Entropy Loss and Random Functions

Andrea Röck
INRIA, projet CODES

INRIA

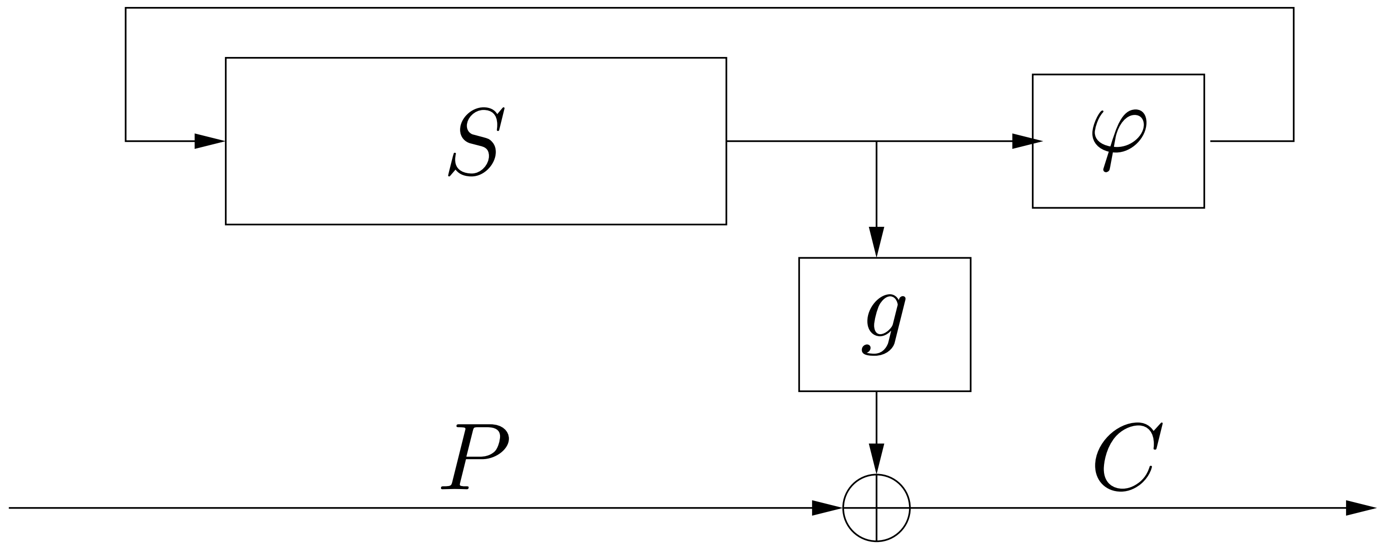
Outline

Part 1
Introduction

Random Function

By *random function* we refer to a function φ which was randomly chosen out of $\mathcal{F}_n = \{\varphi : \Omega_n \to \Omega_n\}$, where Ω_n is a set of n elements.

Stream Cipher Model



- S state with $s_t \in \Omega_n$, $t \geq 0$
- $\varphi \in \mathcal{F}_n$ random function which updates S
- P plaintext
- C ciphertext
- g filter function

Entropy of the State

- $\{p_i\}_{i=1}^n$ distribution of initial state
- $p_i^\varphi(t)$ probability of i after t iterations of φ
- entropy:

$$H_t^\varphi = \sum_{i=1}^n p_i^\varphi(t) \log_2 \left(\frac{1}{p_i^\varphi(t)} \right)$$

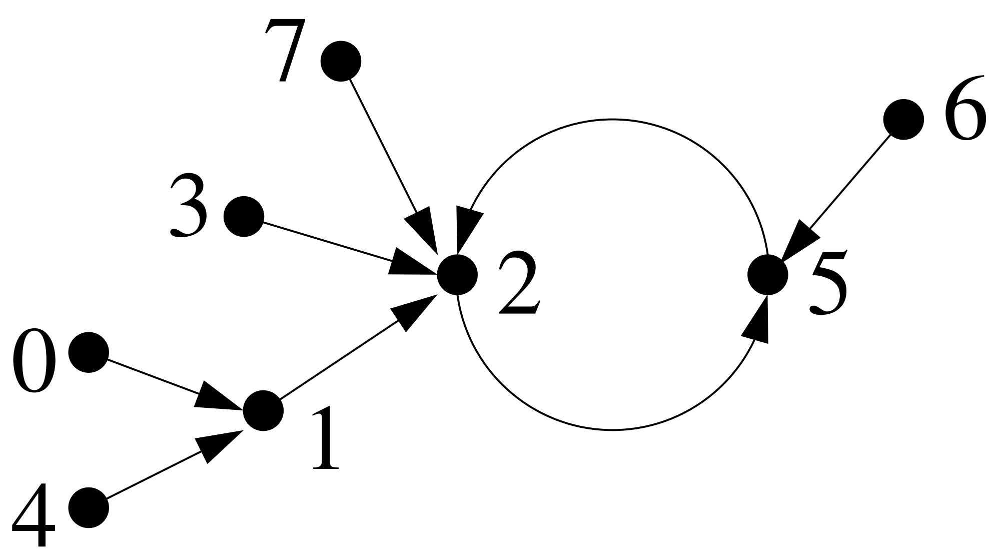
- $E(H_t)$ expected entropy after k iterations

Part 2

Entropy Loss

Properties of Random Functions (1) [Flajolet, Odlyzko 98]

$$f(x) = x^2 \mod 8$$



Properties of Random Functions (2) [Flajolet, Odlyzko 98]

- Expected number of image points after k iterations is

$$(1 - \tau_k)n$$

with $\tau_0 = 0$ and $\tau_{k+1} = e^{\tau_k - 1}$.
- Expected cicle points $cp(n) = \sqrt{\frac{\pi\ n}{2}}$.
- Expected maximal tail length $mtl(n) = \sqrt{n\ 2\pi} \log(2)$.

Properties of Random Functions (3) [Flajolet, Odlyzko 98]

- Expected number of r-nodes after one iteration is

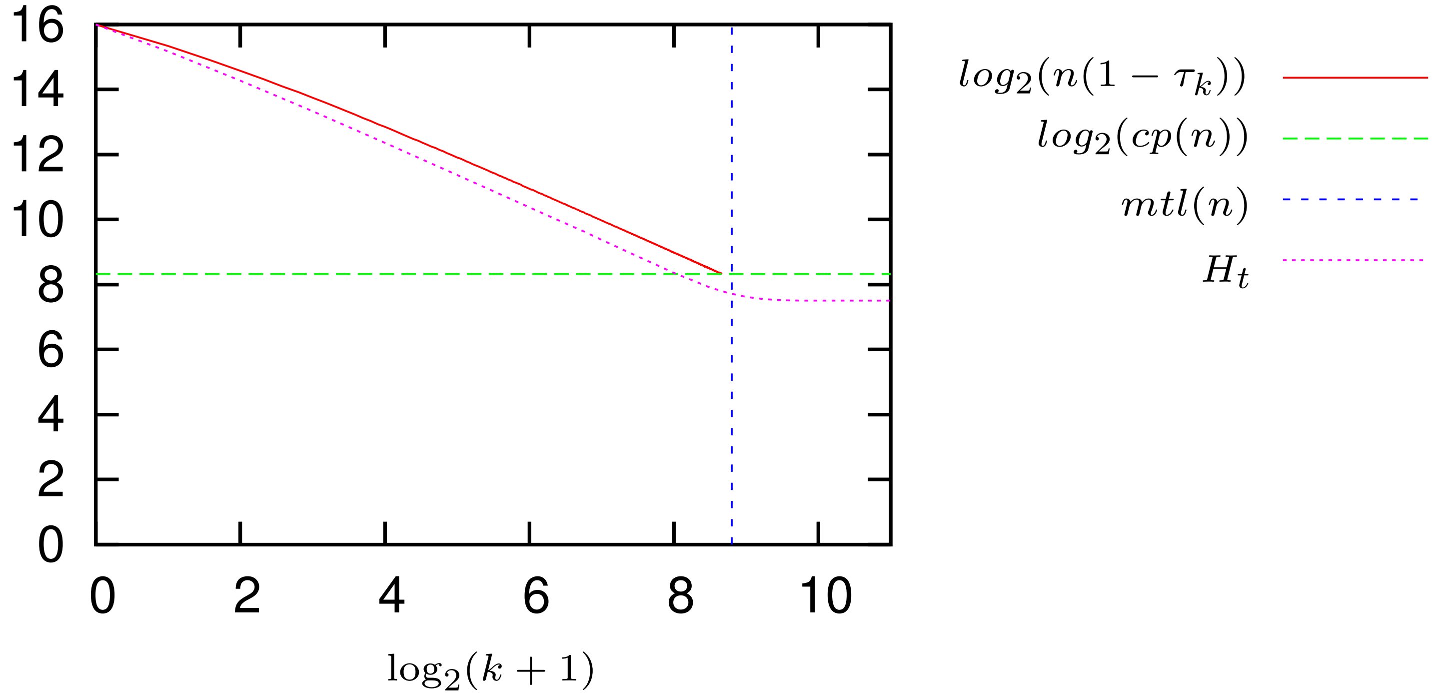
$$\frac{n}{e}\frac{1}{r!}$$

(By an r-node we refer to a node with r incomming edges in the functional graph or respectively a preimage of size r)

Upper bound with image points

$$E(H_t) \leq log_2(n) - log_2(1-\tau_k)$$

for
- $k \leq mtl(n)$ and
- $(1-\tau_k)n \geq cp(n)$.



Entropy by means of r nodes

- Uniform initial distribution

$$E(H_1^U) = \frac{n}{e}\sum_{r=1}^{n} \frac{1}{r!}\frac{r}{n}\log_2 \frac{r}{n}$$

- Arbitrary initial distribution

$$\frac{1}{\binom{n}{r}} \sum_{1\le i_1<\ldots<i_r\le n} (p_{i_1}+\ldots+p_{i_r}) \log_2 \frac{1}{p_{i_1}+\ldots+p_{i_r}}$$

Comparison for $n = 2^{16}$

Method	Approximation	$n = 2^{16}$
image points	$log(n) - 0.6617$	15.3383
r nodes (uniform)	$log(n) - 0.8272$	15.1728
test		15.1728

Part 3

Attacks