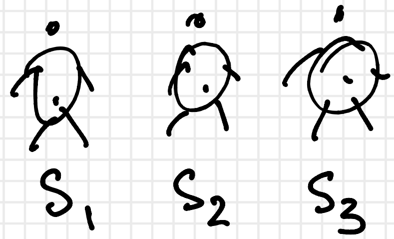
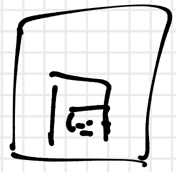
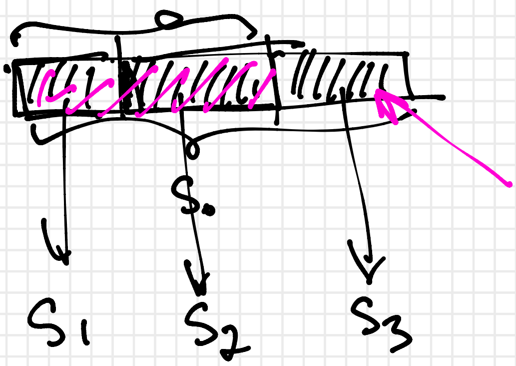
15.12.2020 (Part 2) secret sharing

---

① $S_0 \to \{0,1\}^n$







$S_1, S_2, S_3 \to \{0,1\}^n$

$S_0 = S_1 \oplus S_2 \oplus S_3$

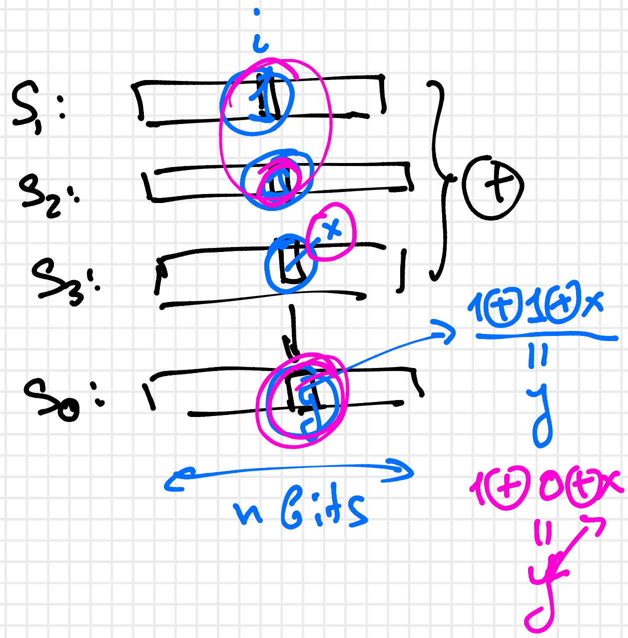
$\langle S_0, S_1, S_2, S_3 \rangle$

$\boxed{S_0 = S_1 \oplus S_2 \oplus S_3}$

(1) ✓ $H(S_0 \mid S_1, S_2, S_3) = 0$

(2) ✓ $H(S_0 \mid S_i\, S_j) = H(S_0)$

$H(S_0 \mid S_i) = H(S_0)$



$\langle S_0, S_1, S_2, S_3 \rangle$

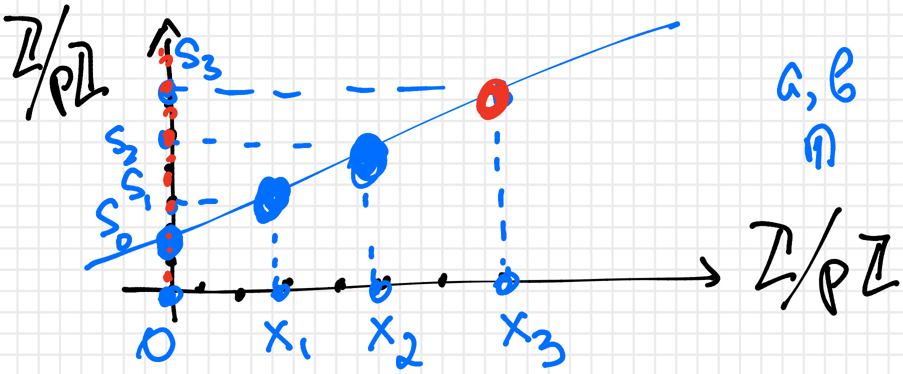
$$\begin{cases} (1) & H(S_0 \mid S_1 S_2) = H(S_0 \mid S_1 S_3) = H(S_0 \mid S_2 S_3) = 0 \\ (2) & H(S_0 \mid S_1) = H(S_0 \mid S_2) = H(S_0 \mid S_3) = H(S_0) \end{cases}$$

$S_0 : \underbrace{\{0, 1, \ldots, p-1\}}_{(\mathbb{Z}/p\mathbb{Z})}$ p: premier

$\lceil \log p \rceil = n$

$\boxed{f(x)=a\cdot x+b}$ ←

$a,b\in \mathbb{Z}/p\mathbb{Z}$



a, b

$$\begin{cases} S_0 = a\cdot 0+\underline{b} = f(0) \\ S_1 = a\cdot x_1+b = f(x_1) \ \checkmark \\ S_2 = f(x_2) \\ S_3 = f(x_3) \ \checkmark \end{cases}$$

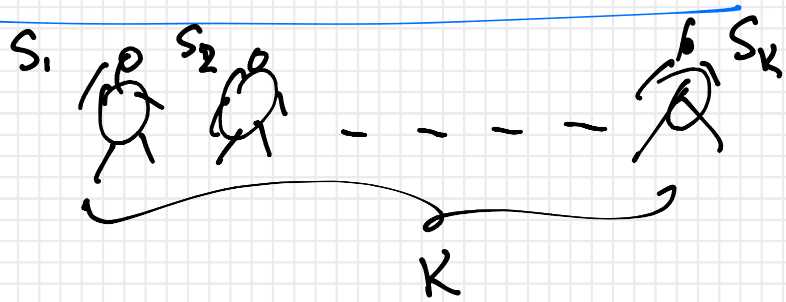
$\langle a,b\rangle \longrightarrow \langle S_0,S_1,S_2,S_3\rangle$

$\langle S_i,S_j\rangle \rightarrow (a,b) \longrightarrow S_0=f(0)$

$S_i \not\rightarrow S_0$

$S_0 \in \mathbb{Z}/p\mathbb{Z}$

$S_1 \dots S_K$



(1) $H(S_0|S_{i_1}\dots S_{i_t})=0$

$t\leq K$

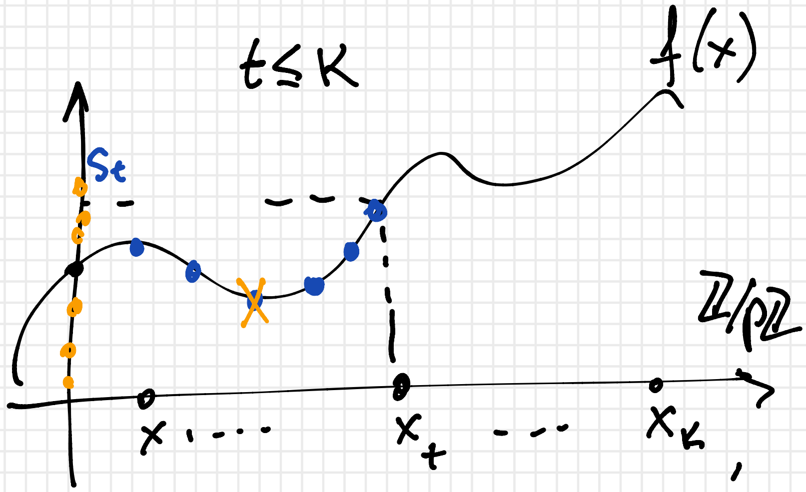
(2) $H(S_0|S_{j_1}\dots S_{j_{t-1}})=H(S_0)$

$f(x)=a_0+a_1x+\dots+a_{t-1}x^{t-1}$

$a_i\in \mathbb{Z}/p\mathbb{Z}$

$\deg(f)\leq t-1$

S_0



$$\begin{cases} S_0=f(0) \\ S_i=f(x_i) \end{cases}$$

① $S_1\dots S_t$

↓

$f(x)$

↓

$S_0=f(0)$

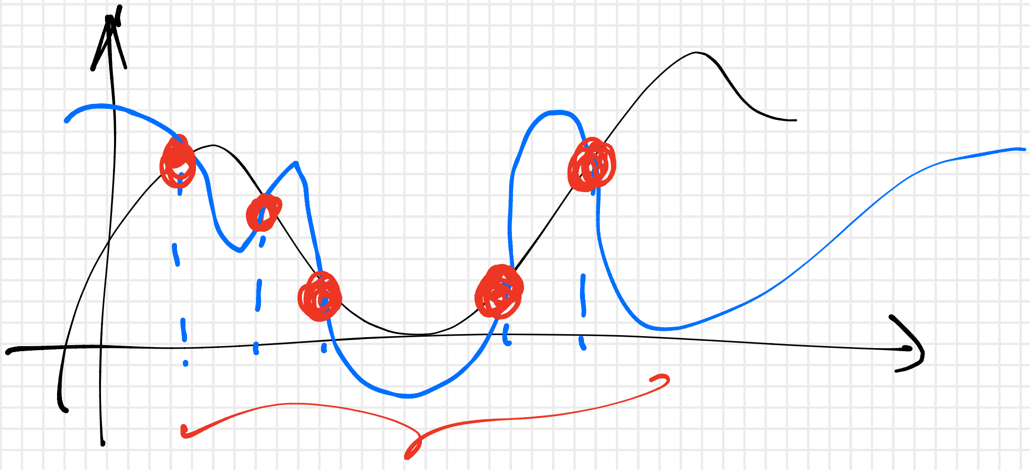
② $S_1\dots S_{t-1}$

$\not\downarrow$

S_0

$\boxed{\text{Shamir}}$ 1979

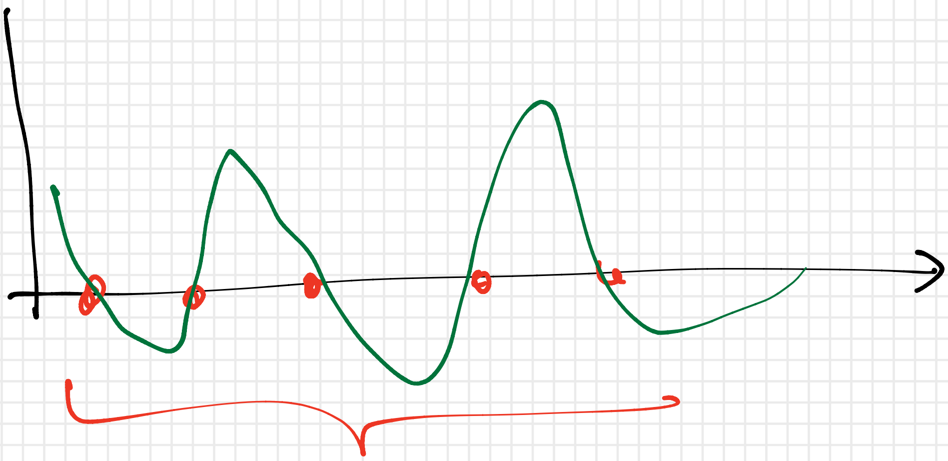
$$f(x) = a_0 + a_1 x + \dots + a_{t-1} \cdot x^{t-1}$$



t

$$g(x) = b_0 + \dots + b_{t-1} \cdot x^{t-1}$$

$\underbrace{f(x) - g(x)}_{\deg(f-g) < t}$:



t

$\mathbb{F}_q$ $\mathbb{F}_{2^n}$

Théorie de l'info algorithmique

$k = \underbrace{00\ldots\ldots 0}_{128}$

$c_i = m_i \oplus k_i = m_i$

$$Pr[k = \underbrace{00\ldots\ 0}_{128}] = 1/2^{128}$$

$$Pr[k = \underbrace{1\ldots 0\ 1\ldots 0}_{128}] = 1/2^{128}$$

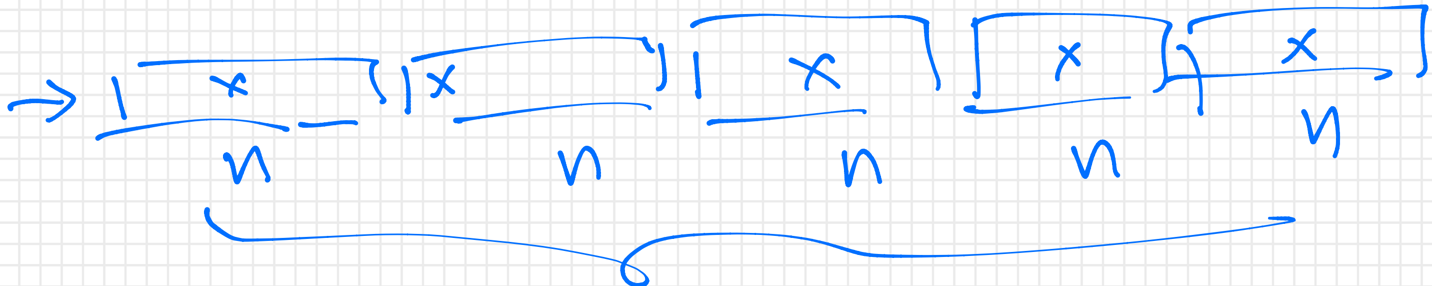
L : une langue de progr.

$L : p \longmapsto x \rightsquigarrow L(p) = x$

<u>Def</u> $C_L(x) = \min\{|p| : L(p) = x\}$

x est aléatoire si $C_L(x) \approx |x|$

$xxxxx$



$C_L(xxxxx) \approx n + \ldots \ll 5 \cdot n$

$L : \{0,1\}^* \longrightarrow \{0,1\}^*$ fonction calculable (partielle)

Def $C_L(x) = \min\{|p| \mid L(p) = x\}$
∞ si $\forall p\ L(p) \neq x$

Def $L_1 \prec L_2$ si $\exists d$
$\forall x\ C_{L_1}(x) \leq C_{L_2}(x) + d$

Th Il existe L_0 t.q. $\forall L$
$L_0 \prec L$

Def $C(x) := C_{L_0}(x)$ complexité de Kolmogorov

MT

$p_0 \quad L_0$
$p_1 \quad L_1$
$p_2 \quad L_2$
$p_3 \quad L_3$
$\vdots \quad \vdots$
$p_n \quad L_n$
$\vdots \quad \vdots$
$p_m \quad L_m$

L_{opt}: $\quad \underbrace{\underbrace{111\ldots1}_{m}\,\boxed{0}\,\overbrace{\boxed{10110\ldots1}}^{q}}_{p}$ $\quad \underbrace{L_m(q)}_{\text{résultat}}$

$$C_{L_{opt}}(x) \leq \underbrace{C_{L_i}(x)}_{\min\{|q| : L_i(q) = x\}} + \underbrace{i+1}_{Const_i}$$

$$p = \overbrace{\underbrace{11111\ldots1}_{i}0q}$$

$H(\alpha)$ $\qquad$ $H(\alpha \mid \beta)$

$C(x)$ $\qquad$ $C(x \mid y)$

Def $L' : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ (calculable)

$$C_{L'}(x \mid y) = \min\{|p| : L'(p, y) = x\}$$

$$y \xmapsto{p} x$$

<u>Def</u> $L'_1 \prec L'_2$ si $\exists d \ \forall x \forall y \ C_{L'_1}(x \mid y) \leq C_{L'_2}(x \mid y) + d$

<u>Th</u> $\exists L'_{opt}$ t.q. $\forall L'_i \quad L'_{opt} \prec L'_i$

<u>Def</u> $C(x \mid y) := C_{L'_{opt}}(x \mid y)$

Properties

① $\exists d \ \forall x \in \{0,1\}^* \quad C(x) \le |x| + d$

$\{ \text{print } "\underbrace{x_0 x_1 x_2 \ldots x_n}_{|x|}" ; \} \quad ||$

$L_{st} : p \longmapsto p$

$C_{L_{st}}(x) = |x|$

$\exists d \ \forall x \quad C_{L_{opt}}(x) \le C_{L_{st}}(x) + d = |x| + d$

---

② $\exists d \ \forall x \in \{0,1\}^* \quad C(xx) \le |x| + d$

$L_{sp} : p \longmapsto pp$

$C_{L_{sp}}(xx) = |x|$

$C_{L_{sp}}(01) = \cancel{X} \ \infty$

$L_{sp} : \cancel{p} \longmapsto 01$

$\exists d \quad C_{L_{opt}}(xx) \le C_{L_{sp}}(xx) + d \le |x| + d$

③ $\exists d\ \forall x\quad C(xx) \leq C(x) + d$

$$L_{double} : p \longmapsto L_{opt}(p) \circ L_{opt}(p)$$

$$C_{L_{double}}(xx) = C_{L_{opt}}(x)$$

$\exists d$ $$C_{L_{opt}}(xx) \leq C_{L_{double}}(xx) + d = C_{L_{opt}}(x) + d$$

4 $\exists d\ \forall x \in \{0,1\}^*$

$$C(\underbrace{xxxx\ldots x}_{n}) \le |x| + \cancel{2}\log n + d$$

$$L: \quad \underbrace{\overset{n}{10110\ldots1}\,|\,\boxed{x}}_{p} \longmapsto \underbrace{xx\ldots x}_{n}$$

$$\underbrace{\overset{n}{10}|\overset{n}{01}|\overset{n}{10}|1}_{p}$$

$$C_L(\underbrace{xx\ldots x}_{n}) \le |x| + \lceil \log n \rceil$$

$$\exists d \quad C(xx\ldots x) \le C_L(x\ldots x) + d \le |x| + \lceil \log n \rceil + d$$
$$\le |x| + \log n + d + 1$$

$$L: \quad \underbrace{\underbrace{11}_{1}\ \underbrace{00}_{0}\ \underbrace{00}_{0}\ \underbrace{11}_{1}\ \underbrace{11}_{1}}_{n}\ 01\ \underbrace{0110\ldots1}_{x}\,| \longmapsto \underbrace{x\ldots x}_{n}$$

p

$$C_L(\underbrace{x\ldots x}_{n}) \le 2\lceil \log n \rceil + 2 + |x| \le 2\log n + |x| + 2 + 2$$

$$\exists d\ \forall x \quad C(\underbrace{x\ldots x}_{n}) \le C_L(x\ldots x) + d \le |x| + 2\log n + \underbrace{4 + d}_{\text{Const}}$$

5

$x = \underbrace{10110\ldots1}_{n}$

$p \cdot n$ "0"

$(1-p)n$ "1"

$$C(x) \le \left(p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}\right)\cdot n + O(\log n)$$

L : $\underbrace{1100001111\ .\ 00}_{bin(n)}01\ \underbrace{1100011\ldots 00}_{bin(pn)}01\ 1\ \text{index } x \mapsto x$

bin(n) → n → $2\lceil\log n\rceil$

01 → 2

bin(pn) → pn → $\le 2\lceil\log n\rceil$

01 → 2

x': $|x'| = n$

pn "0"

$(1-p)n$ "1"

$\log|S|$

liste des candidats x'

$$|S| = C_n^{pn} = 2^{\boxed{(\ldots)\cdot n} + O(\log n)}$$

Prop. $\forall n \; \exists x \in \{0,1\}^n : \; C(x) \geq n$

$\{0,1\}^n \leftarrow 2^n \; x$'s

$\exists x \in \{0,1\}^n$
$C(x) \geq n$

? x: $C(x) < n$

$\# x$: $C(x) = 0 \quad \leq 1$

$\# x$: $C(x) = 1 \leq \# p : |p| = 1 = 2$

$C(x) = 2 \qquad 4$

$\vdots$

$\# x$: $C(x) = n-1 \leq \# p : |p| = n-1 = 2^{n-1}$

$\leq 1 + 2 + \dots + 2^{n-1} = 2^n - 1$

x: $C(x) < n$

Ex: $\exists c \; \forall n$ pour 99% de $x \in \{0,1\}^n$

$$n - c \leq C(x) \leq n + c$$

Th $C(x)$ n'est pas calculable.

$|x| = n$

$L_{opt}(\Lambda) \stackrel{?}{=} x$
$L_{opt}(0) \stackrel{?}{=} x$
$L_{opt}(1) \stackrel{?}{=} x$ ...

$\dots L_{opt}(|[01 \dots 1]) \stackrel{?}{=} x$

$\leq n + C$

Shannon: Def $I(\alpha:\beta) = H(\beta) - H(\beta|\alpha)$

Kolmogorov: Def $I(x:y) \overset{\text{def}}{=} C(y) - C(y|x)$

Shannon: <u>Th.</u> $I(\alpha:\beta) = I(\beta:\alpha)$

$$= H(\alpha) + H(\beta) - H(\alpha,\beta)$$

Kolmogorov: <u>Th</u> $|I(x:y) - I(y:x)| \leq O(\log N)$

$$N = |x| + |y|$$

<u>Th'</u> $|I(x:y) - (C(x) + C(y) - C(xy))| \leq O(\log N)$

$$N = |x| + |y|$$

15/01

\# 16/12 Homework by 22/12 ←

\# ? suppl. ex. by 15/01