On Bounded Storage Key Agreement and One-Way Functions

Chris Brzuska Geoffroy Couteau **Christoph Egger** Willy Quach

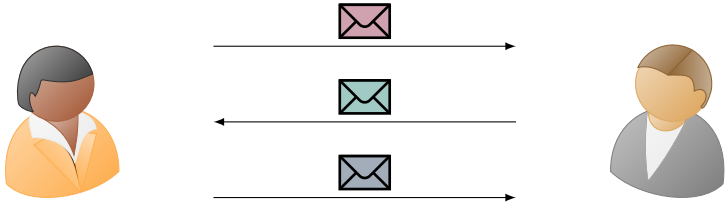
October 15, 2024

INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

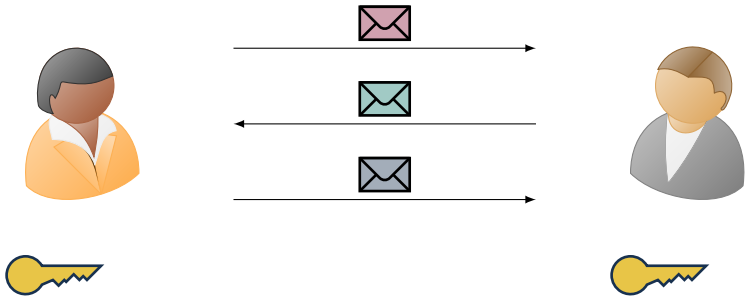
Université
Paris Cité

Marie Sklodowska-Curie
Math in Greater Paris

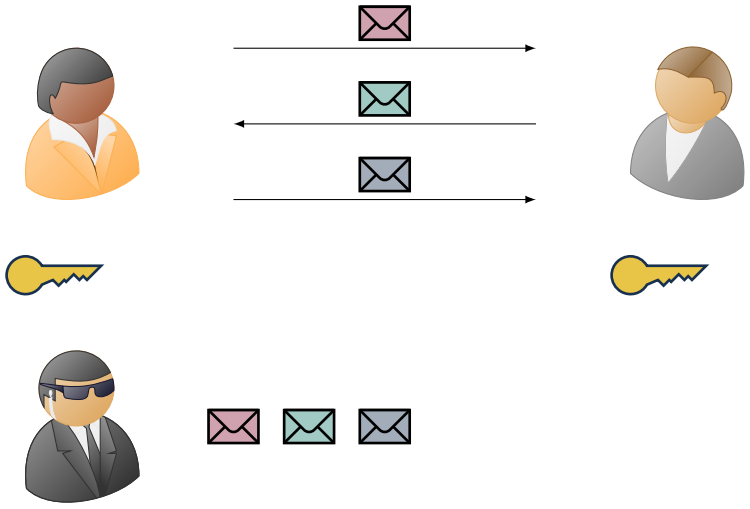
Key Agreement



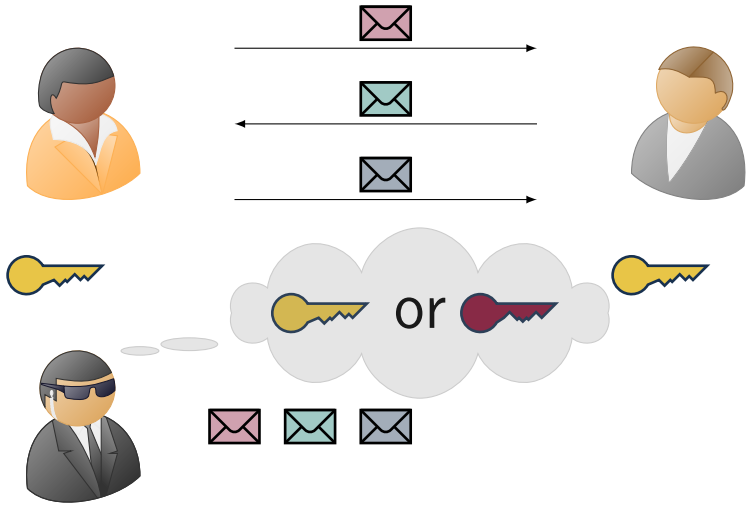
Key Agreement



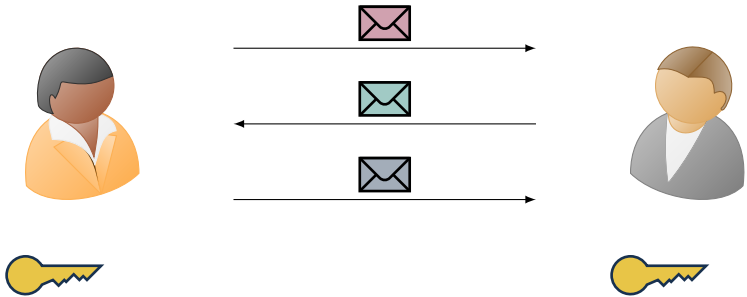
Key Agreement



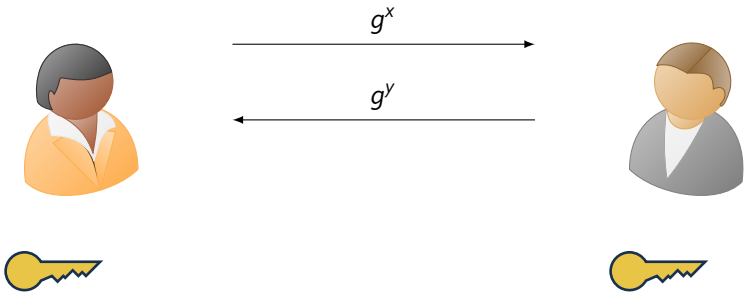
Key Agreement



Key Agreement



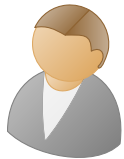
Key Agreement



Key Agreement

g^x

g^y



$(g^x)^y = g^{xy}$

$(g^y)^x = g^{xy}$

Birthday Bound Protocols

- Key Agreement without Public Key Cryptography
- “Cryptography if there is no Cryptography”

Birthday Bound Protocols

- Key Agreement without Public Key Cryptography
- “Cryptography if there is no Cryptography”

- Merkle Puzzles
- Key Agreement in Bounded Space

Birthday Bound Protocols

- Key Agreement without Public Key Cryptography
- “Cryptography if there is no Cryptography”

- Merkle Puzzles
- Key Agreement in Bounded Space

- Simple, Combinatorial Protocols
- Allows Study of Fundamental Bounds (e.g., Communication Complexity)

Birthday Bound Protocols

- Key Agreement without Public Key Cryptography
- "Cryptography if there is no Cryptography"

- Merkle Puzzles
- Key Agreement in Bounded Space

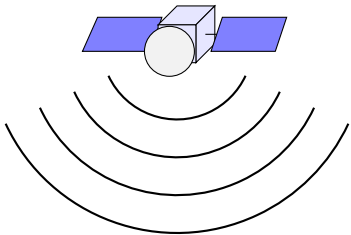
- Simple, Combinatorial Protocols
- Allows Study of Fundamental Bounds (e.g., Communication Complexity)

- Here: Restrict Adversary's Memory **and** Runtime

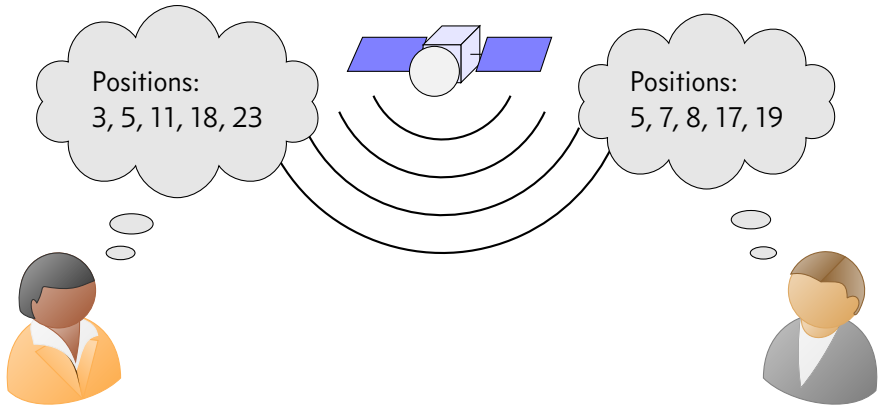
Outline

- Key Agreement in Bounded Space
- …using Computational Assumptions
- …implying Computational Hardness

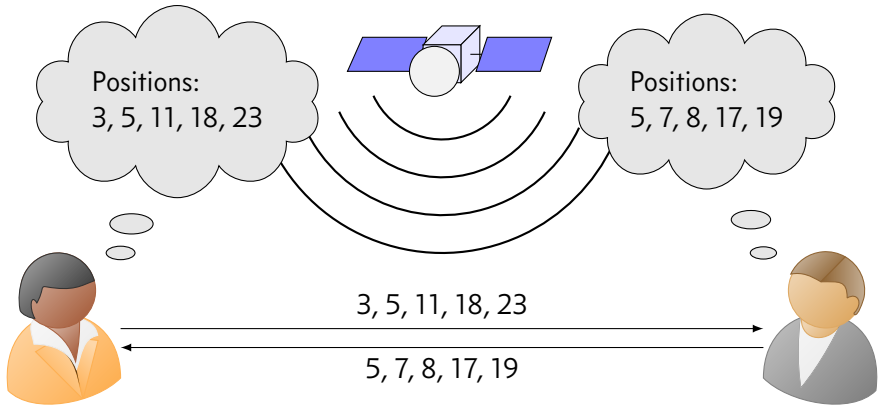
In Bounded Space [Cachin-Maurer]



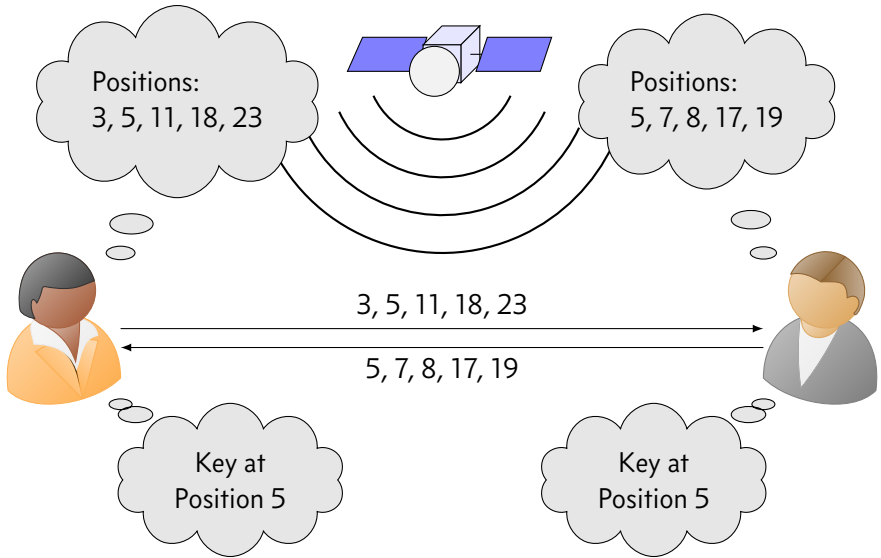
In Bounded Space [Cachin-Maurer]



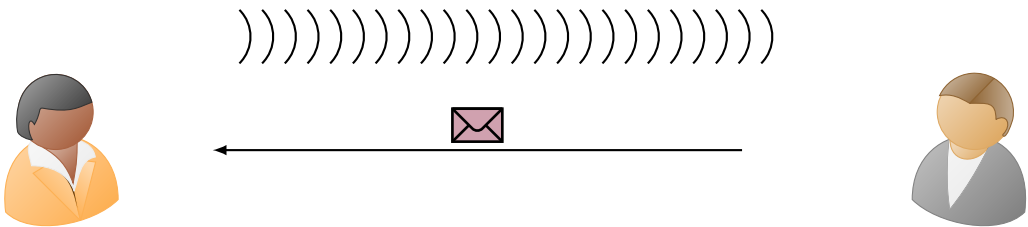
In Bounded Space [Cachin-Maurer]



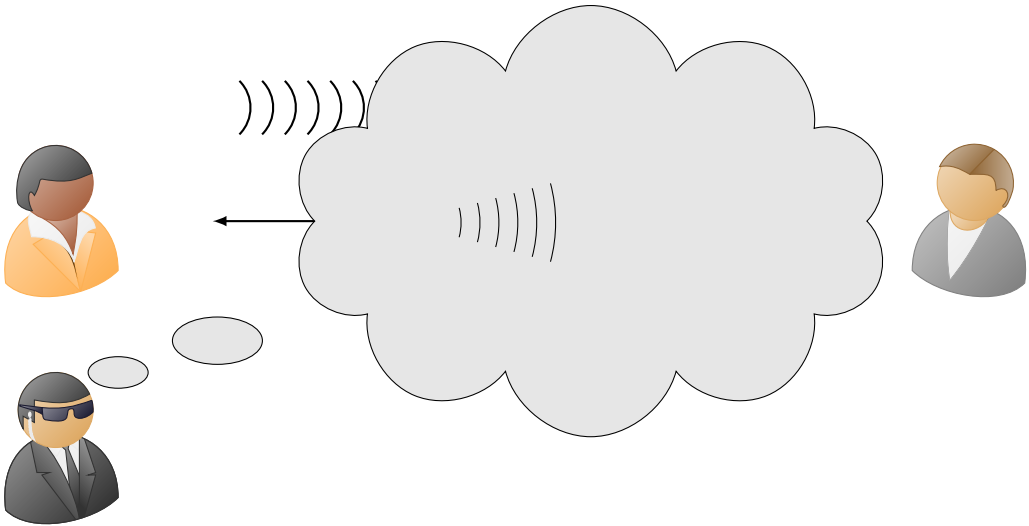
In Bounded Space [Cachin-Maurer]



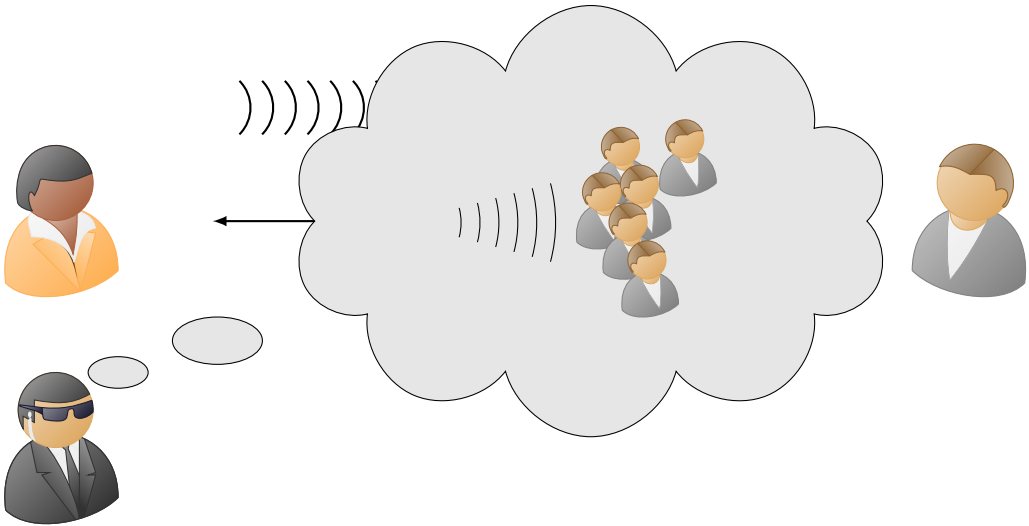
Lower Bounds [Dziembowski-Maurer]



Lower Bounds [Dziembowski-Maurer]



Lower Bounds [Dziembowski-Maurer]



Lower Bounds [Dziembowski-Maurer]

$I($  ,  $)$

becomes large

Information Theoretic Setting

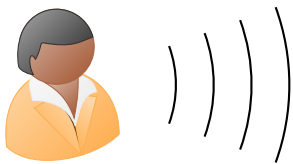
Theorem (Cachin-Maurer)

There exist key agreement protocols in bounded space for honest parties using space s that is secure against adversaries with $o(s^2)$ space.

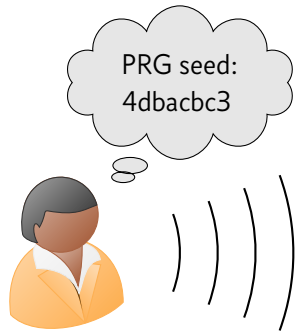
Theorem (Dziembowski-Maurer)

Any key agreement protocol for parties with space s can be broken in $O(s^2)$ space.

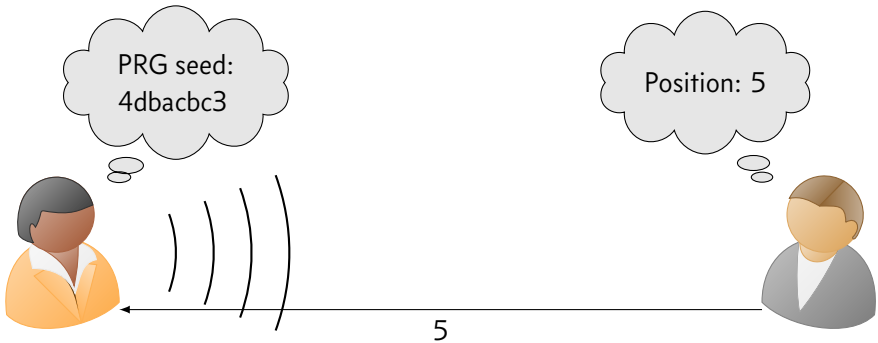
Using Computational Assumptions



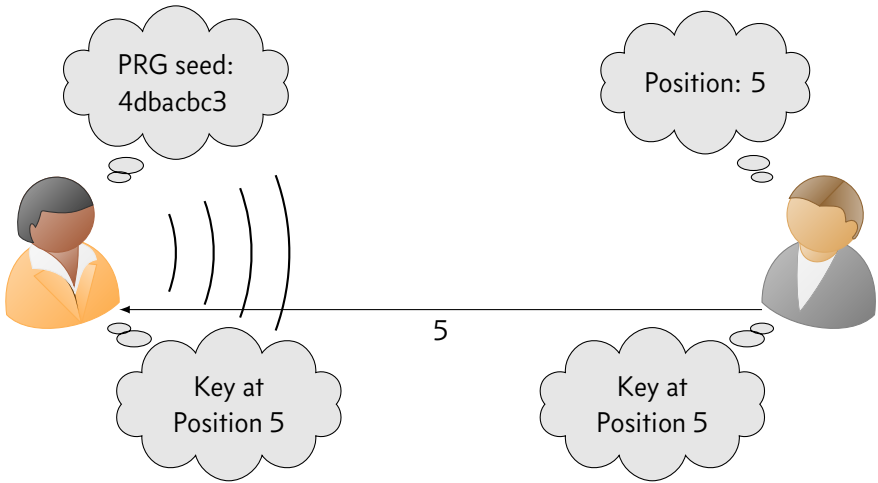
Using Computational Assumptions



Using Computational Assumptions



Using Computational Assumptions



Using Computational Assumptions

What does bounded space mean precisely? Fully Streaming Algorithms? “Unbounded Processing”?

Using Computational Assumptions

What does bounded space mean precisely? Fully Streaming Algorithms? “Unbounded Processing”?

Are Pseudo-Random Number Generators the **right** Cryptographic Tool?
In particular when considering space constraints?

Using Computational Assumptions

What does bounded space mean precisely? Fully Streaming Algorithms? “Unbounded Processing”?

Are Pseudo-Random Number Generators the **right** Cryptographic Tool?
In particular when considering space constraints?

Theorem (informal)

If Key Agreement in Bounded Space exists with better than information-theoretic bounds, then Pseudo-Random Number Generators exist.

Using Computational Assumptions

What does bounded space mean precisely? Fully Streaming Algorithms? “Unbounded Processing”?

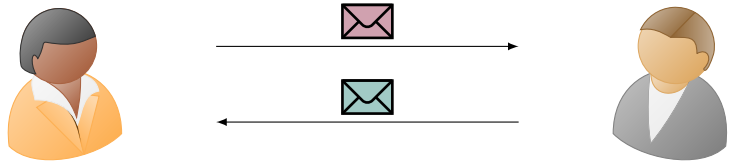
Are Pseudo-Random Number Generators the **right** Cryptographic Tool?
In particular when considering space constraints?

Theorem (informal)

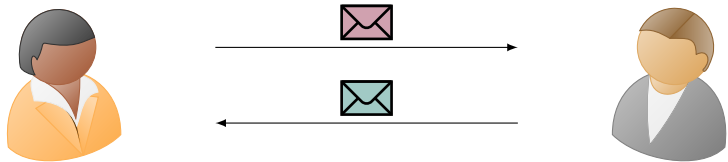
If Key Agreement in Bounded Space exists with better than information-theoretic bounds, then Pseudo-Random Number Generators exist.

$$\mathrm{KA} \Rightarrow \mathrm{dOWF} \Rightarrow \mathrm{wOWF} \Rightarrow \mathrm{OWF} \Rightarrow \mathrm{PRG} \Rightarrow \mathrm{PRF}$$

(Distributional) One-Way Functions

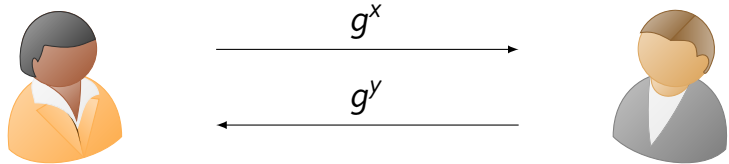


(Distributional) One-Way Functions



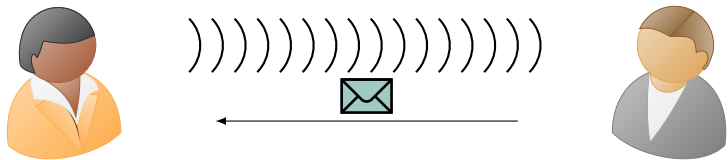
$$f(b, r_A, r_B, k^*) \rightarrow \begin{cases} \text{transcript}, k & \text{if } b = 0 \\ \text{transcript}, k^* & \text{if } b = 1 \end{cases}$$

(Distributional) One-Way Functions



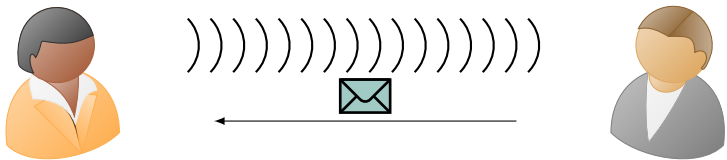
$$f(b, x, y, g^z) \rightarrow \begin{cases} g^x, g^y, g^{xy} \text{ if } b = 0 \\ g^x, g^y, g^z \text{ if } b = 1 \end{cases}$$

(Distributional) One-Way Functions



$$f(b, r_A, r_B, k^*) \rightarrow \begin{cases} \text{transcript}, k & \text{if } b = 0 \\ \text{transcript}, k^* & \text{if } b = 1 \end{cases}$$

(Distributional) One-Way Functions



$$f(b, r_A, r_B, k^*) \rightarrow \begin{cases} \text{👤, 👤, 👤, ✉, } k & \text{if } b = 0 \\ \text{👤, 👤, 👤, ✉, } k^* & \text{if } b = 1 \end{cases}$$

Summary

Theorem

For every polynomial p, there exist key agreement protocols secure against adversaries running in space $o(p(s))$ and time $\text{poly}(\lambda)$ if and only if One-Way functions exist.