\, B \quad \xrightarrow{\textbf{KT}} \quad A \bullet\!\!=\!\!=\!\!\bullet\, B$$

$$A \longrightarrow\!\!\bullet\, B \quad \xrightarrow{\textbf{KT}} \quad A =\!\!=\!\!\bullet\, B$$

Attention: $$A \bullet\!\!\longrightarrow B \quad \xrightarrow{\cancel{\textbf{KT}}} \quad A \bullet\!\!=\!\!= B$$

Symmetric cryptosystem



Symmetric cryptosystem in $\bullet$-calculus

$$\left.\begin{array}{l} A \Longrightarrow\!\!\bullet\ B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\text{SYM}} A \longrightarrow\!\!\bullet\ B$$

Symmetric cryptosystem in $\bullet$-calculus

$$\left.\begin{array}{l} A \;=\!\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\textbf{SYM}} A \longrightarrow\!\!\bullet\; B$$

$$\left.\begin{array}{l} A \;=\!\!=\!\!\bullet\; B \\ A \;\bullet\!\!\longrightarrow B \end{array}\right\} \xrightarrow{\textbf{SYM}} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Message authentication in •-calculus

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\!\!=\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\textbf{MAC}} A \bullet\!\!\longrightarrow B$$

Message authentication in $\bullet$-calculus

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\textbf{MAC}} A \;\bullet\!\!\longrightarrow B$$

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\; B \\ A \longrightarrow\!\!\bullet\; B \end{array}\right\} \xrightarrow{\textbf{MAC}} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Message authentication in •-calculus

$$\left.\begin{array}{l} A \;\bullet\!\!= \;\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\textbf{MAC}} A \;\bullet\!\!\longrightarrow B$$

$$\left.\begin{array}{l} A \;\bullet\!\!= \;\; B \\ A \longrightarrow\!\!\bullet\; B \end{array}\right\} \xrightarrow{\textbf{MAC}} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

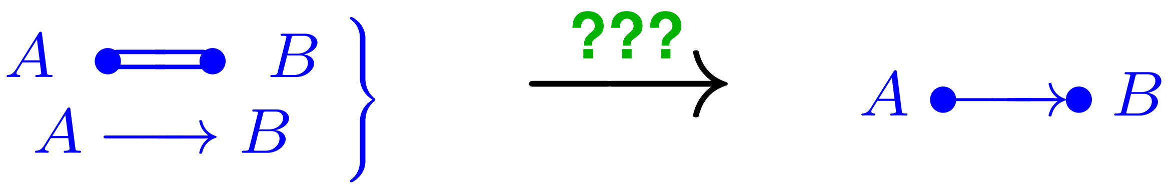
Note: Conservation law of •-calculus.

Combining Encryption and MAC

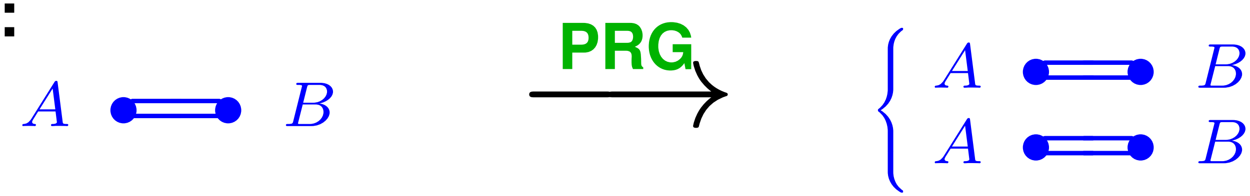
Goal: $\left.\begin{array}{c} A \;\bullet\!\!\!=\!\!=\!\!=\!\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{???} A \;\bullet\!\!\!\longrightarrow\!\!\!\bullet\; B$

Combining Encryption and MAC

Goal:

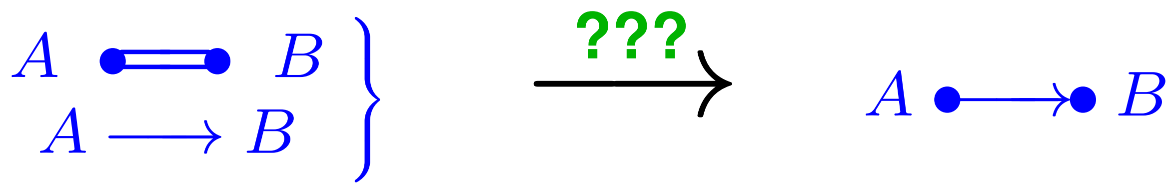


Key expansion:

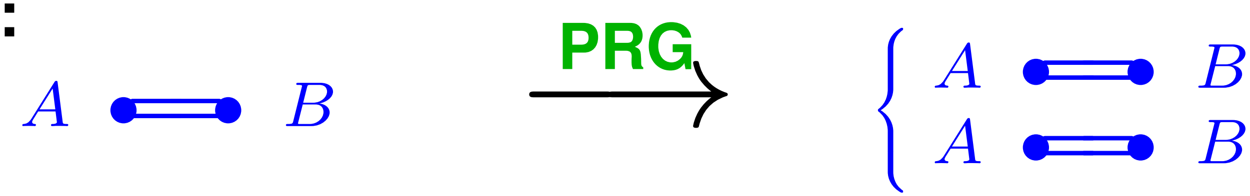


Combining Encryption and MAC

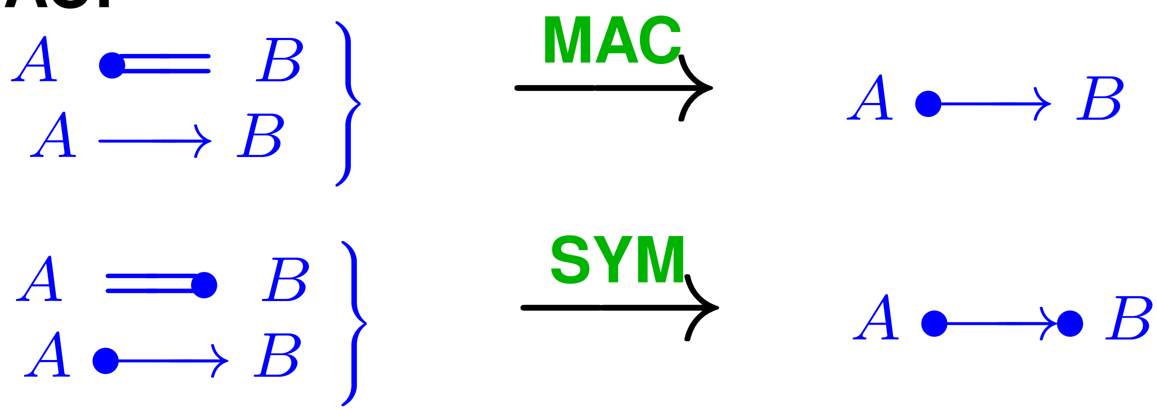
Goal:



Key expansion:



Encrypt-then-MAC:



Combining Encryption and MAC

Goal:

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{???} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Key expansion:

$$A \;\bullet\!\!=\!\!=\!\!\bullet\; B \xrightarrow{PRG} \left\{\begin{array}{l} A \;\bullet\!\!=\!\!=\!\!\bullet\; B \\ A \;\bullet\!\!=\!\!=\!\!\bullet\; B \end{array}\right.$$

Encrypt-then-MAC:

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{MAC} A \;\bullet\!\!\longrightarrow B$$

$$\left.\begin{array}{l} A \;=\!\!=\!\!\bullet\; B \\ A \;\bullet\!\!\longrightarrow B \end{array}\right\} \xrightarrow{SYM} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

MAC-then-encrypt:

$$\left.\begin{array}{l} A \;=\!\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{SYM} A \longrightarrow\!\!\bullet\; B$$

$$\left.\begin{array}{l} A \;\bullet\!\!=\!\!=\; B \\ A \longrightarrow\!\!\bullet\; B \end{array}\right\} \xrightarrow{MAC} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Combining Encryption and MAC

Goal:

$$\left.\begin{array}{l} A \;\bullet\!\!=\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\;???\;} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Key expansion:

$$A \;\bullet\!\!=\!=\!\!\bullet\; B \xrightarrow{\;\text{PRG}\;} \left\{\begin{array}{l} A \;\bullet\!\!=\!=\!\!\bullet\; B \\ A \;\bullet\!\!=\!=\!\!\bullet\; B \end{array}\right.$$

Encrypt-then-MAC:

$$\left.\begin{array}{l} A \;\bullet\!\!=\!=\; B \\ \ldots \end{array}\right\} \xrightarrow{\;\text{MAC}\;} A \;\bullet\!\!\longrightarrow B$$

Applies to computational and inform.-th. security.

$$\left.\begin{array}{l} \ldots \\ A \;\bullet\!\!\longrightarrow B \end{array}\right\} \longrightarrow A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

MAC-then-encrypt:

$$\left.\begin{array}{l} A \;=\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\;\text{SYM}\;} A \longrightarrow\!\!\bullet\; B$$

$$\left.\begin{array}{l} A \;\bullet\!\!=\!=\; B \\ A \longrightarrow\!\!\bullet\; B \end{array}\right\} \xrightarrow{\;\text{MAC}\;} A \;\bullet\!\!\longrightarrow\!\!\bullet\; B$$

Combining Encryption and MAC

Goal: $\left.\begin{array}{c} A \;\bullet\!\!=\!\!=\!\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\text{???}} A \bullet\!\!\longrightarrow\!\!\bullet B$

Key expansion: $A \;\bullet\!\!=\!\!=\!\!=\!\!\bullet\; B \xrightarrow{\text{PRG}} \left\{\begin{array}{c} A \;\bullet\!\!=\!\!=\!\!=\!\!\bullet\; B \\ A \;\bullet\!\!=\!\!=\!\!=\!\!\bullet\; B \end{array}\right.$

Encrypt-then-MAC:

$\left.\begin{array}{c} A \;\bullet\!\!=\!\!=\!\!=\; B \\ \ldots \end{array}\right\} \xrightarrow{\text{MAC}} A \bullet\!\!\longrightarrow B$

Applies to computational and inform.-th. security.

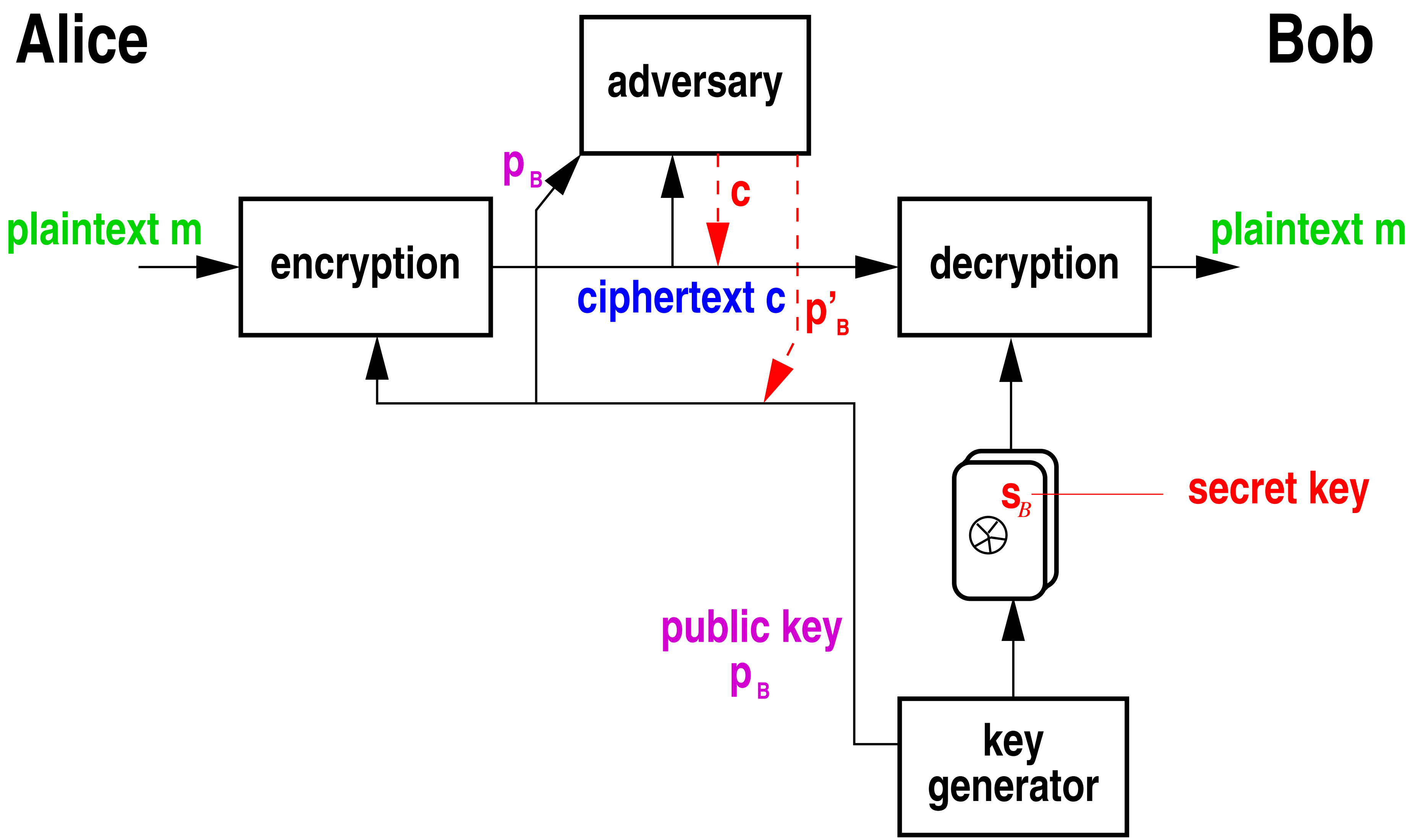
$\left.\begin{array}{c} \ldots \\ A \bullet\!\!\longrightarrow B \end{array}\right\} \longrightarrow A \bullet\!\!\longrightarrow\!\!\bullet B$

MAC-then-encrypt:

$\left.\begin{array}{c} A \;=\!\!=\!\!=\!\!\bullet\; B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\text{SYM}} A \longrightarrow\!\!\bullet B$

$\left.\begin{array}{c} A \;\bullet\!\!=\!\!=\!\!=\; B \\ A \longrightarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\text{MAC}} A \bullet\!\!\longrightarrow\!\!\bullet B$

Public-key cryptosystem



Public-key cryptosystem in $\bullet$-calculus

$$\left.\begin{array}{c} A \bullet\!\!\longrightarrow B \\ A \longleftarrow B \end{array}\right\} \xrightarrow{\textbf{PKC}} A \bullet\!\!\longleftarrow B$$

Public-key cryptosystem in $\bullet$-calculus

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow B \end{array}\right\} \xrightarrow{\textbf{PKC}} A \bullet\!\!\longleftarrow B$$

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet\ B \end{array}\right\} \xrightarrow{\textbf{PKC}} A \bullet\!\!\longleftarrow\!\!\bullet\ B$$

Key agreement in •-calculus

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\textbf{KA}} A \bullet\!\!=\!\!\bullet B$$

Key agreement in •-calculus

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\textbf{KA}} A \bullet\!\!=\!\!\bullet B$$

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \\ A \relbar Q \!\!\rightarrow B \end{array}\right\} \xrightarrow{\textbf{QKD}} A \bullet\!\!=\!\!\bullet B$$

Key agreement in $\bullet$-calculus

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\textbf{KA}} A \bullet\!\!=\!\!=\!\!\bullet B$$

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \\ A \,-\!Q\!\!\longrightarrow B \end{array}\right\} \xrightarrow{\textbf{QKD}} A \bullet\!\!=\!\!=\!\!\bullet B$$

Note: Conservation law of $\bullet$-calculus.

Key agreement in •-calculus

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\textbf{KA}} A \;\bullet\!\!=\!\!=\!\!\bullet\; B$$

$$\left.\begin{array}{l} A \bullet\!\!\longrightarrow B \\ A \longleftarrow\!\!\bullet B \\ A \;\text{—}Q\!\!\longrightarrow B \end{array}\right\} \xrightarrow{\textbf{QKD}} A \;\bullet\!\!=\!\!=\!\!\bullet\; B$$

$$\left.\begin{array}{l} A \longrightarrow B \\ A \longleftarrow\!\!\bullet B \end{array}\right\} \xrightarrow{\textbf{KA}} A \;=\!\!=\!\!\bullet\; B$$

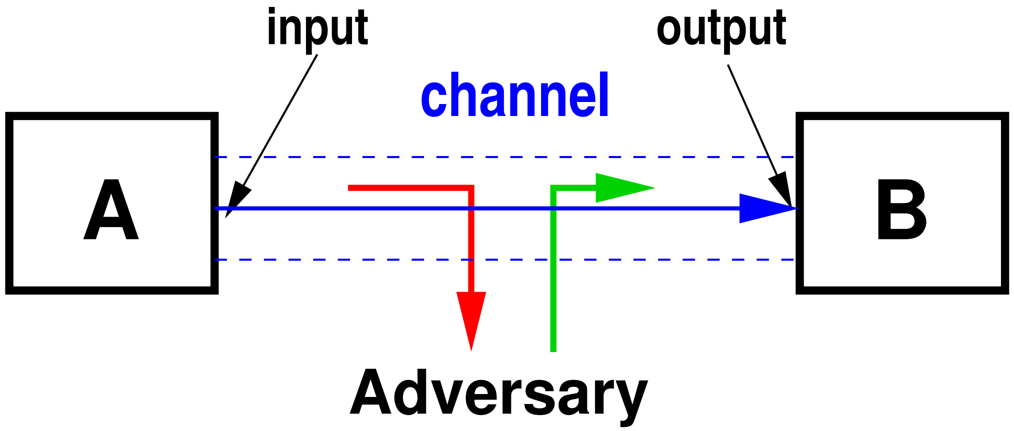
Note: Conservation law of •-calculus.

Digital signature scheme in •-calculus

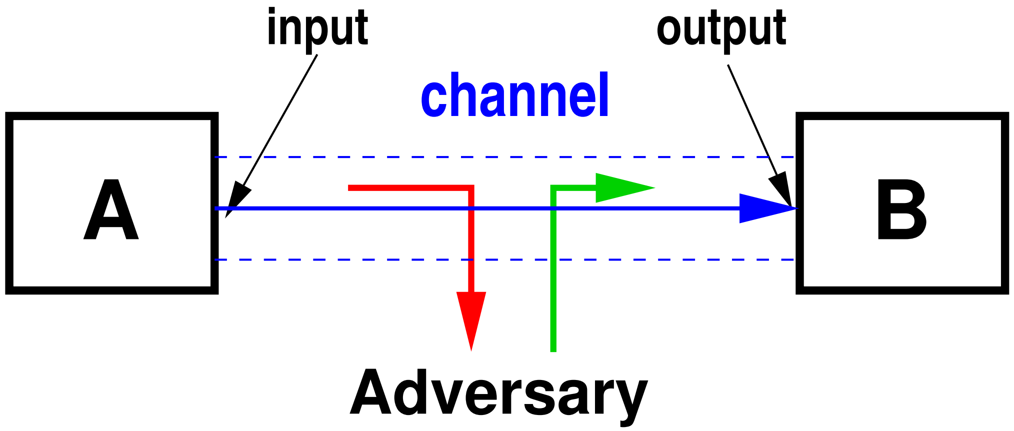
$$\left.\begin{array}{c} A \bullet\!\!\longrightarrow B \\ A \longrightarrow B \end{array}\right\} \xrightarrow{\textbf{DSS}} A \bullet\!\!\longrightarrow B$$

Information-theoretic authentication

Information-theoretic authentication



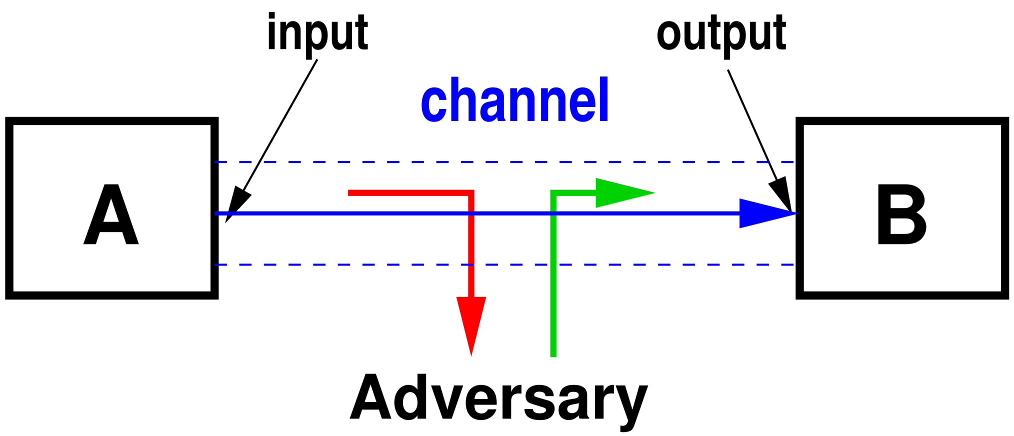
Information-theoretic authentication



Impersonation attack: The adversary sends a fraudulent message **before** observing the real message.

Success probability: P_I

Information-theoretic authentication

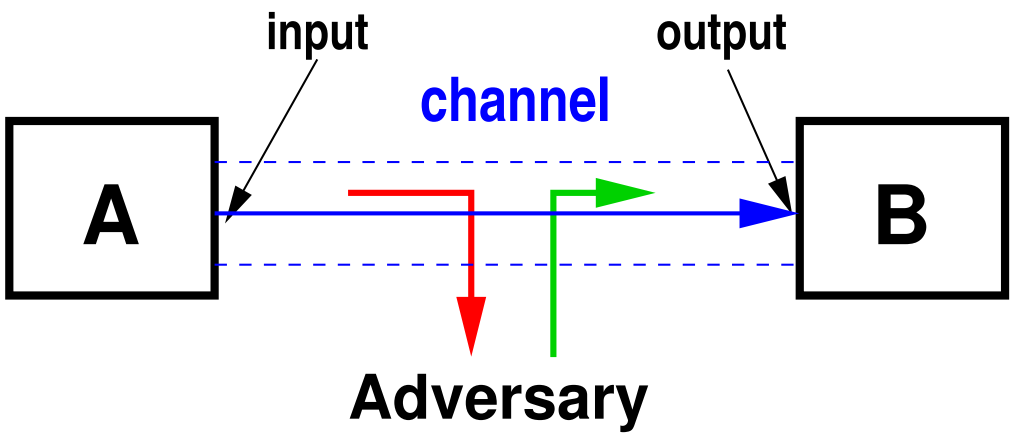


Impersonation attack: The adversary sends a fraudulent message **before** observing the real message.

Success probability: P_I

Note: $P_I \geq |\mathcal{M}|/|\mathcal{C}|$.

Information-theoretic authentication



Impersonation attack: The adversary sends a fraudulent message **before** observing the real message.

Success probability: P_I

Note: $P_I \geq |\mathcal{M}|/|\mathcal{C}|$.

Substitution attack: The adversary sends a fraudulent message **after** observing a correctly auth. message.

Success probability: P_S

Authenticating an ℓ-bit message with a k-bit key

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{ccc} A & \bullet\!\!\overset{k}{=\!=\!=}\!\!\bullet & B \\ A & \xrightarrow{\ \ell\ } & B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\!\xrightarrow{\ \ell\ } B$$

Example 1: $M \in \{0,1\}, \quad C = M||K$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \;\overset{k}{\bullet\!\!=\!\!=\!\!\bullet}\; B \\ A \;\xrightarrow{\ell}\; B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\!\xrightarrow{\ell} B$$

Example 1: $M \in \{0,1\}$, $\quad C = M||K \quad P_I = 2^{-k}, \quad P_S = 1$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{ccc} A & \bullet\!\overset{k}{=\!=\!=}\!\bullet & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\xrightarrow{\ell} B$$

Example 1: $M \in \{0,1\}$, $\quad C = M||K \quad P_I = 2^{-k}, \quad P_S = 1$

Example 2: $M \in \{0,1\}$

$$K = K_1||K_0 \text{ with } K_0, K_1 \in \{0,1\}^{k/2}$$

$$C = \begin{cases} 0||K_0 & \text{if } M = 0 \\ 1||K_1 & \text{if } M = 1 \end{cases}$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!=\!=\!=\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \xrightarrow{\text{ITA}} \quad A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Example 1: $M \in \{0,1\}, \quad C = M||K \quad P_I = 2^{-k}, \quad P_S = 1$

Example 2: $M \in \{0,1\}$

$$K = K_1||K_0 \text{ with } K_0, K_1 \in \{0,1\}^{k/2}$$

$$C = \begin{cases} 0||K_0 & \text{if } M = 0 \\ 1||K_1 & \text{if } M = 1 \end{cases}$$

$$P_I = 2^{-k/2}, \quad P_S = 2^{-k/2}$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!=\!=\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \quad \xrightarrow{\text{ITA}} \quad A \bullet\!\xrightarrow{\ell} B$$

Example 1: $M \in \{0,1\}, \quad C = M||K \quad P_I = 2^{-k}, \quad P_S = 1$

Example 2: $M \in \{0,1,2\}$

$$K = K_1||K_0 \text{ with } K_0, K_1 \in \{0,1\}^{k/2}$$

$$C = \begin{cases} 0||K_0 & \text{if } M = 0 \\ 1||K_1 & \text{if } M = 1 \\ 2||K_0 \oplus K_1 & \text{if } M = 2 \end{cases}$$

$$P_I = 2^{-k/2}, \quad P_S = 2^{-k/2}$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{lcl} A & \overset{k}{\bullet\!=\!=\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \quad \xrightarrow{\textbf{ITA}} \quad A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Example 1: $M \in \{0, 1\}, \quad C = M||K \quad P_I = 2^{-k}, \quad P_S = 1$

Example 2: $M \in \{0, 1, 2\}$

$$K = K_1||K_0 \text{ with } K_0, K_1 \in \{0, 1\}^{k/2}$$

$$C = \begin{cases} 0||K_0 & \text{if } M = 0 \\ 1||K_1 & \text{if } M = 1 \\ 2||K_0 \oplus K_1 & \text{if } M = 2 \end{cases}$$

$$P_I = 2^{-k/2}, \quad P_S = 2^{-k/2}$$

Example 3: $M \in GF(2^{k/2}), \quad C = M \cdot K_1 + K_0$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} B \\ A \xrightarrow{\ell} B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\xrightarrow{\ell} B$$

Exampl $P_S = 1$

Q: Is a lower cheating probability possible?

Exampl

$$K = K_1 || K_0 \text{ with } K_0, K_1 \in \{0,1\}^{k/2}$$

$$C = \begin{cases} 0||K_0 & \text{if } M = 0 \\ 1||K_1 & \text{if } M = 1 \\ 2||K_0 \oplus K_1 & \text{if } M = 2 \end{cases}$$

$$P_I = 2^{-k/2}, \quad P_S = 2^{-k/2}$$

Example 3: $M \in GF(2^{k/2}), \quad C = M \cdot K_1 + K_0$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!=\!=\!\bullet} B \\ A \xrightarrow{\ \ell\ } B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\xrightarrow{\ \ell\ } B$$

Exampl … $P_S = 1$

Q: Is a lower cheating probability possible?

Exampl …

Q: What about longer messages?

$$C = \begin{cases} 1 \| K_1 & \text{if } M = 1 \\ 2 \| K_0 \oplus K_1 & \text{if } M = 2 \end{cases}$$

$$P_I = 2^{-k/2}, \quad P_S = 2^{-k/2}$$

Example 3: $M \in GF(2^{k/2}), \quad C = M \cdot K_1 + K_0$

Lower bounds on the cheating probability

$$\left.\begin{array}{l} A \quad \overset{k}{\bullet\!=\!=\!=\!\bullet} \quad B \\ A \quad \xrightarrow{\ \ell\ } \quad B \end{array}\right\} \quad \xrightarrow{\text{ITA}} \quad A \bullet\!\xrightarrow{\ \ell\ } B$$

Lower bounds on the cheating probability

Theorem: For every authentication system we have

$$P_I \geq 2^{-I(C;K)}$$

Lower bounds on the cheating probability

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!=\!=\!=\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \quad \xrightarrow{\textbf{ITA}} \quad A \bullet\!\!\xrightarrow{\ell} B$$

Theorem: For every authentication system we have

$$P_I \geq 2^{-I(C;K)}$$
$$P_S \geq 2^{-H(K|C)}$$

Lower bounds on the cheating probability

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \xrightarrow{\textbf{ITA}} A \bullet\!\xrightarrow{\ell} B$$

Theorem: For every authentication system we have

$$P_I \geq 2^{-I(C;K)}$$
$$P_S \geq 2^{-H(K|C)}$$

$$\boxed{I(C;K) = H(K) - H(K|C)}$$

Lower bounds on the cheating probability

$$\left.\begin{array}{l} A \ \overset{k}{\bullet\!=\!=\!=\!\bullet}\ B \\ A \ \xrightarrow{\ \ell\ }\ B \end{array}\right\} \quad \xrightarrow{\ \text{ITA}\ } \quad A \ \bullet\!\!\xrightarrow{\ \ell\ } B$$

Theorem: For every authentication system we have

$$\begin{aligned} P_I &\geq 2^{-I(C;K)} \\ P_S &\geq 2^{-H(K|C)} \\ P_I \cdot P_S &\geq 2^{-H(K)} \end{aligned}$$

$$\boxed{I(C;K) = H(K) - H(K|C)}$$

Lower bounds on the cheating probability

Theorem: For every authentication system we have

$$
\begin{aligned}
P_I &\geq 2^{-I(C;K)} \\
P_S &\geq 2^{-H(K|C)} \\
P_I \cdot P_S &\geq 2^{-H(K)} \\
\max(P_I, P_S) &\geq 2^{-H(K)/2} = 2^{-k/2}
\end{aligned}
$$

$$\boxed{I(C;K) = H(K) - H(K|C)}$$

Lower bounds on the cheating probability

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \quad \xrightarrow{\text{ITA}} \quad A \bullet\!\!\xrightarrow{\ell} B$$

Theorem: For every authentication system we have

$$\begin{aligned} P_I &\geq 2^{-I(C;K)} \\ P_S &\geq 2^{-H(K|C)} \\ P_I \cdot P_S &\geq 2^{-H(K)} \\ \max(P_I, P_S) &\geq 2^{-H(K)/2} = 2^{-k/2} \end{aligned}$$

$$\boxed{s = -\log_2(\max(P_I, P_S)) \leq k/2}$$

$$\boxed{I(C;K) = H(K) - H(K|C)}$$

Lower bounds on the cheating probability

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!=\!=\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \xrightarrow{\textbf{ITA}} A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Theorem: For every authentication system we have

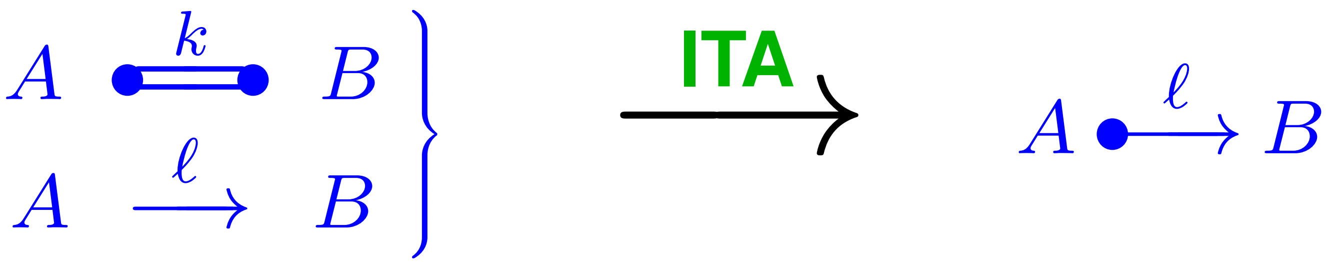
$$\begin{aligned} P_I &\geq 2^{-I(C;K)} \\ P_S &\geq 2^{-H(K|C)} \\ P_I \cdot P_S &\geq 2^{-H(K)} \\ \max(P_I, P_S) &\geq 2^{-H(K)/2} = 2^{-k/2} \end{aligned}$$

$$\boxed{s = -\log_2(\max(P_I, P_S)) \leq k/2}$$

$$\boxed{k \geq 2s}$$

$$\boxed{I(C;K) = H(K) - H(K|C)}$$

Authenticating an ℓ-bit message with a k-bit key



Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \quad \overset{k}{\bullet\!=\!=\!=\!\bullet} \quad B \\ A \quad \xrightarrow{\ \ell\ } \quad B \end{array}\right\} \quad \xrightarrow{\textbf{ITA}} \quad A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Block length n, field $F = GF(2^n)$,

$m = [m_{b-1}, \ldots, m_1, m_0]$, $\qquad \ell = bn$

$K = K_1 || K_0$, $\qquad k = 2n$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \quad \overset{k}{\bullet\!=\!=\!\bullet} \quad B \\ A \quad \xrightarrow{\ell} \quad B \end{array}\right\} \quad \xrightarrow{\text{ITA}} \quad A \bullet\!\xrightarrow{\ell} B$$

Block length n, field $F = GF(2^n)$,

$m = [m_{b-1}, \ldots, m_1, m_0]$, $\qquad \ell = bn$

$K = K_1 || K_0$, $\qquad k = 2n$

Message polynomials:

$$p_m(x) = m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) = m_{b-1}x^b + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} B \\ A \xrightarrow{\ell} B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\xrightarrow{\ell} B$$

Block length n, field $F = GF(2^n)$,

$m = [m_{b-1}, \ldots, m_1, m_0]$, $\ell = bn$

$K = K_1 || K_0$, $k = 2n$

Authentication scheme (ITA): $C = M \,||\, q_M(K_1) + K_0$

Message polynomials:

$$p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) \;=\; m_{b-1}x^b + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{ccc} A & \overset{k}{\bullet\!\!=\!=\!\!\bullet} & B \\ A & \xrightarrow{\ell} & B \end{array}\right\} \xrightarrow{\text{ITA}} A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Block length n, field $F = GF(2^n)$,

$m = [m_{b-1}, \ldots, m_1, m_0]$, $\quad \ell = bn$

$K = K_1 || K_0$, $\quad k = 2n$

Authentication scheme (ITA): $C = M \,||\, q_M(K_1) + K_0$

Theorem: $P_I = P_S = b \cdot 2^{-n}$; $\quad s = \frac{k}{2} - \log(2\ell/k)$

Message polynomials:

$$p_m(x) = m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) = m_{b-1}x^{b} + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} B \\ A \xrightarrow{\ell} B \end{array}\right\} \xrightarrow{\text{ITA}} A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Q: Trade-off between ℓ, k, s ?

Block length n, field $F =$

$m = [m_{b-1}, \ldots, m_1, m_0]$, $\qquad \ell = bn$

$K = K_1 || K_0$, $\qquad k = 2n$

Authentication scheme (ITA): $C = M \,||\, q_M(K_1) + K_0$

Theorem: $P_I = P_S = b \cdot 2^{-n}$; $\quad s = \frac{k}{2} - \log(2\ell/k)$

Message polynomials:

$$p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) \;=\; m_{b-1}x^b + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!\!=\!\!=\!\!=\!\!\bullet} B \\ A \xrightarrow{\ell} B \end{array}\right\} \xrightarrow{\text{ITA}} A \bullet\!\!\xrightarrow{\ell} B$$

Block length n, field $F = G$

$m = [m_{b-1}, \ldots, m_1, m_0]$,

$K = K_1 || K_0$,

Q: Trade-off between ℓ, k, s ?

This is essentially optimal!

Authentication scheme (ITA): $C = M \,||\, q_M(K_1) + K_0$

Theorem: $P_I = P_S = b \cdot 2^{-n}$; $\quad s = \frac{k}{2} - \log(2\ell/k)$

Message polynomials:

$$p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) \;=\; m_{b-1}x^b + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message with a k-bit key

$$\left.\begin{array}{l} A \overset{k}{\bullet\!\!=\!\!=\!\!\bullet} B \\ A \xrightarrow{\ell} B \end{array}\right\} \xrightarrow{\text{ITA}} A \overset{\ell}{\bullet\!\!\longrightarrow} B$$

Block length n, field $F = G$

$m = [m_{b-1}, \ldots, m_1, m_0]$,

$K = K_1 \| K_0$

Authenti $+ K_0$

Q: Trade-off between ℓ, k, s ?

This is essentially optimal!

Q: Can we nevertheless do better?

Theorem: $P_I = P_S = b \cdot 2^{-n}$; $s = \frac{k}{2} - \log(2\ell/k)$

Message polynomials:

$$p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$$

$$q_m(x) = x \cdot p_m(x) \;=\; m_{b-1}x^{b} + \cdots m_1 x^2 + m_0 x$$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\textbf{A-Ampl}} A \bullet\!\xrightarrow{\ell} B$$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{c} A \xrightarrow{\ell} B \\ A \bullet\!\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\textbf{A-Ampl}} A \bullet\!\!\xrightarrow{\ell} B$$

Message poly.: $p_m(x) = m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{c} A \xrightarrow{\ell} B \\ A \bullet\!\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\textbf{A-Ampl}} A \bullet\!\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\!\xrightarrow{t} B$, for a random R.

Message poly.: $p_m(x) = m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1)\cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Message poly.: $p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1) \cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Message poly.: $p_m(x) \ = \ m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1)\cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Theorem: If used recursively, then $t = 2s + O(1)$.

Message poly.: $p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{c} A \xrightarrow{\ell} B \\ A \bullet\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1) \cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Theorem: If used recursively, then $t = 2s + O(1)$.

Theorem: Combine with key-based scheme: $k \approx 2s$

Message poly.: $p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\!\xrightarrow{\ell} B$$

Protocol (A-Ampl): Send m over $A \xrightarrow{\ell} B$, then $R||p_m(R)$ over $A \bullet\!\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1) \cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Theorem: If used recursively, then $t = 2s + O$

Optimal!

Theorem: Combine with key-based scheme: $k \approx 2s$

Message poly.: $p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ell} B \\ A \bullet\!\xrightarrow{t} B \end{array}\right\} \xrightarrow{\text{A-Ampl}} A \bullet\!\xrightarrow{\ell} B$$

Q: What does all of this really mean?

Pr)

over $A \bullet\!\xrightarrow{t} B$, for a random R.

Theorem: $P_I = P_S = (b-1) \cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Theorem: If used recursively, then $t = 2s + O$

Optimal!

Theorem: Combine with key-based scheme: $k \approx 2s$

Message poly.: $p_m(x) \ = \ m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Authenticating an ℓ-bit message by auth. t bits

$$\left.\begin{array}{l} A \xrightarrow{\ \ell\ } B \\ A \bullet\!\!\xrightarrow{\ t\ } B \end{array}\right\} \quad \xrightarrow{\text{A-Ampl}} \quad A \bullet\!\!\xrightarrow{\ \ell\ } B$$

Q: What does all of this really mean? (e.g. for QKD?)

Pr

over $A \bullet\!\!\xrightarrow{\ t\ } B$, for a random R.

Theorem: $P_I = P_S = (b-1)\cdot 2^{-n}$; $\quad s = n - \log(b-1)$

Proof: For any m, m', $P(p_m(R) = p_{m'}(R)) \leq (b-1)/|F|$ because $p_m(R) - p_{m'}$ has at most $b-1$ roots.

Theorem: If used recursively, then $t = 2s + O$

Optimal!

Theorem: Combine with key-based scheme: $k \approx 2s$

Message poly.: $p_m(x) \;=\; m_{b-1}x^{b-1} + \cdots m_1 x + m_0$

Security definitions in classical cryptography

Security definitions in classical cryptography

Definition: A **public-key cryptosystem (PKC)** is a triple of polynomial-time algorithms (PPT) with security parameter k:

1. **KeyGen:** input: k; output: a secret key s, a public key p.
2. **Enc:** input: k, message m, p; output: ciphertext c.
3. **Dec:** input: k, c, s; output: message m.

Security definitions in classical cryptography

Definition: A **public-key cryptosystem (PKC)** is a triple of polynomial-time algorithms (PPT) with security parameter k:

1. **KeyGen:** input: k; output: a secret key s, a public key p.
2. **Enc:** input: k, message m, p; output: ciphertext c.
3. **Dec:** input: k, c, s; output: message m.

Correctness: $\textbf{Dec}(k, \textbf{Enc}(k, m, p), s) = m$.

Security definitions in classical cryptography

Definition: A **public-key cryptosystem (PKC)** is a triple of polynomial-time algorithms (PPT) with security parameter k:

1. **KeyGen:** input: k; output: a secret key s, a public key p.
2. **Enc:** input: k, message m, p; output: ciphertext c.
3. **Dec:** input: k, c, s; output: message m.

Correctness: $\textbf{Dec}(k, \textbf{Enc}(k, m, p), s) = m$.

Security: A PKC is **IND-CPA secure** if no probabilistic polynomial time-bounded adversary A can win the following game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Definition: A **public-key cryptosystem (PKC)** is a triple of polynomial-time algorithms (PPT) with security parameter k:

1. **KeyGen:** input: k; output: a secret key s, a public key p.
2. **Enc:** input: k, message m, p; output: ciphertext c.
3. **Dec:** input: k, c, s; output: message m.

Correctness: $\textbf{Dec}(k, \textbf{Enc}(k, m, p), s) = m$.

Security: A PKC is **IND-CPA secure** if no probabilistic polynomial time-bounded adversary A can win the following game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

Where can we use an IND-CPA secure PKC?

game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

Where can we use an IND-CPA secure PKC?

Which is the right definition for a given application?

game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

Where can we use an IND-CPA secure PKC?

Which is the right definition for a given application?

Q2: Are artefacts like Turing machines, asymptotics, poly-time, negligibility, etc. really needed?

game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

W

A1: Constructive cryptography

W on?

Q2: Are artefacts like Turing machines, asymptotics, poly-time, negligibility, etc. really needed?

game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

Security definitions in classical cryptography

Two questions that arise:

Q1: What does the definition really mean?

W

W on?

A1: Constructive cryptography

Q2: Are artefacts like Turing machines, asymptotics,

pol

A2: Abstraction

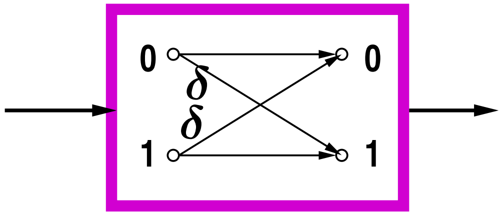
game with probability non-negligibly greater than 1/2:

1. p is generated with **KeyGen**, and given to A.
2. A generates two equal-length messages m_0 and m_1.
3. A random bit b is chosen, and A gets $c = \textbf{Enc}(k, m_b, p)$.
4. A guesses the bit b.

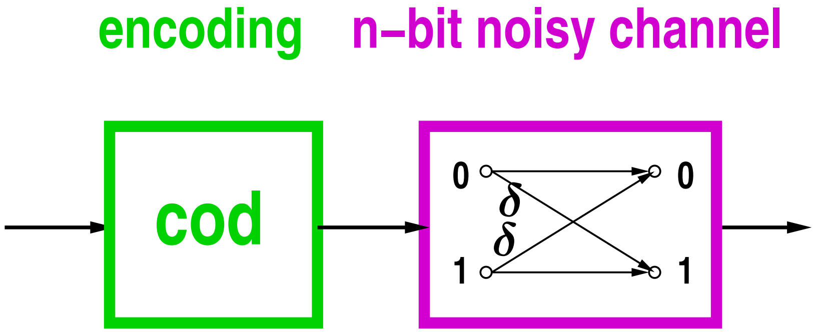
Shannon's channel coding theorem

Shannon's channel coding theorem

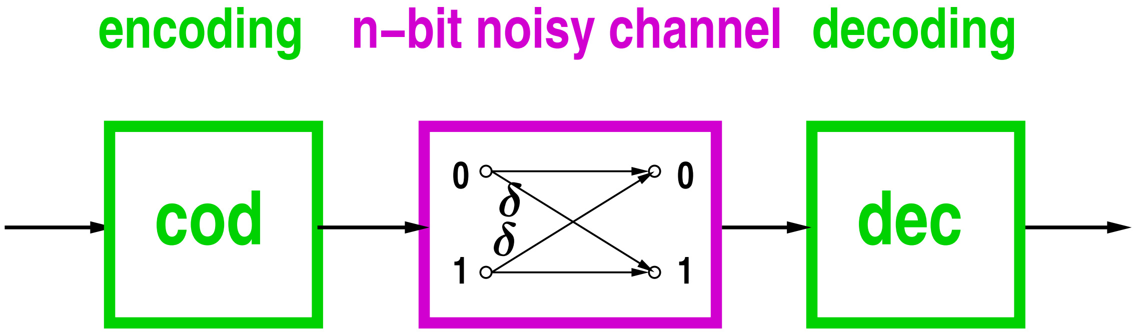
n−bit noisy channel



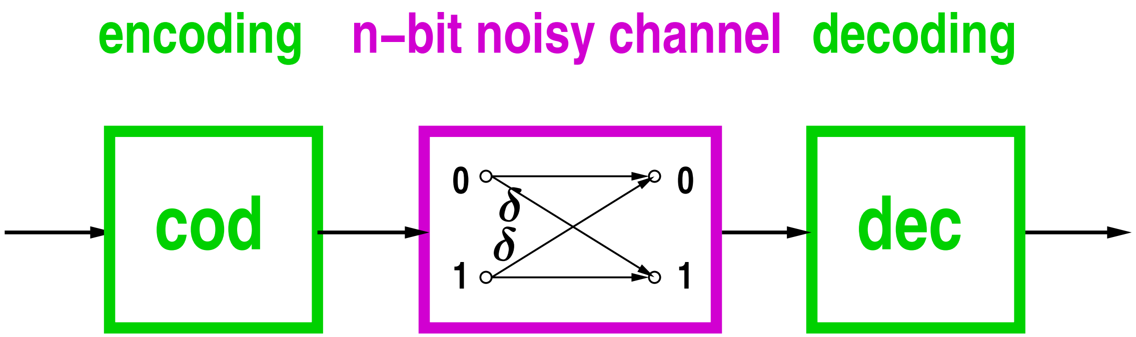
Shannon's channel coding theorem

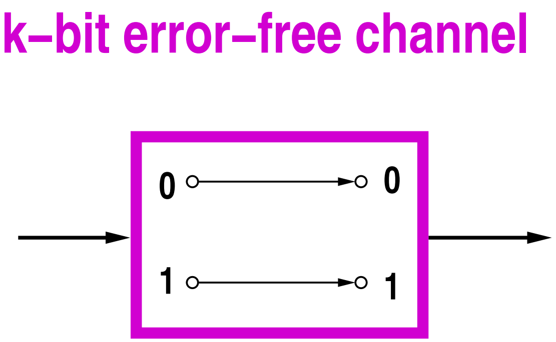


Shannon's channel coding theorem

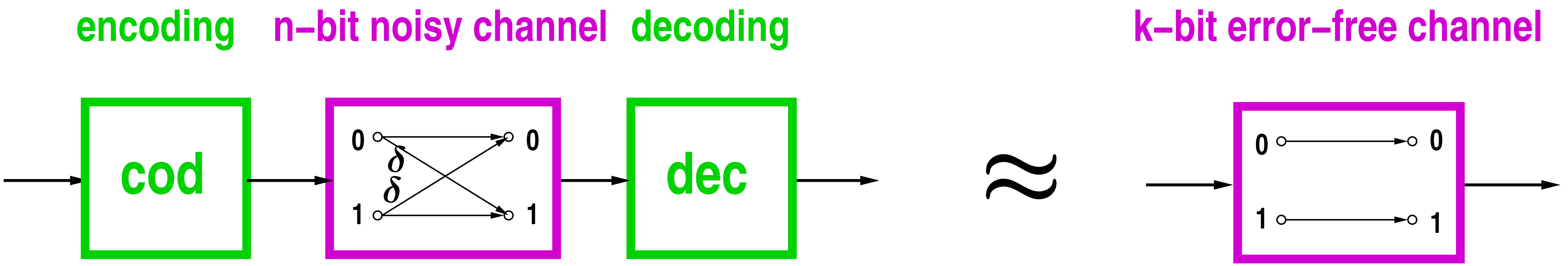


Shannon's channel coding theorem

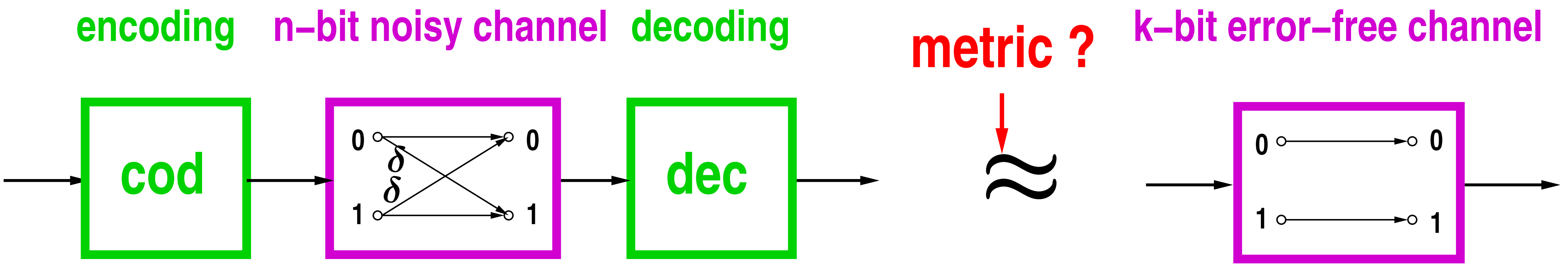




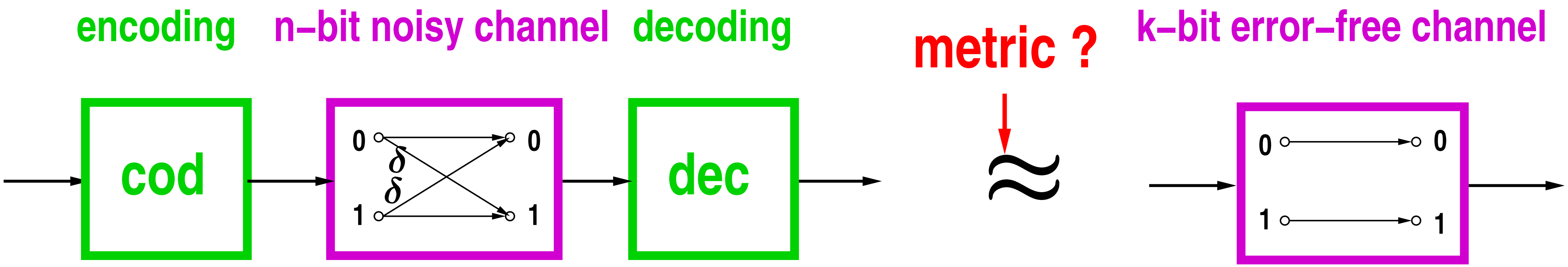
Shannon's channel coding theorem



Shannon's channel coding theorem

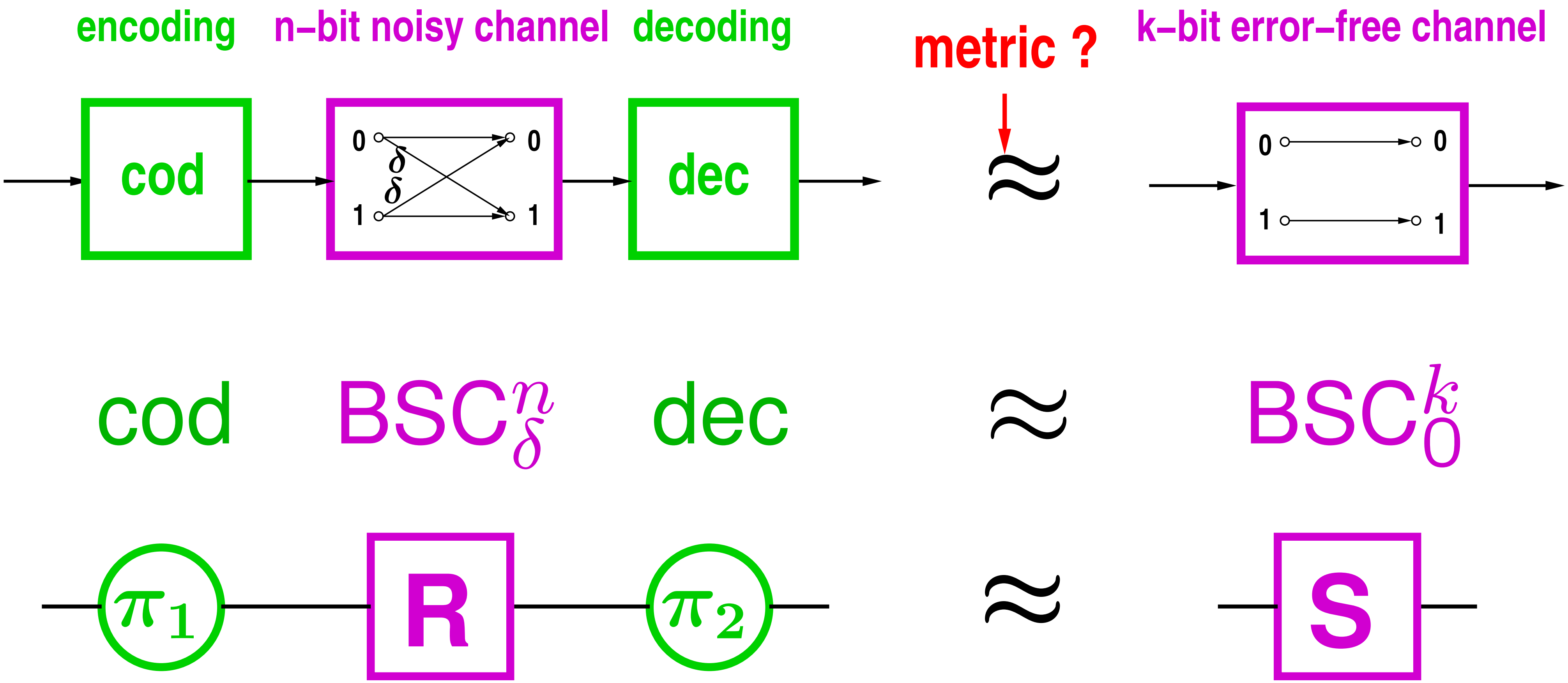


Shannon's channel coding theorem

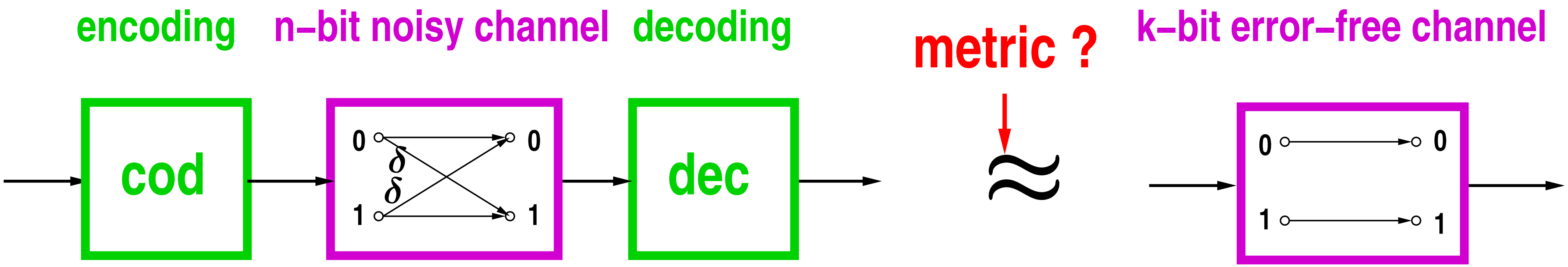


cod $\quad \mathrm{BSC}_\delta^n \quad$ dec $\quad \approx \quad \mathrm{BSC}_0^k$

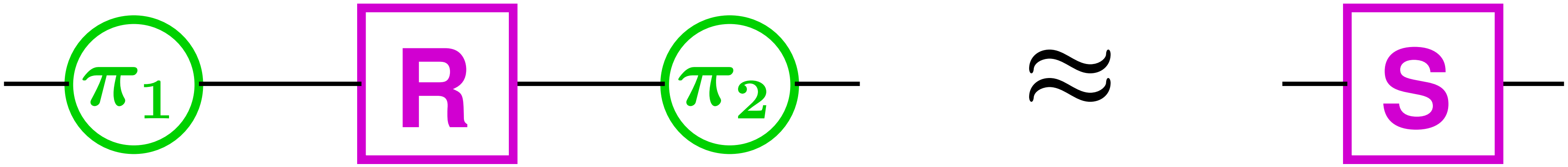
Shannon's channel coding theorem



Shannon's channel coding theorem

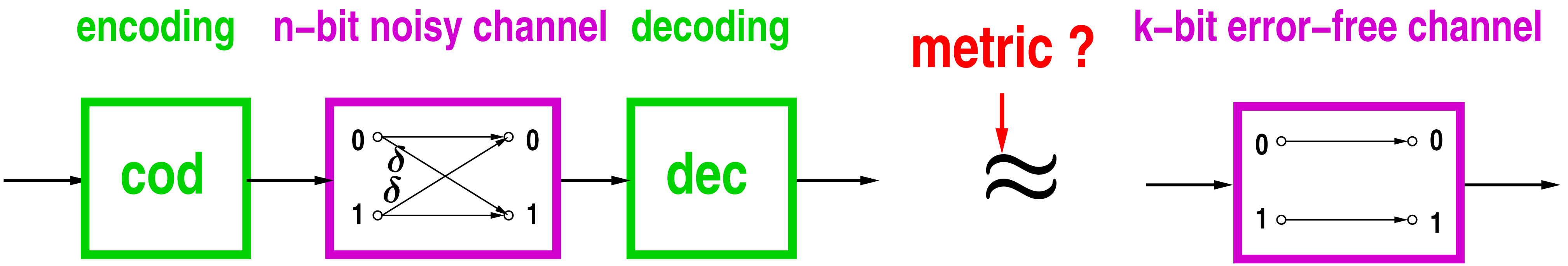


$$\text{cod} \quad \text{BSC}_\delta^n \quad \text{dec} \qquad \approx \qquad \text{BSC}_0^k$$



$$\pi_1 \ \mathbf{R} \ \pi_2 \quad \approx \quad \mathbf{S}$$

Shannon's channel coding theorem

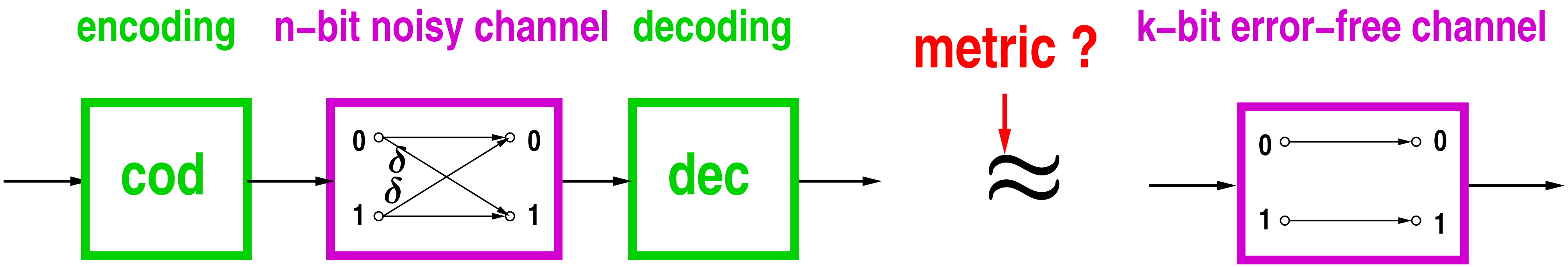


cod $\quad \mathrm{BSC}_\delta^n \quad$ dec $\quad \approx \quad \mathrm{BSC}_0^k$

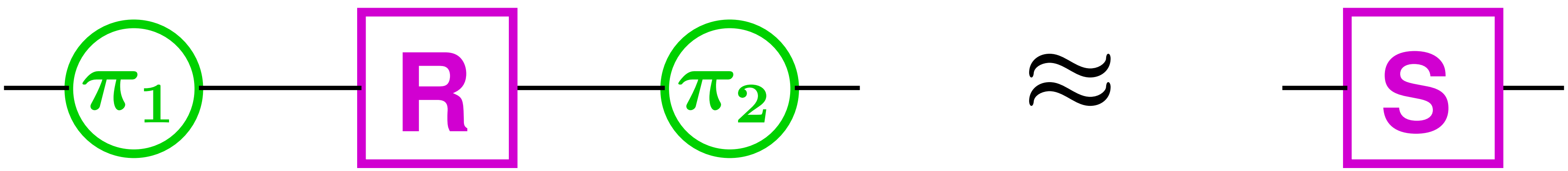
π_1 — **R** — π_2 $\quad \approx \quad$ — **S** —

π_1 **R** π_2 $\quad \approx \quad$ **S**

Shannon's channel coding theorem

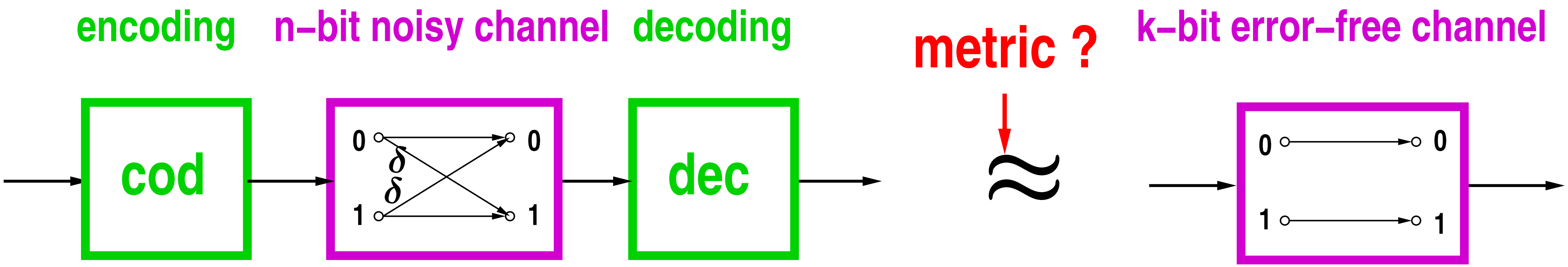


$$\mathsf{cod} \qquad \mathsf{BSC}_{\delta}^{n} \qquad \mathsf{dec} \qquad \approx \qquad \mathsf{BSC}_{0}^{k}$$

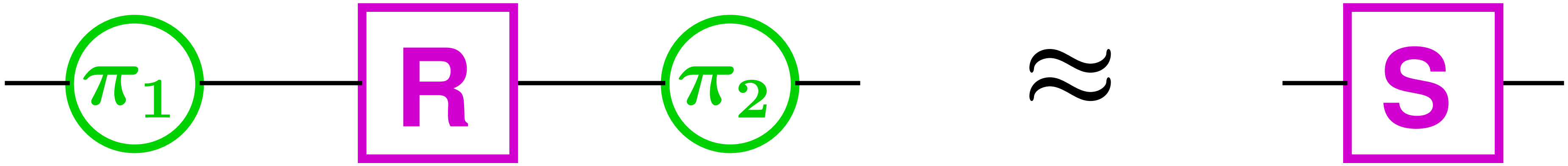


$$\pi_1 \ \mathbf{R} \ \pi_2 \quad \approx \quad \mathbf{S} \qquad \Longleftrightarrow: \qquad \mathbf{R} \xrightarrow{(\pi_1,\pi_2)} \mathbf{S}$$

Shannon's channel coding theorem



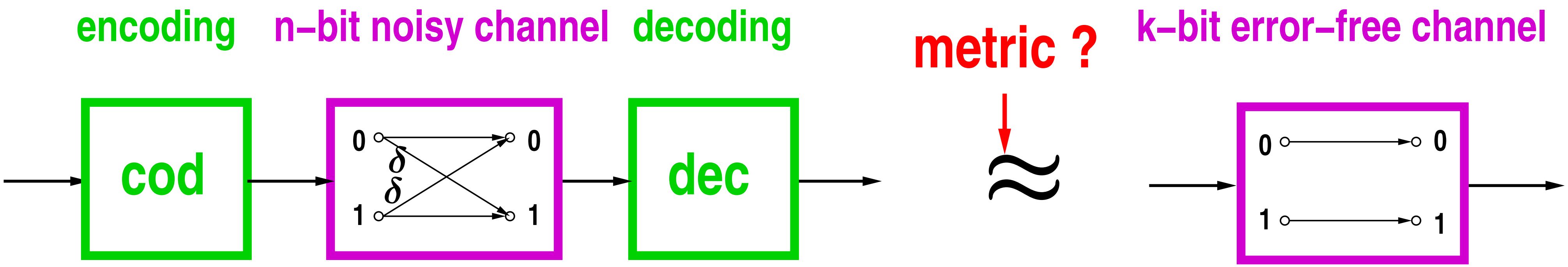
$$\text{cod} \qquad \text{BSC}^n_\delta \qquad \text{dec} \qquad \approx \qquad \text{BSC}^k_0$$



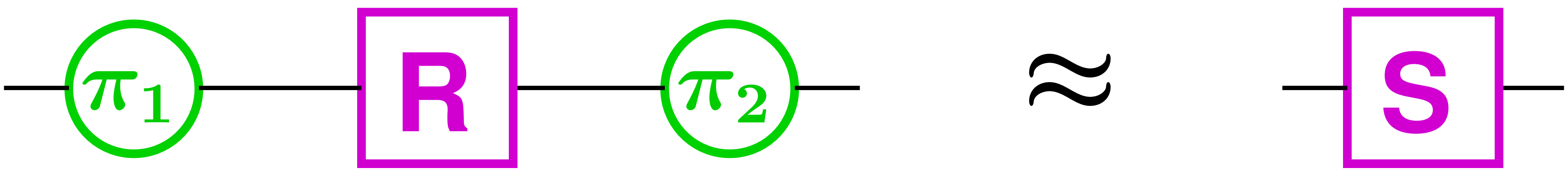
Construction:

$$\pi_1 \; \mathbf{R} \; \pi_2 \quad \approx \quad \mathbf{S} \qquad \iff: \quad \mathbf{R} \xrightarrow{(\pi_1, \pi_2)} \mathbf{S}$$

Shannon's channel coding theorem



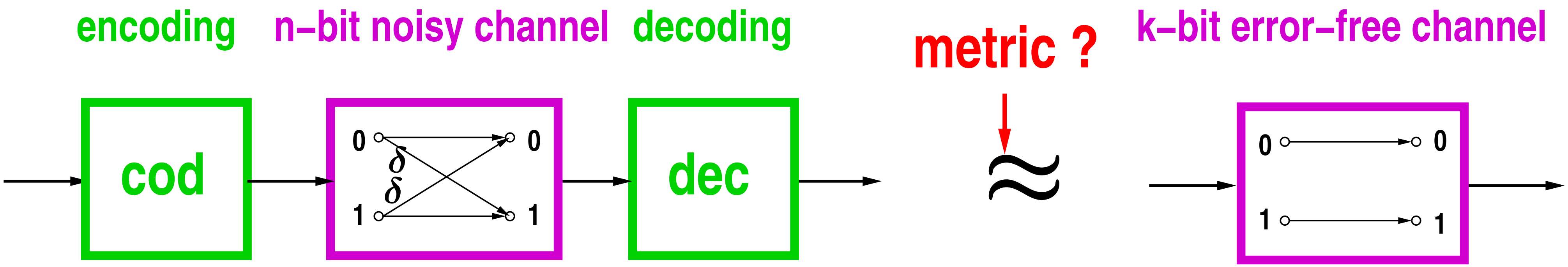
$$\text{cod} \quad \text{BSC}_\delta^n \quad \text{dec} \quad \approx \quad \text{BSC}_0^k$$



Construction:

$$\pi_1 \, \mathbf{R} \, \pi_2 \;\approx_\epsilon\; \mathbf{S} \quad \Longleftrightarrow: \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

Shannon's channel coding theorem



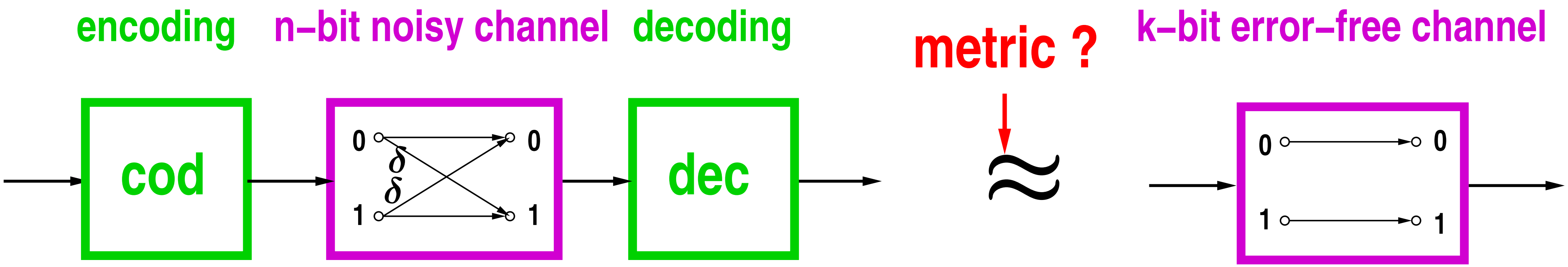
$$\text{cod} \quad BSC^n_\delta \quad \text{dec} \quad \approx \quad BSC^k_0$$

$$BSC^n_\delta \xrightarrow{(\text{cod},\text{dec}),\epsilon} BSC^k_0$$

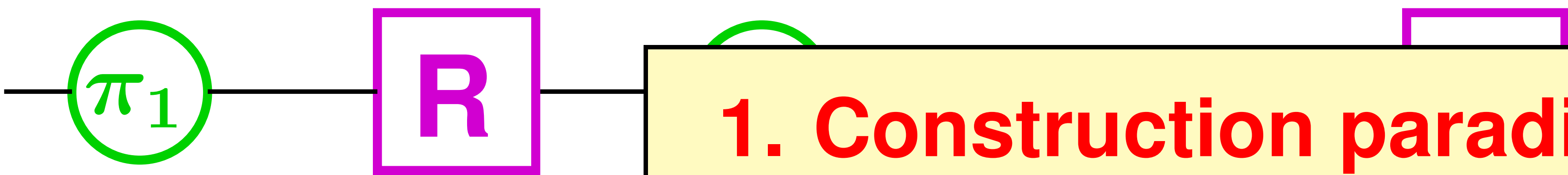
Construction:

$$\pi_1 \; \mathbf{R} \; \pi_2 \quad \approx_\epsilon \quad \mathbf{S} \quad \iff: \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\epsilon} \mathbf{S}$$

Shannon's channel coding theorem



cod $\quad \mathrm{BSC}_\delta^n \quad$ dec $\quad \approx \quad \mathrm{BSC}_0^k$

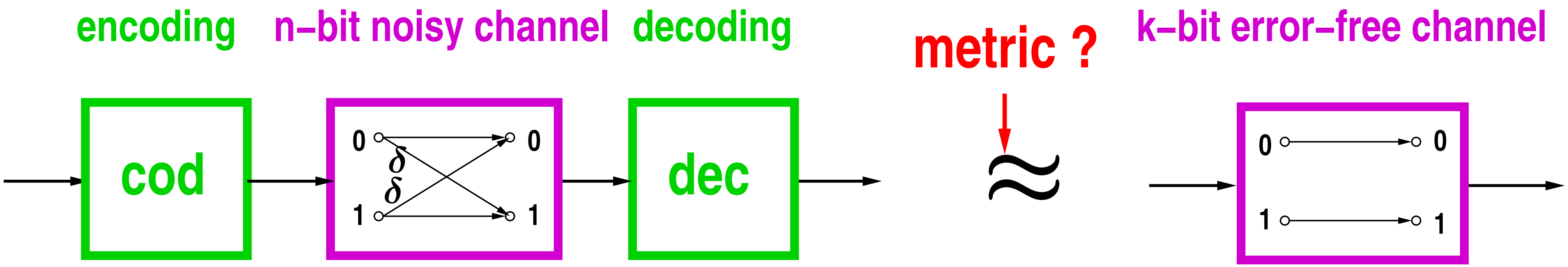


1. Construction paradigm

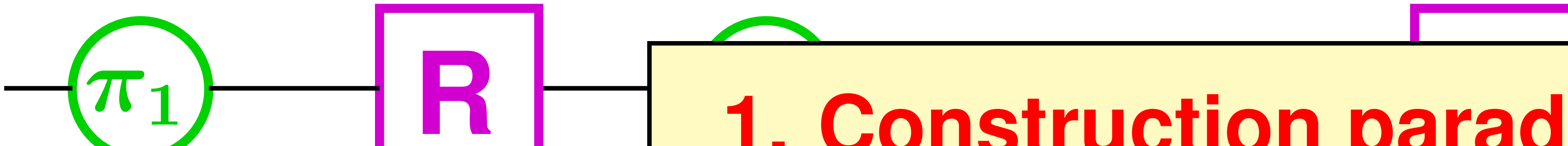
Construction:

$$\pi_1 \; \mathbf{R} \; \pi_2 \quad \approx_\epsilon \quad \mathbf{S} \quad :\Longleftrightarrow \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

Shannon's channel coding theorem



$$\text{cod} \quad \text{BSC}_\delta^n \quad \text{dec} \quad \approx \quad \text{BSC}_0^k$$



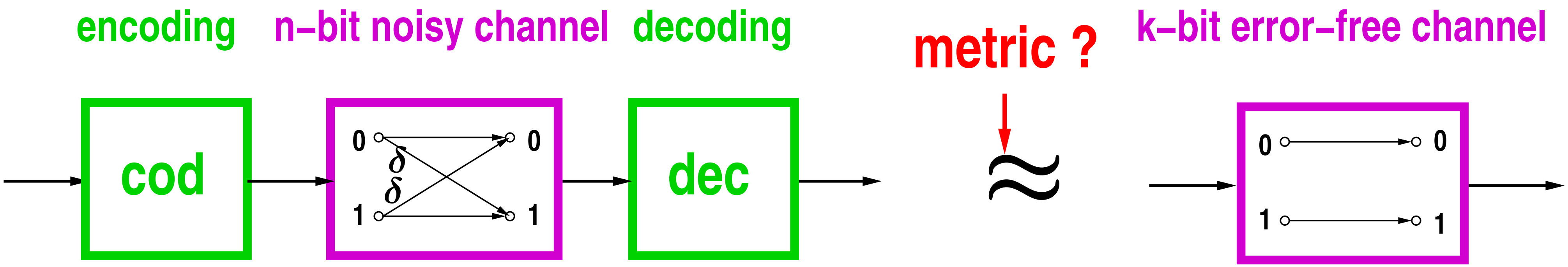
1. Construction paradigm

2. Abstract system algebra

on:

$$\pi_1 \ \mathbf{R} \ \pi_2 \quad \approx_\epsilon \quad \mathbf{S} \quad :\Longleftrightarrow \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

Shannon's channel coding theorem



cod BSC

3. Constructive cryptography

π_1 R

1. Construction paradigm

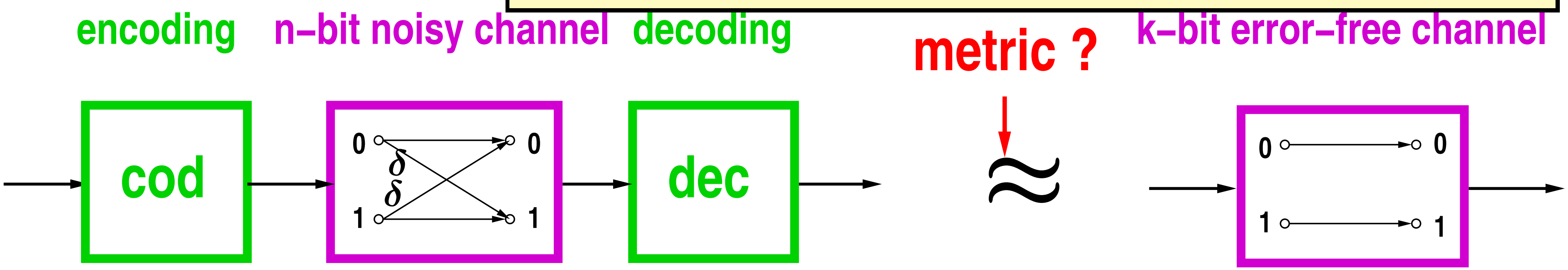
2. Abstract system algebra

on:

$$\pi_1 \, \mathbf{R} \, \pi_2 \;\approx_\epsilon\; \mathbf{S} \quad :\Longleftrightarrow \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

Shannon's channel coding theorem

4. Discrete systems, metric



cod BSC

3. Constructive cryptography

π_1 **R**

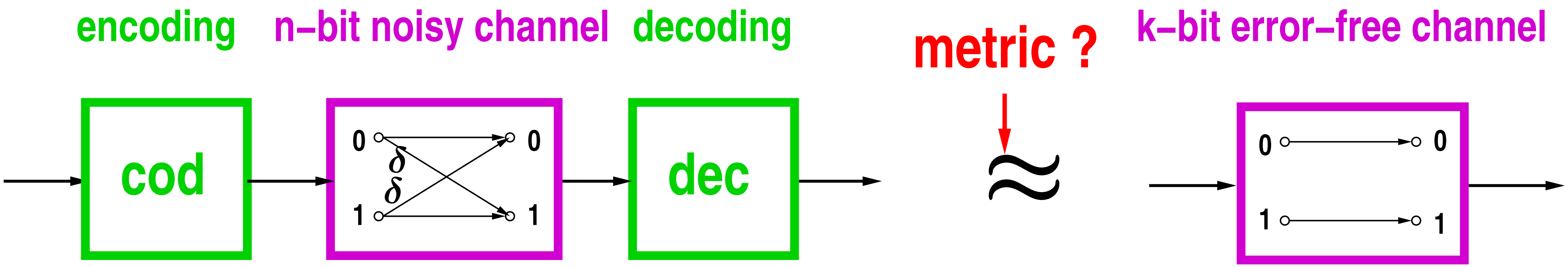
1. Construction paradigm

2. Abstract system algebra

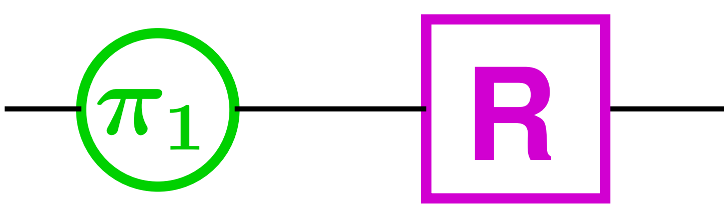
on:

$$\pi_1 \, \mathbf{R} \, \pi_2 \;\; \approx_\epsilon \;\; \mathbf{S} \quad \Longleftrightarrow: \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

Shannon's channel coding theorem



$$\text{cod} \quad \mathrm{BSC}_\delta^n \quad \text{dec} \quad \approx \quad \mathrm{BSC}_0^k$$



1. Construction paradigm

Construction:

$$\pi_1\ \mathbf{R}\ \pi_2 \quad \approx_\epsilon \quad \mathbf{S} \quad :\Longleftrightarrow \quad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

The construction paradigm

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Examples:

$$\mathrm{BSC}_{\delta}^{n} \xrightarrow{\text{(cod,dec)},\epsilon} \mathrm{BSC}_{0}^{k}$$

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Examples:

A (k, m)-pseudo-random generator (PRG) constructs a uniform m-bit string from a uniform k-bit string:

$$\mathrm{U}_k \xrightarrow{\text{PRG}} \mathrm{U}_m$$

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Examples:

A key agreement protocol (KAP) constructs a shared secret n-bit key from ???:

$$??? \xrightarrow{\text{KAP}} \text{KEY}_n$$

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Examples:

A complexity-theoretic reduction constructs an efficient algorithm for problem P from an efficient algorithm for problem Q.

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Formally: set of objects Ω,
constructor set $\langle \Gamma, \circ, \mathrm{id} \rangle$,
construction $\subseteq \Omega \times \Gamma \times \Omega$

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

Construct an object **S** from another object **R** via construction α.

Formally: set of objects Ω,
constructor set $\langle \Gamma, \circ, \mathrm{id} \rangle$,
construction $\subseteq \Omega \times \Gamma \times \Omega$

Definition: A construction is **composable** if

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta'} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha \circ \beta} \mathbf{T}$$

The construction paradigm

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

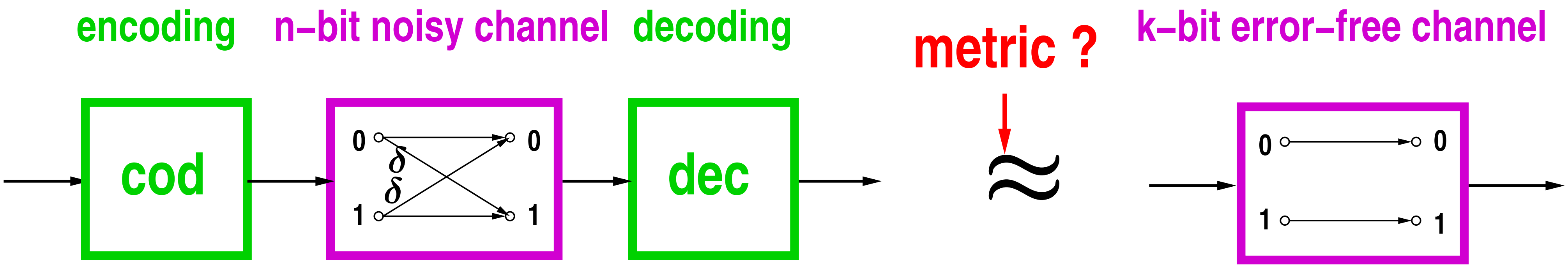
Construct an object **S** from another object **R** via construction α.

Formally: set of objects Ω, metric
constructor set $\langle \Gamma, \circ, \mathrm{id} \rangle$,
construction $\subseteq \Omega \times \Gamma \times \Omega$

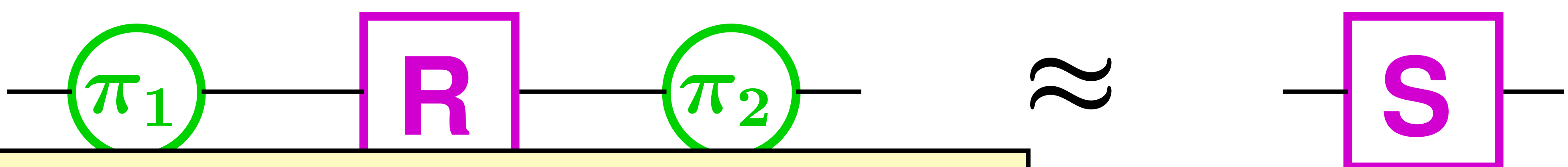
Definition: A construction is **composable** if

$$\mathbf{R} \xrightarrow{\alpha,\epsilon} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta,\epsilon'} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta,\epsilon+\epsilon'} \mathbf{T}$$

Shannon's channel coding theorem



$$\text{cod} \quad \mathrm{BSC}_\delta^n \quad \text{dec} \qquad \approx \qquad \mathrm{BSC}_0^k$$



2. Abstract system algebra

on:

$$\pi_1 \ \mathbf{R} \ \pi_2 \quad \approx_\epsilon \quad \mathbf{S} \qquad :\Longleftrightarrow \qquad \mathbf{R} \xrightarrow{(\pi_1,\pi_2),\,\epsilon} \mathbf{S}$$

A dilemma in computer science

A dilemma in computer science

“Theorem” means theorem !!!

A dilemma in computer science

"Theorem" means theorem !!!

$\Rightarrow$ One must precisely define computation, efficiency, infeasibility, non-negligible, security, ...

A dilemma in computer science

"Theorem" means theorem !!!

$\Rightarrow$ One must precisely define computation, efficiency, infeasibility, non-negligible, security, ...

$\Rightarrow$ Turing machines, communication tapes, asymptotics, polynomial-time, ...

A dilemma in computer science

"Theorem" means theorem !!!

$\Rightarrow$ One must precisely define computation, efficiency, infeasibility, non-negligible, security, ...

$\Rightarrow$ Turing machines, communication tapes, asymptotics, polynomial-time, ...

$\Rightarrow$ **enormous complexity, imprecise papers, ...**

A dilemma in computer science

Proposed paradigm shift in Computer Science:

Top-down abstraction

instead of

bottom-up definitions

security, ...

$\Rightarrow$ Turing machines, communication tapes, asymptotics, polynomial-time, ...

$\Rightarrow$ **enormous complexity, imprecise papers, ...**

A dilemma in computer science

Proposed paradigm shift in Computer Science:

Top-down abstraction

instead of

bottom-up definitions

security

Goals of abstraction:

- eliminate irrelevant details, minimality
- simpler definitions
- generality of results
- simpler proofs, elegance
- didactic suitability, better understanding

$\Rightarrow$

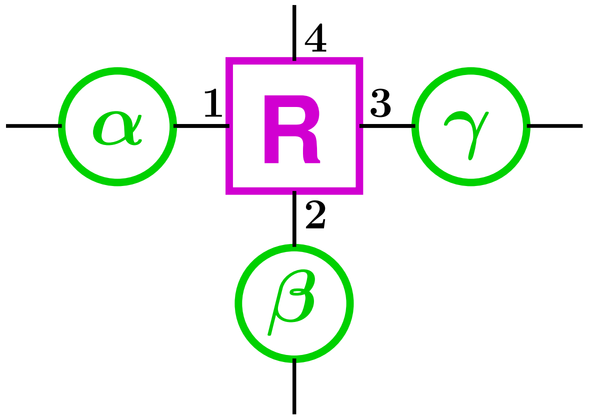
$\Rightarrow$ **e** ... **rs, ...**

Abstract system algebra $\langle \Phi, \Sigma \rangle$ [M-Renner11]

Abstract system algebra $\langle \Phi, \Sigma \rangle$ [M-Renner11]

Resource set Φ for interface set $\mathcal{I}$ (e.g. $\mathcal{I} = \{1, 2, 3, 4\}$)

Converter set Σ



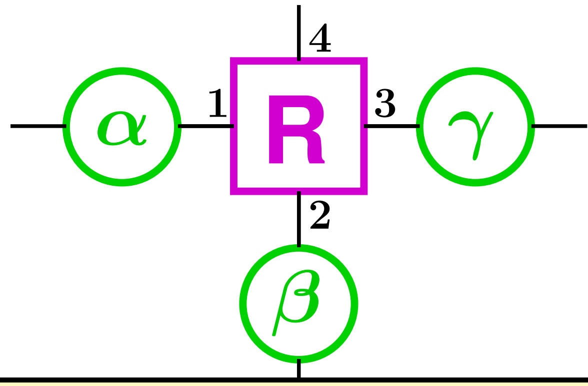
Algebraic laws:

- $\mathbf{R} || \mathbf{S} \in \Phi$ notation: $[\mathbf{R}, \mathbf{S}]$
- $\alpha^i \mathbf{R} \in \Phi$ for all $\mathbf{R} \in \Phi$, $\alpha \in \Sigma$, $i \in \mathcal{I}$
- $\alpha^i \beta^j \mathbf{R} = \beta^j \alpha^i \mathbf{R}$ for all $i \neq j$
- $1^i \mathbf{R} = \mathbf{R}$ for all i

Abstract system algebra $\langle \Phi, \Sigma \rangle$ [M-Renner11]

Resource set Φ for interface set $\mathcal{I}$ (e.g. $\mathcal{I} = \{1,2,3,4\}$)

Converter set Σ



Pseudo-metric d on Φ:

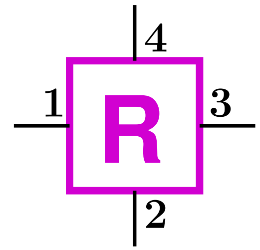
Def.: **d** is **non-expanding** $\Longleftrightarrow$ **d**(α^i**R**,α^i**S**) $\leq$ **d**(**R**,**S**)

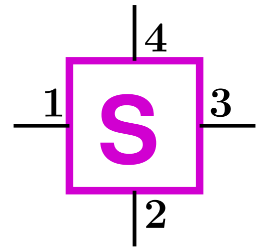
- $\alpha^i \mathbf{R} \in \Phi$ for all $\mathbf{R} \in \Phi$, $\alpha \in \Sigma$, $i \in \mathcal{I}$
- $\alpha^i \beta^j \mathbf{R} = \beta^j \alpha^i \mathbf{R}$ for all $i \neq j$
- $1^i \mathbf{R} = \mathbf{R}$ for all i

Abstract system algebra $\langle \Phi, \Sigma \rangle$ [M-Renner11]

Resource set Φ for interface set $\mathcal{I}$ (e.g. $\mathcal{I} = \{1,2,3,4\}$)

Converter set Σ





Pseudo-metric d on Φ:

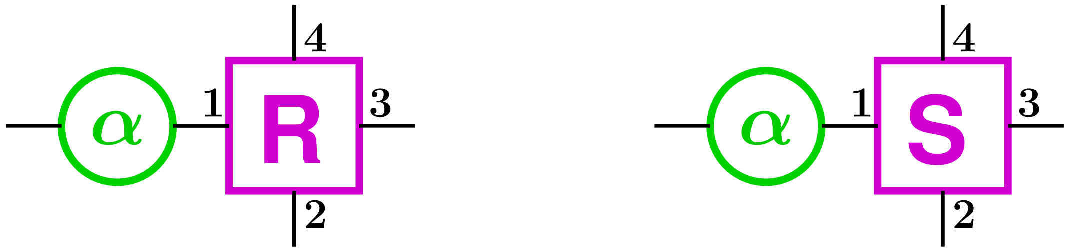
Def.: **d** is **non-expanding** $\iff$ $\mathbf{d}(\alpha^i\mathbf{R},\alpha^i\mathbf{S}) \leq \mathbf{d}(\mathbf{R},\mathbf{S})$

- $\alpha^i\mathbf{R} \in \Phi$ for all $\mathbf{R} \in \Phi$, $\alpha \in \Sigma$, $i \in \mathcal{I}$
- $\alpha^i\beta^j\mathbf{R} = \beta^j\alpha^i\mathbf{R}$ for all $i \neq j$
- $1^i\mathbf{R} = \mathbf{R}$ for all i

Abstract system algebra $\langle \Phi, \Sigma \rangle$ [M-Renner11]

Resource set Φ for interface set $\mathcal{I}$ (e.g. $\mathcal{I} = \{1,2,3,4\}$)

Converter set Σ



- $\alpha^i \mathbf{R} \in \Phi$ for all $\mathbf{R} \in \Phi$, $\alpha \in \Sigma$, $i \in \mathcal{I}$
- $\alpha^i \beta^j \mathbf{R} = \beta^j \alpha^i \mathbf{R}$ for all $i \neq j$
- $1^i \mathbf{R} = \mathbf{R}$ for all i

Pseudo-metric d on Φ:

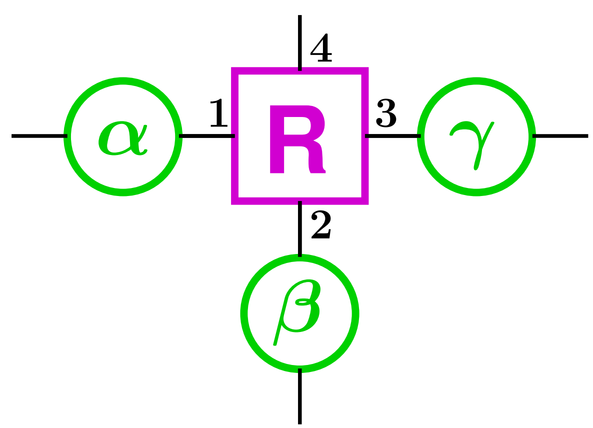
Def.: **d** is **non-expanding** $\Longleftrightarrow$ **d**(α^i**R**,α^i**S**) $\leq$ **d**(**R**,**S**)

Levels of abstraction

#	level	concepts treated at this level
0.	Constructions	composability, construction trees
1.	Abstract systems	composability proof
2.	Discrete systems	I/O bahavior, indistinguish. proofs
3.	System implem.	complexity, efficiency, asymptotics

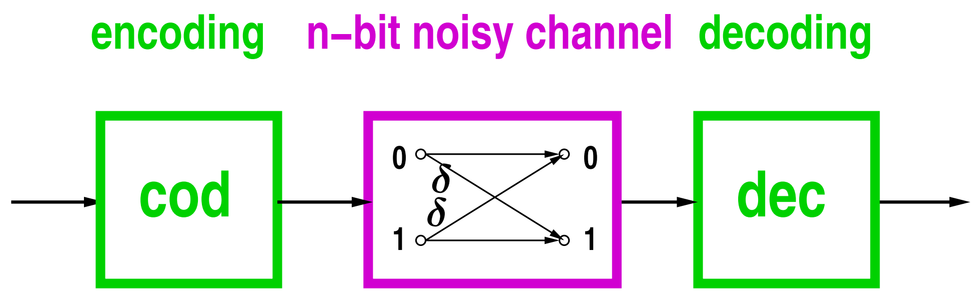
Levels of abstraction

#	level	concepts treated at this level
0.	Constructions	composability, construction trees
1.	Abstract systems	composability proof
2.	Discrete systems	I/O bahavior, indistinguish. proofs
3.	System implem.	complexity, efficiency, asymptotics



Levels of abstraction

#	level	concepts treated at this level
0.	Constructions	composability, construction trees
1.	Abstract systems	composability proof
2.	Discrete systems	I/O bahavior, indistinguish. proofs
3.	System implem.	complexity, efficiency, asymptotics



Levels of abstraction

#	level	concepts treated at this level
0.	Constructions	composability, construction trees
1.	Abstract systems	composability proof
2.	Discrete systems	I/O bahavior, indistinguish. proofs
3.	System implem.	complexity, efficiency, asymptotics

system ENCRYPT
read x at outside interface
read k at inside interface
$c \leftarrow$ enc(x, k)
.....

Abstraction levels in algebra:

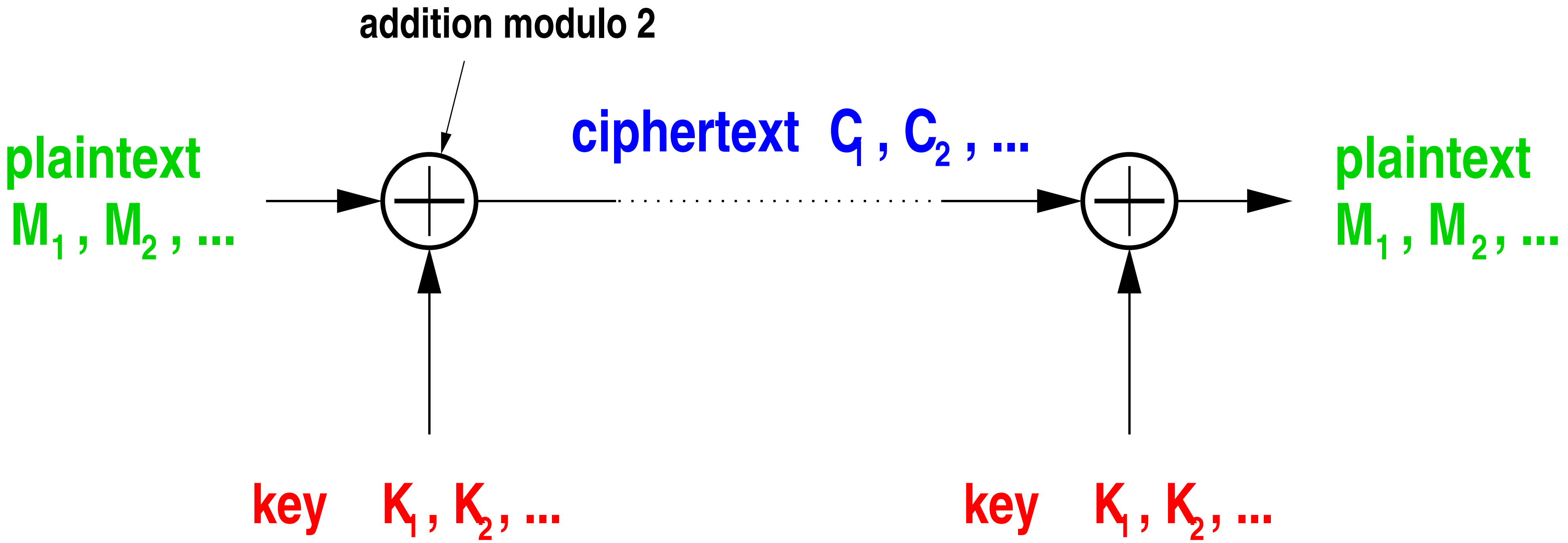
1. **Abstract group:** $\langle G, \star, e, (\cdot)^{-1} \rangle$
2. **Instantiations:** Integers, real number, elliptic curves
3. **Representations:** e.g. projective coordinates for ECs

1.	**Abstract systems**	composability proof
2.	**Discrete systems**	I/O bahavior, indistinguish. proofs
3.	**System implem.**	complexity, efficiency, asymptotics

Constructive cryptography

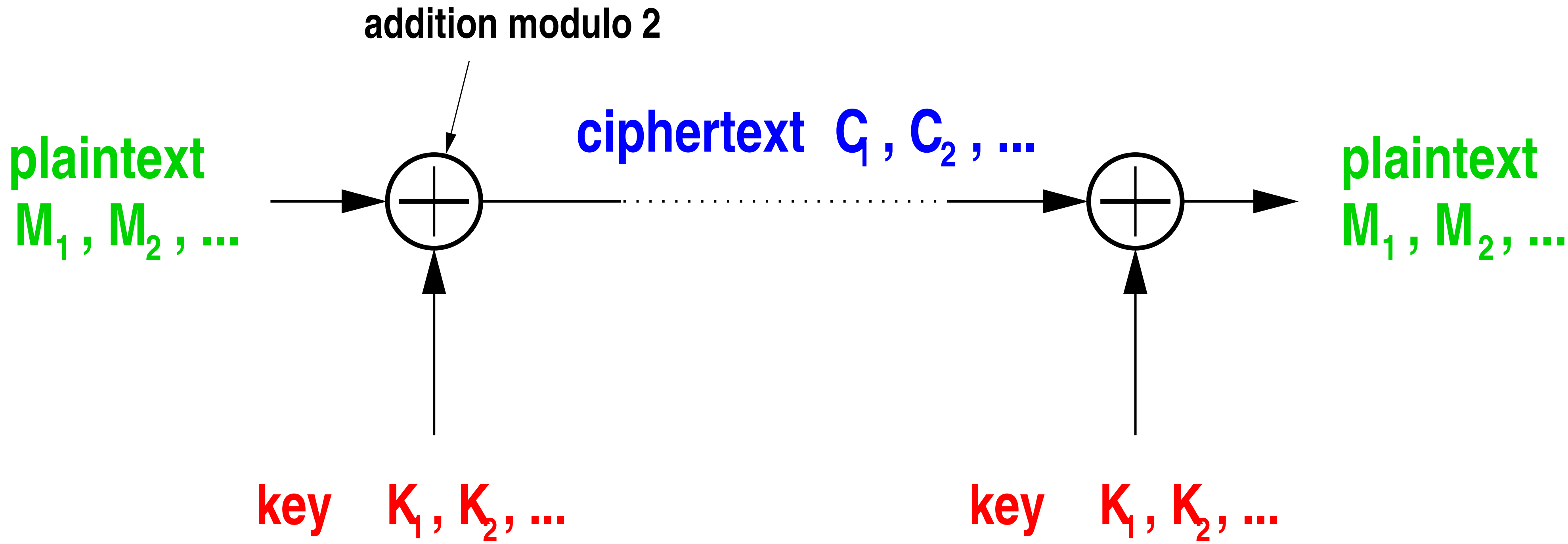
Constructive cryptography

One-time pad:



Constructive cryptography

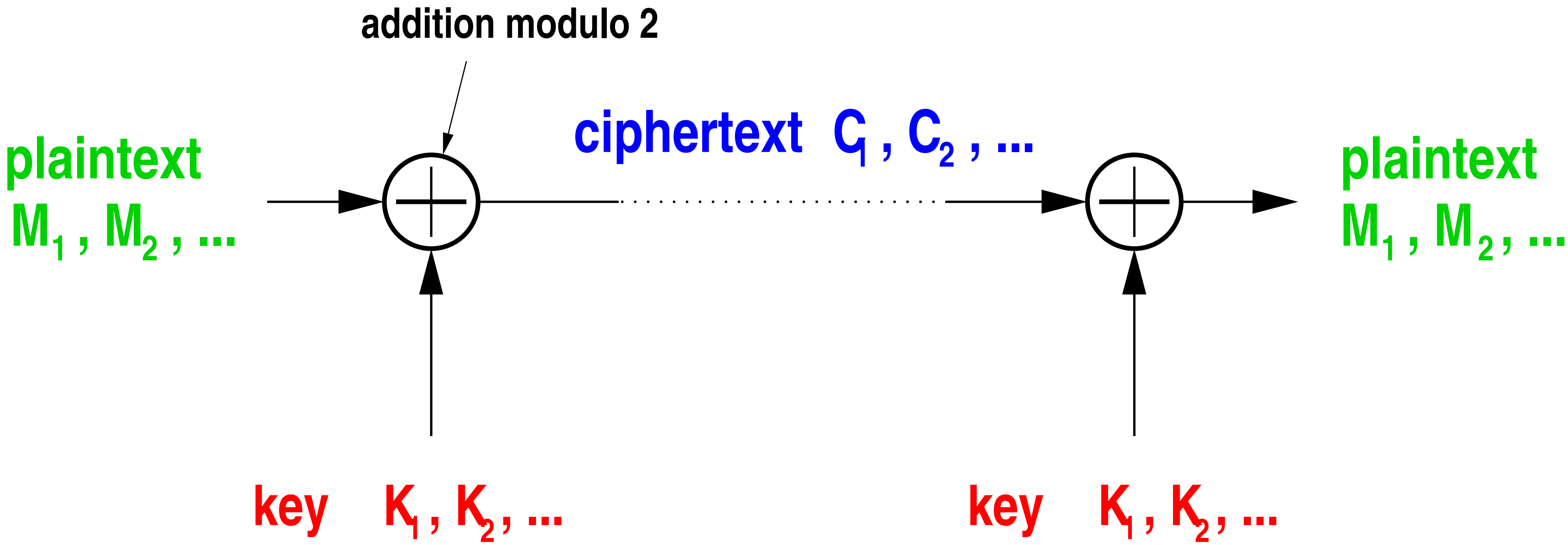
One-time pad:



Security ?

Constructive cryptography

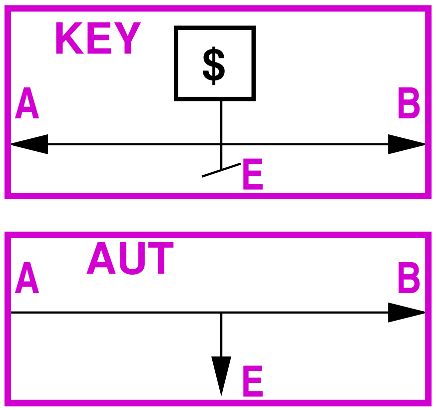
One-time pad:



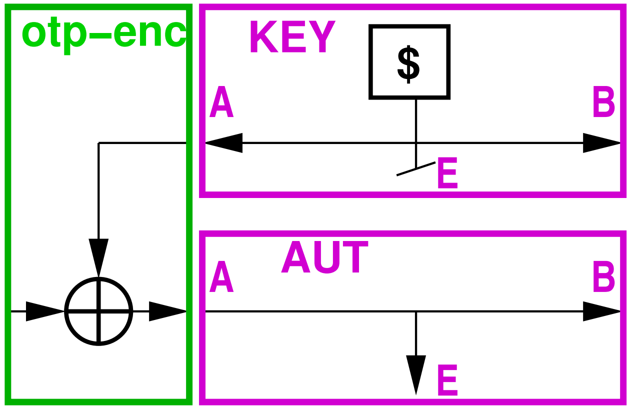
Security [SHANNON]: $\mathbf{I}(\mathbf{C},\mathbf{M}) = 0$ (perfect secrecy)

One-time pad in constructive cryptography

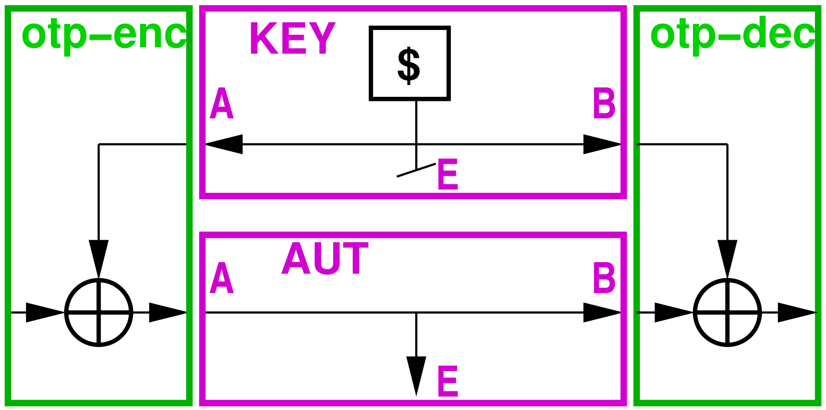
One-time pad in constructive cryptography



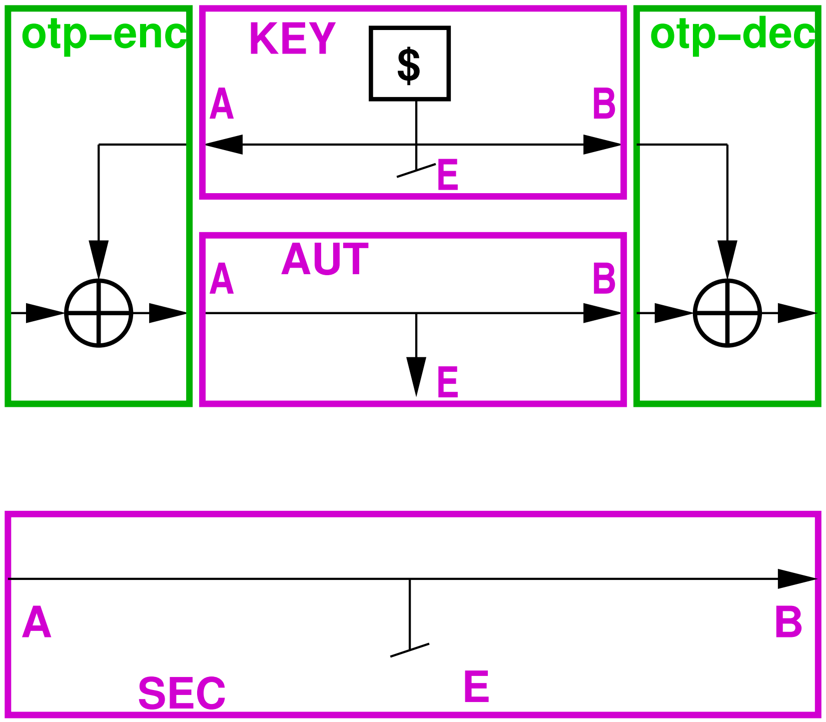
One-time pad in constructive cryptography



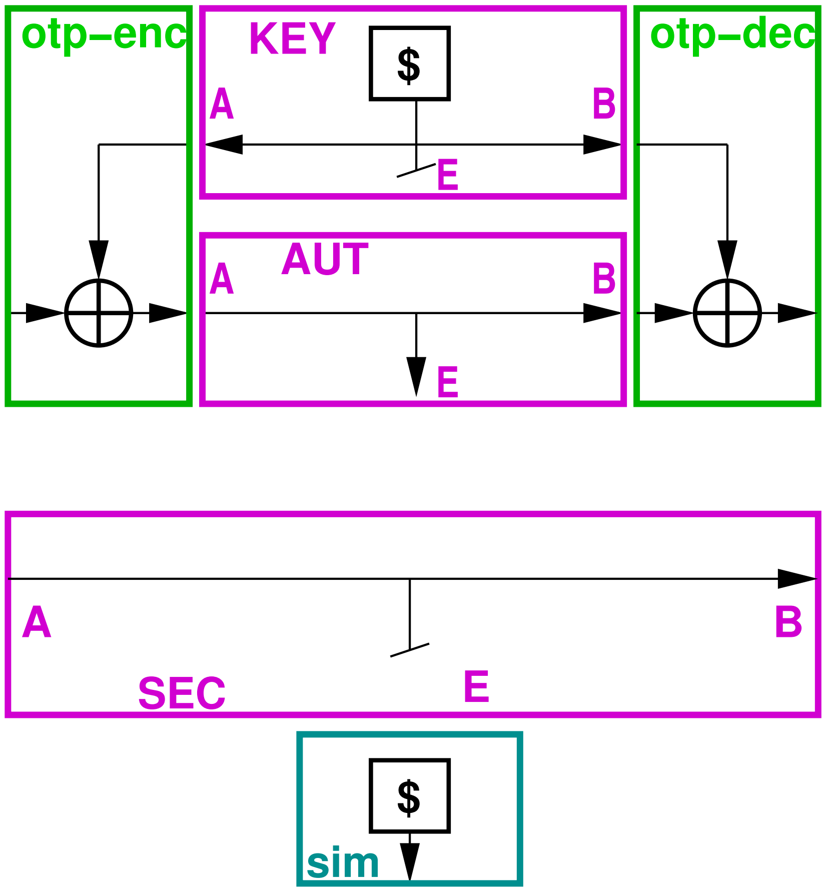
One-time pad in constructive cryptography



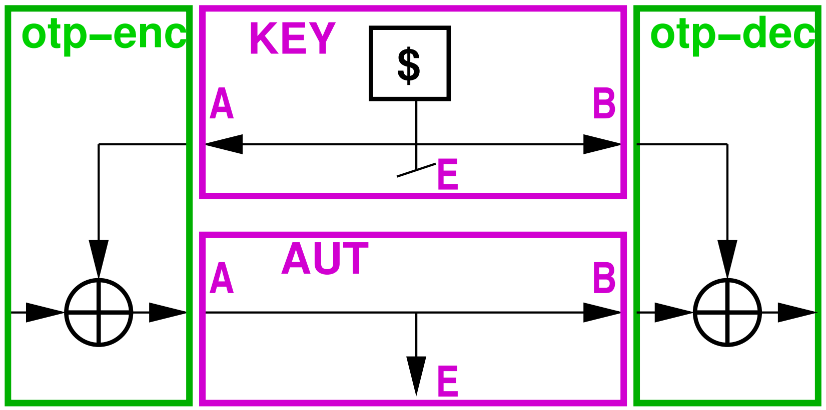
One-time pad in constructive cryptography

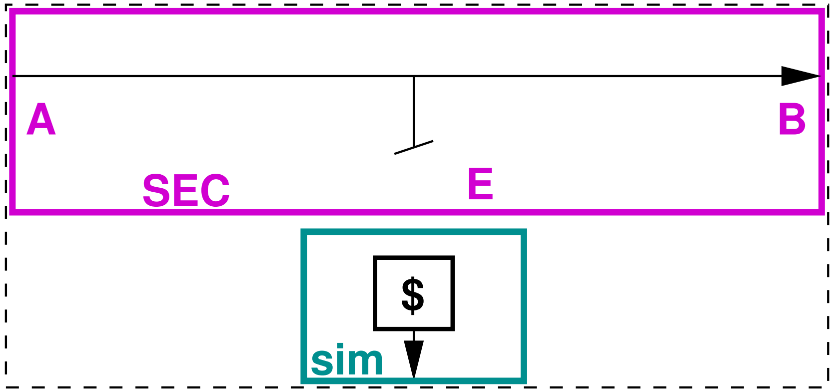


One-time pad in constructive cryptography

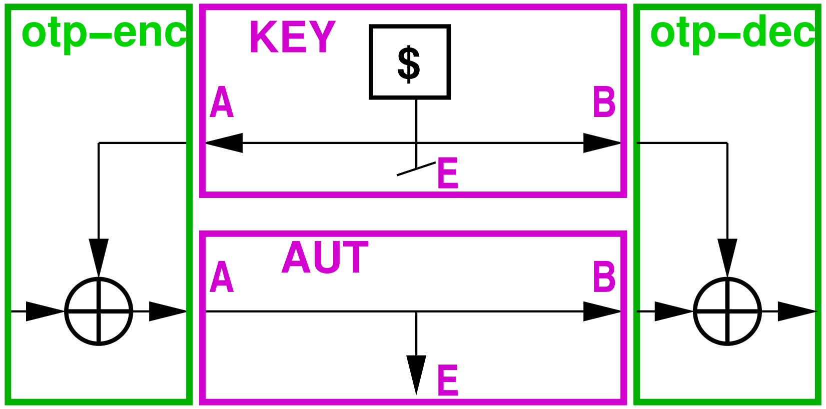


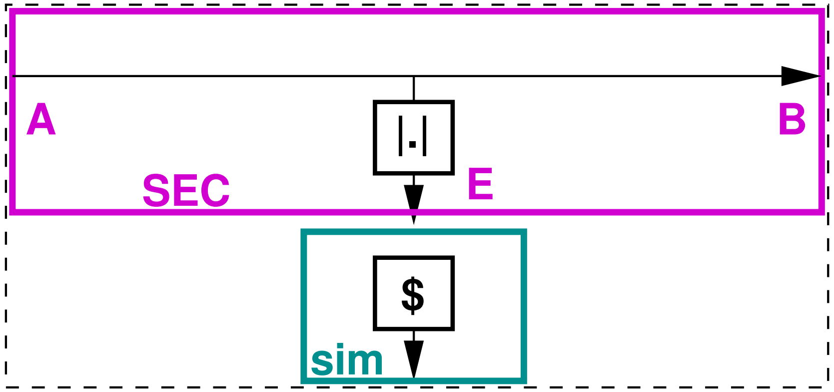
One-time pad in constructive cryptography



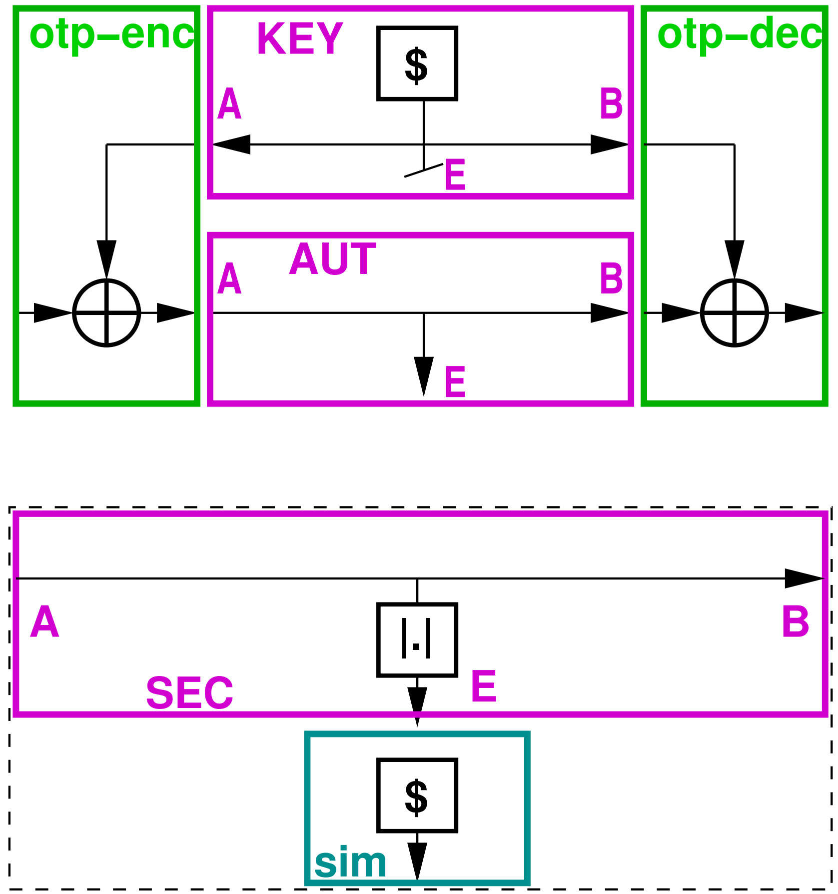


One-time pad in constructive cryptography



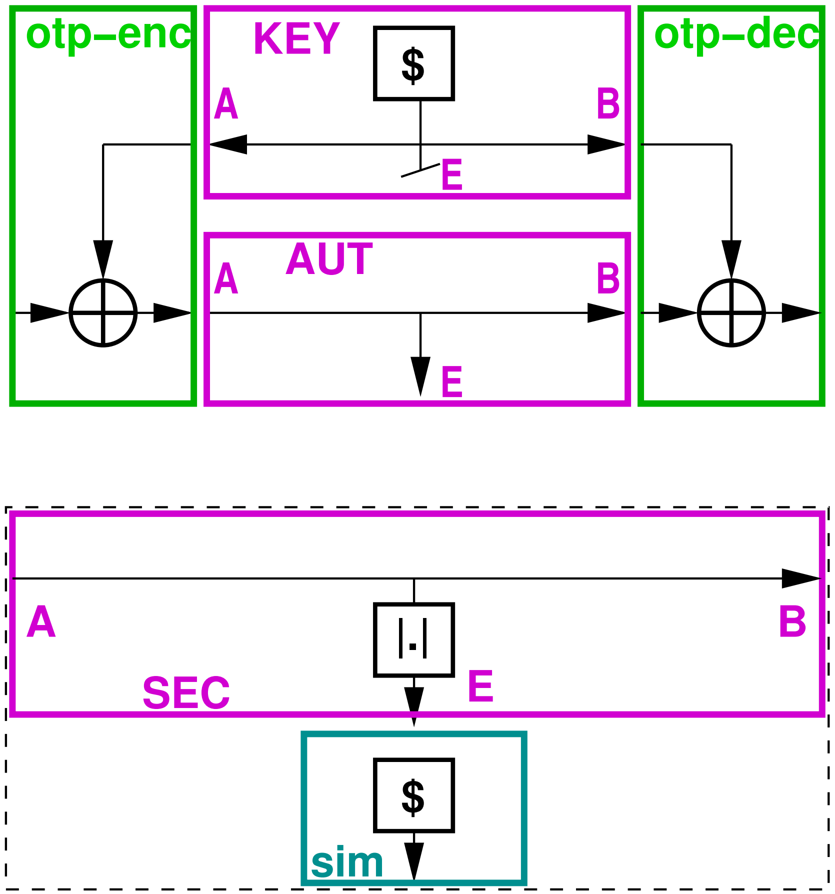


One-time pad in constructive cryptography



$$\textbf{otp-dec}^{B}\ \textbf{otp-enc}^{A}\ [\textbf{KEY}, \textbf{AUT}] \equiv \textbf{sim}^{E}\ \textbf{SEC}$$

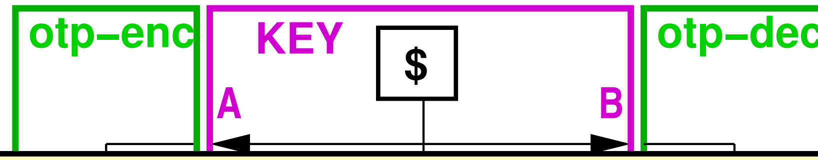
One-time pad in constructive cryptography



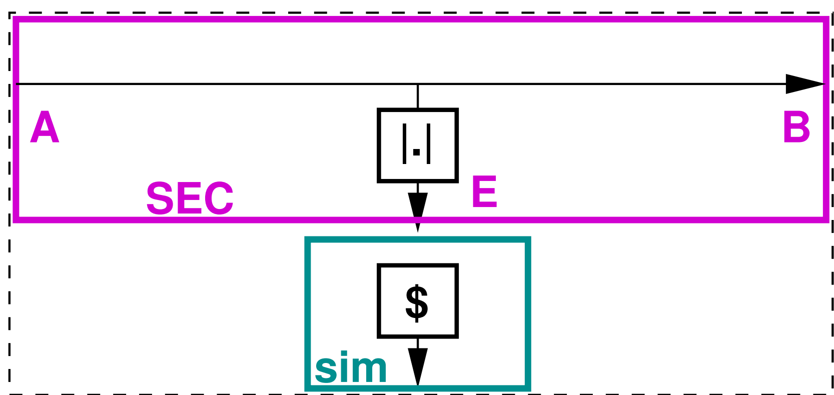
$$\text{otp-dec}^{B}\ \text{otp-enc}^{A}\ [\mathbf{KEY}, \mathbf{AUT}] \equiv \text{sim}^{E}\ \mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{OTP}} \mathbf{SEC}$

One-time pad in constructive cryptography



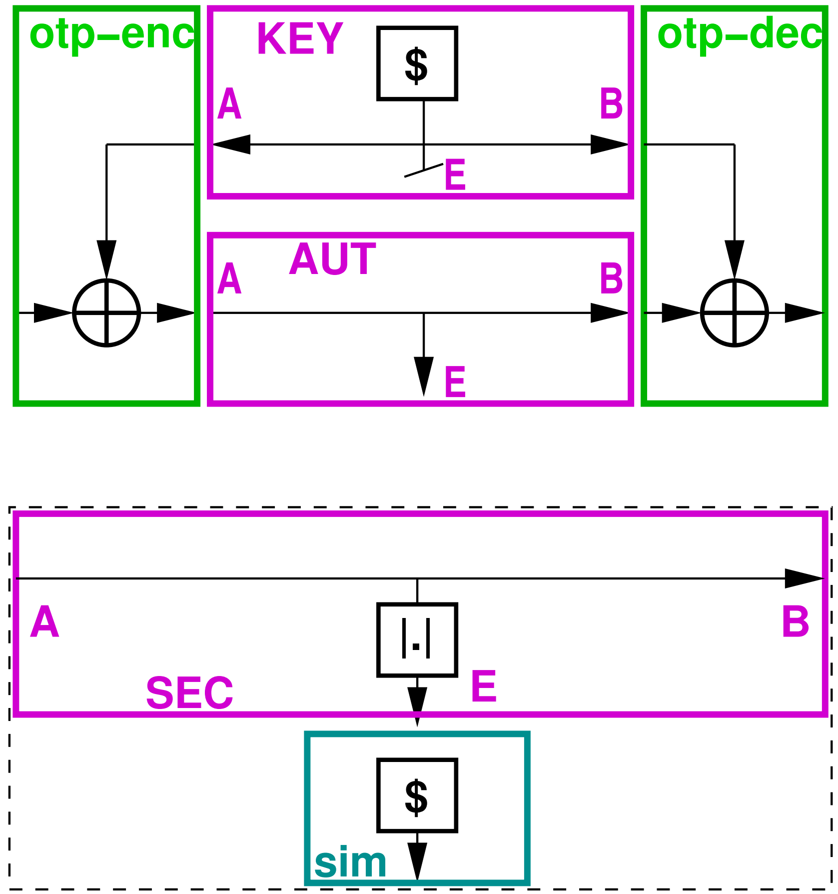
Draws on work by [Goldreich-Micali-Wigderson85], [Canetti01], [Pfitzmann-Waidner], [M.-Schmid96], ...



$$\textbf{otp-dec}^{B}\,\textbf{otp-enc}^{A}\,[\textbf{KEY},\textbf{AUT}] \equiv \textbf{sim}^{E}\,\textbf{SEC}$$

as a construction: $[\textbf{KEY},\textbf{AUT}] \xrightarrow{\textbf{OTP}} \textbf{SEC}$

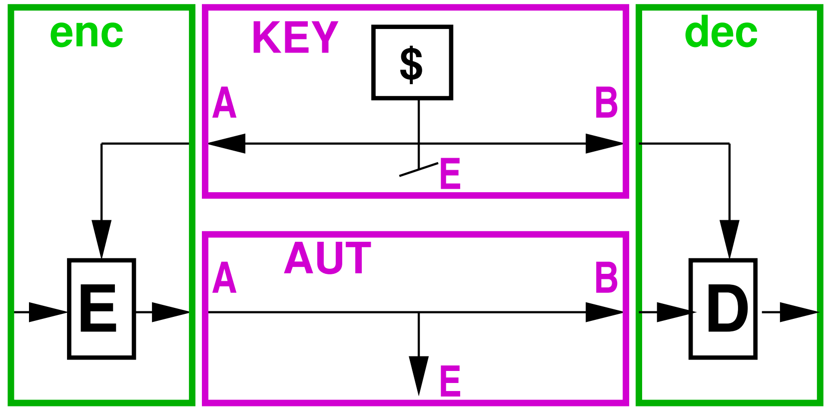
One-time pad in constructive cryptography

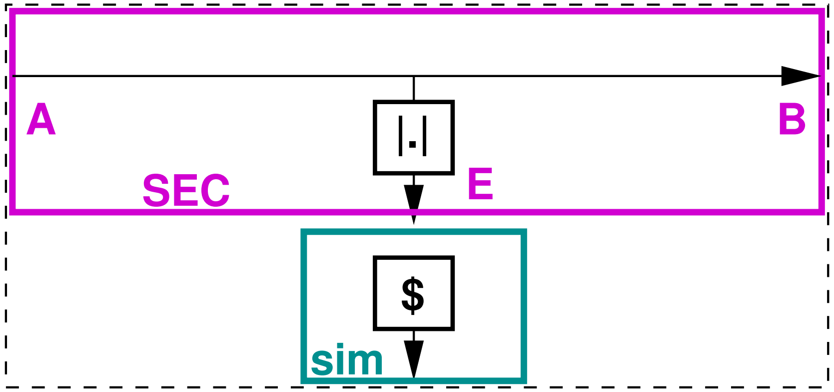


$$\textbf{otp-dec}^{B}\ \textbf{otp-enc}^{A}\ [\textbf{KEY}, \textbf{AUT}] \quad \equiv \quad \textbf{sim}^{E}\ \textbf{SEC}$$

as a construction: $[\textbf{KEY}, \textbf{AUT}] \xrightarrow{\textbf{OTP}} \textbf{SEC}$

Encryption in constructive cryptography

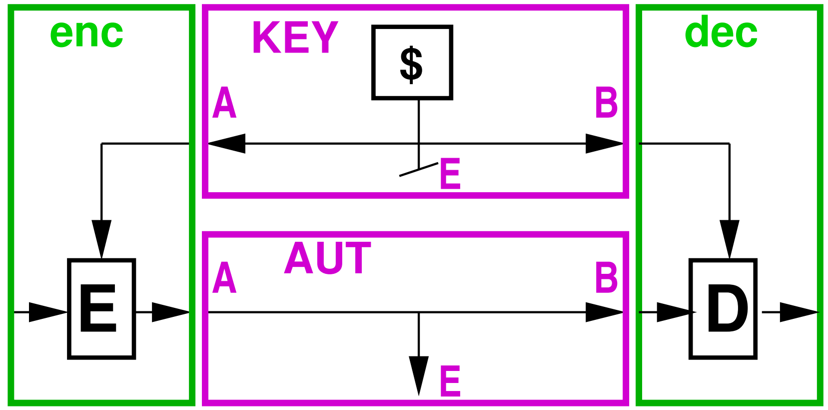


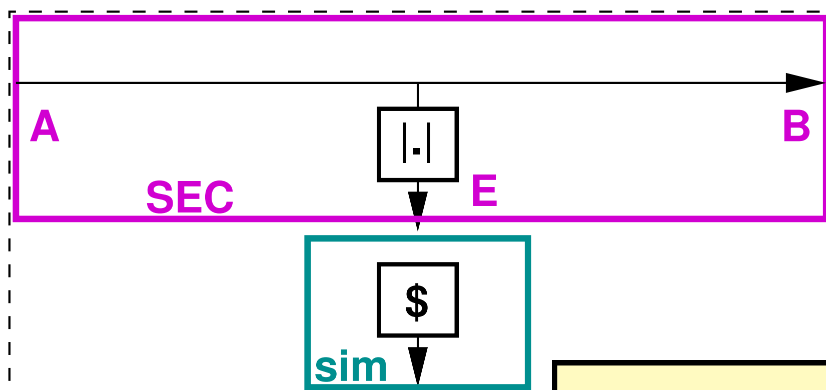


$$\mathbf{dec}^{B}\,\mathbf{enc}^{A}\,[\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{E}\,\mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography



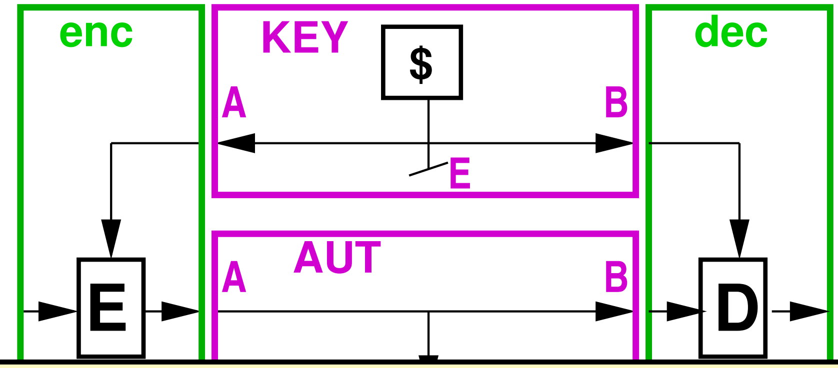


metric?

$$\mathbf{dec}^{\mathsf{B}}\,\mathbf{enc}^{\mathsf{A}}\,[\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{\mathsf{E}}\,\mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography

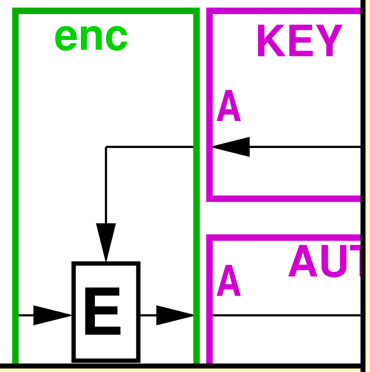


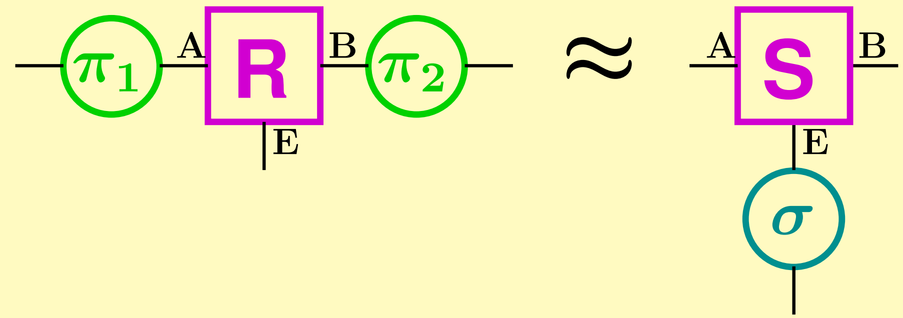
$$\mathbf{R} \xrightarrow{(\pi_1,\pi_2)} \mathbf{S} \quad :\Leftrightarrow \quad \exists\sigma : \ \pi_1^{\mathsf{A}} \pi_2^{\mathsf{B}} \mathbf{R} \approx \sigma^{\mathsf{E}} \mathbf{S}$$

$$\mathbf{dec}^{\mathsf{B}}\, \mathbf{enc}^{\mathsf{A}}\, [\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{\mathsf{E}}\, \mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography



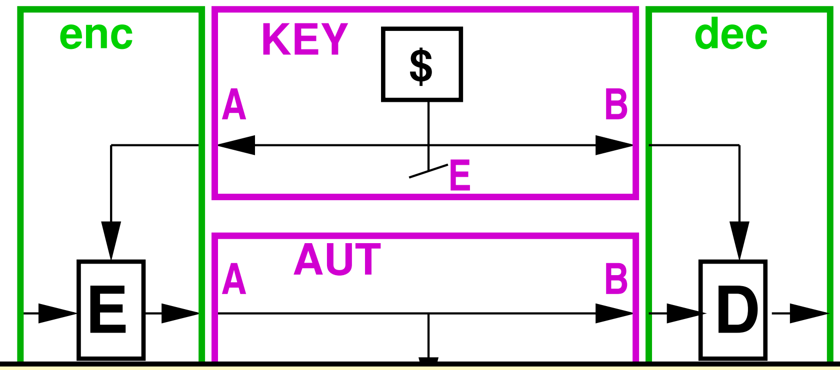


$$\mathbf{R} \xrightarrow{(\pi_1,\pi_2)} \mathbf{S} \;:\Leftrightarrow\; \exists\sigma : \pi_1^{A}\,\pi_2^{B}\,\mathbf{R} \approx \sigma^{E}\,\mathbf{S}$$

$$\mathbf{dec}^{B}\,\mathbf{enc}^{A}\,[\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{E}\,\mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography



$$\mathbf{R} \xrightarrow{(\pi_1,\pi_2)} \mathbf{S} \;:\Leftrightarrow\; \exists\sigma : \pi_1^{\mathsf{A}}\,\pi_2^{\mathsf{B}}\,\mathbf{R} \approx \sigma^{\mathsf{E}}\,\mathbf{S}$$

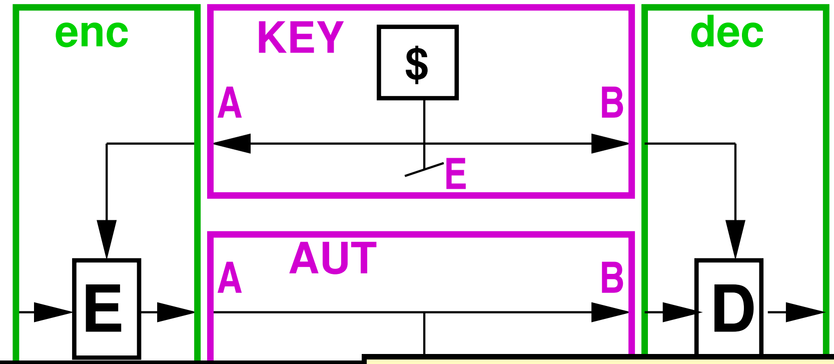
and

$$\pi_1^{\mathsf{A}}\,\pi_2^{\mathsf{B}}\,\perp^{\mathsf{E}}\mathbf{R} \approx \perp^{\mathsf{E}}\mathbf{S}$$

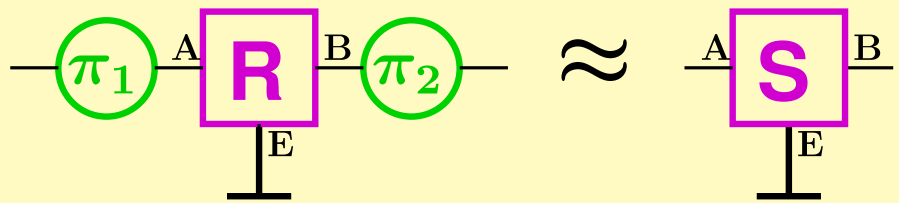
$$\mathbf{dec}^{\mathsf{B}}\,\mathbf{enc}^{\mathsf{A}}\,[\mathbf{KEY},\mathbf{AUT}] \approx \mathbf{sim}^{\mathsf{E}}\,\mathbf{SEC}$$

as a construction: $[\mathbf{KEY},\mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography



$$R \xrightarrow{(\pi_1,\pi_2)} S \quad :\Leftrightarrow$$

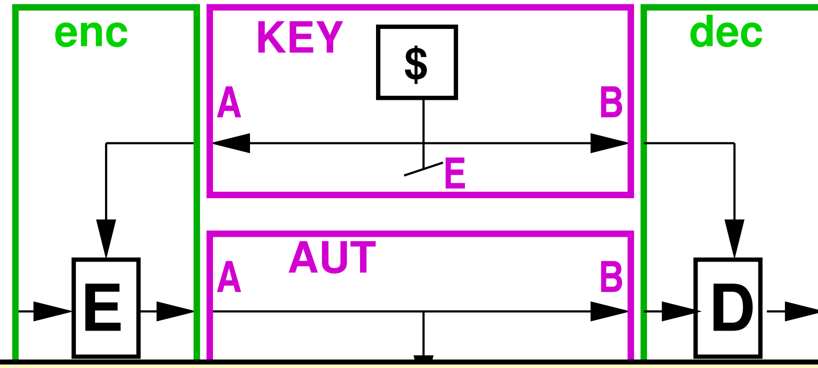


$$\pi_1^{A}\ \pi_2^{B}\ \perp^{E}\ R \approx \perp^{E}\ S$$

$$\mathbf{dec}^{B}\ \mathbf{enc}^{A}\ [\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{E}\ \mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

Encryption in constructive cryptography



$$\mathbf{R} \xrightarrow{(\pi_1,\pi_2)} \mathbf{S} \quad :\Leftrightarrow \quad \exists \sigma : \pi_1^{\mathsf{A}} \pi_2^{\mathsf{B}} \mathbf{R} \approx \sigma^{\mathsf{E}} \mathbf{S}$$

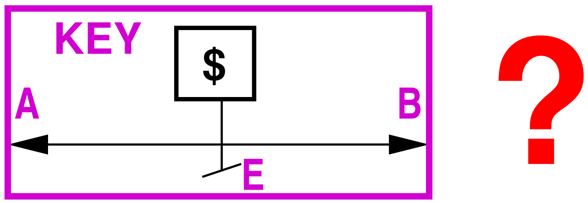
and

$$\pi_1^{\mathsf{A}} \pi_2^{\mathsf{B}} \perp^{\mathsf{E}} \mathbf{R} \approx \perp^{\mathsf{E}} \mathbf{S}$$

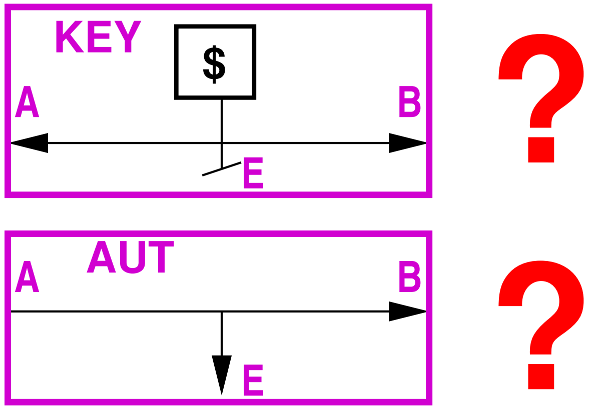
$$\mathbf{dec}^{\mathsf{B}}\, \mathbf{enc}^{\mathsf{A}}\, [\mathbf{KEY}, \mathbf{AUT}] \approx \mathbf{sim}^{\mathsf{E}}\, \mathbf{SEC}$$

as a construction: $[\mathbf{KEY}, \mathbf{AUT}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}$

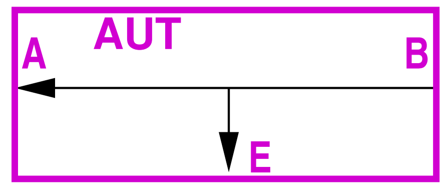
Encryption in constructive cryptography

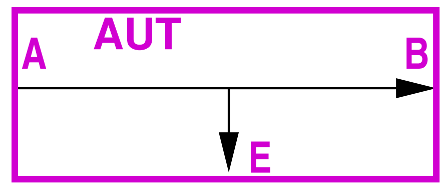


Encryption in constructive cryptography

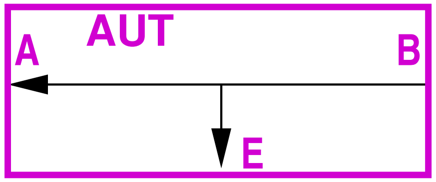


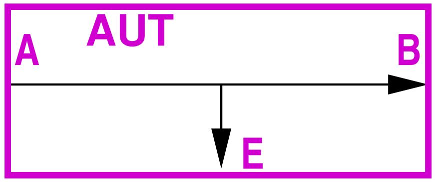
Key agreement in CC

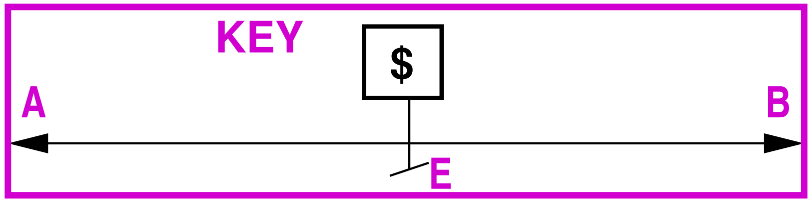




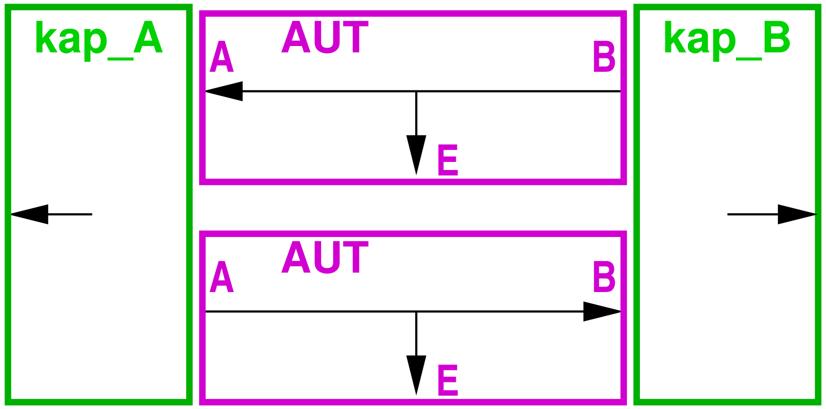
Key agreement in CC

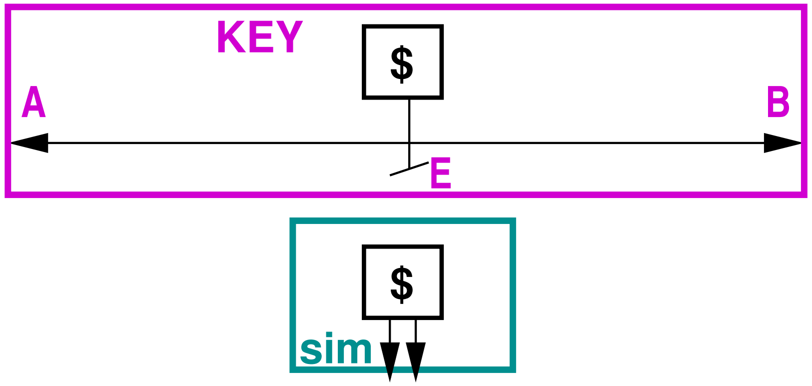




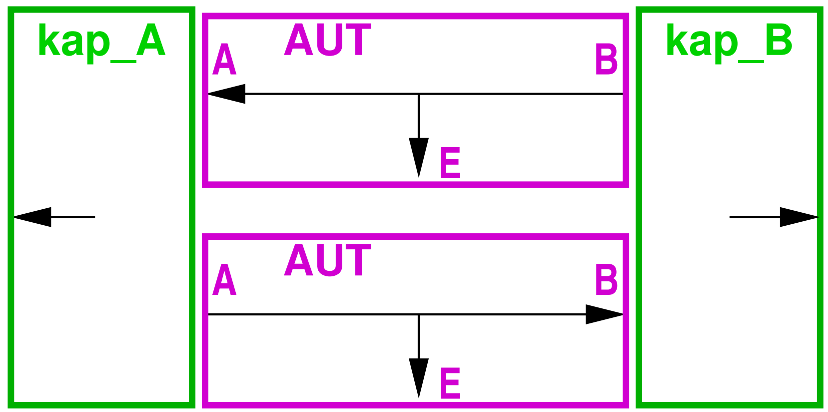


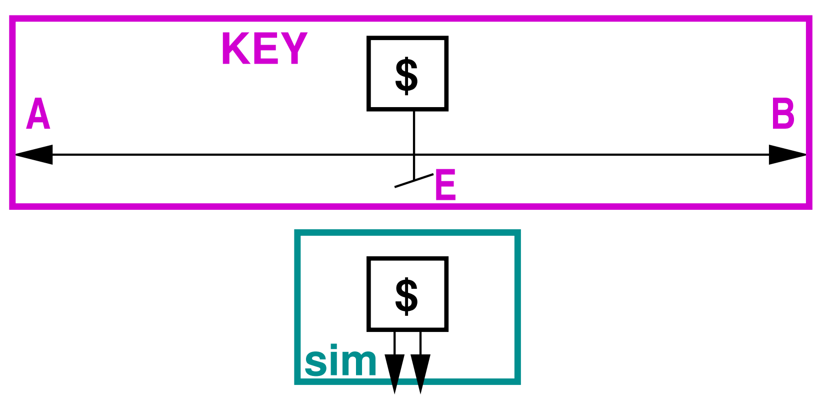
Key agreement in CC





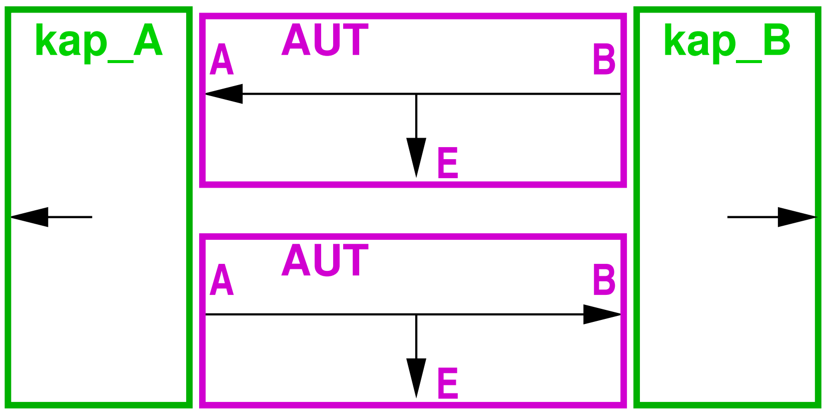
Key agreement in CC

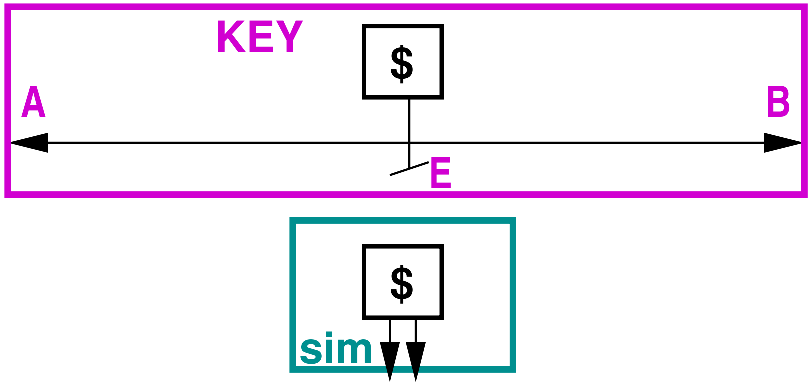




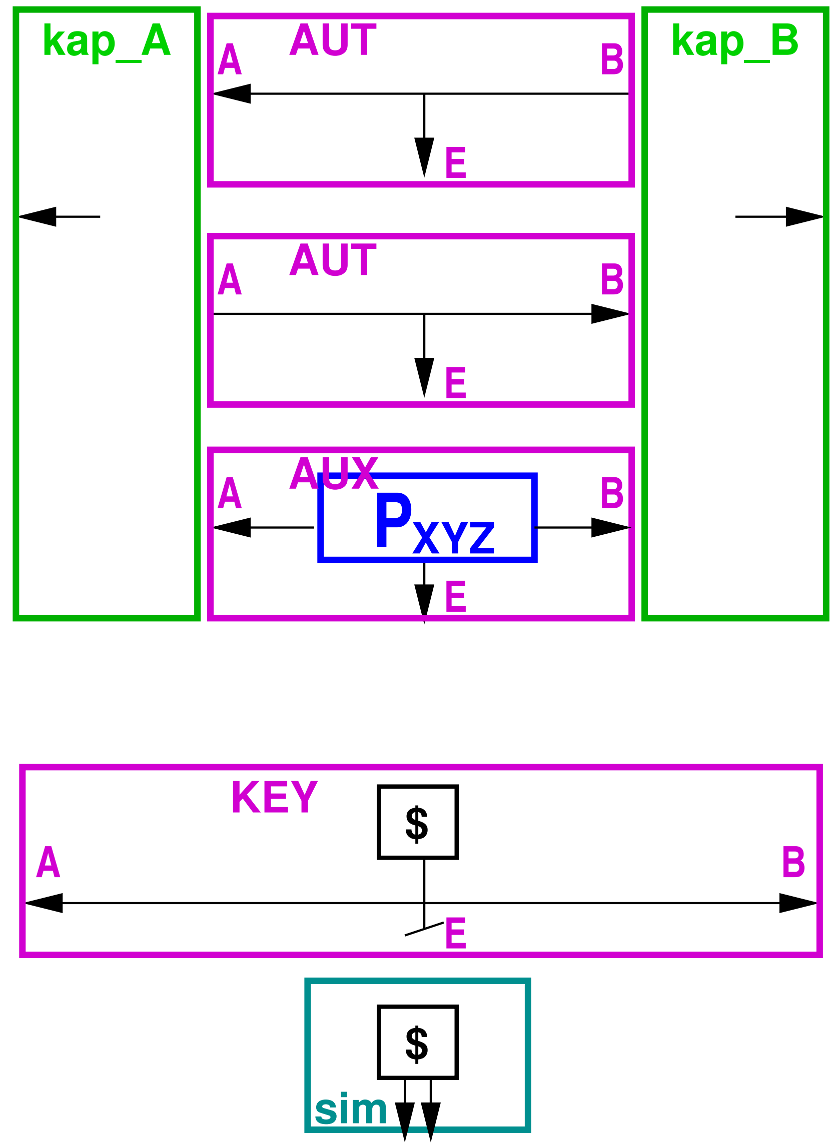
$$[\mathrm{AUT}, \mathrm{AUT'}] \xrightarrow{\mathrm{DifHel}} \mathrm{KEY}$$

Key agreement in CC (i.t. security)



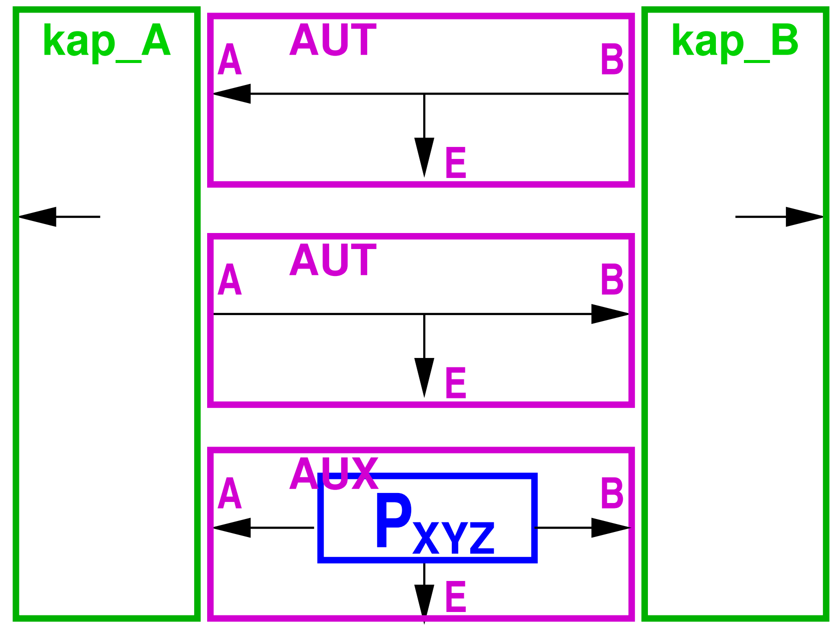


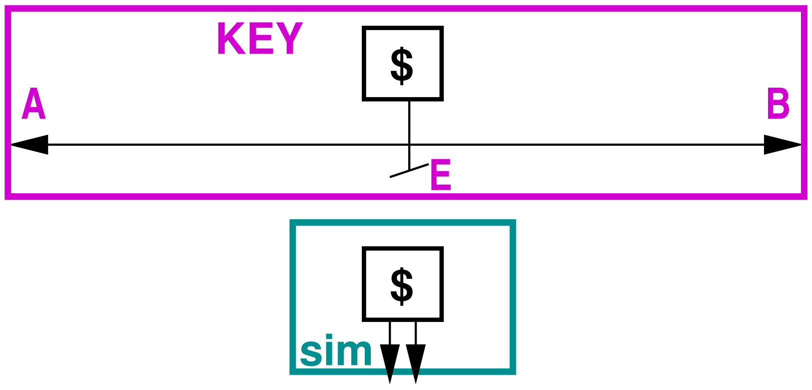
Key agreement in CC (i.t. security)



$$[\mathrm{AUT}, \mathrm{AUT'}, P_{XYZ}] \xrightarrow{\mathrm{KA\_PD}} \mathrm{KEY}$$

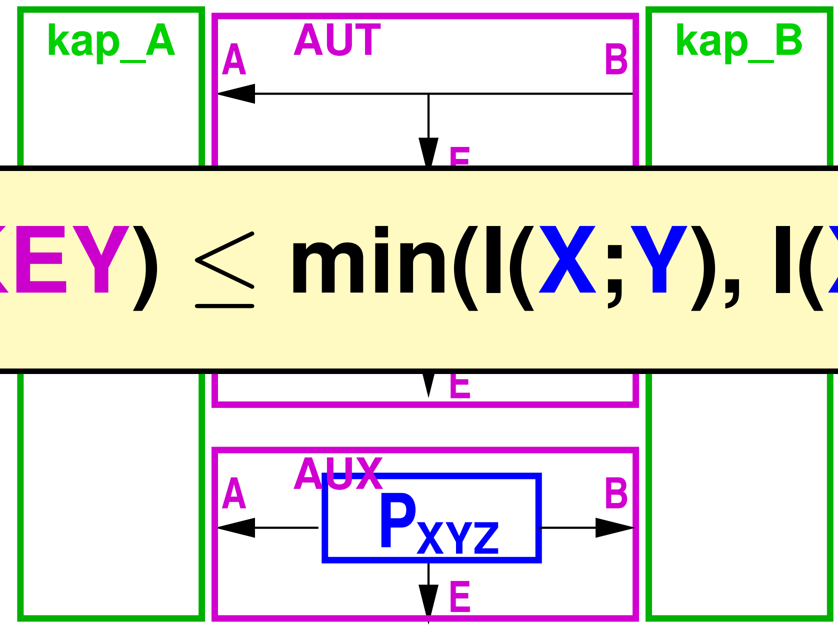
Key agreement in CC (i.t. security)



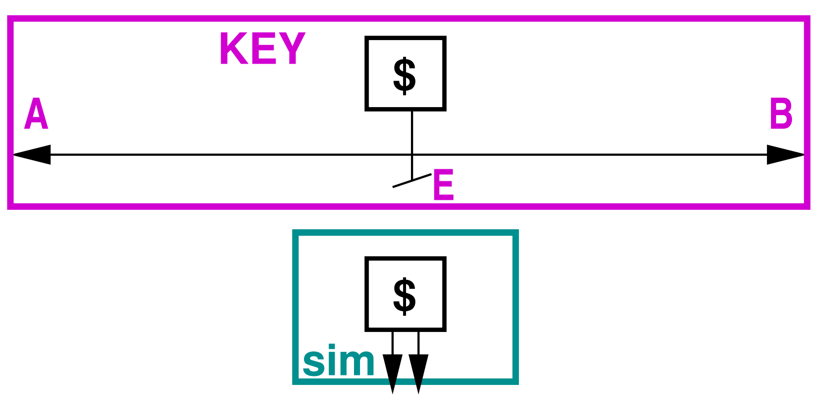


$$[\mathrm{AUT}, \mathrm{AUT'}, P_{XYZ}] \xrightarrow{\mathrm{KA\_PD},\ \epsilon} \mathrm{KEY}$$

Key agreement in CC (i.t. security)

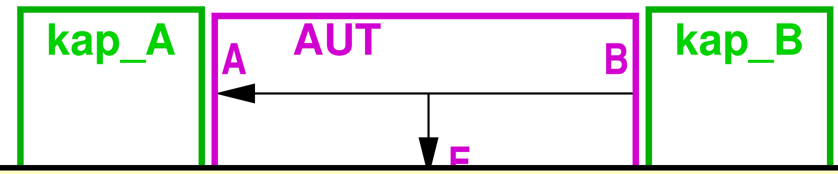


Theorem: $H(\text{KEY}) \leq \min(I(X;Y), I(X;Y|Z))$ if $\epsilon = 0$.

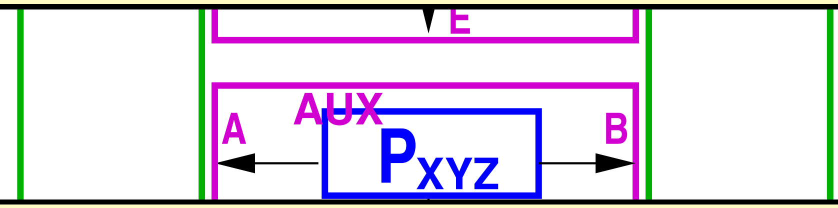


$$[\text{AUT}, \text{AUT'}, P_{XYZ}] \xrightarrow{\text{KA\_PD}, \ \epsilon} \text{KEY}$$

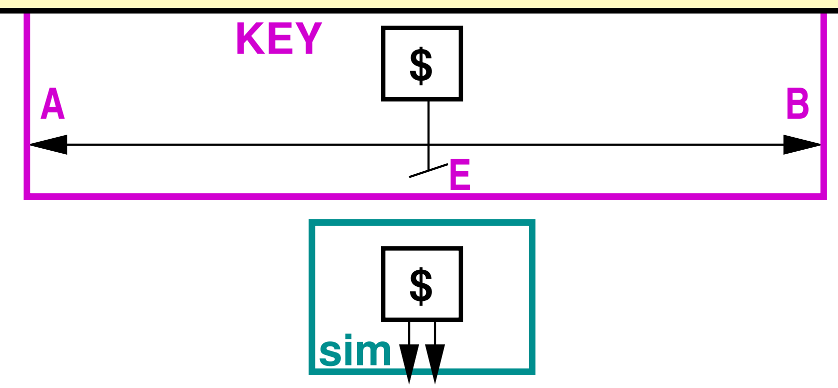
Key agreement in CC (i.t. security)



Theorem: $H(\text{KEY}) \leq \min(I(X;Y), I(X;Y|Z))$ if $\epsilon = 0$.



Theorem: $\epsilon \geq f(\, H(\text{KEY}) - I(X;Y|Z))$



$$[\text{AUT}, \text{AUT'}, P_{XYZ}] \xrightarrow{\text{KA\_PD}, \, \epsilon} \text{KEY}$$

Composition: an example

Composition: an example

$$\left.\begin{array}{l}[\text{AUT}, \text{AUT'}] \xrightarrow{\text{DifHel}} \text{KEY} \\ [\text{KEY}, \text{AUT''}] \xrightarrow{\text{SYM}} \text{SEC}\end{array}\right\} \Rightarrow$$

$$[[\text{AUT}, \text{AUT'}], \text{AUT''}] \xrightarrow{\text{DifHel} \circ \text{SYM}} \text{SEC}$$

Composition: an example

$$\left.\begin{array}{l}[\mathbf{AUT}, \mathbf{AUT'}] \xrightarrow{\mathbf{DifHel}} \mathbf{KEY} \\ [\mathbf{KEY}, \mathbf{AUT''}] \xrightarrow{\mathbf{SYM}} \mathbf{SEC}\end{array}\right\} \Rightarrow$$

$$[[\mathbf{AUT}, \mathbf{AUT'}], \mathbf{AUT''}] \xrightarrow{\mathbf{DifHel} \circ \mathbf{SYM}} \mathbf{SEC}$$

$$[\mathbf{AUT}, \mathbf{QC}] \xrightarrow{\mathbf{QKD} \circ \mathbf{OTP}} \mathbf{SEC}$$

Composition: an example

$$\left.\begin{array}{l}[\text{AUT}, \text{AUT'}] \xrightarrow{\text{DifHel}} \text{KEY} \\ [\text{KEY}, \text{AUT''}] \xrightarrow{\text{SYM}} \text{SEC}\end{array}\right\} \Rightarrow$$

$$[[\text{AUT}, \text{AUT'}], \text{AUT''}] \xrightarrow{\text{DifHel} \circ \text{SYM}} \text{SEC}$$

$$[\text{AUT}, \text{QC}] \xrightarrow{\text{QKD} \circ \text{OTP}} \text{SEC}$$

Attention: Quantum Key Distribution, though proven secure, did not compose before 2005 [KRBM07,Renner05]

Composition: an example

$[\text{AUT}, \text{AUT'}] \xrightarrow{\text{DifHel}} \text{KEY}$

$[\text{KEY}, \text{AUT''}] \xrightarrow{\text{SYM}} \text{SEC}$ $\Rightarrow$

$[\text{KEY}, \text{IC}, \text{QC}] \xrightarrow{\text{ITA}\circ\text{QKD}\circ\text{ITA}\circ\text{OTP}} \text{SEC}$??

$[\text{AUT}, \text{QC}] \xrightarrow{\text{QKD}\circ\text{OTP}} \text{SEC}$

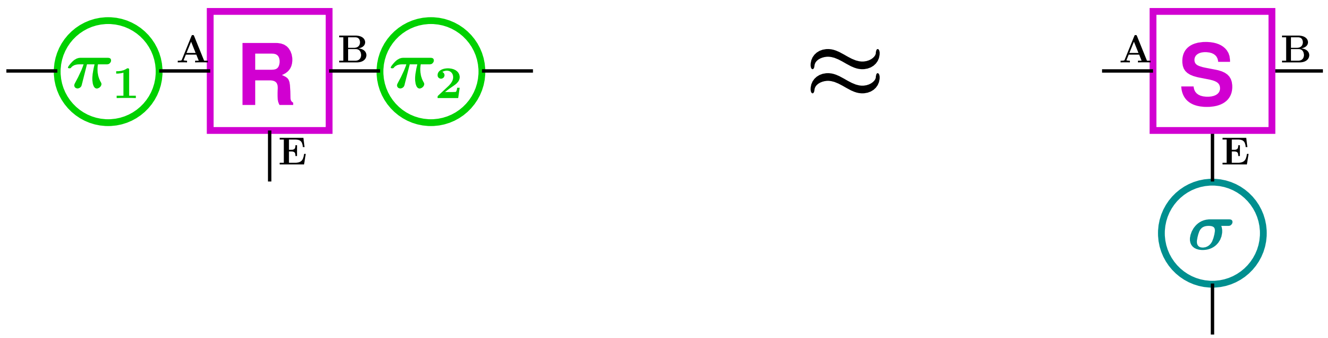
Attention: Quantum Key Distribution, though proven secure, did not compose before 2005 [KRBM07,Renner05]

Proof of composition (for ABE-setting)

Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

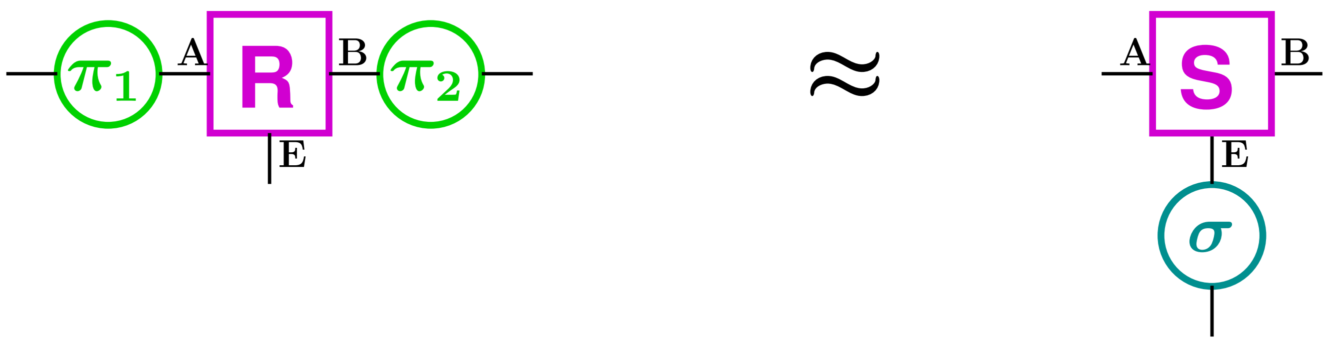
$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$

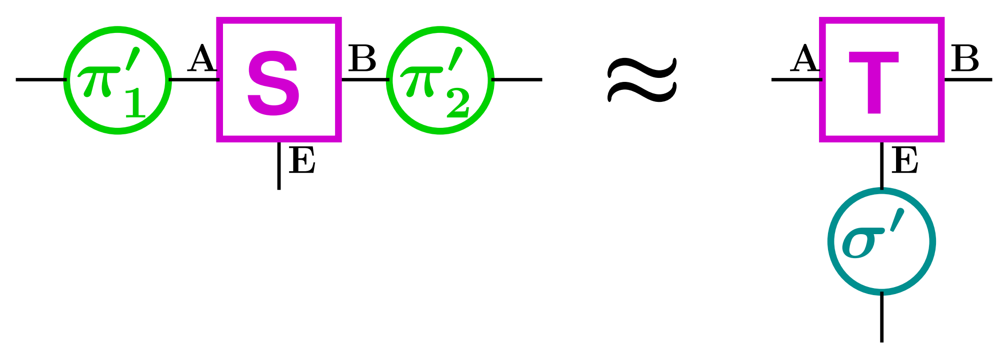


Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

$$\mathsf{R} \xrightarrow{\alpha} \mathsf{S} \ \wedge\ \mathsf{S} \xrightarrow{\beta} \mathsf{T} \ \Rightarrow\ \mathsf{R} \xrightarrow{\alpha\circ\beta} \mathsf{T}$$

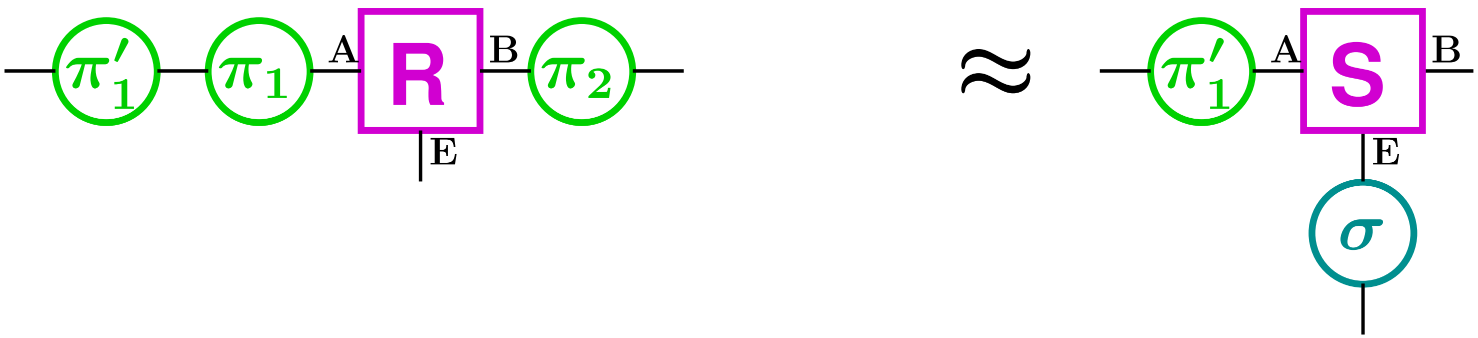


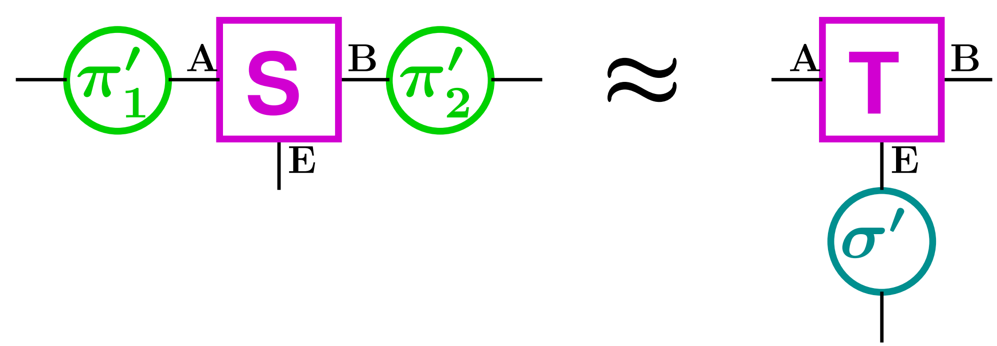


Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

$$\mathsf{R} \xrightarrow{\alpha} \mathsf{S} \;\wedge\; \mathsf{S} \xrightarrow{\beta} \mathsf{T} \;\Rightarrow\; \mathsf{R} \xrightarrow{\alpha\circ\beta} \mathsf{T}$$

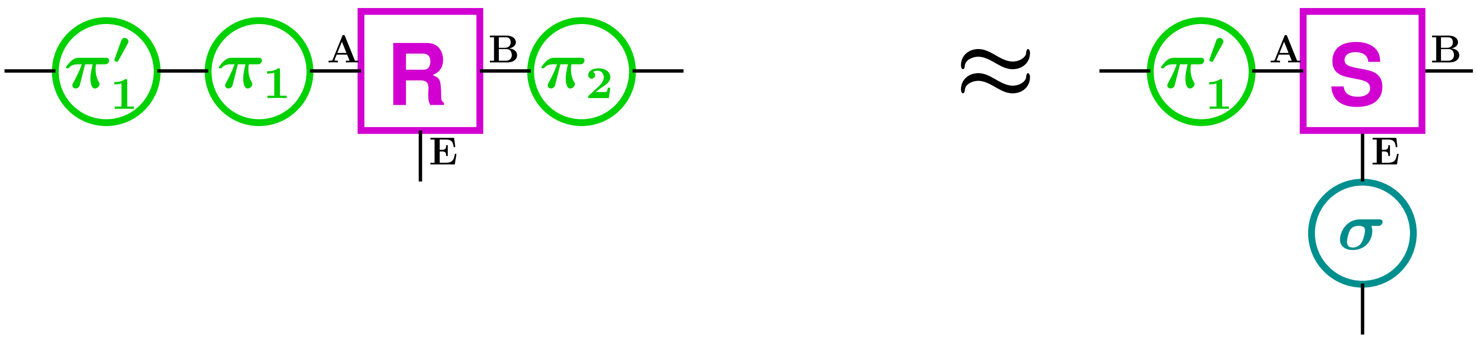




Proof of composition (for ABE-setting)

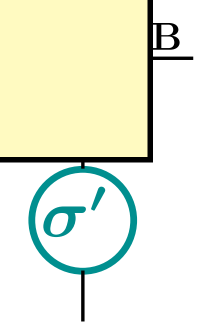
Definition: A construction is **composable** if

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$



Pseudo-metric **d** on Φ is **non-expanding** if

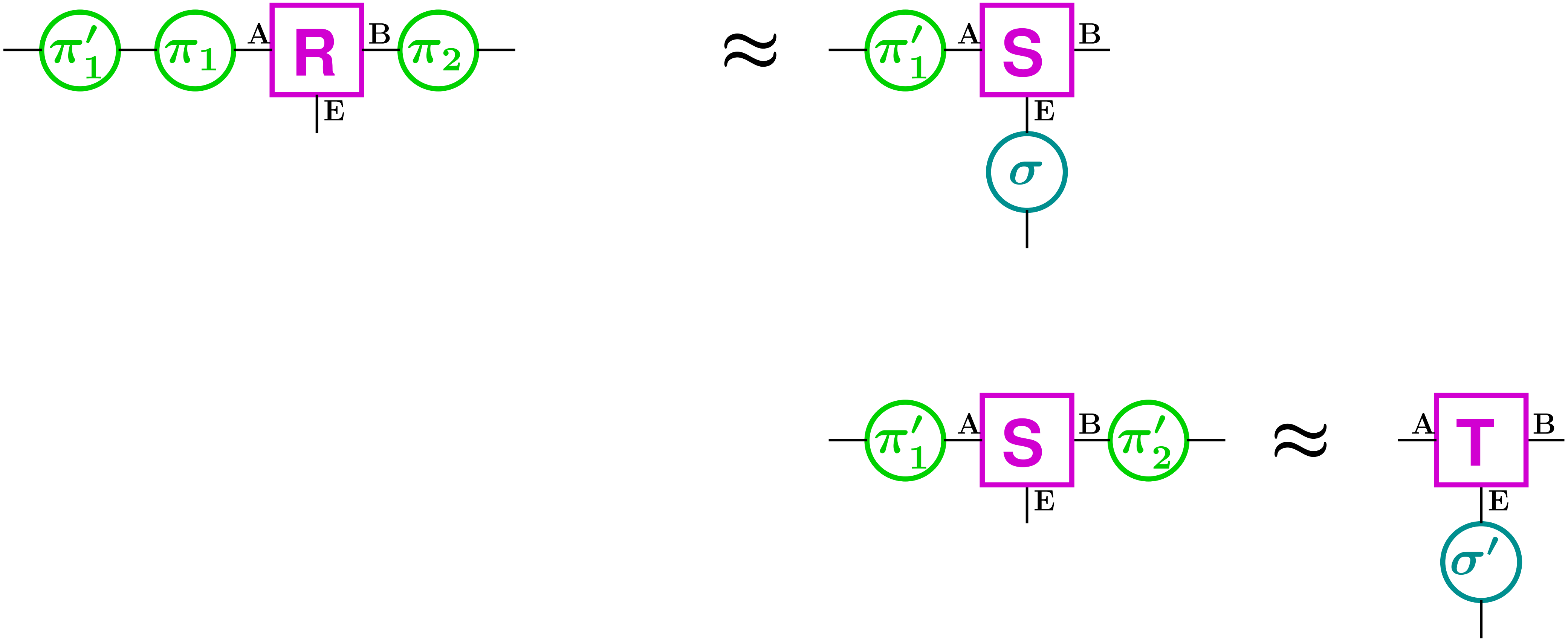
$$\mathbf{d}(\gamma^i\mathbf{R},\gamma^i\mathbf{S}) \;\leq\; \mathbf{d}(\mathbf{R},\mathbf{S})$$



Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

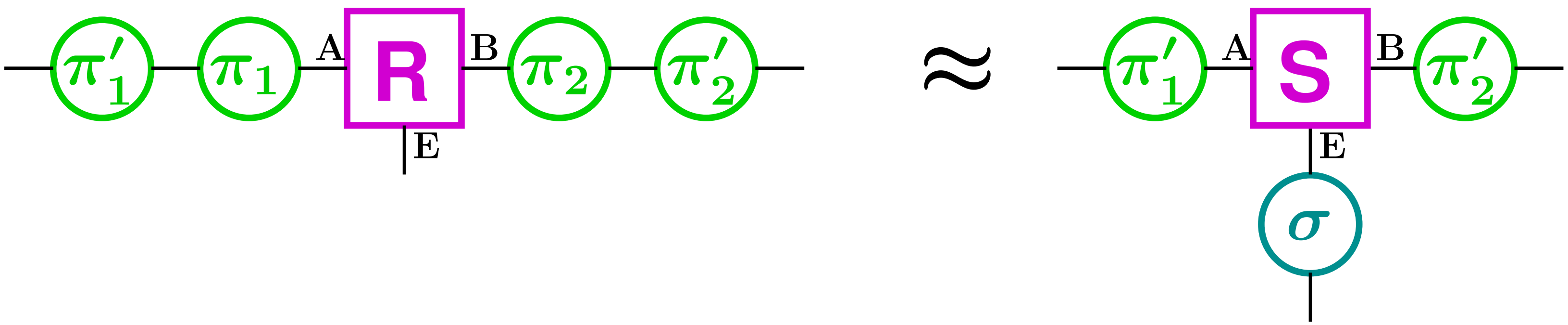
$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$

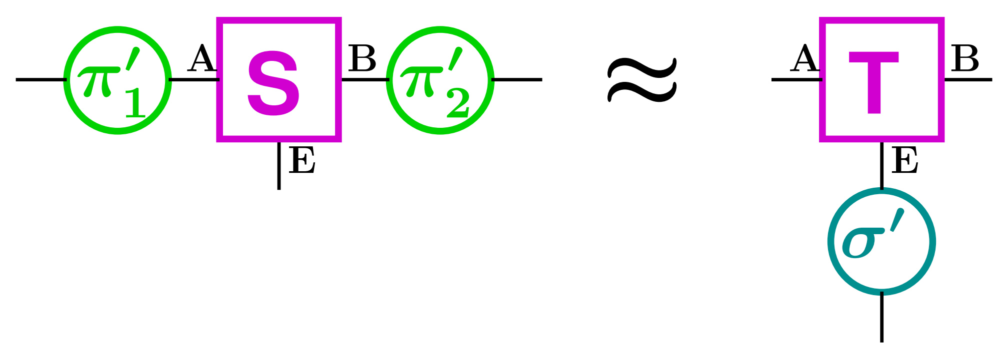


Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

$$\mathsf{R} \xrightarrow{\alpha} \mathsf{S} \;\wedge\; \mathsf{S} \xrightarrow{\beta} \mathsf{T} \;\Rightarrow\; \mathsf{R} \xrightarrow{\alpha\circ\beta} \mathsf{T}$$

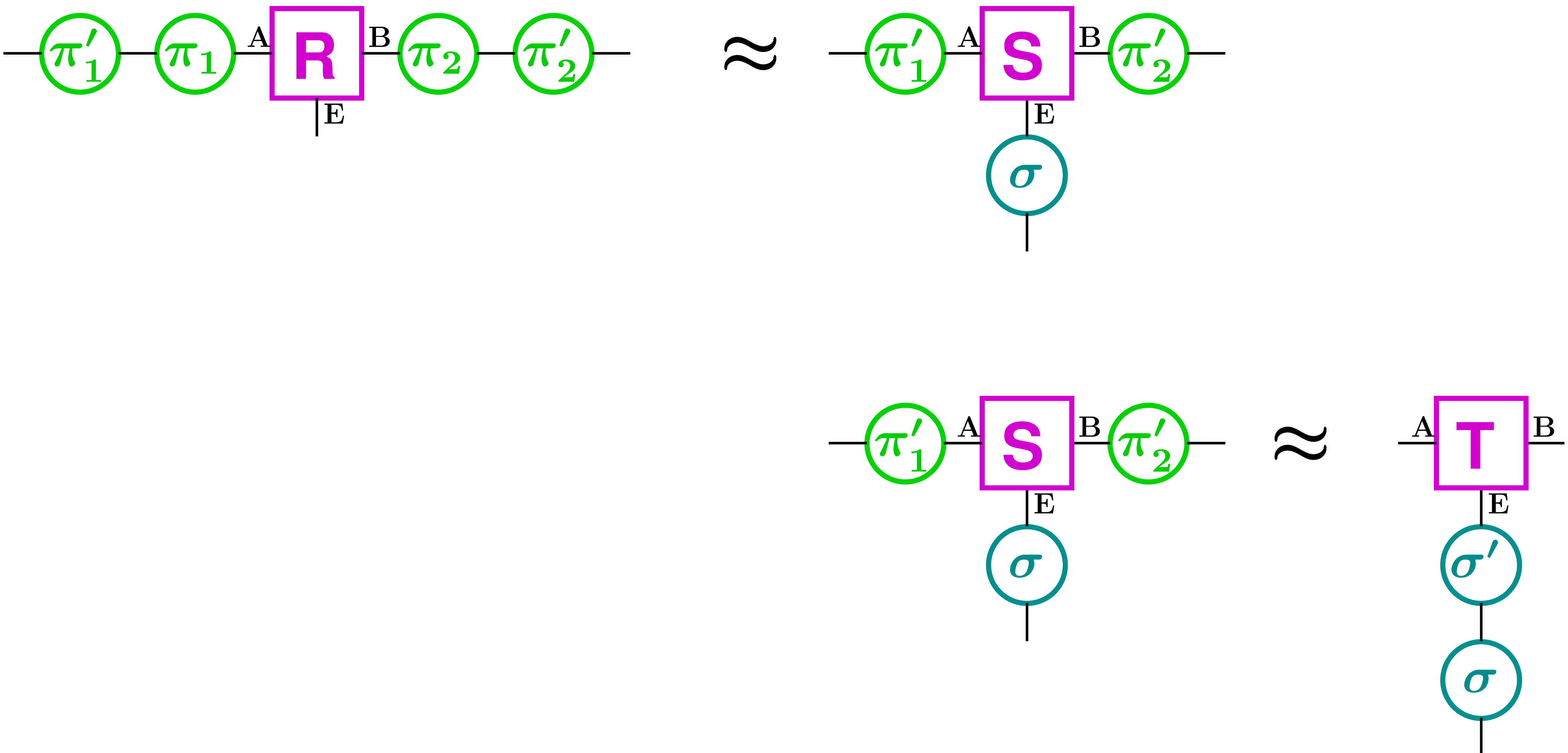




Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

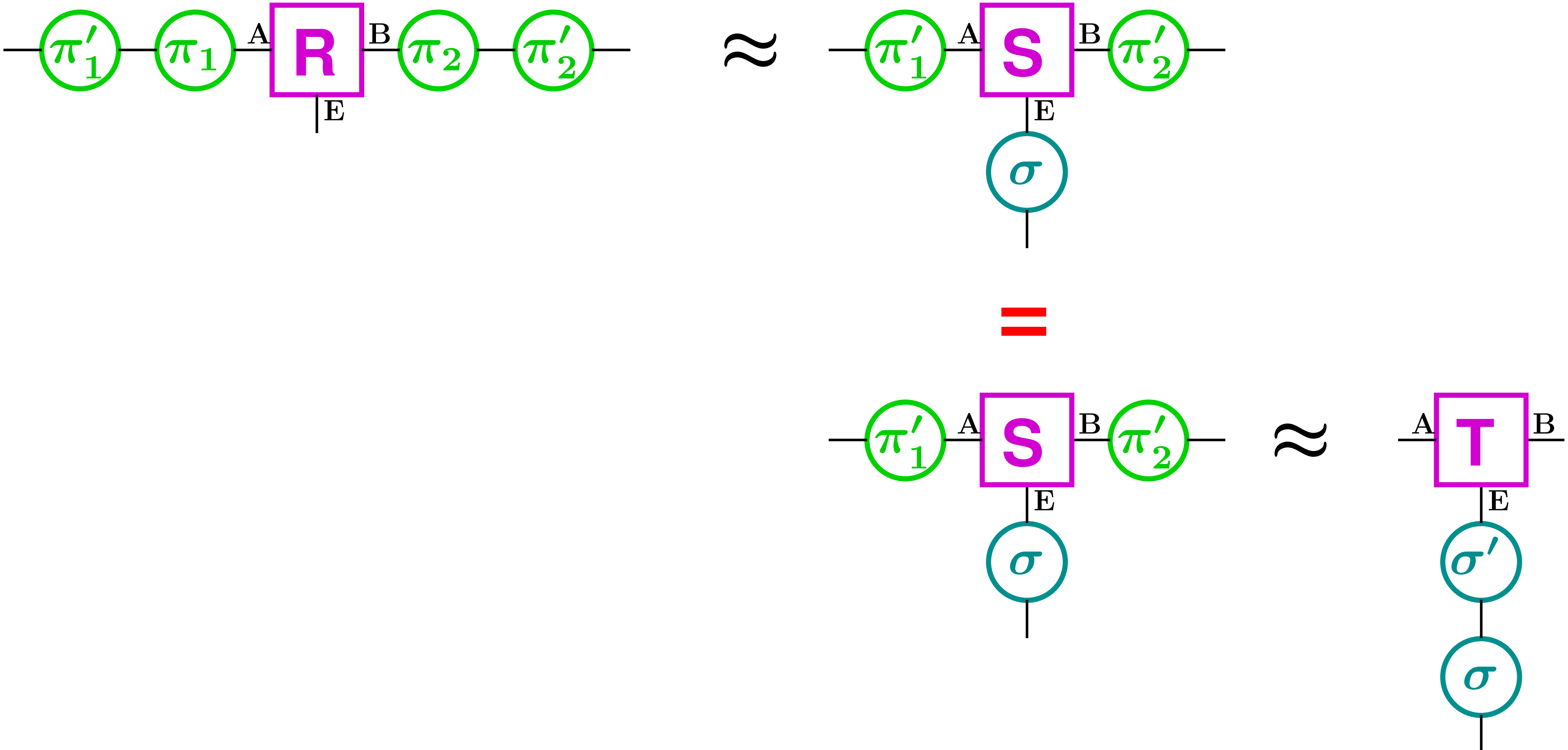
$$\mathsf{R} \xrightarrow{\alpha} \mathsf{S} \;\wedge\; \mathsf{S} \xrightarrow{\beta} \mathsf{T} \;\Rightarrow\; \mathsf{R} \xrightarrow{\alpha\circ\beta} \mathsf{T}$$



Proof of composition (for ABE-setting)

Definition: A construction is **composable** if

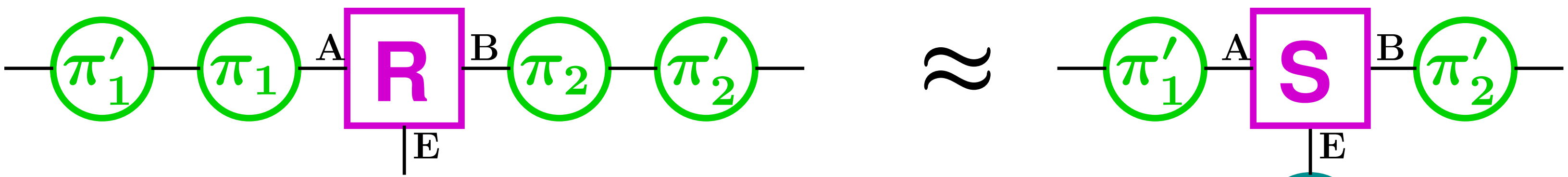
$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$



Proof of composition (for ABE-setting)

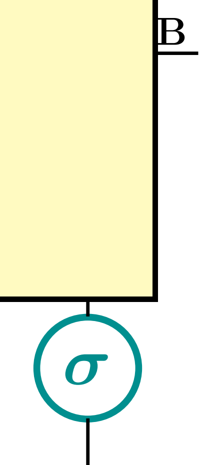
Definition: A construction is **composable** if

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$



Generalizations of the ABE-setting:

- n≠3 parties
- any party can be dishonest



Thank you!

U. Maurer, **Authentication Theory and Hypothesis Testing**, *IEEE Trans. on Information Theory, 2005,*

U. Maurer and R. Renner, **Abstract Cryptography**, *Second Symposium in Innovations in Computer Science, ICS 2011,*

U. Maurer, **Constructive cryptography – A new paradigm for security definitions and proofs**, *Theory of Security and Applications (TOSCA 2011)*.