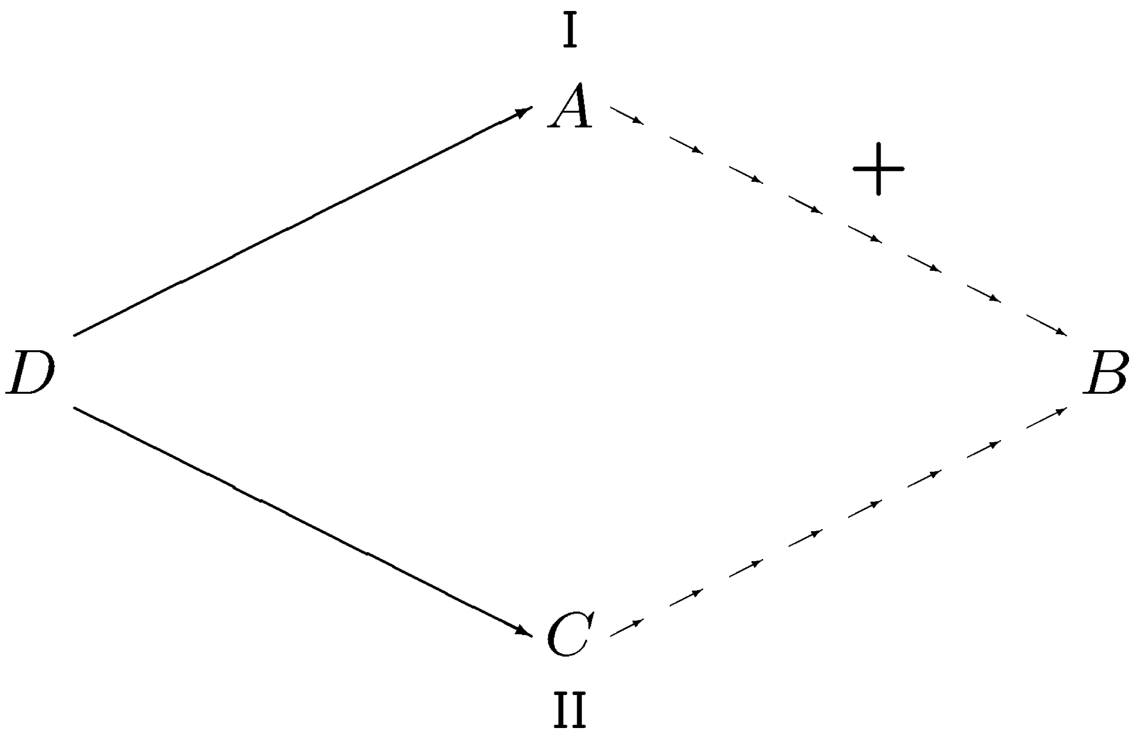
Cryptography in the Context of Kolmogorov Entropy

Alexei Semenov Andrej Muchnik

Institute of New Technologies
Moscow

Cryptographical problem in Kolmogorov theory of complexity:



$K(B|AD) \approx 0$
$K(B|CD) \approx K(B|C)$
$K(D) \approx K(B|A)$

($\approx$ holds up to logarithm of lengths)

The Aim:
for any given values
$K(A), K(B), K(C),\ K(AB), K(BC), K(AC), K(ABC)$

- either to prove that for all such A, B, C the problem has a solution (D exists)

- or to prove that for some such A, B, C the problem has no solution.

$K(A) \approx \ell(A),\ K(B) \approx \ell(B),\ K(C) \approx \ell(C).$

1. $K(B|C) \approx 0$

   $K(B|CD) \approx K(B|C)$ for any D

2. $K(B|A) \approx 0$

   D is empty word

3. $K(A|C) \lnsim K(B|C)$

   The problem is never solvable:
   if $K(B|AD) \approx 0$, then $K(B|CD) \lesssim K(A|C)$

4. $K(ABC) \approx K(A) + K(B) + K(C)$,
   $K(A) \gtrsim K(B)$

   $D = A' \oplus B$,
   where A' is a beginning of A, $\ell(A') = \ell(B)$

$I(A:B) \approx 0$, $I(B:C) \approx 0$, $I(A:C) \approx 0$

Theorem 1

$K(A) \gtrsim 2K(B)$

The problem is always solvable.

Theorem 2

$K(A) \lesssim 2K(B)$

The problem can be unsolvable.

Moreover, $\forall A, B$
if $K(A) \lesssim 2K(B)$, then
$\exists C \;\; \forall D$
$$K(B|AD) \approx 0 \wedge K(D) \approx K(B) \Rightarrow K(B|CD) \lesssim K(B)$$
(in addition,
$K(B|AC) \approx 0$, $K(C) \leq K(B) + \gamma \log K(B)$)

The proof is based on effective constructing an auxiliary function f with several properties.

In particular, the condition $K(B|AC) \approx 0$ is provided by the property $f(AC) = B$.

We look for the function f in a finite set. Namely, we consider finite functions that map binary words of length $\ell(A)+\ell(C)$ into binary words of length $\ell(B)$.

Using a probabilistic argument, it is proved that the fraction of functions without the properties required is negligibly small.

The properties of f that we require are effectively verifiable, if the function K is known.

But K is not computable.

Consider a finite set of functions similar to K by their combinatorial properties.

As f, we take a function that has the properties required for all of those K-like functions. Even in this case, a probabilistic argument shows that there exists such function f.

Thus we can find f by exhaustive search.