Quantitative Security of Block Ciphers: Designs and Cryptanalysis Tools

Thomas Baignères

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

PhD Defense
November 14, 2008

Prologue

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Bob

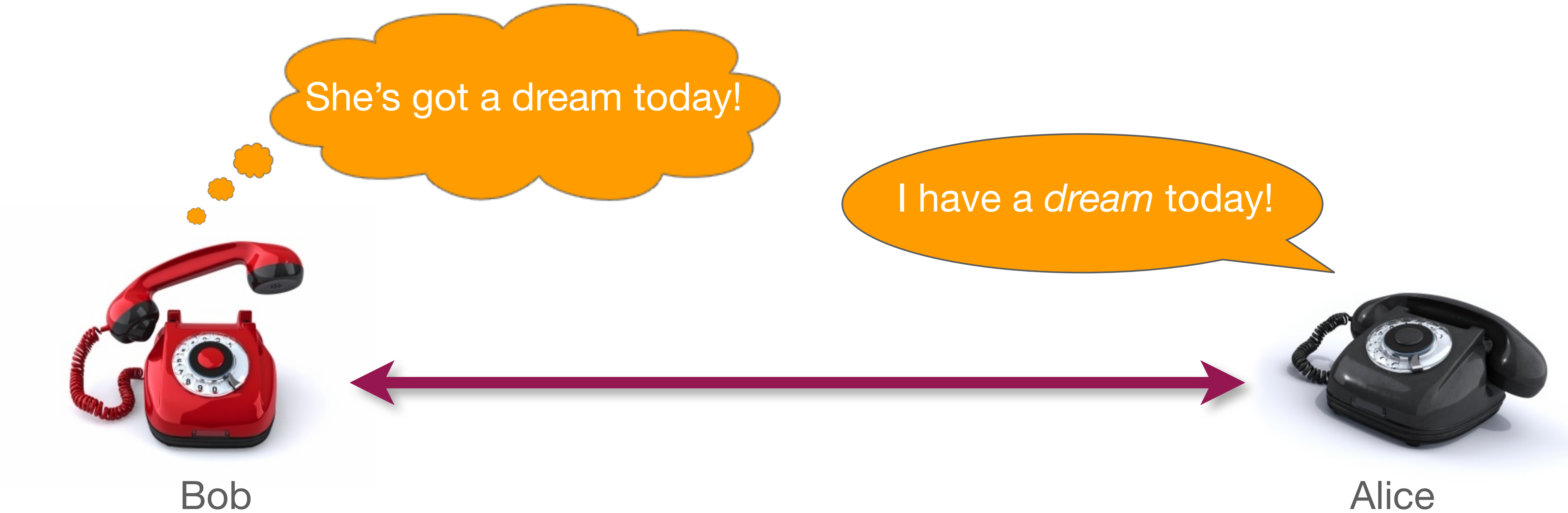
Alice

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

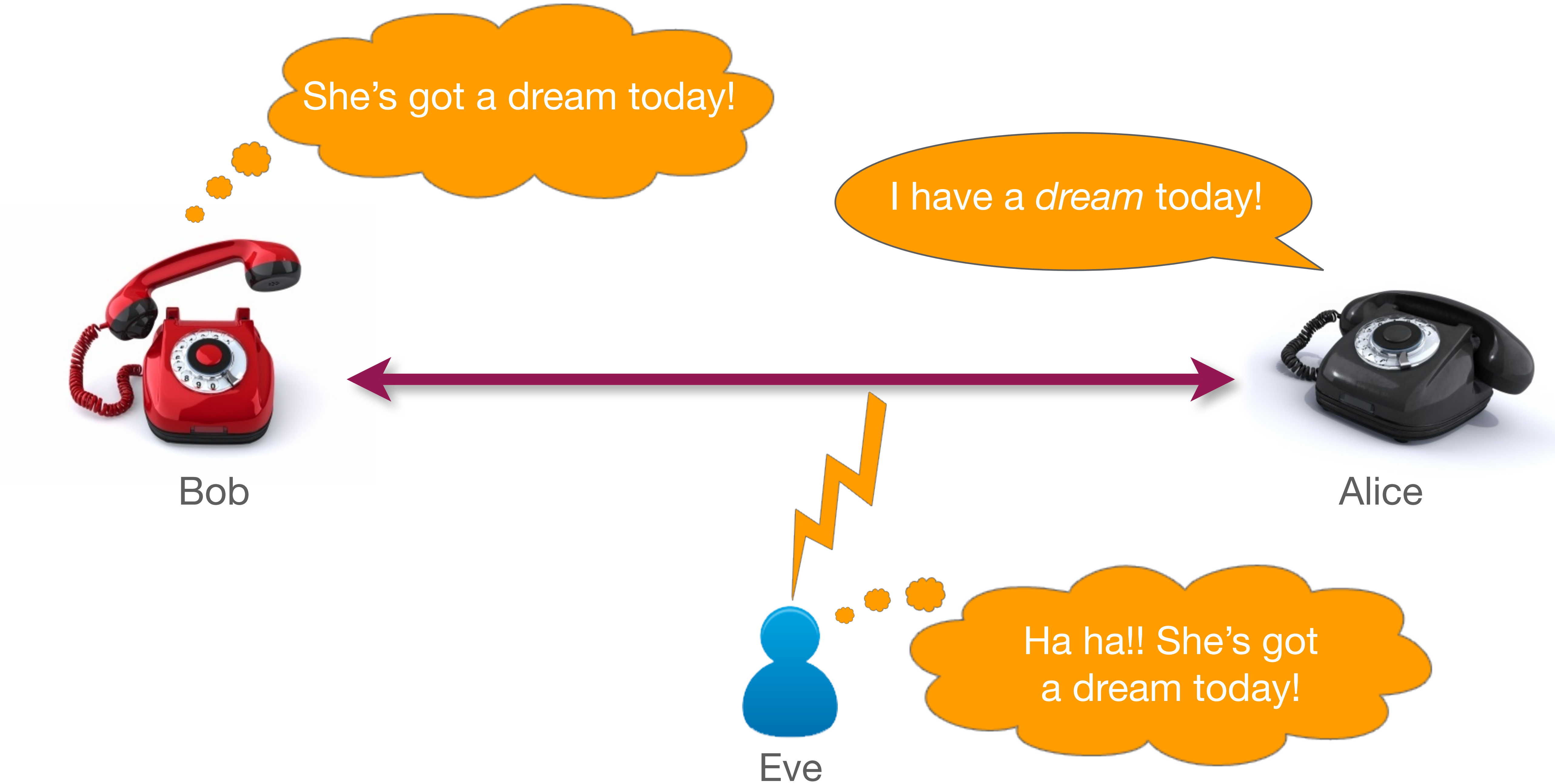
Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.



Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.



Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Bob

Alice

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Cryptography: the Basics

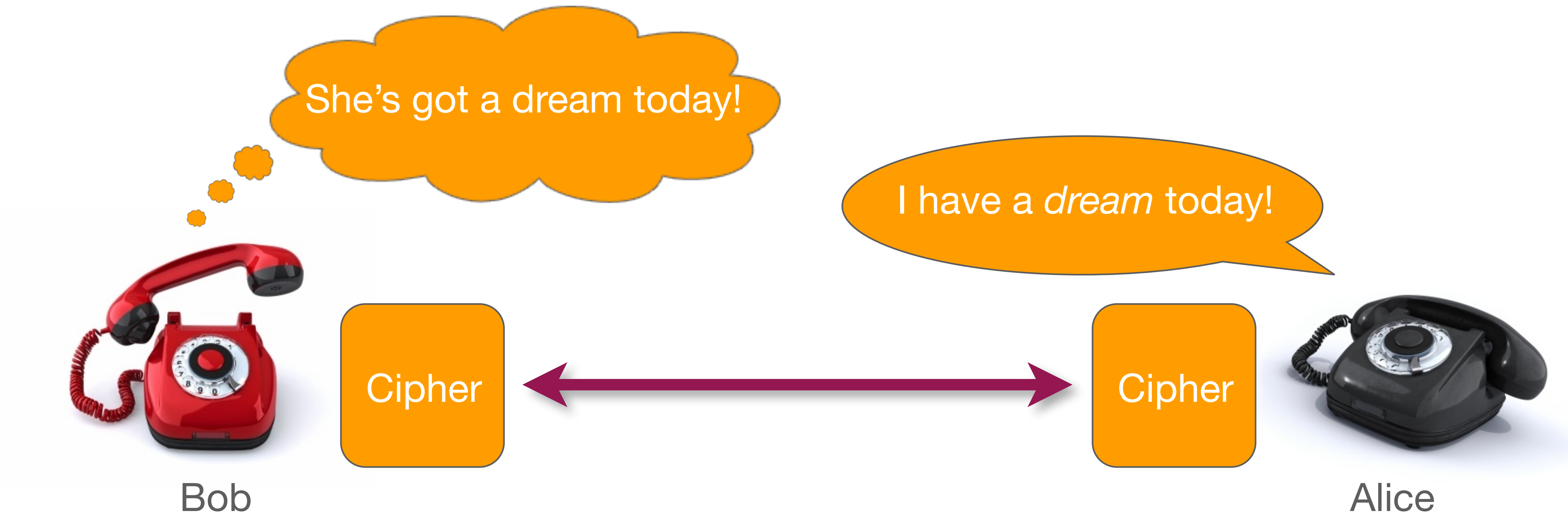
Originally, cryptography aims at ensuring confidentiality through an insecure channel.

Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.

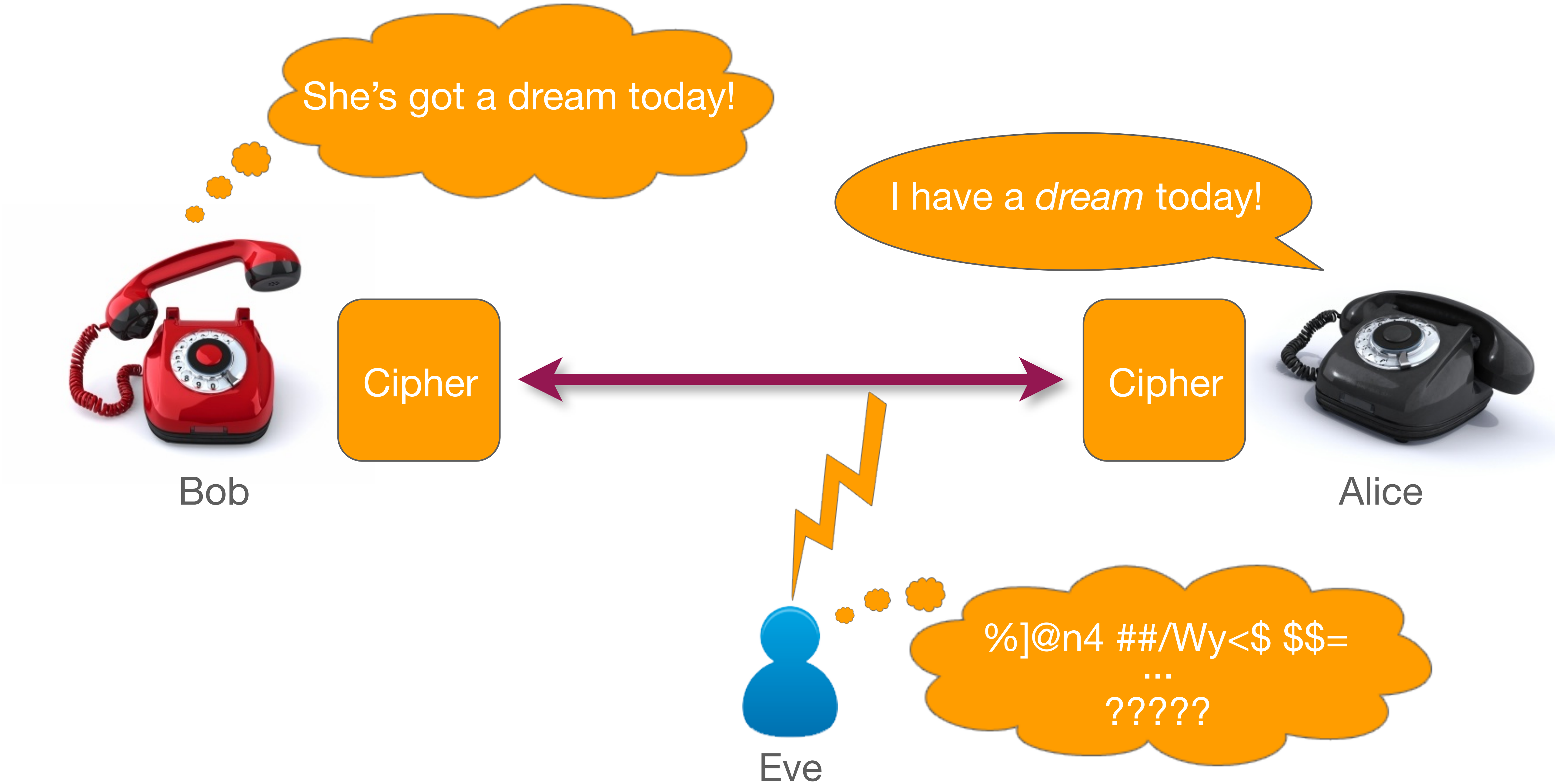
Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.



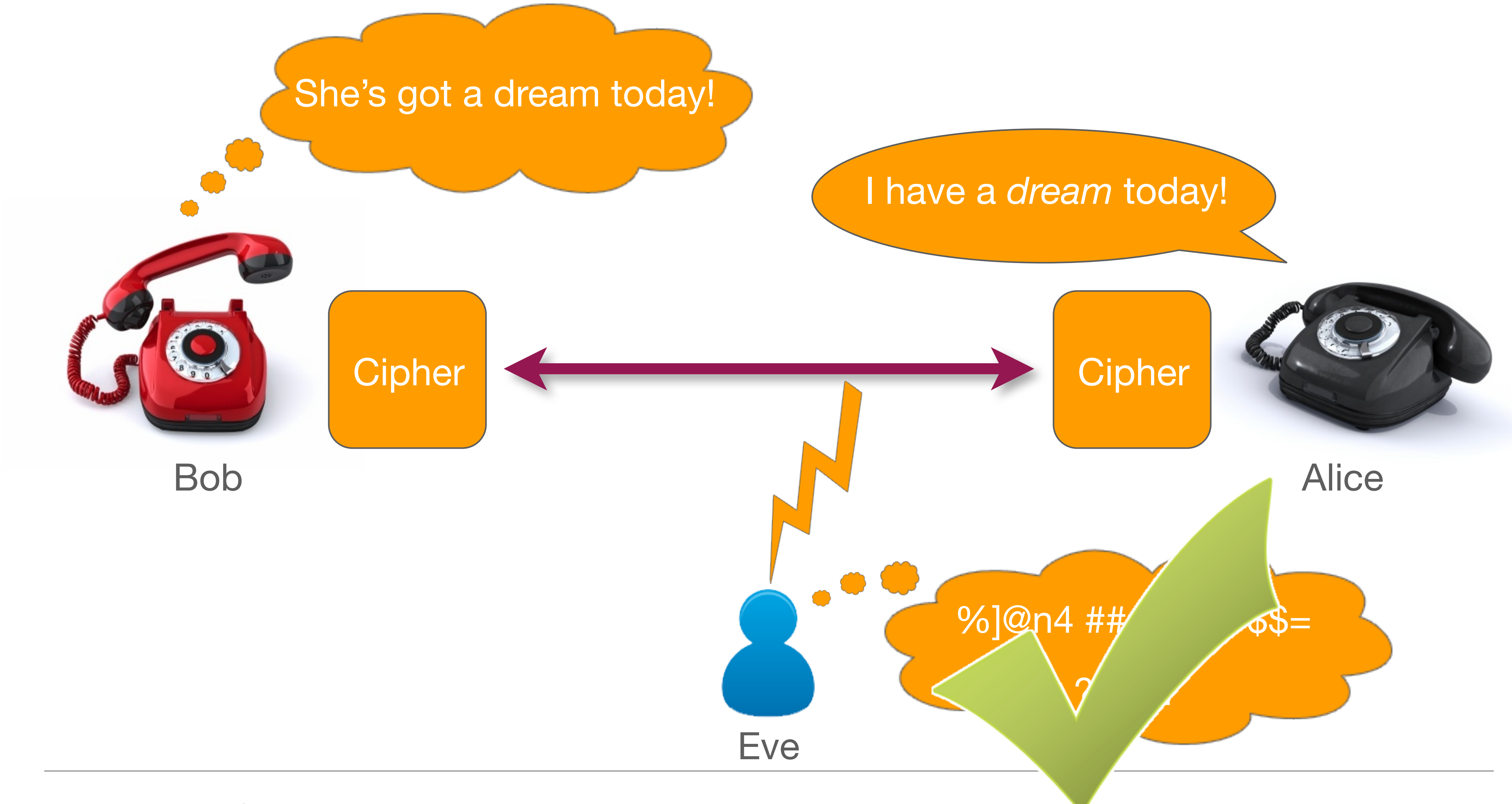
Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.



Cryptography: the Basics

Originally, cryptography aims at ensuring confidentiality through an insecure channel.



What should we expect from the cipher?

What should we expect from the cipher?

Intuitively, turning *%]@n4 ##/Wy<$ $$=* into *I have a dream today!* should be hard, except for Alice and Bob.

What should we expect from the cipher?

Intuitively, turning *%]@n4 ##/Wy<$ $$=* into *I have a dream today!* should be hard, except for Alice and Bob.

Fact: cryptographers are parnoïac ➡ they sometimes require more !

What should we expect from the cipher?

Intuitively, turning *%]@n4 ##/Wy<$ $$=* into *I have a dream today!* should be hard, except for Alice and Bob.

Fact: cryptographers are parnoïac → they sometimes require more !

I have a dream today! → Cipher → *%]@n4 ##/Wy<$ $$=*

What should we expect from the cipher?

Intuitively, turning *%]@n4 ##/Wy<$ $$=* into *I have a dream today!* should be hard, except for Alice and Bob.

Fact: cryptographers are parnoïac → they sometimes require more !

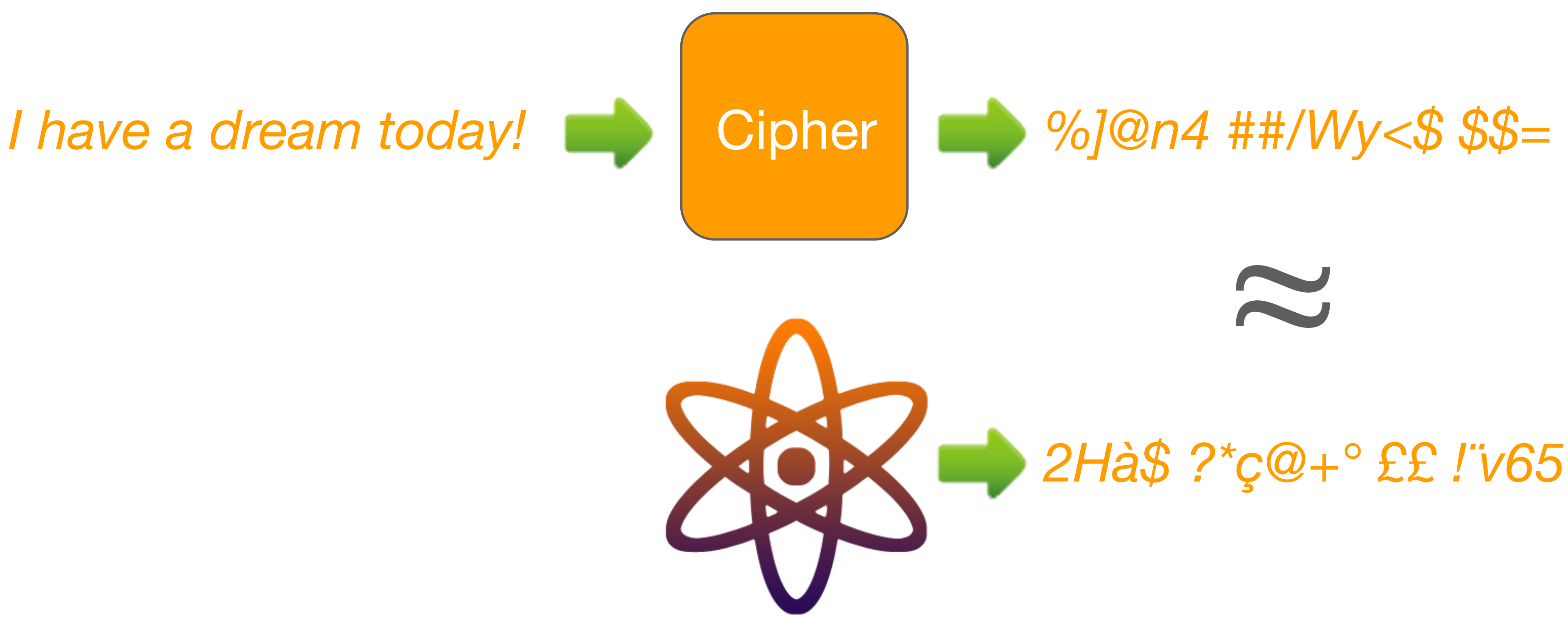
I have a dream today! → Cipher → *%]@n4 ##/Wy<$ $$=*

 → *2Hà$?*ç@+° ££ !¨v65*

What should we expect from the cipher?

Intuitively, turning *%]@n4 ##/Wy<$ $$=* into *I have a dream today!* should be hard, except for Alice and Bob.

Fact: cryptographers are parnoïac ➡ they sometimes require more !



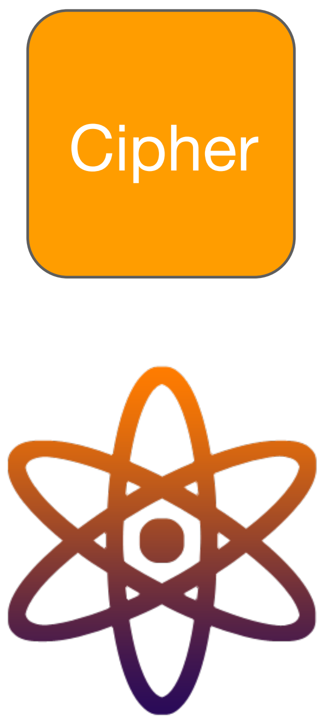
It should be hard for Eve to guess wether she's looking at an encrypted message (ciphertext) or to pure rubish (random string).

The security requirements in terms of a game...

... or “Cryptographers will never grow up”.

The security requirements in terms of a game...

... or “Cryptographers will never grow up”.



The security requirements in terms of a game...

... or “Cryptographers will never grow up”.

The security requirements in terms of a game...

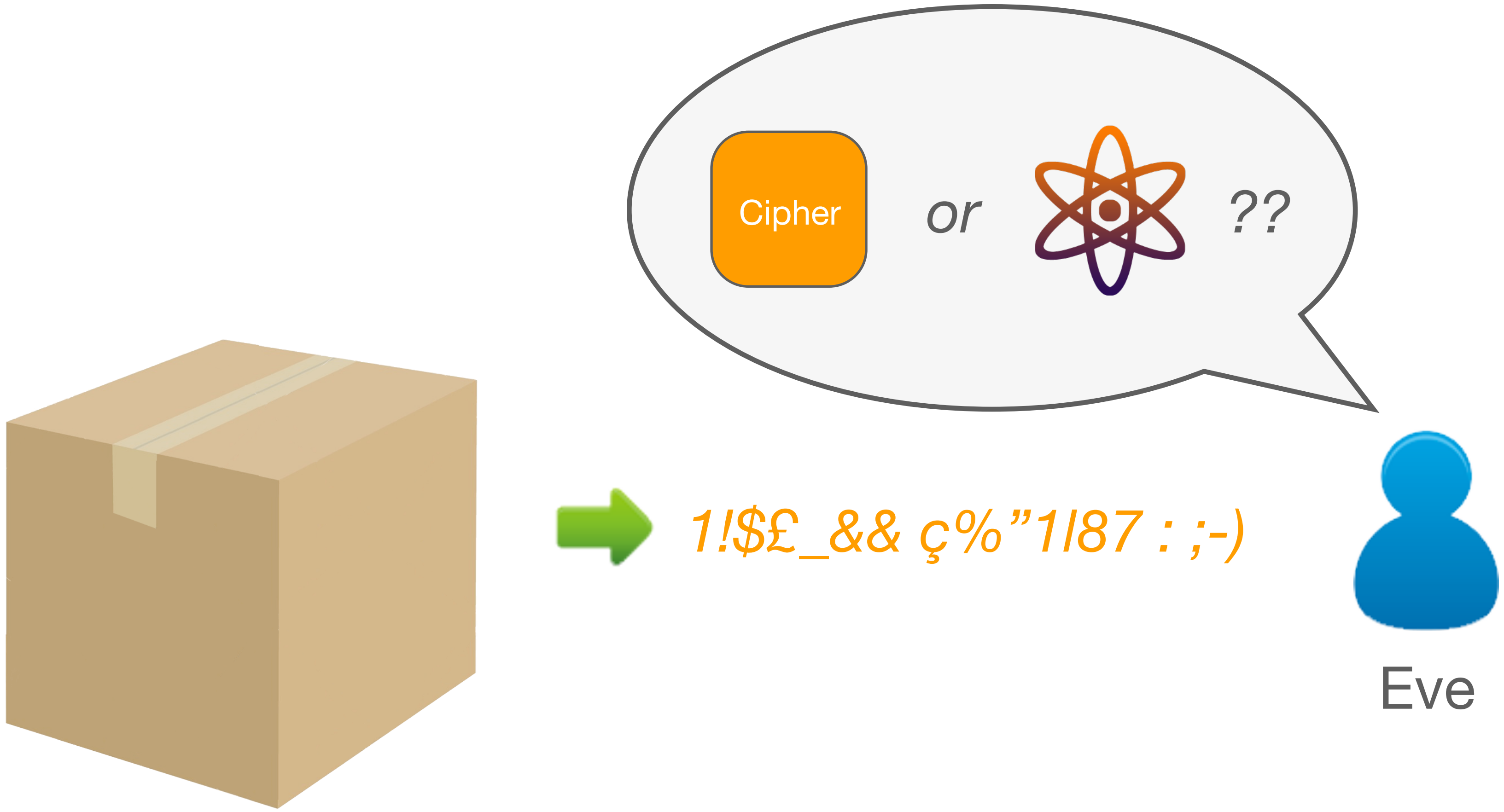
... or "Cryptographers will never grow up".

The security requirements in terms of a game...

... or "Cryptographers will never grow up".

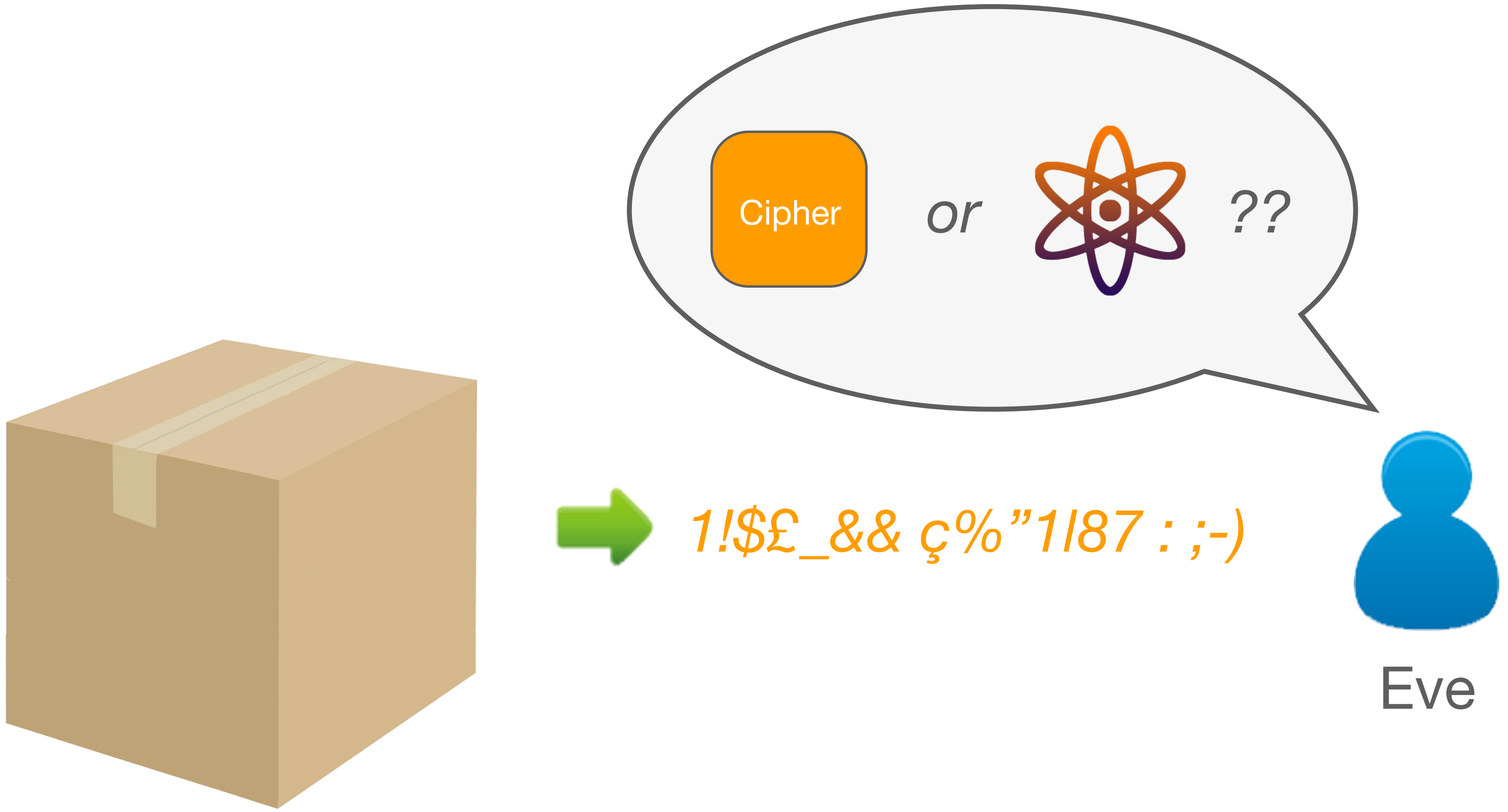
The security requirements in terms of a game...

... or “Cryptographers will never grow up”.



The security requirements in terms of a game...

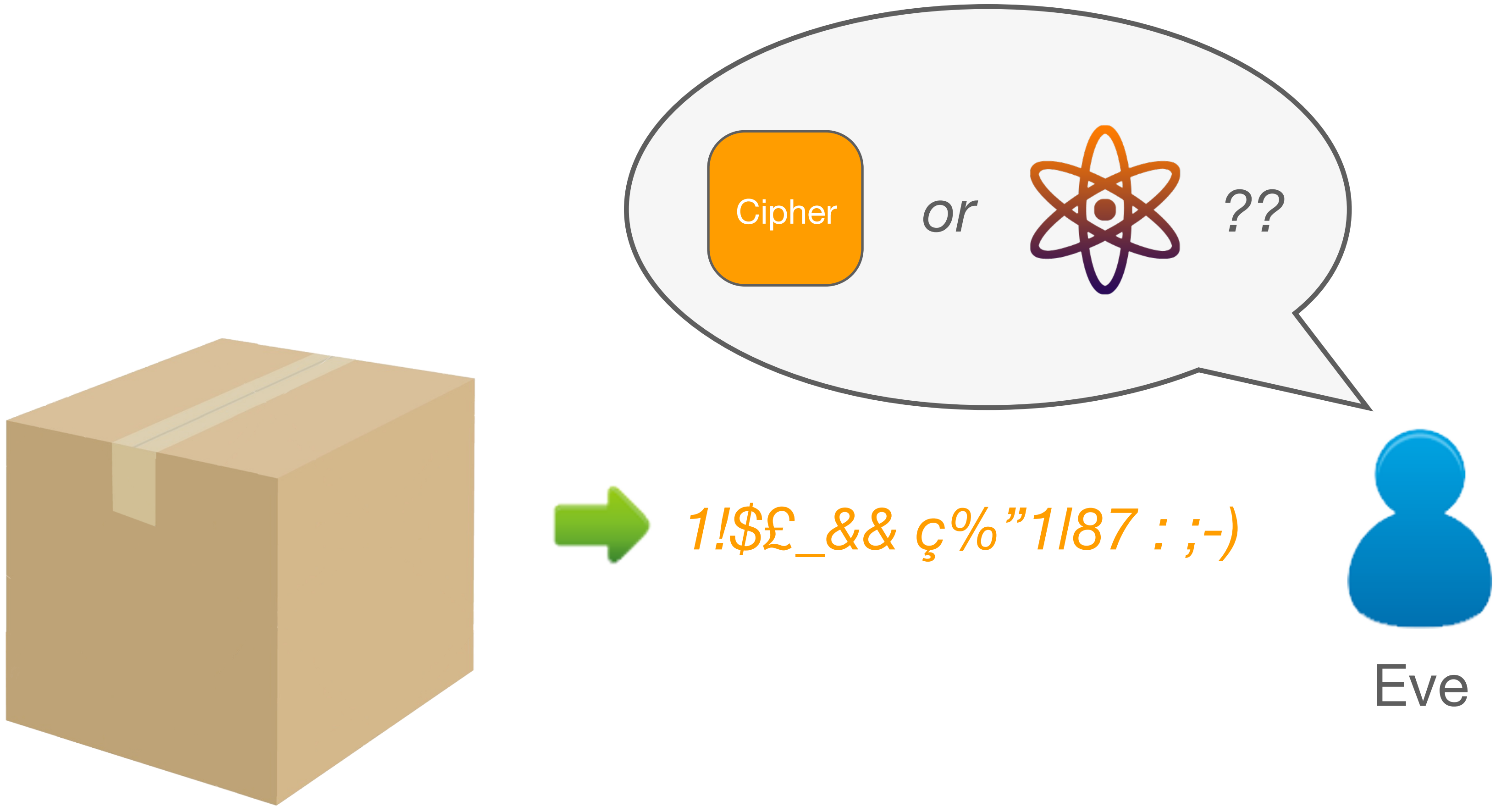
... or “Cryptographers will never grow up”.



- Eve wins if she guesses correctly.

The security requirements in terms of a game...

... or “Cryptographers will never grow up”.



- Eve wins if she guesses correctly.
- Objective for the cryptographer: make sure that Eve cannot do better than guessing correctly 50% of the time.

Part I: On the (In)Security of Block Ciphers: Tools for the Security Analysis

Outline

Distinguishers between two sources

Projection-based distinguishers
between two sources

Practical Implications for block ciphers

Outline

- Distinguishers between two sources
- Projection-based distinguishers between two sources
- Practical Implications for block ciphers

- The game: distinguishing between two sources of randomness
- The optimal solution
- Complexity analysis: How many samples do we need to distinguish with a given efficiency?

Outline

Distinguishers between two sources

Projection-based distinguishers between two sources

Practical Implications for block ciphers

- What if the optimal solution cannot be implemented?
- Distinguishing in practice using compression
- Example: Generalized linear distinguisher

Outline

Distinguishers between two sources

Projection-based distinguishers between two sources

Practical Implications for block ciphers

- Cryptanalysis of SAFER K/SK
- DEAN

Outline

- Distinguishers between two sources
- Projection-based distinguishers between two sources
- Practical Implications for block ciphers
  - Cryptanalysis of SAFER K/SK
  - DEAN

[BJVa04] [BSVsac07] [BVicits08]

Part I: On the (In)Security of Block Ciphers:
Tools for the Security Analysis

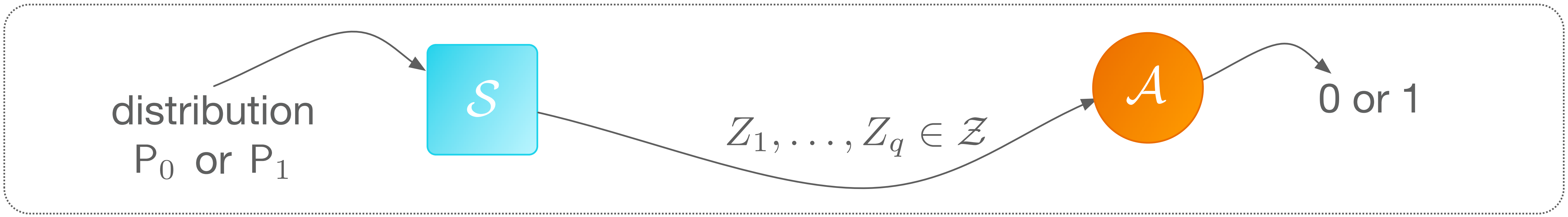
- Distinguisher between two Sources

The Game

- P_0 and P_1 are two arbitrary distributions over a finite set $\mathcal{Z}$.

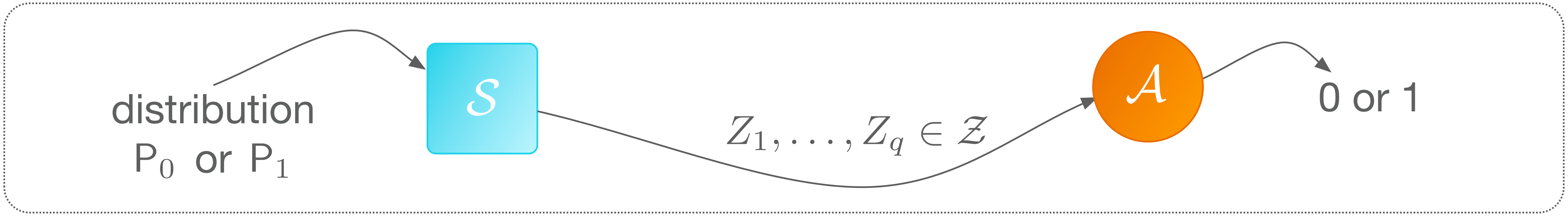
The Game

- P_0 and P_1 are two arbitrary distributions over a finite set $\mathcal{Z}$.



The Game

- P_0 and P_1 are two arbitrary distributions over a finite set $\mathcal{Z}$.



- The ability of $\mathcal{A}$ to distinguish P_0 from P_1 is its advantage:

$$\mathrm{Adv}_{\mathcal{A}}(\mathsf{P}_0, \mathsf{P}_1) = \left|\Pr_{\mathsf{P}_0}[\mathcal{A}(Z_1, \ldots, Z_q) = 1] - \Pr_{\mathsf{P}_1}[\mathcal{A}(Z_1, \ldots, Z_q) = 1]\right|$$

Example: Biased Dice

Example: Biased Dice

Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

Example: Biased Dice

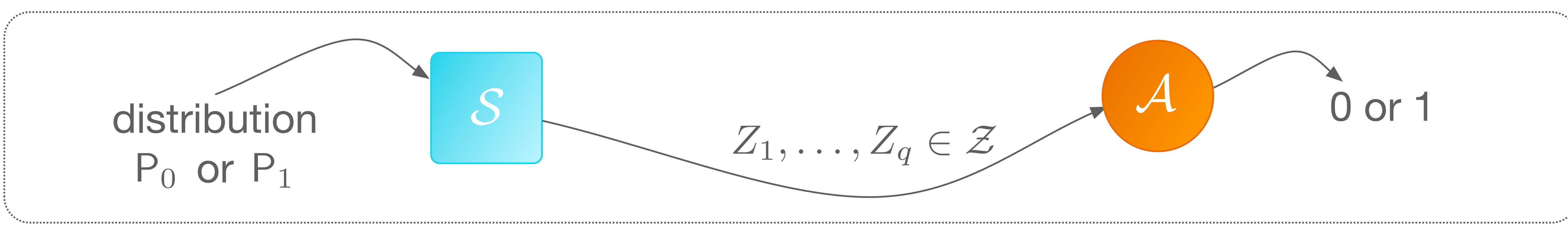
$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

$\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$

Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

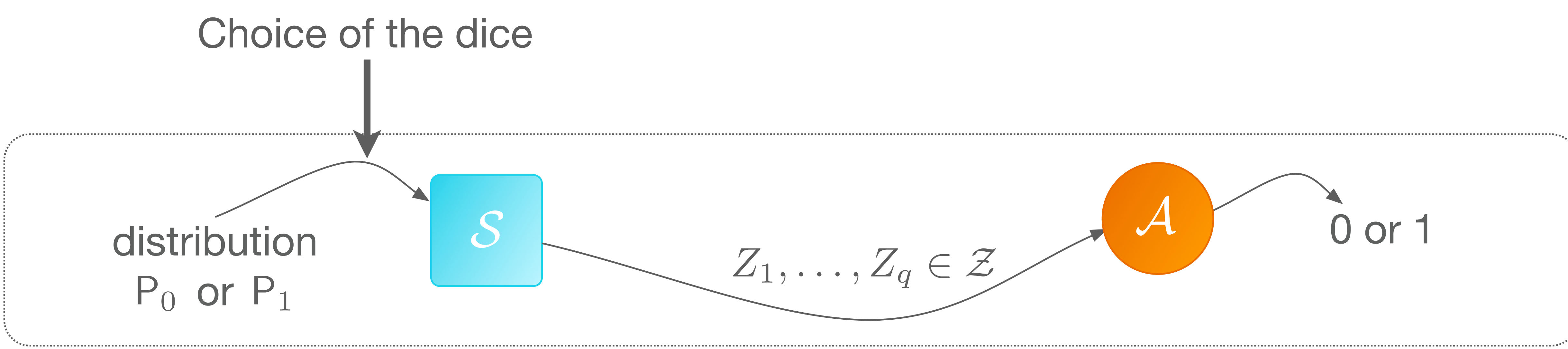
$\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$



Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

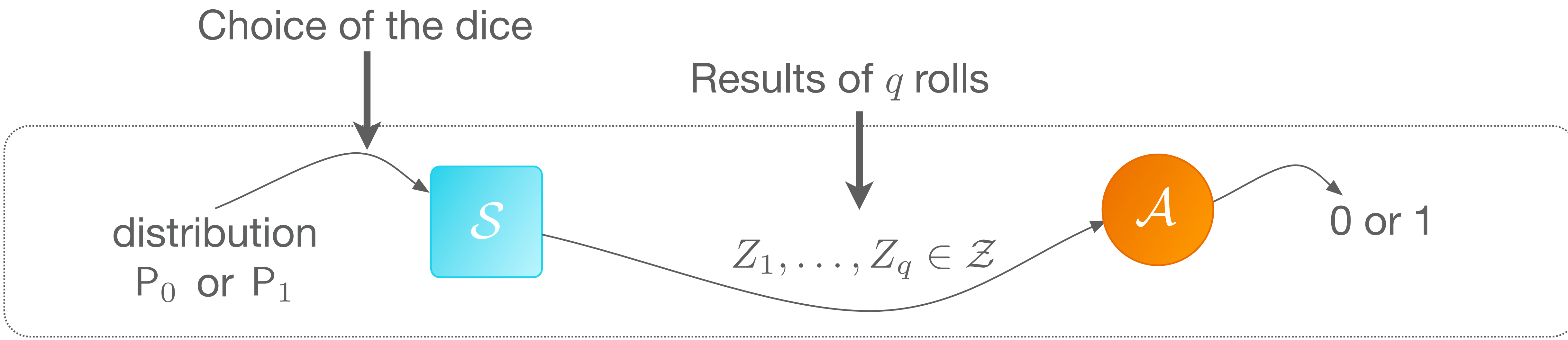
$\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$



Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

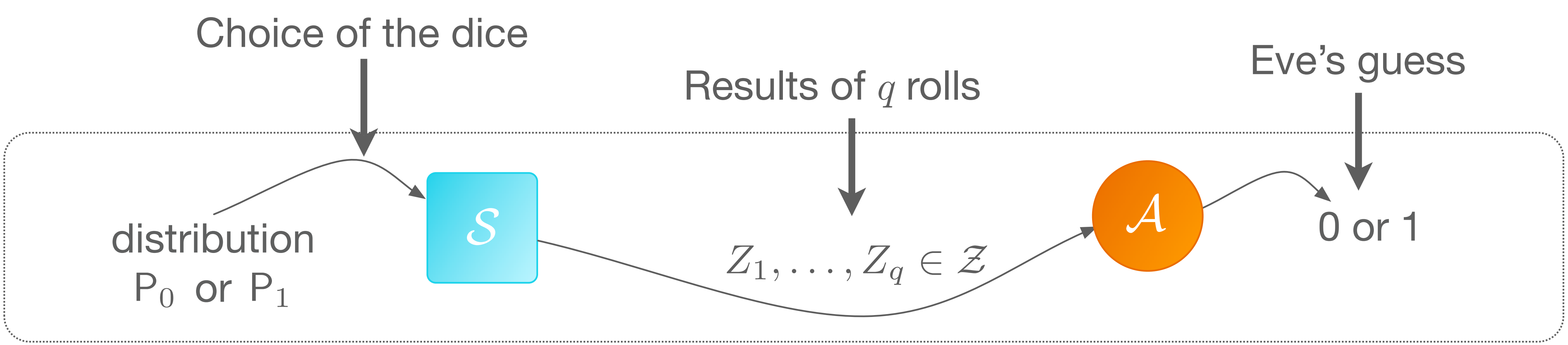
$\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$



Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$

$\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$



An Optimal Distinguisher

Using maximum-likelihood techniques, the q-limited distinguisher $\mathcal{A}^\star$ which outputs 1 when by

$$\boxed{\mathrm{D}(\mathsf{P}\|\mathsf{P}_1) \leq \mathrm{D}(\mathsf{P}\|\mathsf{P}_0)}$$

can be shown to be optimal.

An Optimal Distinguisher

Using maximum-likelihood techniques, the q-limited distinguisher $\mathcal{A}^\star$ which outputs 1 when by

$$\boxed{\mathrm{D}(\mathsf{P}\|\mathsf{P}_1) \leq \mathrm{D}(\mathsf{P}\|\mathsf{P}_0)}$$

can be shown to be optimal.

$$\left(\mathrm{D}(p\|q) = \sum_{a \in \mathcal{Z}} p[a] \log \frac{p[a]}{q[a]} \right)$$

always non-negative, 0 iff $p=q$, infinite iff $\mathsf{Supp}(p) \not\subseteq \mathsf{Supp}(q)$

Data Complexity Analysis

Using the theory of types & Sanov's theorem asymptotic data complexity of $\mathcal{A}^{\star}$.

Data Complexity Analysis

Using the theory of types & Sanov's theorem ➡ asymptotic data complexity of $\mathcal{A}^\star$.

Data Complexity Analysis

Using the theory of types & Sanov's theorem ➡ asymptotic data complexity of $\mathcal{A}^\star$.

Theorem

Let P_0 and P_1 be two distributions s.t. $\mathrm{Supp}(\mathsf{P}_0) \cup \mathrm{Supp}(\mathsf{P}_1) = \mathcal{Z}$. The advantage of $\mathcal{A}^\star$ verifies

$$\boxed{1 - \mathrm{BestAdv}_q(\mathsf{P}_0, \mathsf{P}_1) \doteq 2^{-q\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1)}}$$

where

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = - \inf_{0<\lambda<1} \log \sum_{a \in \mathsf{Supp}(\mathsf{P}_0) \cap \mathsf{Supp}(\mathsf{P}_1)} \mathsf{P}_0[a]^{1-\lambda} \mathsf{P}_1[a]^{\lambda}$$

is the Chernoff information between P_0 and P_1.

Data Complexity Analysis

Using the theory of types & Sanov's theorem ➡ asymptotic data complexity of $\mathcal{A}^\star$.

Theorem

Let P_0 and P_1 be two distributions s.t. $\mathrm{Supp}(\mathsf{P}_0) \cup \mathrm{Supp}(\mathsf{P}_1) = \mathcal{Z}$. The advantage of $\mathcal{A}^\star$ verifies

$$\boxed{1 - \mathrm{BestAdv}_q(\mathsf{P}_0, \mathsf{P}_1) \doteq 2^{-q\mathrm{C}(\mathsf{P}_0,\mathsf{P}_1)}}$$

where

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = -\inf_{0<\lambda<1} \log \sum_{a \in \mathsf{Supp}(\mathsf{P}_0) \cap \mathsf{Supp}(\mathsf{P}_1)} \mathsf{P}_0[a]^{1-\lambda} \mathsf{P}_1[a]^\lambda$$

is the Chernoff information between P_0 and P_1.

Notation: $f(q) \doteq g(q)$ means that $f(q) = g(q)e^{o(q)}$, i.e., $\lim_{q\to\infty} \frac{1}{q} \log \frac{f(q)}{g(q)} = 0$.

Data Complexity Analysis

Using the theory of types & Sanov's theorem ➡ asymptotic data complexity of $\mathcal{A}^\star$.

Theorem

Let P_0 and P_1 be two distributions s.t. $\mathrm{Supp}(\mathsf{P}_0) \cup \mathrm{Supp}(\mathsf{P}_1) = \mathcal{Z}$. The advantage of $\mathcal{A}^\star$ verifies

$$\boxed{1 - \mathrm{BestAdv}_q(\mathsf{P}_0, \mathsf{P}_1) \doteq 2^{-q\mathrm{C}(\mathsf{P}_0,\mathsf{P}_1)}}$$

where

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) \approx \frac{\|\mathsf{P}_1 - \mathsf{P}_0\|_2^2}{8 \ln 2}$$

is the Chernoff information between P_0 and P_1.

Notation: $f(q) \doteq g(q)$ means that $f(q) = g(q)e^{o(q)}$, i.e., $\lim_{q\to\infty} \frac{1}{q} \log \frac{f(q)}{g(q)} = 0$.

Data Complexity Analysis

Using the theory of types & Sanov's theorem ➡ asymptotic data complexity of $\mathcal{A}^\star$.

Theorem

Let P_0 and P_1 be two distributions s.t. $\mathrm{Supp}(\mathsf{P}_0) \cup \mathrm{Supp}(\mathsf{P}_1) = \mathcal{Z}$. The advantage of $\mathcal{A}^\star$ verifies

$$\boxed{1 - \mathrm{BestAdv}_q(\mathsf{P}_0, \mathsf{P}_1) \approx 2^{-q\mathrm{C}(\mathsf{P}_0,\mathsf{P}_1)}}$$

where

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) \approx \frac{\|\mathsf{P}_1 - \mathsf{P}_0\|_2^2}{8 \ln 2}$$

is the Chernoff information between P_0 and P_1.

Data Complexity Analysis

Using the theory of types & Sanov's theorem asymptotic data complexity of $\mathcal{A}^\star$.

Theorem

Let P_0 and P_1 be two distributions s.t. $\mathrm{Supp}(\mathrm{P}_0) \cup \mathrm{Supp}(\mathrm{P}_1)$ … age of $\mathcal{A}^\star$ verifies

$1 - \mathrm{BestAdv}$ …

where

…

is the … information between P_0 and P_1.

Heuristic: $q \approx 1/\mathrm{C}(\mathrm{P}_0, \mathrm{P}_1)$ allows $\mathcal{A}^\star$ to reach a non-negligible advantage

Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$ $\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$

Example: Biased Dice

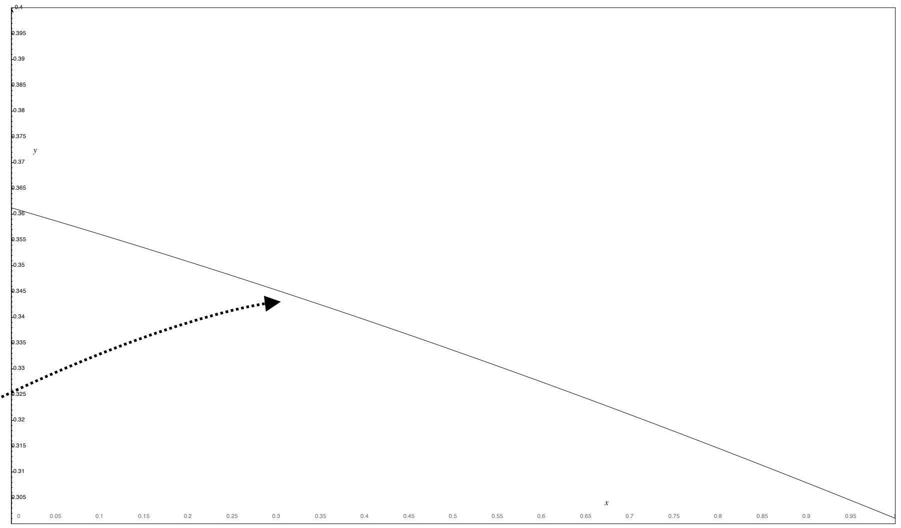
$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$ $\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = \max_{0<\lambda<1} \log\left(\frac{6}{2^{\lambda}+4}\right)$$

Example: Biased Dice

$$\mathsf{P}_0 = (\tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}) \qquad \mathsf{P}_1 = (\tfrac{1}{6}, \tfrac{1}{6}, \tfrac{2}{6}, 0, \tfrac{1}{6}, \tfrac{1}{6})$$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = \max_{0<\lambda<1} \boxed{\log\left(\frac{6}{2^{\lambda}+4}\right)}$$

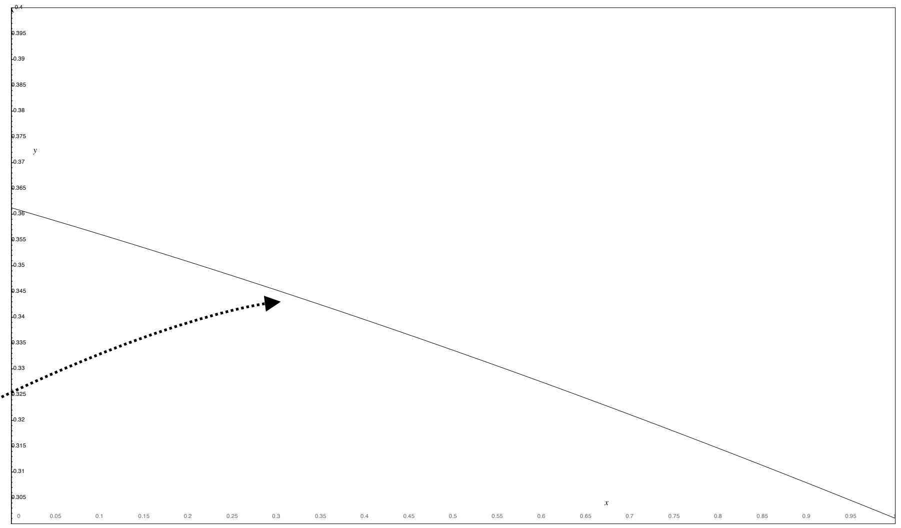


Example: Biased Dice

$$\mathsf{P}_0 = (\tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}, \tfrac{1}{6}) \qquad \mathsf{P}_1 = (\tfrac{1}{6}, \tfrac{1}{6}, \tfrac{2}{6}, 0, \tfrac{1}{6}, \tfrac{1}{6})$$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = \max_{0<\lambda<1} \log\left(\frac{6}{2^\lambda + 4}\right)$$

$$\approx 0.263$$

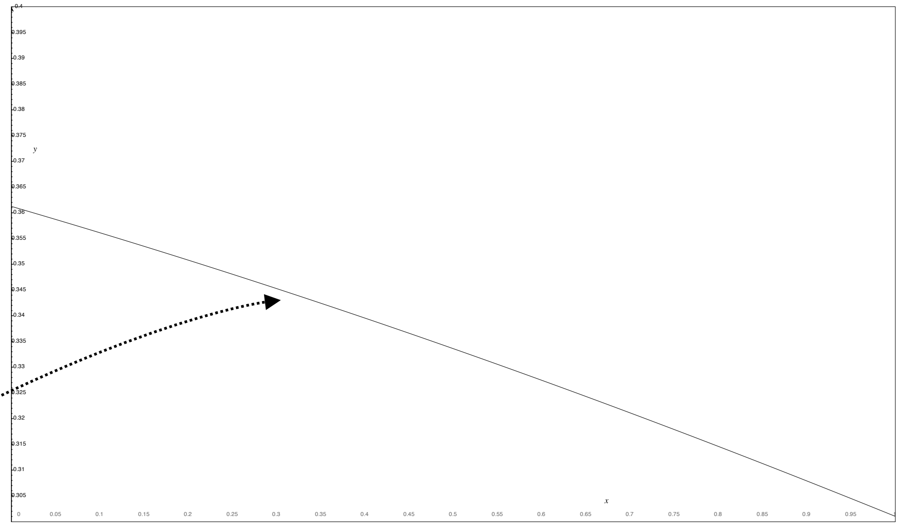


Example: Biased Dice

$\mathsf{P}_0 = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$ $\qquad$ $\mathsf{P}_1 = (\frac{1}{6}, \frac{1}{6}, \frac{2}{6}, 0, \frac{1}{6}, \frac{1}{6})$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = \max_{0<\lambda<1} \boxed{\log\left(\frac{6}{2^\lambda + 4}\right)}$$

$$\approx 0.263$$



- approx. $\dfrac{1}{0.263} \approx 3.8$ queries (rolls) are sufficient to distinguish one dice from the other.
- This is the proof that all this theory has a practical application...

Example: Biased Coin

$\mathsf{P}_0 = (\frac{1}{2}, \frac{1}{2})$ $\qquad$ $\mathsf{P}_1 = \left(\frac{1}{2}(1-\epsilon), \frac{1}{2}(1+\epsilon)\right)$

Example: Biased Coin

$\mathsf{P}_0 = \left(\frac{1}{2}, \frac{1}{2}\right)$ $\quad$ $\mathsf{P}_1 = \left(\frac{1}{2}(1-\epsilon), \frac{1}{2}(1+\epsilon)\right)$

Example: Biased Coin

$\mathsf{P}_0 = (\frac{1}{2}, \frac{1}{2})$ $\qquad$ $\mathsf{P}_1 = \left(\frac{1}{2}(1-\epsilon), \frac{1}{2}(1+\epsilon)\right)$

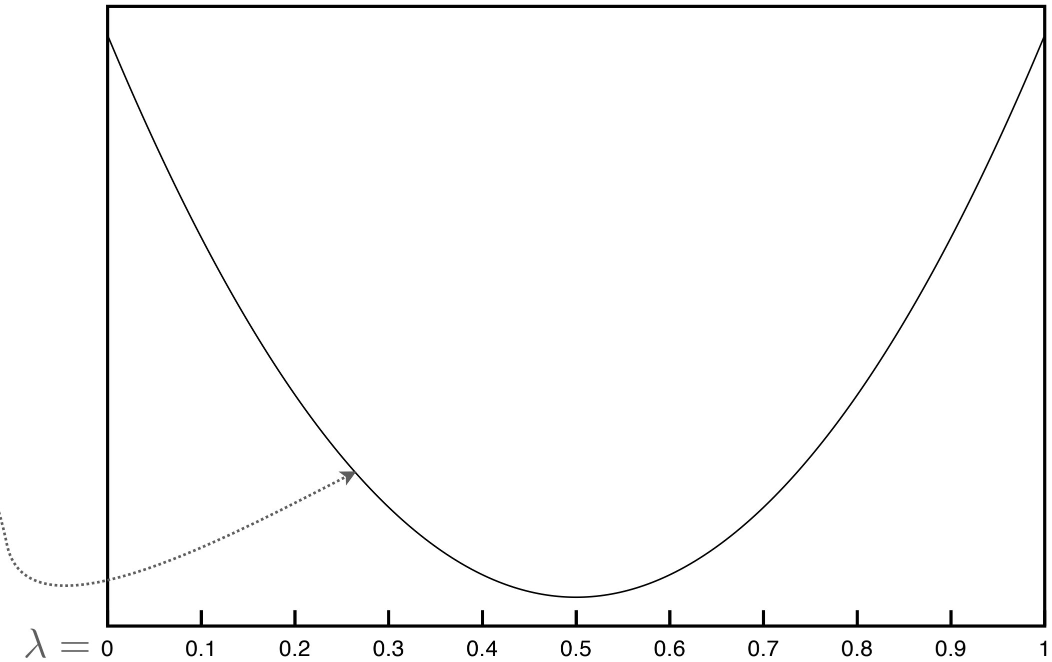
$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = -\inf_{0<\lambda<1} \log \tfrac{1}{2}\left((1-\epsilon)^\lambda + (1+\epsilon)^\lambda\right)$$

Example: Biased Coin

$$\mathsf{P}_0 = \left(\tfrac{1}{2}, \tfrac{1}{2}\right) \qquad \mathsf{P}_1 = \left(\tfrac{1}{2}(1-\epsilon), \tfrac{1}{2}(1+\epsilon)\right)$$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = -\inf_{0<\lambda<1} \log \tfrac{1}{2}\left(\boxed{(1-\epsilon)^\lambda + (1+\epsilon)^\lambda}\right)$$

Example with $\epsilon = 0.01$



Example: Biased Coin

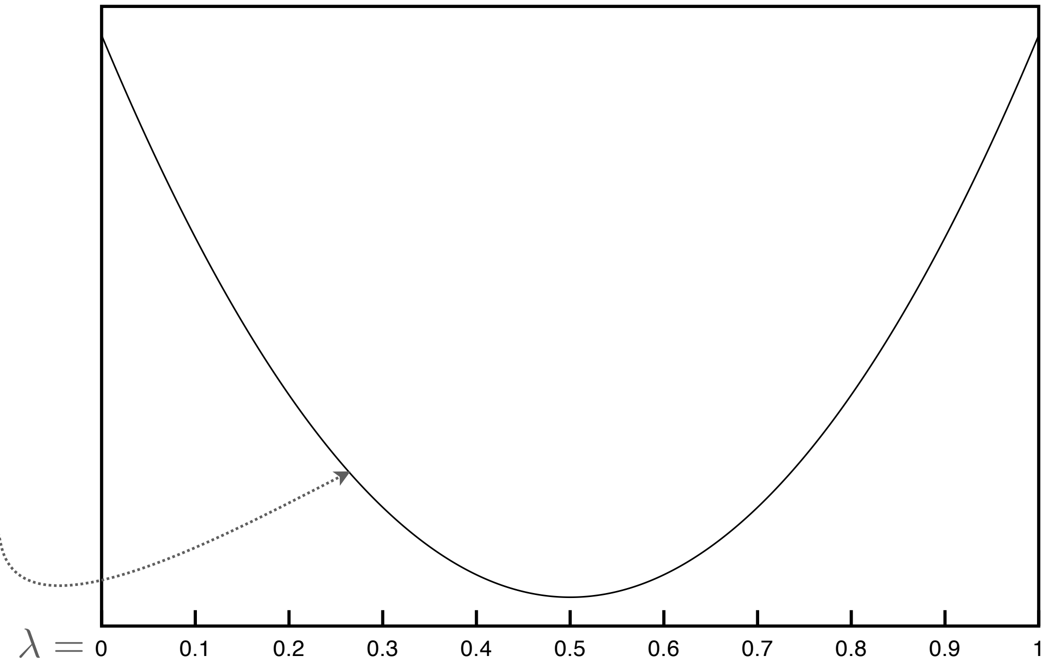
$\mathsf{P}_0 = (\frac{1}{2}, \frac{1}{2})$ $\qquad$ $\mathsf{P}_1 = \left(\frac{1}{2}(1-\epsilon), \frac{1}{2}(1+\epsilon)\right)$

$$C(\mathsf{P}_0, \mathsf{P}_1) = -\inf_{0<\lambda<1} \log \tfrac{1}{2}\left((1-\epsilon)^\lambda + (1+\epsilon)^\lambda\right)$$

Minimum reached for $\lambda \approx \frac{1}{2}$

$$C(\mathsf{P}_0, \mathsf{P}_1) \approx -\log\left(1 - \frac{\epsilon^2}{8}\right) \approx \frac{\epsilon^2}{8 \ln 2}$$

Example with $\epsilon = 0.01$



Example: Biased Coin

$\mathsf{P}_0 = (\frac{1}{2}, \frac{1}{2})$ $\qquad$ $\mathsf{P}_1 = \left(\frac{1}{2}(1-\epsilon), \frac{1}{2}(1+\epsilon)\right)$

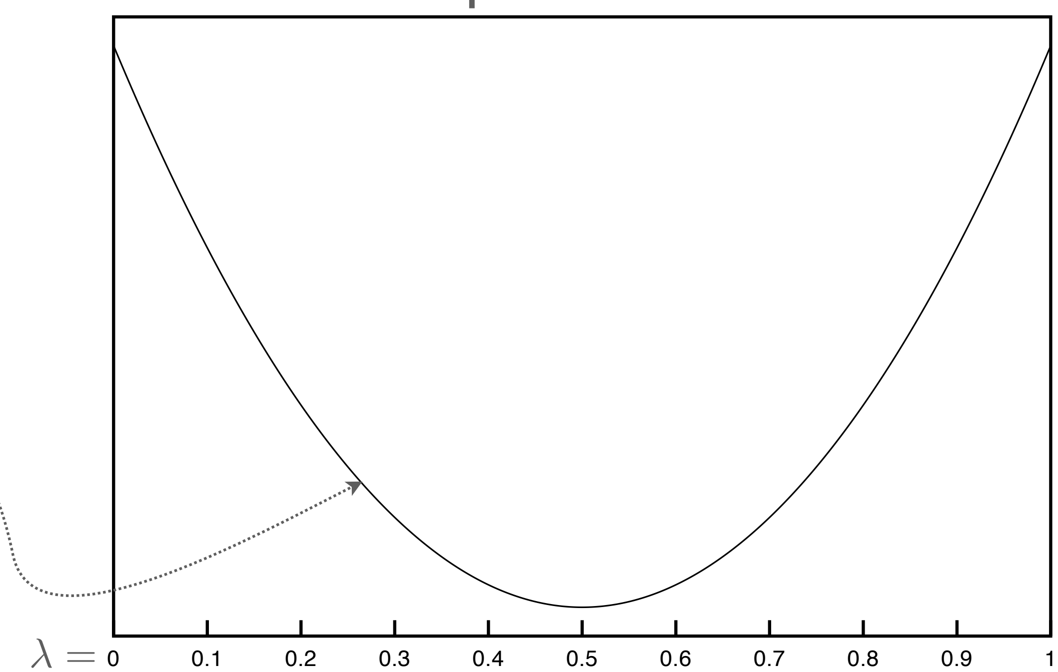
$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) = -\inf_{0<\lambda<1} \log \tfrac{1}{2}\left((1-\epsilon)^\lambda + (1+\epsilon)^\lambda\right)$$

Minimum reached for $\lambda \approx \frac{1}{2}$

$$\mathrm{C}(\mathsf{P}_0, \mathsf{P}_1) \approx -\log\left(1 - \frac{\epsilon^2}{8}\right) \approx \frac{\epsilon^2}{8 \ln 2}$$

$q \approx \dfrac{8 \ln 2}{\epsilon^2}$ allow to reach a non-negligible advantage.

Example with $\epsilon = 0.01$



Possible Extensions

- Case where the distributions are "close" to each other
- Case where one of the hypotheses is composite
- Case where one of the two distributions is unknown
- etc.

Part I: On the (In)Security of Block Ciphers:

Tools for the Security Analysis

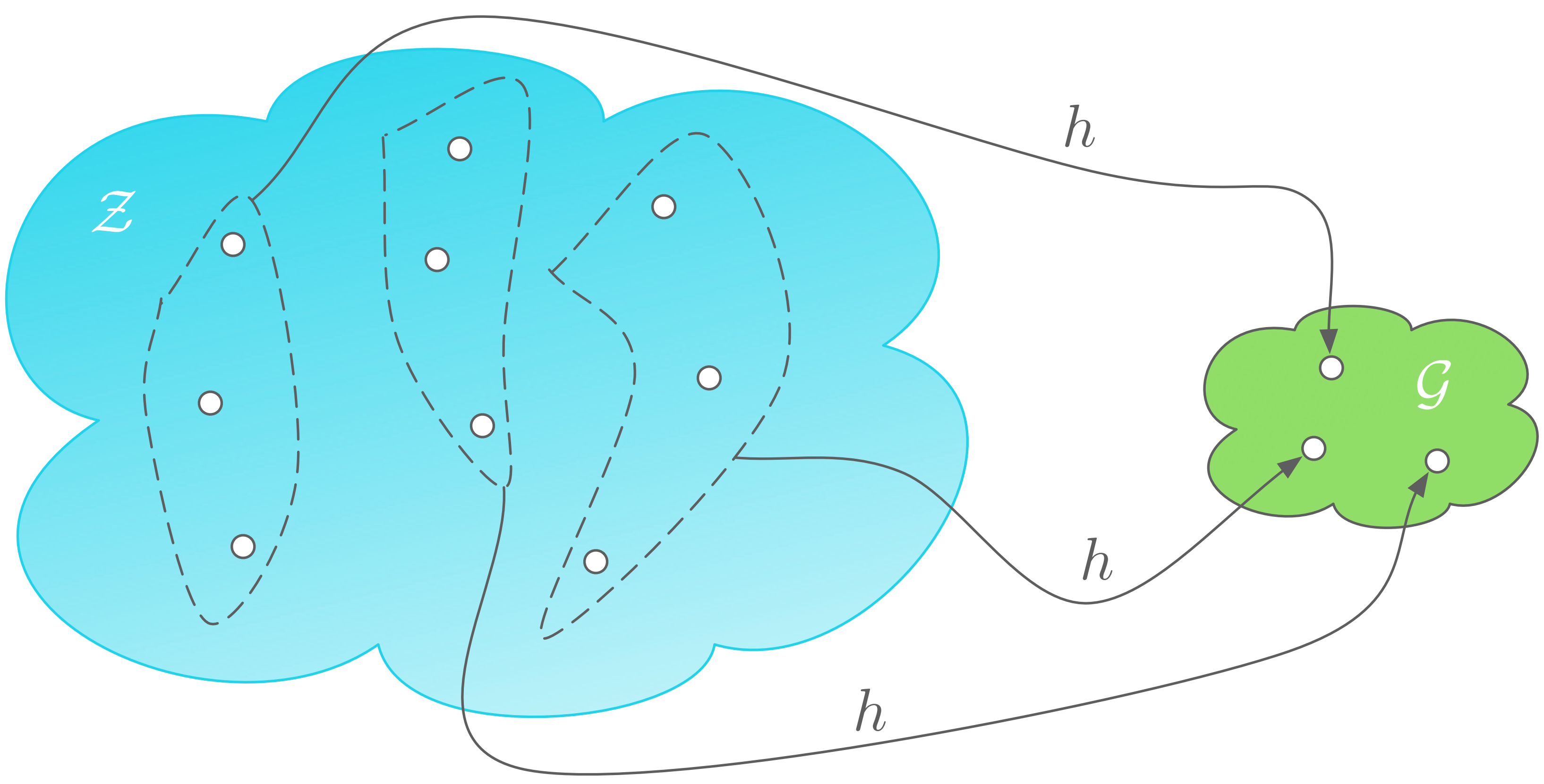
- Projection Based Distinguishers

On the Need for Projection-Based Distinguishers

- If $|\mathcal{Z}|$ is too large, the best distinguisher cannot be implemented.

On the Need for Projection-Based Distinguishers

- If $|\mathcal{Z}|$ is too large, the best distinguisher cannot be implemented.
- Possible solution: reduce the sample size using a projection:



✔ Distinguish in $\mathcal{G}$ instead of $\mathcal{Z}$.

🚫 This reduces the power of the distinguisher.

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.
- By implementing the optimal strategy (after the linear compression), the advantage of this linear distinguisher verifies:

$$\boxed{1 - \mathrm{Adv}(\mathsf{U},\mathsf{P}) \doteq 2^{-q\mathrm{C}(\overline{\mathsf{U}},\overline{\mathsf{P}})}}$$

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.
- By implementing the optimal strategy (after the linear compression), the advantage of this linear distinguisher verifies:

$$1 - \mathrm{Adv}(\mathsf{U},\mathsf{P}) \doteq 2^{-q\mathrm{C}(\overline{\mathsf{U}},\overline{\mathsf{P}})}$$

$$a \cdot Z \sim \overline{\mathsf{P}} \Leftrightarrow Z \sim \mathsf{P}$$
$$a \cdot Z \sim \overline{\mathsf{U}} \Leftrightarrow Z \sim \mathsf{U}$$

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.
- By implementing the optimal strategy (after the linear compression), the advantage of this linear distinguisher verifies:

$$\boxed{1 - \mathrm{Adv}(\mathsf{U},\mathsf{P}) \doteq 2^{-q\mathrm{C}(\overline{\mathsf{U}},\overline{\mathsf{P}})}}$$

$$a \cdot Z \sim \overline{\mathsf{P}} \Leftrightarrow Z \sim \mathsf{P}$$

$$a \cdot Z \sim \overline{\mathsf{U}} \Leftrightarrow Z \sim \mathsf{U}$$

- Definition: linear probability of P: $\boxed{\mathrm{LP}_a(\mathsf{P}) = \left(\mathrm{E}_{\mathsf{P}}\left((-1)^{a \cdot Z}\right)\right)^2}$

Example: Linear Distinguishers

- $\mathcal{Z} = \{0,1\}^n \qquad \mathcal{G} = \{0,1\} \qquad \mathsf{P}_0 = \mathsf{U} \qquad \mathsf{P}_1 = \mathsf{P} \qquad h(Z) = a \cdot Z = a_1 Z_1 \oplus \cdots \oplus a_n Z_n$
- This is a linear distinguisher based on the mask a.
- By implementing the optimal strategy (after the linear compression), the advantage of this linear distinguisher verifies:

$$1 - \mathrm{Adv}(\mathsf{U},\mathsf{P}) \doteq 2^{-q\mathrm{C}(\overline{\mathsf{U}},\overline{\mathsf{P}})}$$

$$a \cdot Z \sim \overline{\mathsf{P}} \Leftrightarrow Z \sim \mathsf{P}$$

$$a \cdot Z \sim \overline{\mathsf{U}} \Leftrightarrow Z \sim \mathsf{U}$$

- Definition: linear probability of P: $\mathrm{LP}_a(\mathsf{P}) = \left(\mathrm{E}_{\mathsf{P}}\left((-1)^{a \cdot Z}\right)\right)^2$
- Roughly: $\mathrm{C}(\mathsf{U},\mathsf{P}) \approx \dfrac{\mathrm{LP}_a(\mathsf{P})}{8 \ln 2}$ $\Rightarrow$ $q \approx \dfrac{8 \ln 2}{\mathrm{LP}_a(\mathsf{P})}$ are enough (well known...)

Extending the Notion of Linear Probability

- The previous example only works for sets of the form $\mathcal{Z} = \{0, 1\}^n$.

- We at least need to generalize the notion of linear probability to arbitrary sets.

Extending the Notion of Linear Probability

- The previous example only works for sets of the form $\mathcal{Z} = \{0,1\}^n$.
- We at least need to generalize the notion of linear probability to arbitrary sets.

Extending the Notion of Linear Probability

- The previous example only works for sets of the form $\mathcal{Z} = \{0,1\}^n$.
- We at least need to generalize the notion of linear probability to arbitrary sets.

Definition

The linear probability of P over the group $\mathcal{Z}$ with respect to the character χ is

$$\mathrm{LP}_\chi(\mathsf{P}) = \left|\mathrm{E}_{\mathsf{P}}\left(\chi(Z)\right)\right|^2$$

Extending the Notion of Linear Probability

- The previous example only works for sets of the form $\mathcal{Z} = \{0,1\}^n$.
- We at least need to generalize the notion of linear probability to arbitrary sets.

Definition

The linear probability of P over the group $\mathcal{Z}$ with respect to the character χ is

$$\mathrm{LP}_\chi(\mathsf{P}) = \left|\mathrm{E}_{\mathsf{P}}\left(\chi(Z)\right)\right|^2$$

- A character of $\mathcal{Z}$ is a homomorphism $\chi : \mathcal{Z} \longrightarrow \mathbf{C}^\times$
- Example: when $\mathcal{Z} = \{0,1\}^n$ we have $\chi(a) = (-1)^{u \cdot a}$ for some u

Extending the Notion of Linear Probability

- The previous example only works for sets of the form $\mathcal{Z} = \{0,1\}^n$.
- We at least need to generalize the notion of linear probability to arbitrary sets.

Definition

The linear probability of P over the group $\mathcal{Z}$ with respect to the character χ is

$$\mathrm{LP}_\chi(\mathsf{P}) = \left|\mathrm{E}_{\mathsf{P}}\left(\chi(Z)\right)\right|^2$$

- A character of $\mathcal{Z}$ is a homomorphism $\chi : \mathcal{Z} \longrightarrow \mathbf{C}^\times$
- Example: when $\mathcal{Z} = \{0,1\}^n$ we have $\chi(a) = (-1)^{u \cdot a}$ for some u
- Consequence: when $\mathcal{Z} = \{0,1\}^n$ this new definition corresponds to the old one!

Lin. Dist. for Sources overs Arbitrary Sets

We have wonderful lemma...

Lin. Dist. for Sources overs Arbitrary Sets

We have wonderful lemma...

Lemma 7.5 *Let* P_0 *be the uniform distribution on a finite subgroup* H *of* $\mathbf{C}^\times$ *of order* d. *Let* $\mathcal{D} = \{\mathsf{P}_u : u \in \mathsf{H}\}$ *be a set of* d *distributions on* H *defined by* (7.10). *The* q*-limited distinguisher between the null hypothesis* $\mathsf{H}_0 : \mathsf{P} = \mathsf{P}_0$ *and the alternate hypothesis* $\mathsf{H}_1 : \mathsf{P} \in \mathcal{D}$ *defined by the distribution acceptance region* $\Pi_q^\star = \Pi^\star \cap \mathcal{P}_q$, *where*

$$\Pi^\star = \left\{ \mathsf{P} \in \mathcal{P} \;:\; \|\mathsf{P}\|_\infty \geq \frac{\log(1-\epsilon)}{\log(1-\epsilon) - \log(1+(d-1)\epsilon)} \right\}, \tag{7.11}$$

is asymptotically optimal and its advantage $\mathrm{BestAdv}_q$ *is such that*

$$1 - \mathrm{BestAdv}_q(\mathsf{H}_0, \mathsf{H}_1) \doteq 2^{q \inf_{0<\lambda<1} \log \frac{1}{d}\left((1+(d-1)\epsilon)^\lambda + (d-1)(1-\epsilon)^\lambda\right)}.$$

Lin. Dist. for Sources overs Arbitrary Sets

We have wonderful lemma...

Lemma 7.5 *Let P_0 be the uniform distribution on a finite subgroup H of $\mathbf{C}^\times$ of order d. Let $\mathcal{D} = \{\mathsf{P}_u : u \in \mathsf{H}\}$ be a set of d distributions on H defined by (7.10). The q-limited distinguisher between the null hypothesis $\mathsf{H}_0 : \mathsf{P} = \mathsf{P}_0$ and the alternate hypothesis $\mathsf{H}_1 : \mathsf{P} \in \mathcal{D}$ defined by the distribution acceptance region $\Pi^\star_q = \Pi^\star \cap \mathcal{P}_q$, where*

$$\Pi^\star = \left\{ \mathsf{P} \in \mathcal{P} : \|\mathsf{P}\|_\infty \geq \frac{\log(1-\epsilon)}{\log(1-\epsilon) - \log(1+(d-1)\epsilon)} \right\} \quad (7.11)$$

is asymptotically optimal and its advantage $\mathrm{BestAdv}_q$ is such that

$$1 - \mathrm{BestAdv}_q(\mathsf{H}_0, \mathsf{H}_1) \doteq 2^{q \inf_{0<\lambda<1} \log \frac{1}{d}\left((1+(d-1)\epsilon)^\lambda + (d-1)(1-\epsilon)^\lambda\right)}.$$

Which shows how to use the generalized LP to build a linear distinguisher over arbitrary sets...

and allows to conclude that a linear distinguisher needs $q \approx \dfrac{8 \ln 2}{(d-1)\mathrm{LP}^{\chi}(\mathsf{P})}$ to reach a good advantage.

Part I: On the (In)Security of Block Ciphers:

Tools for the Security Analysis

Practical Implications for Block Ciphers

Applications on SAFER K/SK

- We attack SAFER with a $\boxplus$-linear cryptanalysis.
- Use the toolbox to find characteristics within SAFER K/SK.
- To compute the complexities we consider several characteristics among the hull (i.e., all characteristics share the same input/output characters).
- To turn distinguishing attacks into key recovery attacks, we also take advantage of the linearity of the key schedule.

Applications on SAFER K/SK

- We attack SAFER with a $\boxplus$-linear cryptanalysis.
- Use the toolbox to find characteristics within SAFER K/SK.
- To compute the complexities we consider several characteristics among the hull (i.e., all characteristics share the same input/output characters).
- To turn distinguishing attacks into key recovery attacks, we also take advantage of the linearity of the key schedule.

Nbr Rounds	Complexity
2	$2^{23}/2^{31}$
3	2^{38}
4	2^{49}
5	2^{56}

Other Applications

- Two new Digital Encryption Algorithm for Numbers (based on the AES): DEAN18 and DEAN27 which respectively encrypts blocks made of 18 and 27 decimal digits.

- Resistance against our generalization of linear cryptanalysis.

- New attacks on TOY100 (toy cipher that encrypts blocks of 32 decimal digits).

- Break 9 (10 ?) rounds out of 12.

Part II: Designs and Security Proofs

Outline

Block Ciphers

Dial $\mathbf{C}$ for Cipher

KFC: the Krazy Feistel Cipher

Outline

- Block Ciphers
- Dial $\mathbf{C}$ for Cipher
- KFC: the Krazy Feistel Cipher

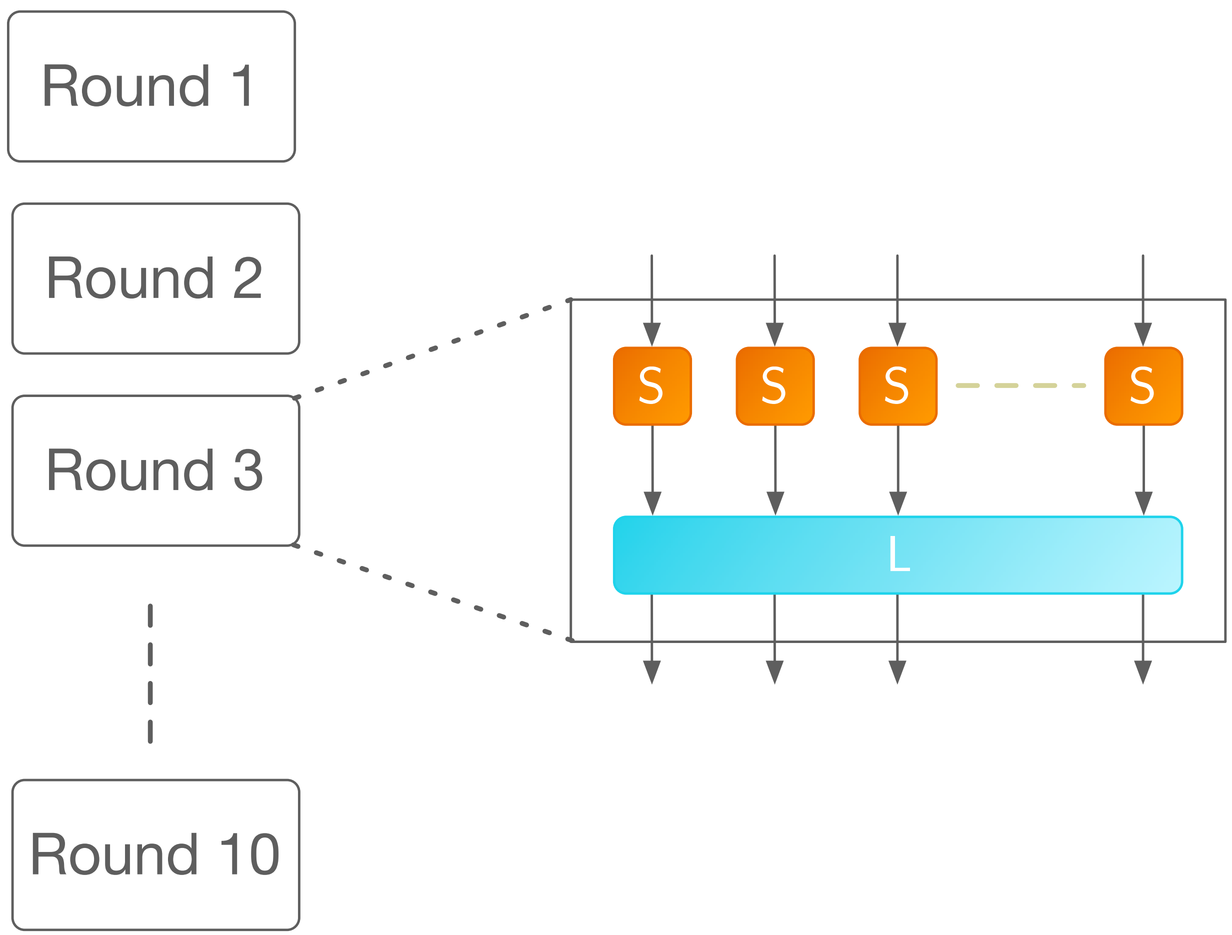
- The Luby-Rackoff Model
- Vaudenay’s decorrelation theory

Outline

Block Ciphers

Dial C for Cipher

KFC: the Krazy Feistel Cipher

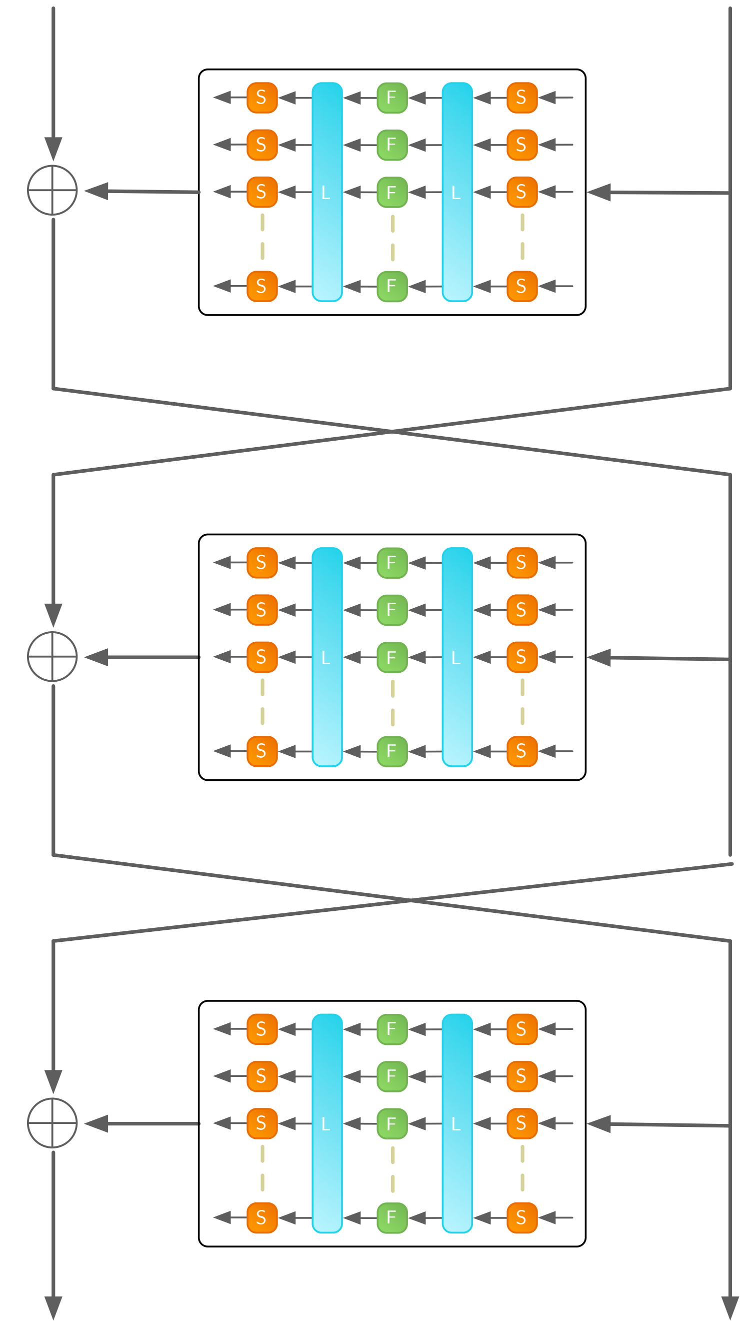


Outline

Block Ciphers

Dial C for Cipher

KFC: the Krazy Feistel Cipher



Outline

Block Ciphers

Dial $\mathbf{C}$ for Cipher

KFC: the Krazy Feistel Cipher

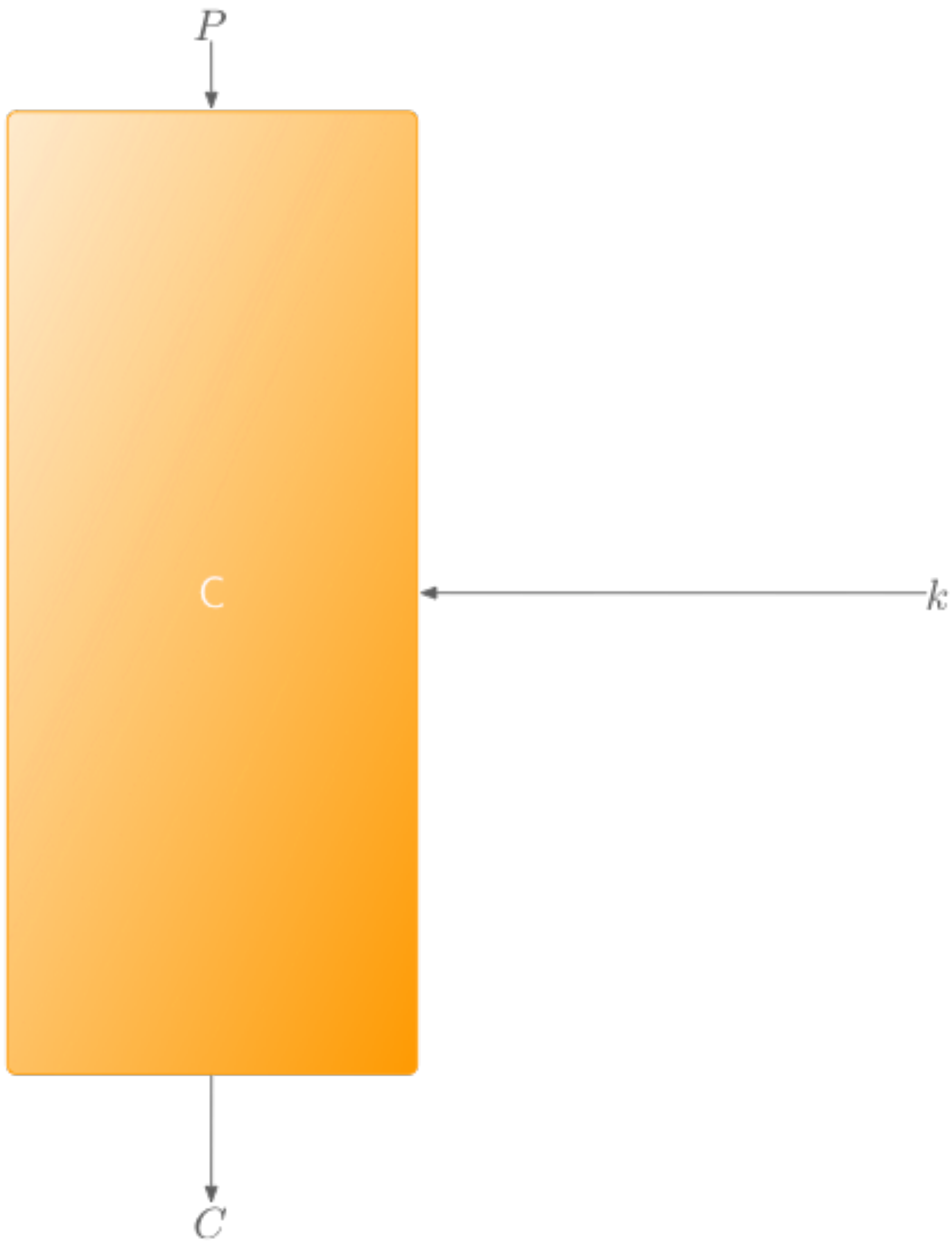
[BVsac05] [BFsac06] [BFa06]

Part II: Designs and Security Proofs

- Block Ciphers

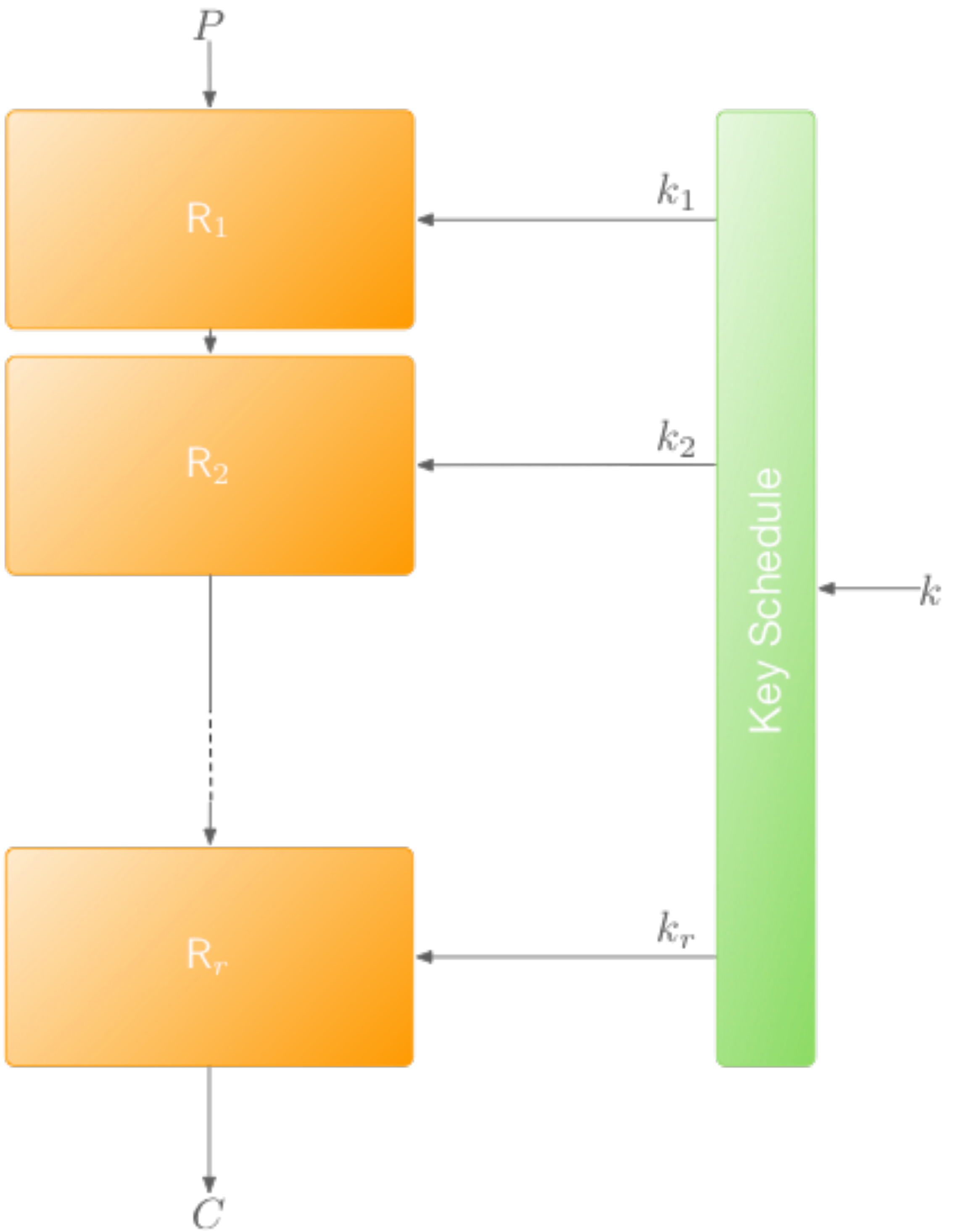
A Typical Iterated Block Cipher

- A block cipher on a finite set is a family of permutations on that set, indexed by a parameter call the key.



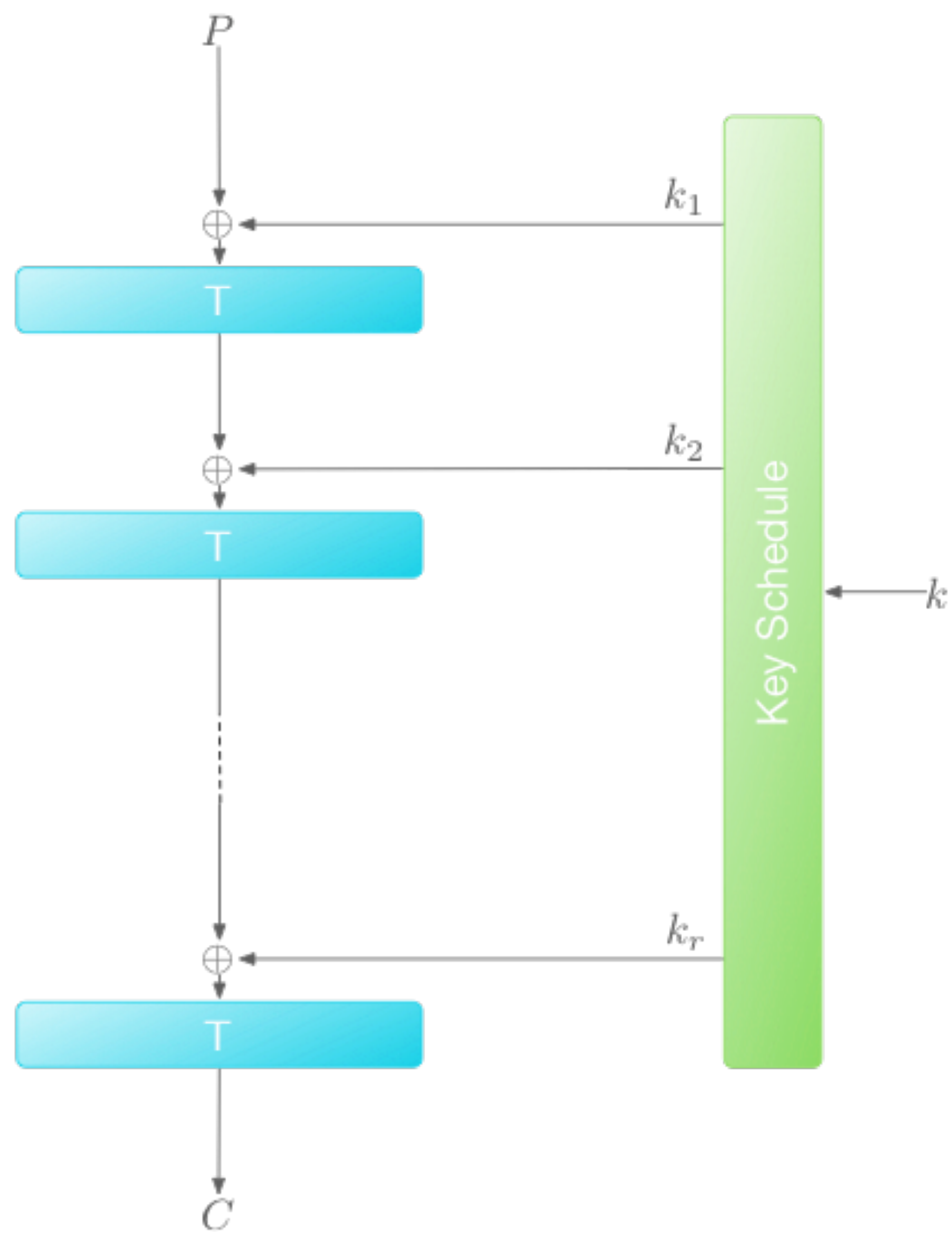
A Typical Iterated Block Cipher

- A block cipher on a finite set is a family of permutations on that set, indexed by a parameter call the key.
- Such a cipher is usually iterated, i.e., made of several rounds.
- Each round is parameterized by a key derived from the main secret key by means of a Key Schedule.



A Typical Iterated Block Cipher

- A block cipher on a finite set is a family of permutations on that set, indexed by a parameter call the key.
- Such a cipher is usually iterated, i.e., made of several rounds.
- Each round is parameterized by a key derived from the main secret key by means of a Key Schedule.
- Usually, the rounds all share the same design, e.g., a round key addition followed by a fixed (nonlinear) transformation.

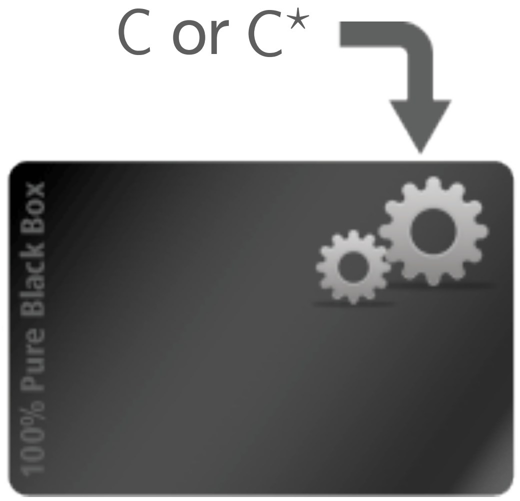


What Should we Expect from a Block Cipher?

It should be fast and secure!

What Should we Expect from a Block Cipher?

It should be fast and secure!



What Should we Expect from a Block Cipher?

It should be fast and secure!

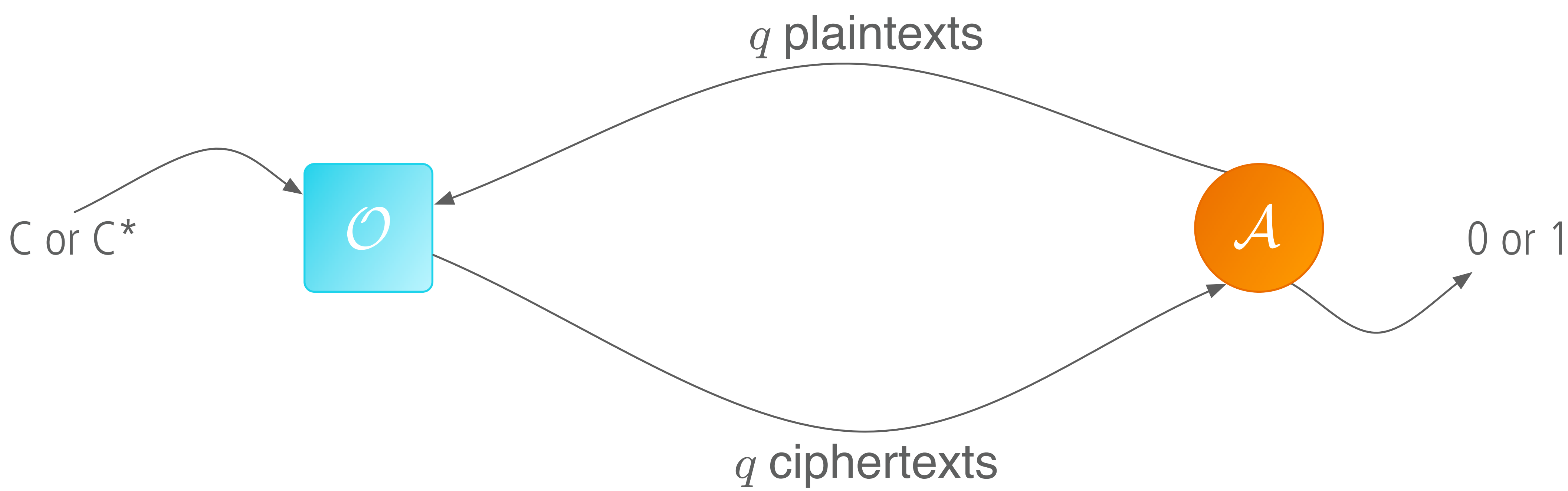
What Should we Expect from a Block Cipher?

It should be fast and secure!

$P_1, P_2, \ldots, P_q$ →  → $C_1, C_2, \ldots, C_q$

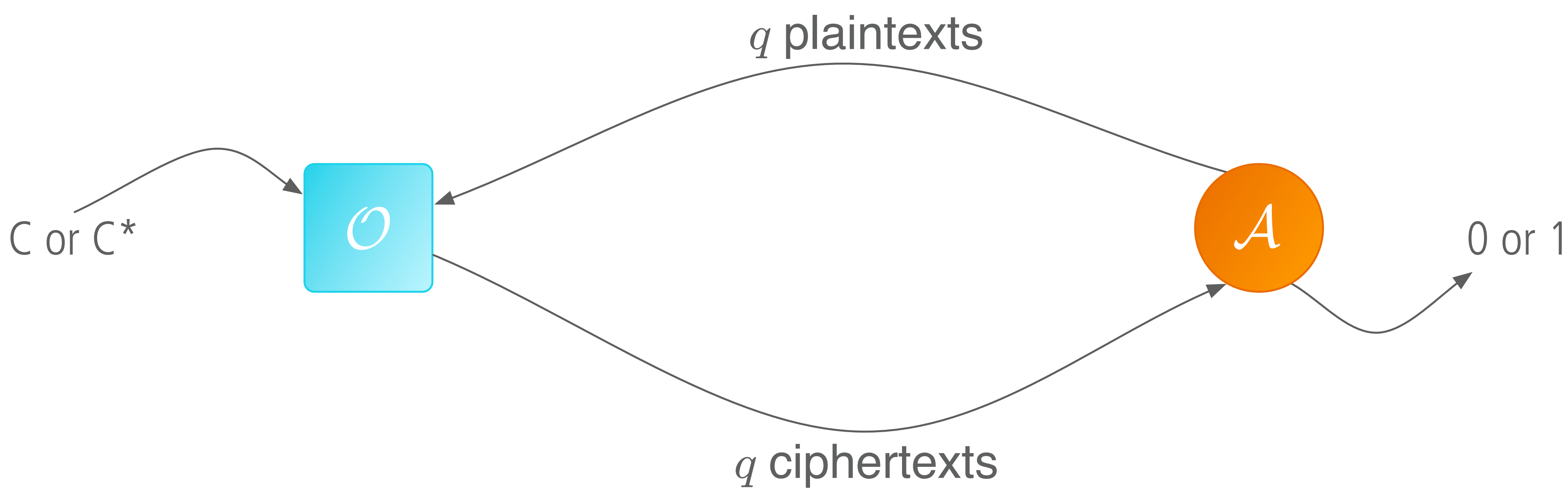
The Luby-Rackoff Model

We consider a q-limited adversary $\mathcal{A}$ in the Luby-Rackoff Model:



The Luby-Rackoff Model

We consider a q-limited adversary $\mathcal{A}$ in the Luby-Rackoff Model:



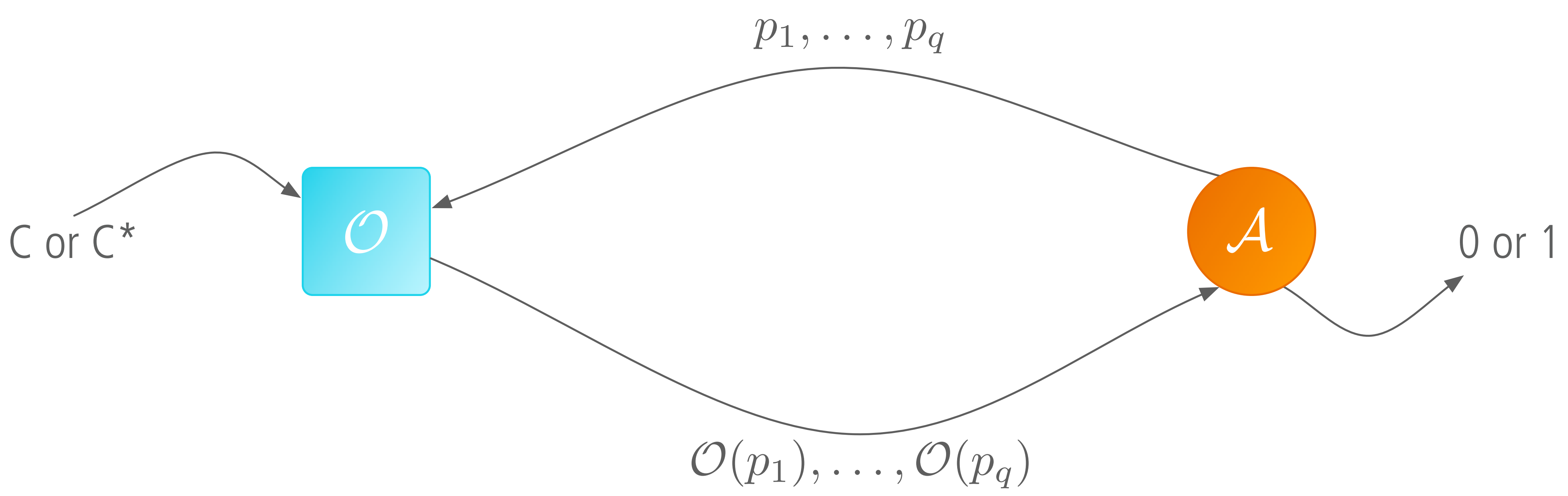
$$\mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star) = |\Pr[\mathcal{A}(\mathsf{C}) = 1] - \Pr[\mathcal{A}(\mathsf{C}^\star) = 1]|$$

Advantage of the q-limited adversary $\mathcal{A}$ between C and $\mathsf{C}^\star$

✔ The block cipher C is secure if the advantage of $\mathcal{A}$ is negligible for all $\mathcal{A}$'s.

The Luby-Rackoff Model

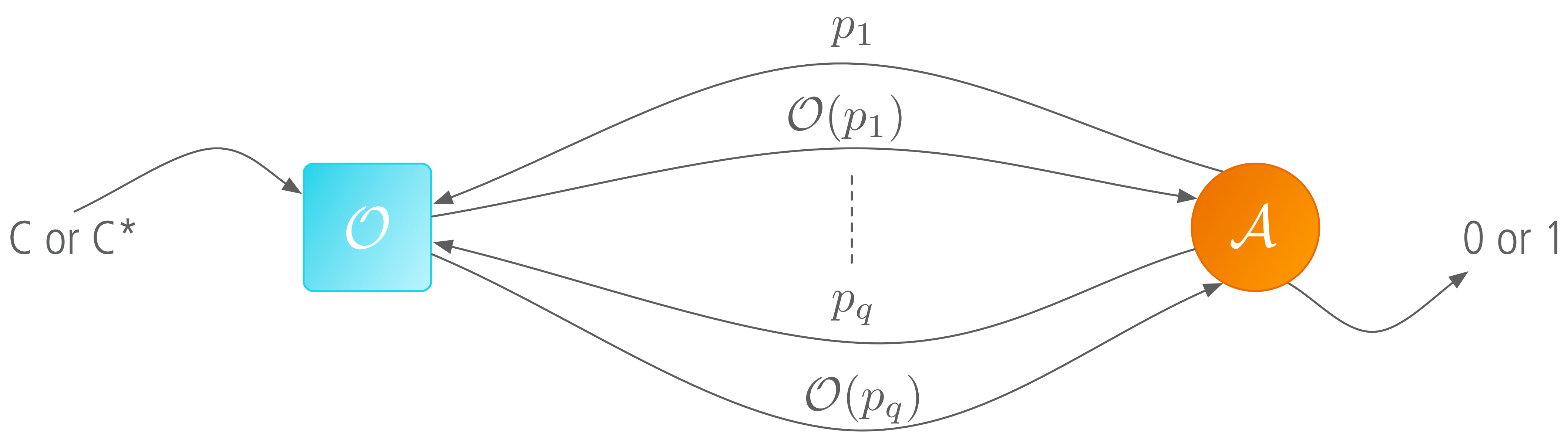
We consider a q-limited adversary $\mathcal{A}$ in the Luby-Rackoff Model:



$\mathcal{A}$ is non-adaptive if the q plaintexts are chosen "at once".

The Luby-Rackoff Model

We consider a q-limited adversary $\mathcal{A}$ in the Luby-Rackoff Model:

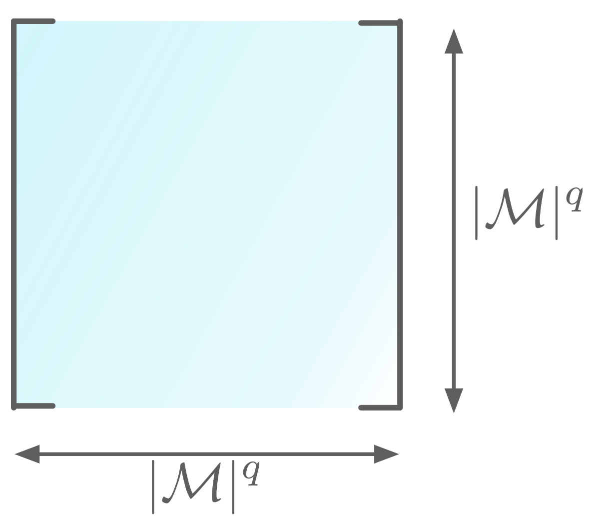


$\mathcal{A}$ is adaptive if plaintext i depends on ciphertexts $1, \ldots, i-1$.

Computing $\mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star)$

- Computing the advantage is not a trivial task in general.
- Possible solution: use Vaudenay's Decorrelation Theory.

$$\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star) = \frac{1}{2} \| [\mathsf{C}]^q - [\mathsf{C}^\star]^q \|$$

$[\mathsf{C}]^q =$ 

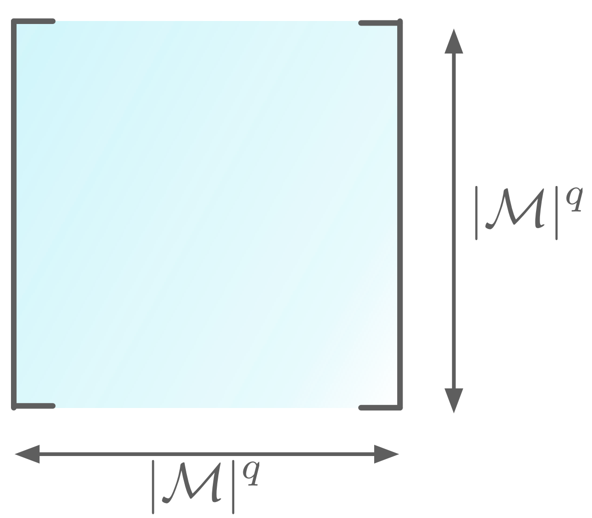
$|\mathcal{M}|^q = 2^{128 \cdot q}$ for a 128-bits block cipher

Computing $\mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star)$

- Computing the advantage is not a trivial task in general.
- Possible solution: use Vaudenay's Decorrelation Theory.

$$\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star) = \frac{1}{2} \| [\mathsf{C}]^q - [\mathsf{C}^\star]^q \|$$

$[\mathsf{C}]^q =$

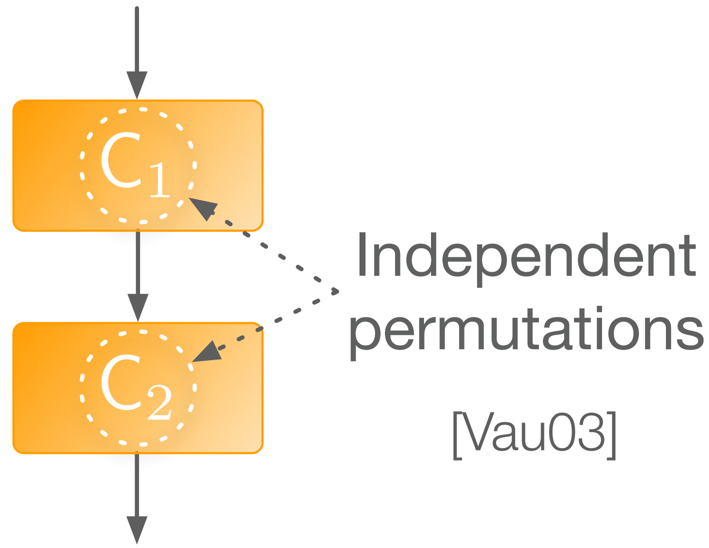


$|\mathcal{M}|^q = 2^{128 \cdot q}$ for a 128-bits block cipher

Tricks for Computing $\mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star)$

To deal with the size of the distribution matrices:

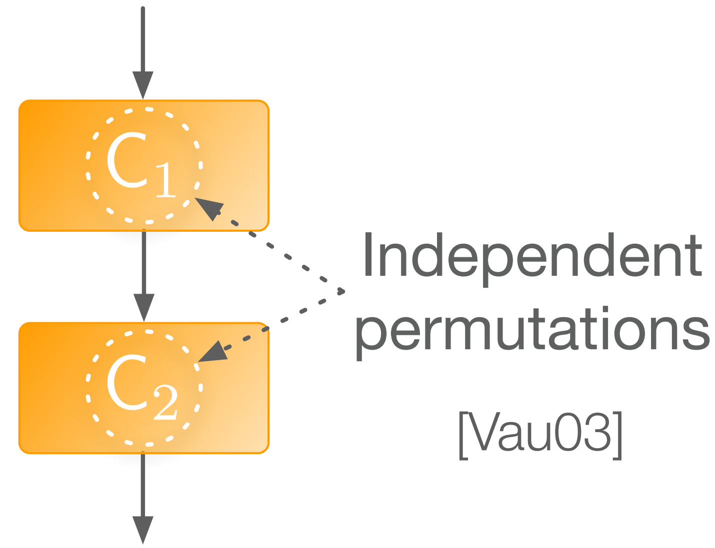
- $[\mathsf{C}_2 \circ \mathsf{C}_1]^q = [\mathsf{C}_1]^q \times [\mathsf{C}_2]^q$



Tricks for Computing $\mathrm{Adv}_{\mathcal{A}}(\mathsf{C}, \mathsf{C}^\star)$

To deal with the size of the distribution matrices:

- $[\mathsf{C}_2 \circ \mathsf{C}_1]^q = [\mathsf{C}_1]^q \times [\mathsf{C}_2]^q$



- Take advantage of the symmetries of the block cipher in order to compute the distribution matrix of each round

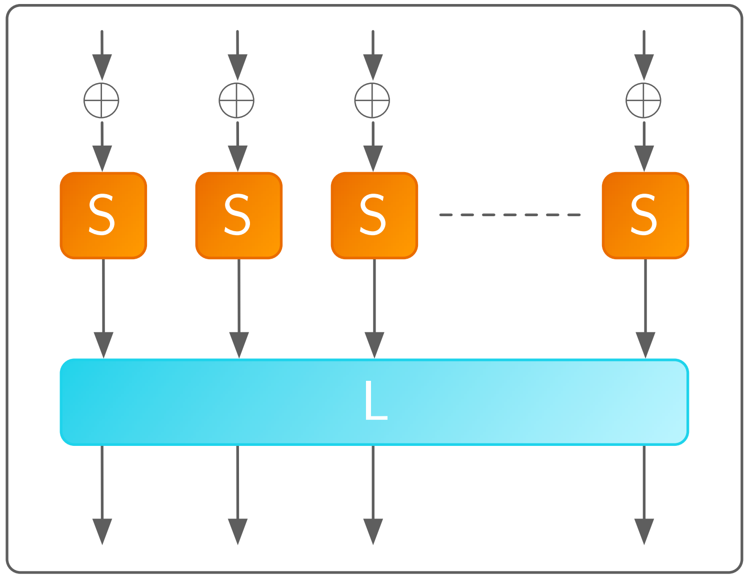
Part II: Designs and Security Proofs

- Dial C for Cipher

Description of $\mathbf{C}$

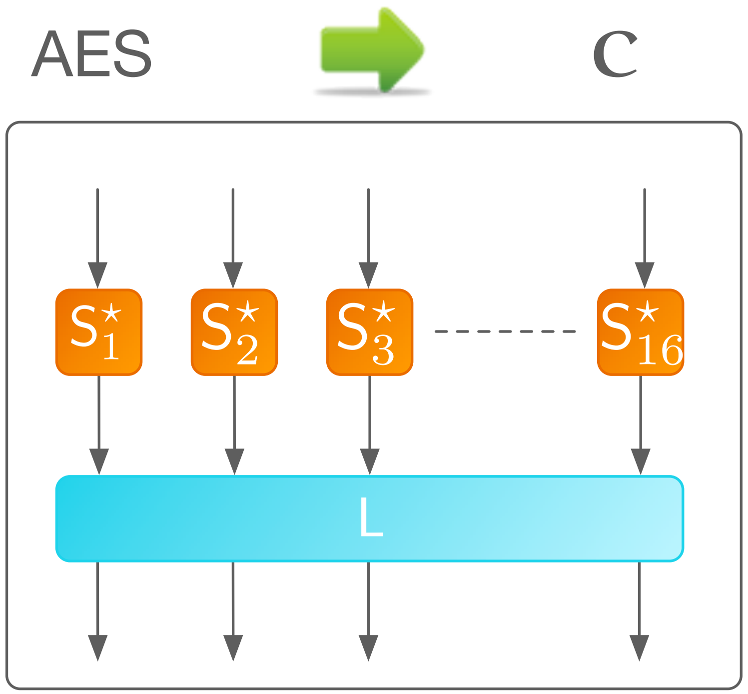
$\mathbf{C}$ corresponds to the AES where "`addRoundKeys` → `SubBytes`" is replaced by mutually independent random permutations.

AES



Description of $\mathbf{C}$

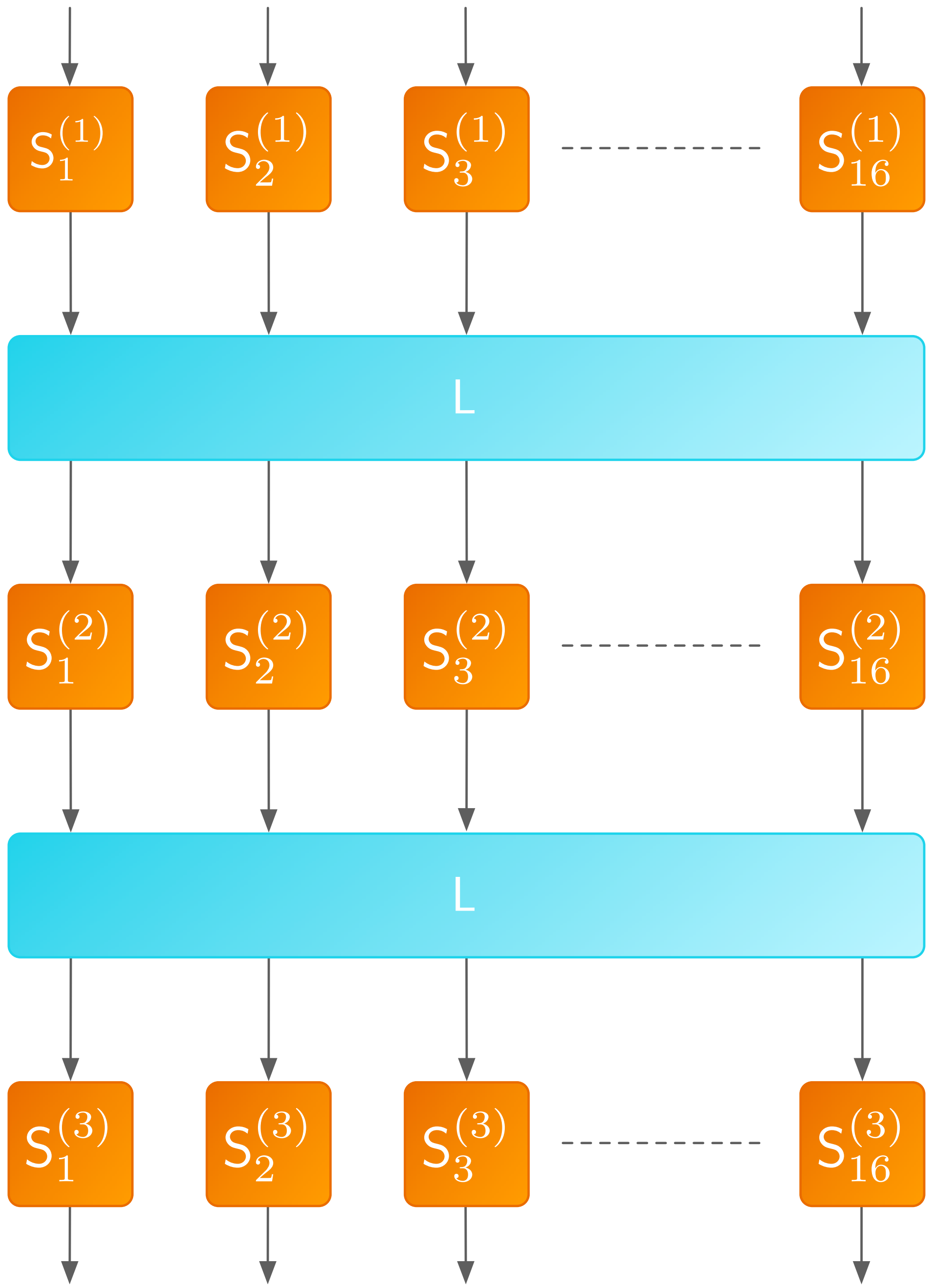
$\mathbf{C}$ corresponds to the AES where "`addRoundKeys` → `SubBytes`" is replaced by mutually independent random permutations.



- $\mathbf{C}$ is made of 9 identical rounds, followed by a layer of substitution boxes.
- $\mathbf{C}$ uses $16 \cdot 10 = 160$ mutually independent random 8-bits substitution boxes

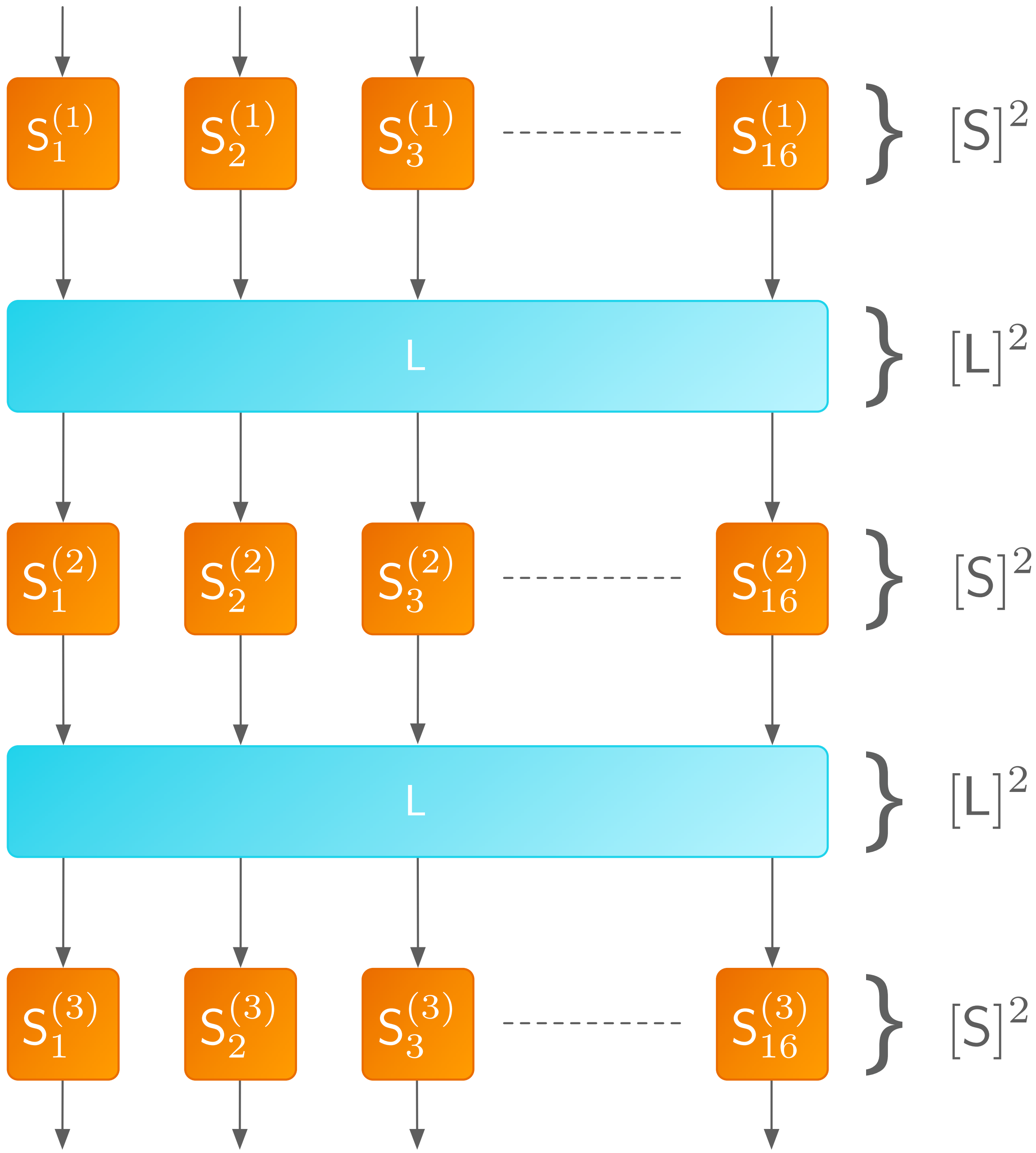
Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:



Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:



Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

$$[\mathbf{C}]^2 = [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2$$

Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

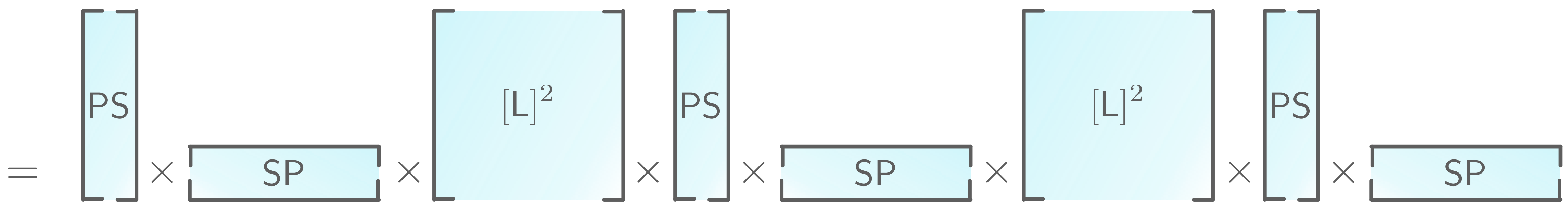
$$[\mathbf{C}]^2 = \quad \times [\mathsf{L}]^2 \times [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2$$

$$[\mathsf{S}]^2 = \begin{bmatrix} \\ \mathsf{PS} \\ \\ \end{bmatrix} \times \begin{bmatrix} \mathsf{SP} \end{bmatrix}$$

Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

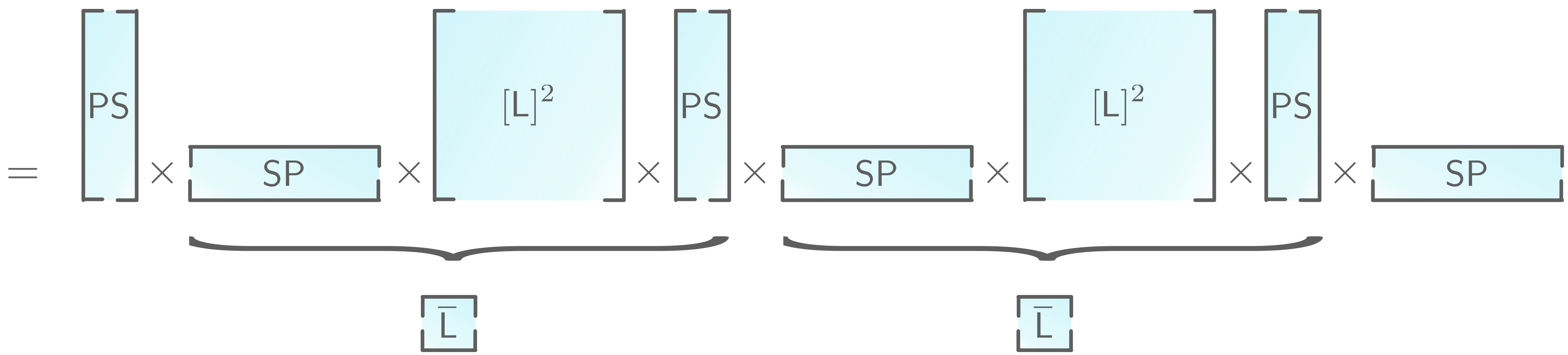
$$[\mathbf{C}]^2 = [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2$$



Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

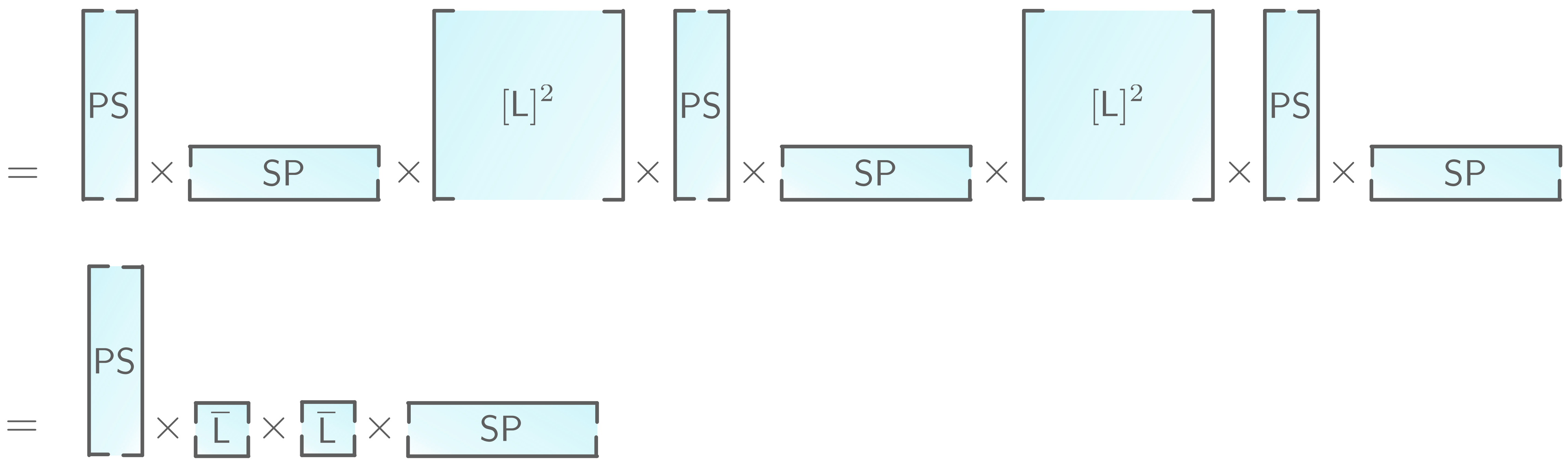
$$[\mathbf{C}]^2 = [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2$$



Computing $[\mathbf{C}]^2$

We consider a version of $\mathbf{C}$ reduced to 3 rounds:

$$[\mathbf{C}]^2 = [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2 \times [\mathsf{L}]^2 \times [\mathsf{S}]^2$$



Computing $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star)$

For a r-round version of $\mathbf{C}$ we have:

$$[\mathbf{C}]^2 = \mathsf{PS} \times (\overline{\mathsf{L}})^{r-1} \times \mathsf{SP}$$

where $\overline{\mathsf{L}}$ is a $2^{16} \times 2^{16}$ matrix.

Computing $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^{\star})$

For a r-round version of $\mathbf{C}$ we have:

$$[\mathbf{C}]^2 = \mathsf{PS} \times (\overline{\mathsf{L}})^{r-1} \times \mathsf{SP}$$

where $\overline{\mathsf{L}}$ is a $2^{16} \times 2^{16}$ matrix.

$$\boxed{\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^{\star}) = \frac{1}{2} |||(\overline{\mathsf{L}})^{r-1} - \overline{\mathsf{C}^{\star}}|||_{\infty}}$$

Computing $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star)$

For a r-round version of $\mathbf{C}$ we have:

$$[\mathbf{C}]^2 = \mathsf{PS} \times (\overline{\mathsf{L}})^{r-1} \times \mathsf{SP}$$

where $\overline{\mathsf{L}}$ is a $2^{16} \times 2^{16}$ matrix.

$$\boxed{\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star) = \frac{1}{2} |||(\overline{\mathsf{L}})^{r-1} - \overline{\mathsf{C}^\star}|||_\infty}$$

Can we reduce the computational complexity even further?

✔ Yes! But the diffusion has to be chosen with care...

Computing $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star)$

For a r-round version of $\mathbf{C}$ we have:

$$[\mathbf{C}]^2 = \mathsf{PS} \times (\overline{\mathsf{L}})^{r-1} \times \mathsf{SP}$$

where $\overline{\mathsf{L}}$ is a $2^{16} \times 2^{16}$ matrix.

$$\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star) = \frac{1}{2} |||(\overline{\mathsf{L}})^{r-1} - \overline{\mathsf{C}^\star}|||_\infty$$

Can we reduce the computational complexity even further?

Yes! But the diffusion has to be chosen with care...

$$\max_{\mathcal{A}} \mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star) = \frac{1}{2} ||| \left(\overline{\overline{\mathsf{L}}} \times \mathsf{W}\right)^{r-2} \times \overline{\overline{\mathsf{L}}} - \overline{\overline{\mathsf{C}^\star}}|||_\infty$$

Computing the advantage of the best distinguisher (either adaptive or not) only requires operations on 625×625 matrices (instead of $2^{256} \times 2^{256}$ initially).

Values of $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star)$

r	1	2	3	4	5	6
$\mathrm{Adv}(\mathsf{C}, \mathsf{C}^\star)$	1	1	$2^{-4.0}$	$2^{-23.4}$	$2^{-45.8}$	$2^{-71.0}$

r	7	8	9	10	11	12
$\mathrm{Adv}(\mathsf{C}, \mathsf{C}^\star)$	$2^{-126.3}$	$2^{-141.3}$	$2^{-163.1}$	$2^{-185.5}$	$2^{-210.8}$	$2^{-238.9}$

Values of $\mathrm{Adv}_{\mathcal{A}}(\mathbf{C}, \mathsf{C}^\star)$

r	1	2	3	4	5	6
$\mathrm{Adv}(\mathsf{C}, \mathsf{C}^\star)$	1	1	$2^{-4.0}$	$2^{-23.4}$	$2^{-45.8}$	$2^{-71.0}$

r	7	8	9	10	11	12
$\mathrm{Adv}(\mathsf{C}, \mathsf{C}^\star)$	$2^{-126.3}$	$2^{-141.3}$	$2^{-163.1}$	$2^{-185.5}$	$2^{-210.8}$	$2^{-238.9}$

7 rounds of $\mathbf{C}$ are enough to obtain provable security against 2-limited adversaries

Part II: Designs and Security Proofs

- KFC: the Krazy Feistel Cipher

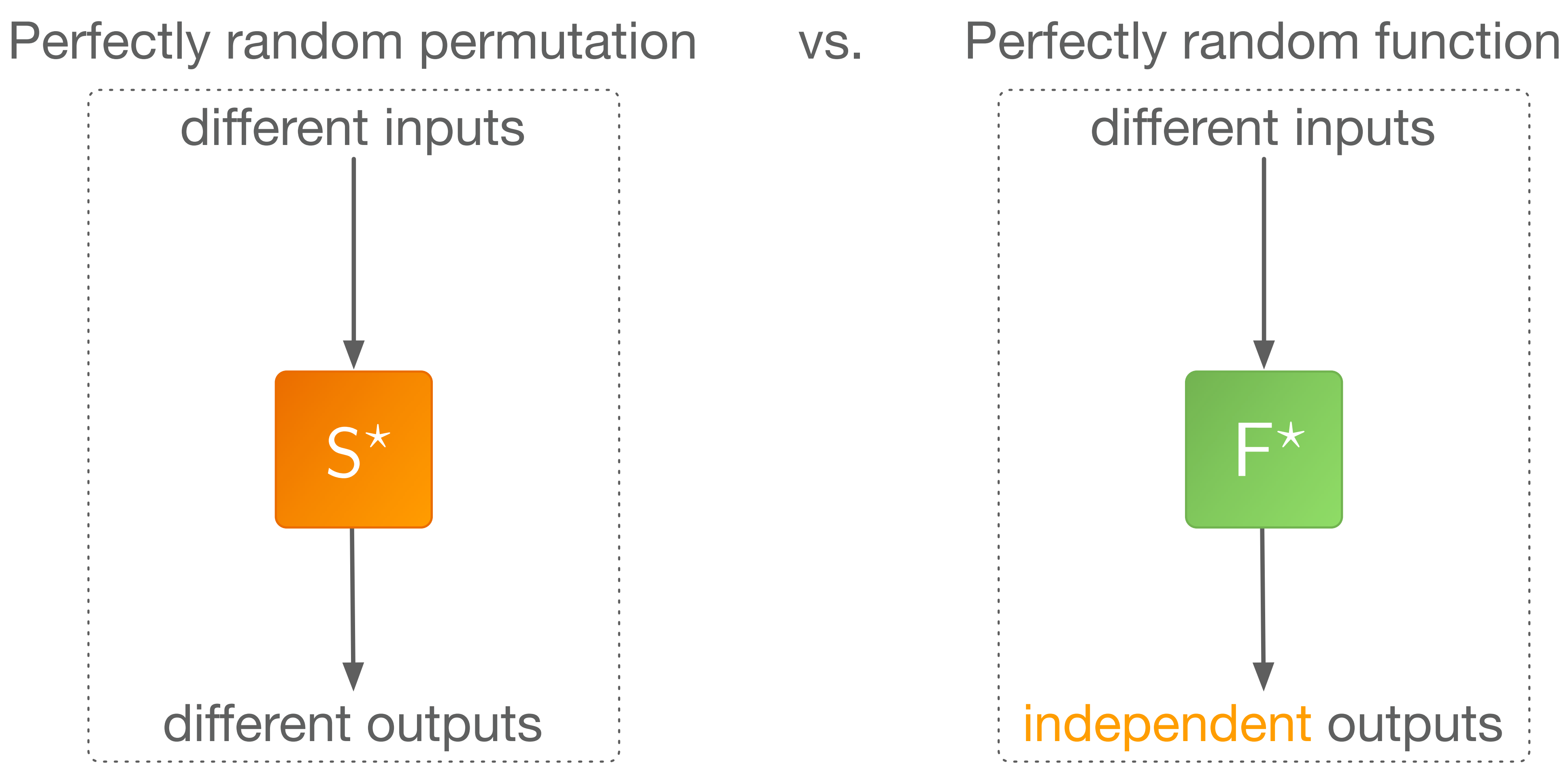
What about Higher Orders?

We did not manage to prove the security of $\mathbf{C}$ against higher q-limited adversaries for $q > 2$.

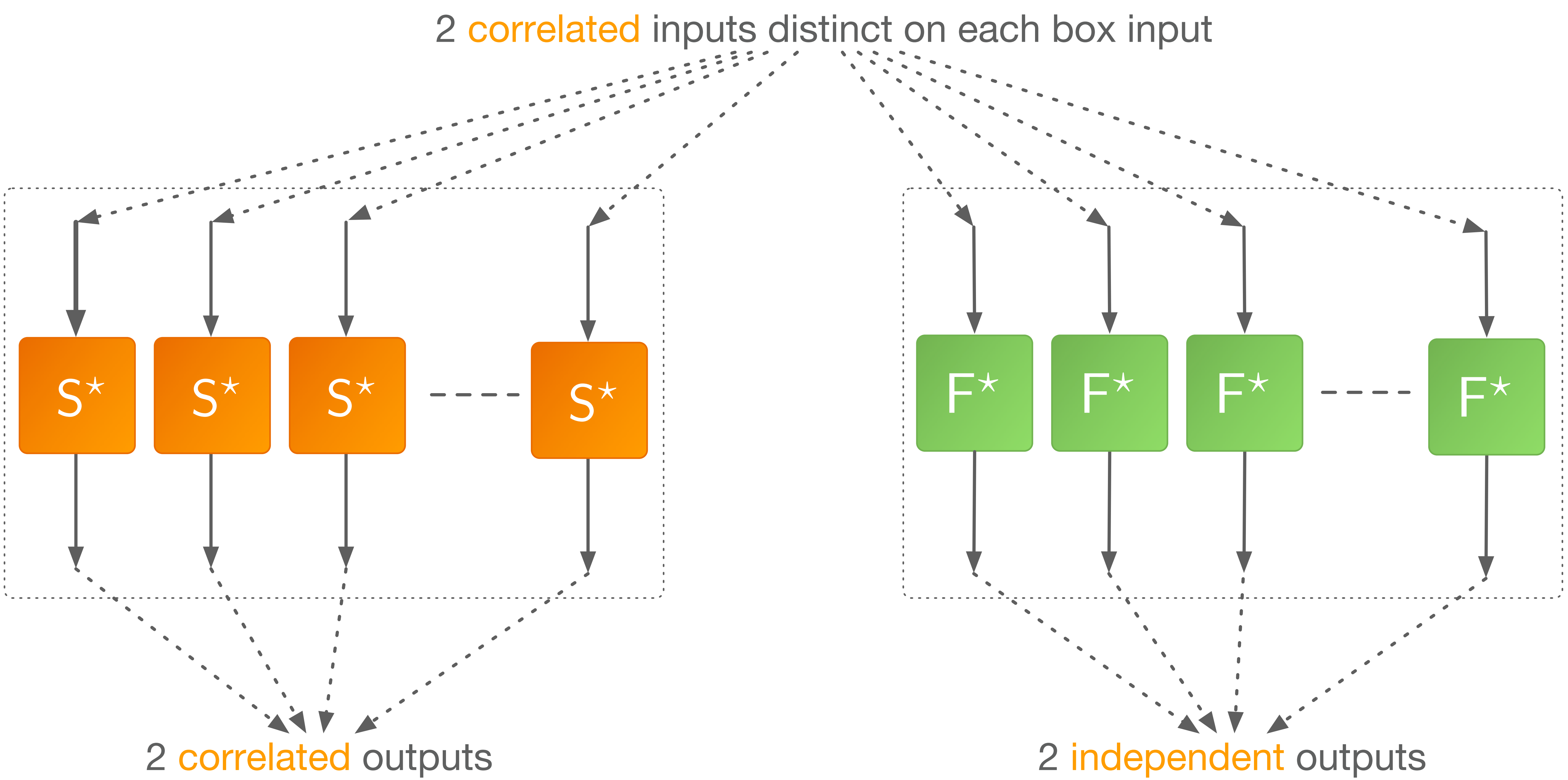
What about Higher Orders?

We did not manage to prove the security of $\mathbf{C}$ against higher q-limited adversaries for $q > 2$.

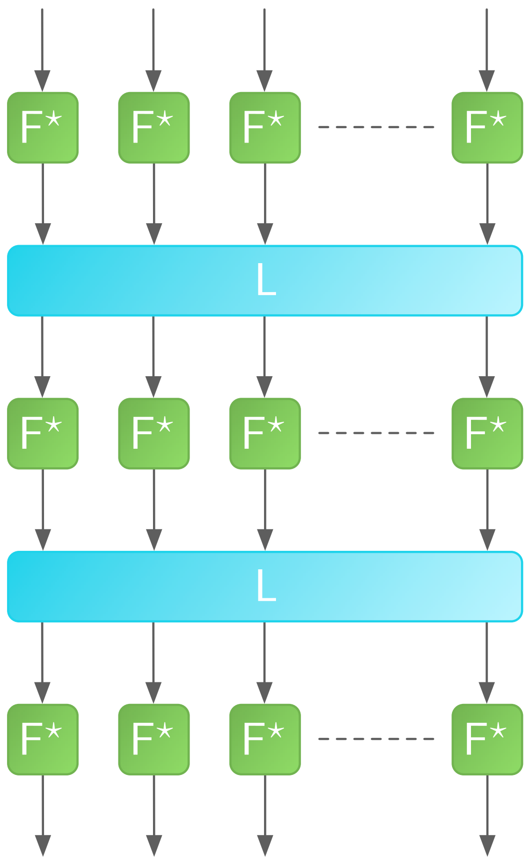
Idea: try to bound the advantage of the best q-limited adversary by that of the best (q-1)-limited adversary.



Rand. Permutations vs. Rand. Functions

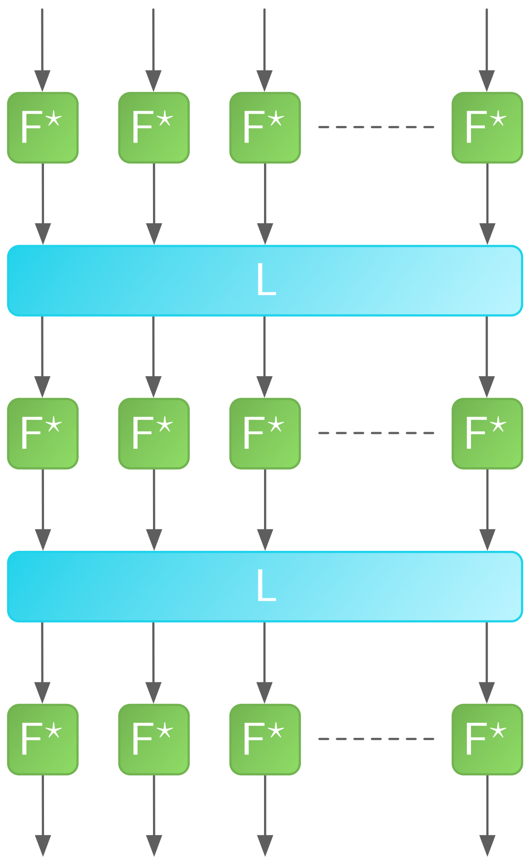


Towards a New Construction



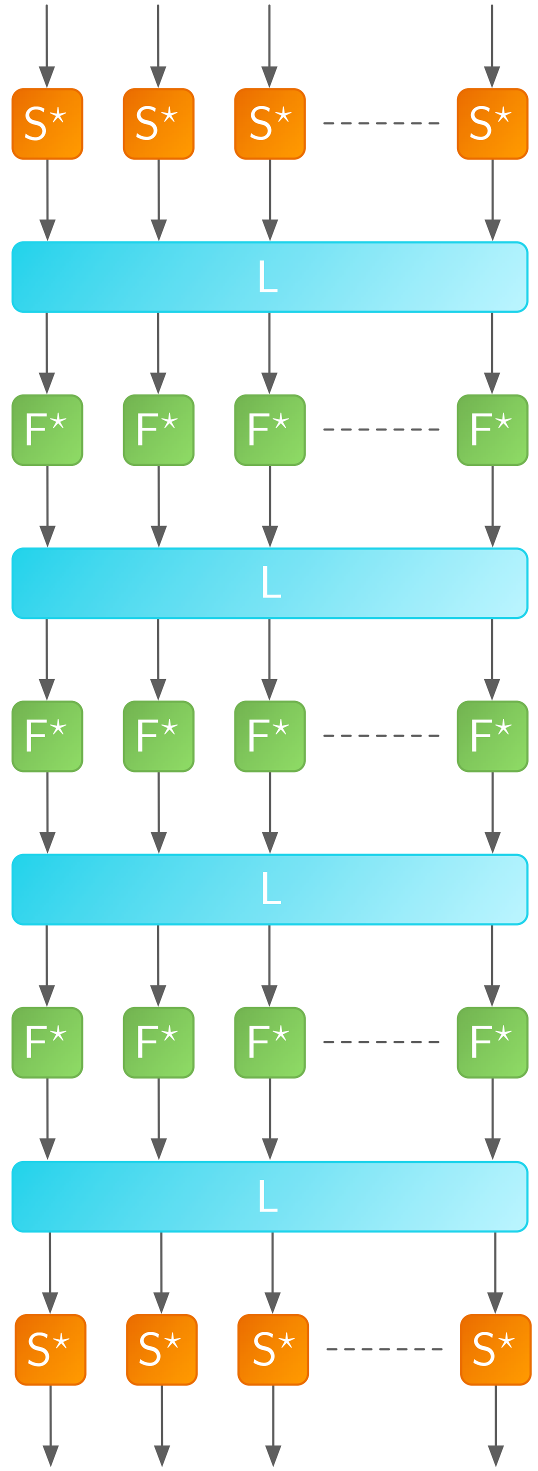
Towards a New Construction

- Non negligible risk of collision after a F-box



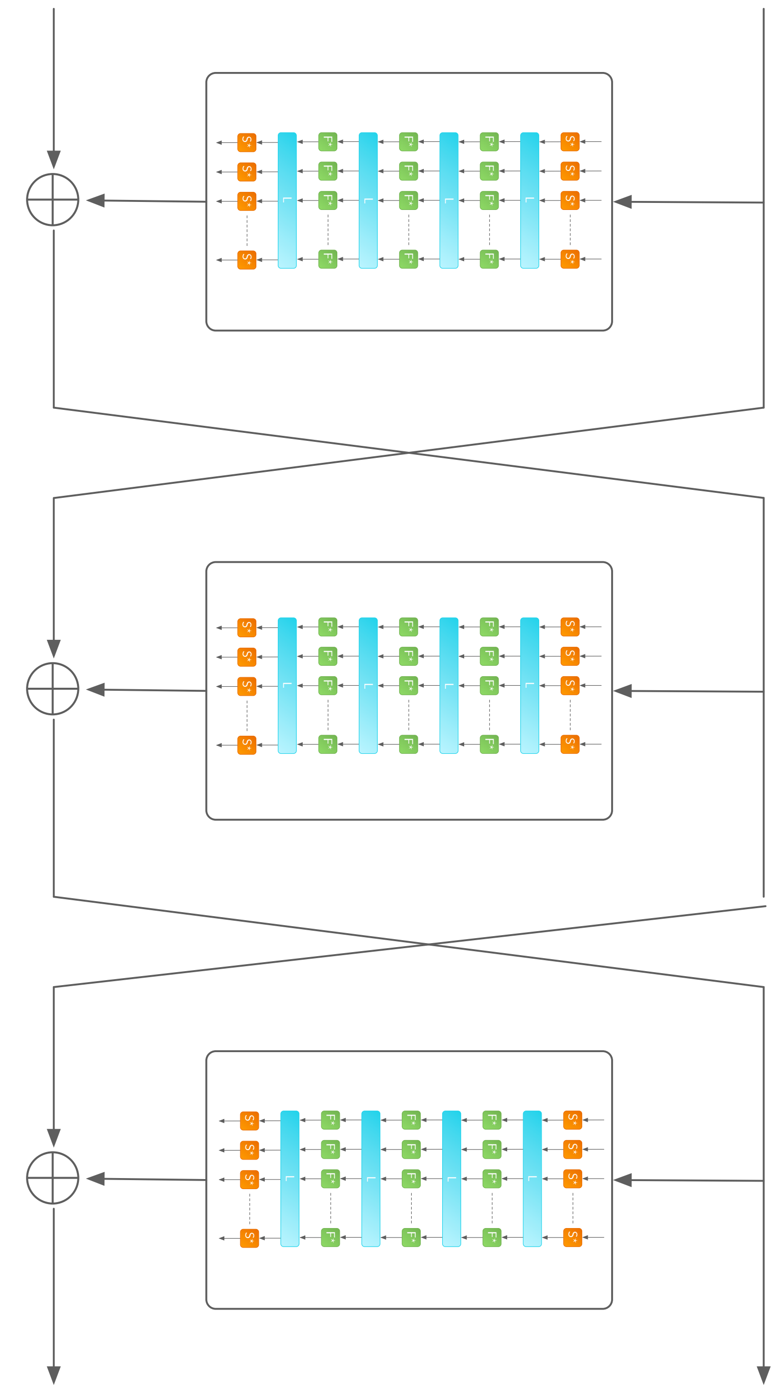
Towards a New Construction

- Non negligible risk of collision after a F-box
- Use the “sandwich technique” to obtain (almost) pairwise independent inputs before the layer of random functions.



Towards a New Construction

- Non negligible risk of collision after a F-box
- Use the “sandwich technique” to obtain (almost) pairwise independent inputs before the layer of random functions.
- The construction is not invertible. We plug it in a Feistel scheme.



Results obtained on KFC

- With this approach, we manage to prove the security against adversaries up to the order 70 (for an unreasonable set of parameters).
- The bounds are not tight at all   it is certainly possible to improve our results.

Results obtained on KFC

- With this approach, we manage to prove the security against adversaries up to the order 70 (for an unreasonable set of parameters).
- The bounds are not tight at all it is certainly possible to improve our results.

Conclusion

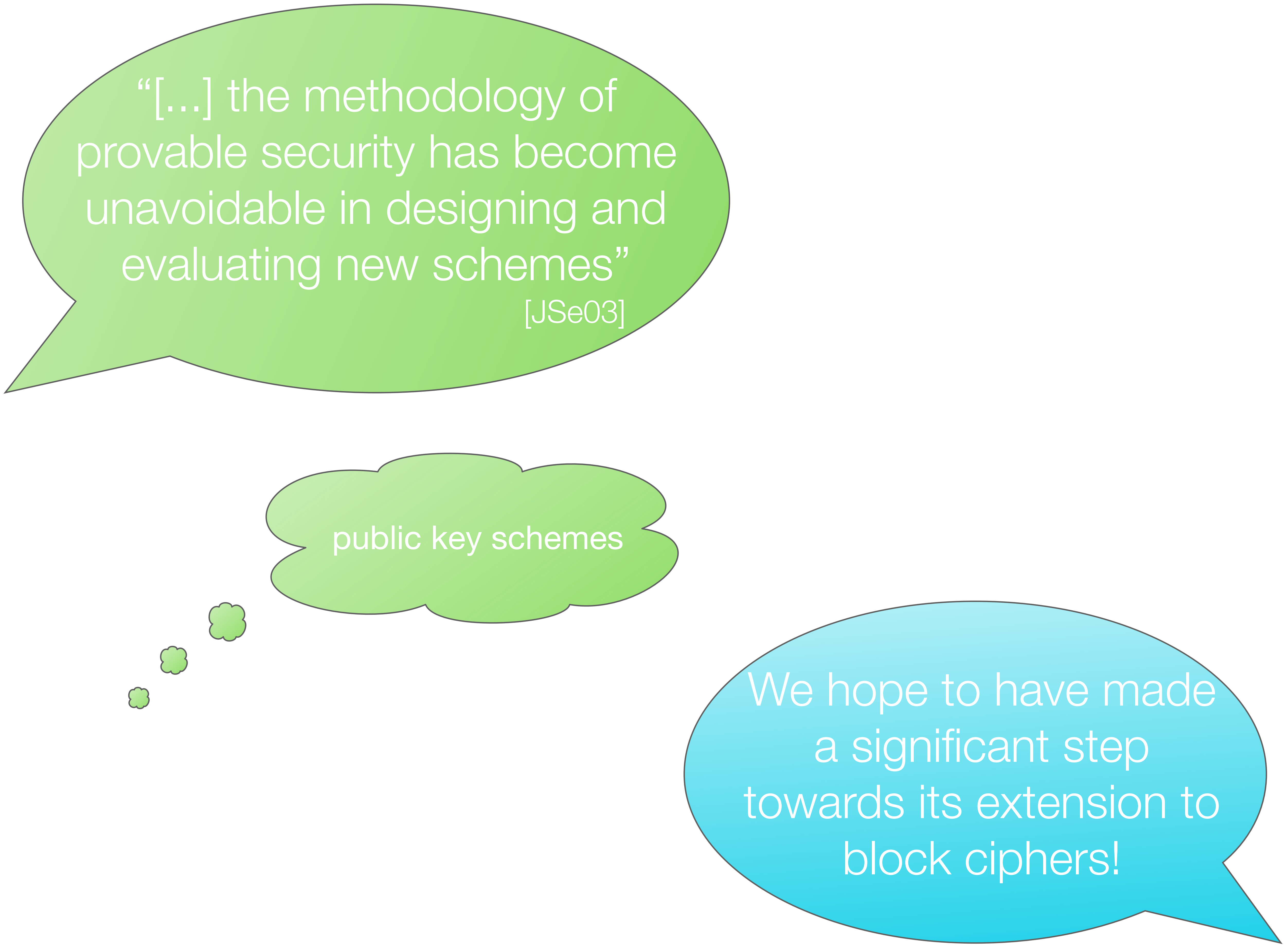
"[...] the methodology of provable security has become unavoidable in designing and evaluating new schemes"

[JSe03]

"[...] the methodology of provable security has become unavoidable in designing and evaluating new schemes"

[JSe03]

public key schemes


"[...] the methodology of provable security has become unavoidable in designing and evaluating new schemes"
[JSe03]
public key schemes
We hope to have made a significant step towards its extension to block ciphers!

Thank you for your attention!

☺

Publications

[BVicits08] *The Complexity of Distinguishing Distributions*
Joint work with Serge Vaudenay
Published in the proceedings of ICITS 08 (Calgary, Canada)

[BSVsac07] *Linear Cryptanalysis of Non Binary Ciphers (with an application to* SAFER*)*
Joint work with Jacques Stern & Serge Vaudenay
Published in the proceedings of SAC 07 (Ottawa, Canada)

[BFa06] KFC - *The Krazy Feistel Cipher*
Joint work with Matthieu Finiasz
Published in the proceedings of Asiacrypt 06 (Shangai, China)

[BFsac06] *Dial* C *for Cipher*
Joint work with Matthieu Finiasz
Published in the proceedings of SAC 06 (Montreal, Canada)

[BVsac05] *Proving the Security of the* AES *Substitution-Permutation Network*
Joint work with Serge Vaudenay
Published in the proceedings of SAC 05 (Kingston, Canada)

[BJVa04] *How Far Can We Go Beyond Linear Cryptanalysis?*
Joint work with Pascal Junod & Serge Vaudenay
Published in the proceedings of Asiacrypt 04 (Jeju Island, Korea)