On Generating the Initial Key in the Bounded-Storage Model

Main idea

Instead of assuming that

Motivation

Motivation

Common

Motivation

Common practice in cryptography:

If you need an encryption scheme then take AES (or IDEA, RSA, . . .). Y

A solution to the problem

How to solve this problem?

A solution to the problem

How to solve this problem?

We have to assume that the adversar

A solution to the problem

A solution to the problem

How to solve this problem?

We have to assume that the adversary cannot store the entire communication between the users.

One of the following options come to mind:

1. make some non-standard assumptions about the communication channel (eg. quantum, noisy, . . .)
2. simply assume that the amount of transferred data is to large to be stored in the memory of the adversary.

More on the model

Nice fact about the BSM

Let us assume that

the memory of *Eve* is smaller than the length of the randomizer.

(a precise bound on *Eve's*

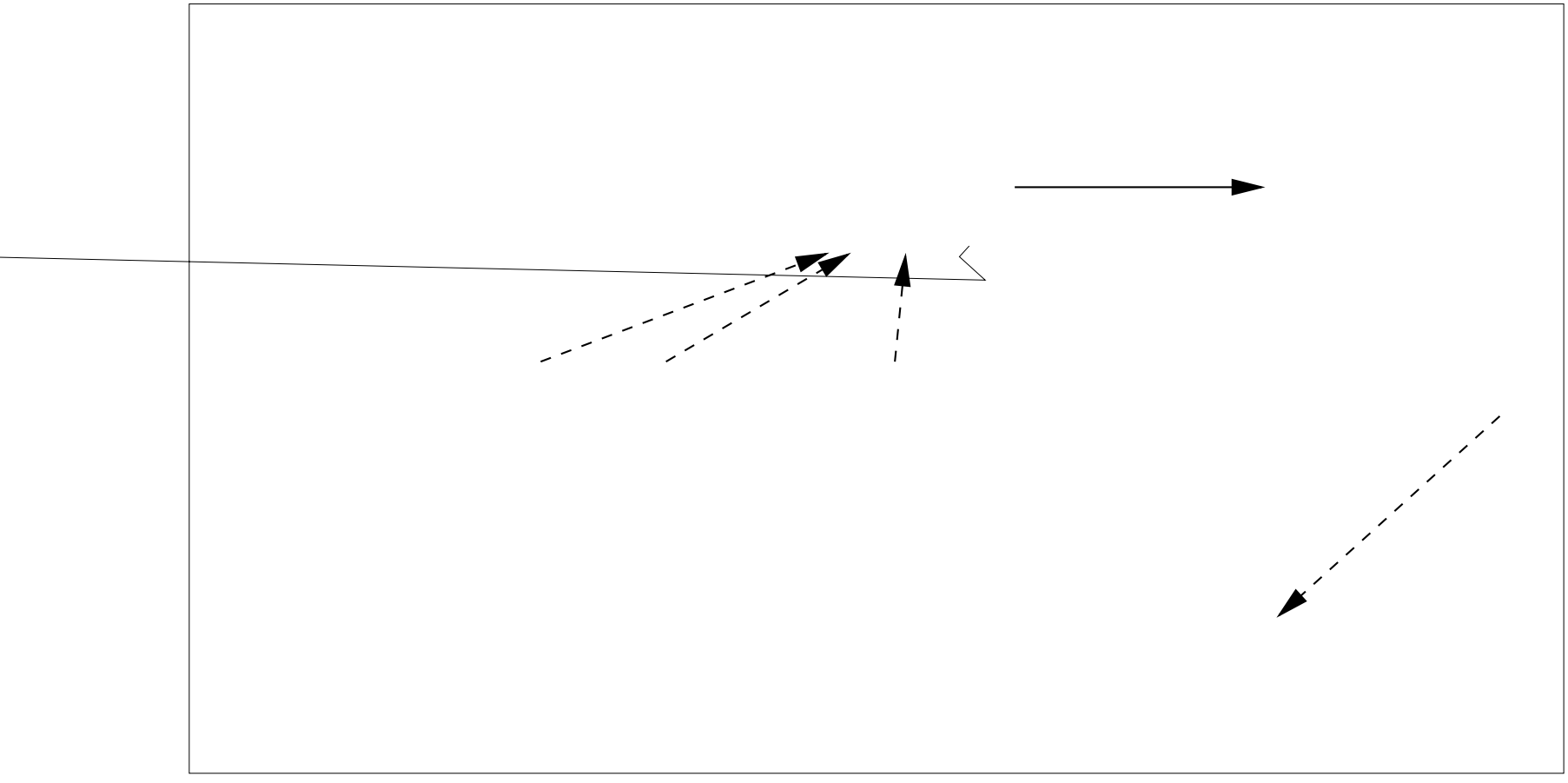
Secret-key encryption in the BSM

Secret-key encryption schemes in the BSM can be viewed as

stream-ciphers

Secret-key encryption in the

Secret-key derivation



The scheme of Aumann and Rabin

The simplest one is a

The scheme of Aumann and Rabin

The simplest one is a function deriving one bit:

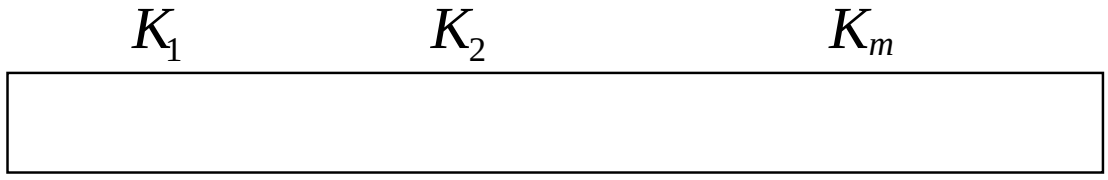
The scheme of Aumann and Rabin

The simplest one is a function deriving one bit:

— security parameter

— length of the randomizer

initial key: $K = (K_1, \ldots, K_m)$, with $1 \leq K_1 < \cdots < K_m \leq$.



Plan

1. A short introduction to the Bounded Storage

Q: How to generate the initial key?

The initial key can be generated:

- in the BSM itself.

  this is called a secret-key agreement in the BSM.

Key agreement in the BSM

The scenario for the

Key

Key agreement in the BSM

The scenario for the key agreement in the BSM is essentially the same as for the secret key-derivation, with the following differences:

- *Alice* and *Bob* don't share any initial key.
- It's essential that the algorithms for *Alice* and *Bob* are randomized.

It was already studied in

Our result

— the memory size of *Alice*

— the memory size of *Bob*

t — the memory size of *Eve*

Plan

1. A short introduction to the Bounded Storage Model. $\surd$
2. Our contributions.
   - Key-Agreement in the BSM $\surd$
   - Hybrid Model ⬅

The hybrid model (1/2)

In the K -hybrid model the initial key is generated by classical (complexity-based) method K

The hybrid

The hybr

The hybrid model (2/2)

The „hybr

The hybrid model (2/2)

The „hybr

The hybrid

Private Infor

Private Information Retrieval (1/2)

PIR is a protocol between two parties:

-

Private Information Retrieval (1/2)

PIR is a protocol between two parties:

-

Private Information Retrieval (1/2)

PIR is a protocol between two parties:

- A user U holding an input $\in \{1, \ldots,$].
- A database $\mathcal{L}$ holding an input $V = (V_1, \ldots, V_n \in \mathcal{L}\{0,$

Private Information Retrieval (1/2)

Private Information Retrieval (2/2)

Every PIR protocol should satisfy the following:

> The total number of bits exchanged between the par

Private Information Retrieval (2/2)

Every PIR protocol should satisfy the following:

The construction of $\mathcal{A}$

DH — the Diffie-Hellman protocol
PIR_1 — the protocol of [KO97].

The construction of $\mathcal{A}$

DH — the Diffie-Hellman protocol
PIR_1 — the protocol of [KO97].

We construct

The construction of $\mathcal{A}$

DH — the Diffie-Hellman protocol

PIR — the protocol of [

Π_A is secure

We now have the following:

Claim: Assuming PIR_1

The attack

1. In the first phase:
   - For each  *Eve* acts

Open problem

Open problem

The key-agreement protocol in our example is very artificial.

One may conjecture that all „natural” key-agreement protocols are „safe” in the context of the BSM.

Question: How to