ALMOST UNIVERSAL HASH

Recall: $F_k(\cdot)$ is a VF-CMA PRF.

$$F' = F(H)$$

$F \equiv$ PRF

$H \equiv$ AU

$F' \equiv$ PRF !

Today: How to get H?

1) Take $\mathbb{F} = GF(2^n)$; any finite

has 2 operations : "+" and "·".

One finite element is n bits.

$\mathbb{G}, \mathbb{F}$

$$a = (a_0, a_1, \dots, a_n) \in \{0,1\}^n$$

$$a \longrightarrow p(X) = a_0 + a_1 \cdot X + \dots + a_{n-1} \cdot X^{n-1}$$

$a + b \in GF(2^n)$ $\quad p(X) + q(X)$

$a \cdot b \in GF(2^n)$

$s(X) = p(X) \cdot q(X) \longrightarrow$ degree $> n-1$?

Let $t(X)$ be "IRREDUCIBLE" polynomial of degree n. Divide $s(X)$ by $t(X)$.

$$(X^2+1)^2 = X^4 + 2X^2 + 1$$

$$\underline{X^2+1} \;\; | \;\; X^n + 1 \qquad \left(n \text{ even.} \; ?\right)$$

$\hookrightarrow$ REMAINDER

$a \cdot b \rightarrow r(X)$ s.t. $s(X) = u(X) \cdot t(X) + r(X)$

For us : $(\mathbb{F}, +, \cdot)$ $\quad \#\mathbb{F} = 2^n$.

Take $x = (x_1, \dots, x_d)$ with $x_i \in \mathbb{F}$

$N = n \cdot d$ $\quad h_s(\cdot) : \{0,1\}^N \to \{0,1\}^n$

The seed is $s = (a_1, \dots, a_d)$ $a_i \in \mathbb{F}$.

$$h_s(x) = \sum_{i=1}^{d} a_i \cdot x_i \quad \text{(INNER PRODUCT)}$$

This is AU. Take any $x = (x_1, \dots, x_d)$ and $x' = (x_1', \dots, x_d')$ and $\delta_i = x_i' - x_i$

As $x \neq x'$, i.f. $\delta_1 \neq 0$

Collision: $h_s(x) = h_s(x')$.

$$\sum a_i x_i = \sum a_i x_i' \iff 0 = \sum_{i=1}^{d} a_i \underbrace{(x_i' - x_i)}_{\delta_i}$$

$$a_1 \delta_1 = -\sum_{i=2}^{d} a_i \delta_i \iff a_1 = \underline{\left(-\sum_{i=2}^{d} a_i \delta_i\right)}$$

$$\Pr_{a}\left[h_a(x) = h_a(x')\right] = 2^{-n}. \qquad \delta_1 \rightsquigarrow \neq 0!$$

a
||
$(a_1, \ldots, a_d)$

2) Choose $s \leftarrow\$ \mathbb{F}$; $x = (x_1, \dots, x_d)$

$$h_s(x) = \sum_{i=1}^{d} x_i \cdot s^{i-1} = q_x(s)$$

$$q_x(S) = x_1 + x_2 \cdot S + x_3 \cdot S^2 + \dots + x_d \cdot S^{d-1}$$

$$h_s(x) = h_s(x') \iff q_x(s) = q_{x'}(s)$$

$$\iff q_{x-x'}(s) = 0$$

$$\iff \sum_{i=1}^{d} (x_i - x_i') \cdot s^{i-1} = 0$$

The degree of the polynomial $q_{x-x'}$ is $d-1$

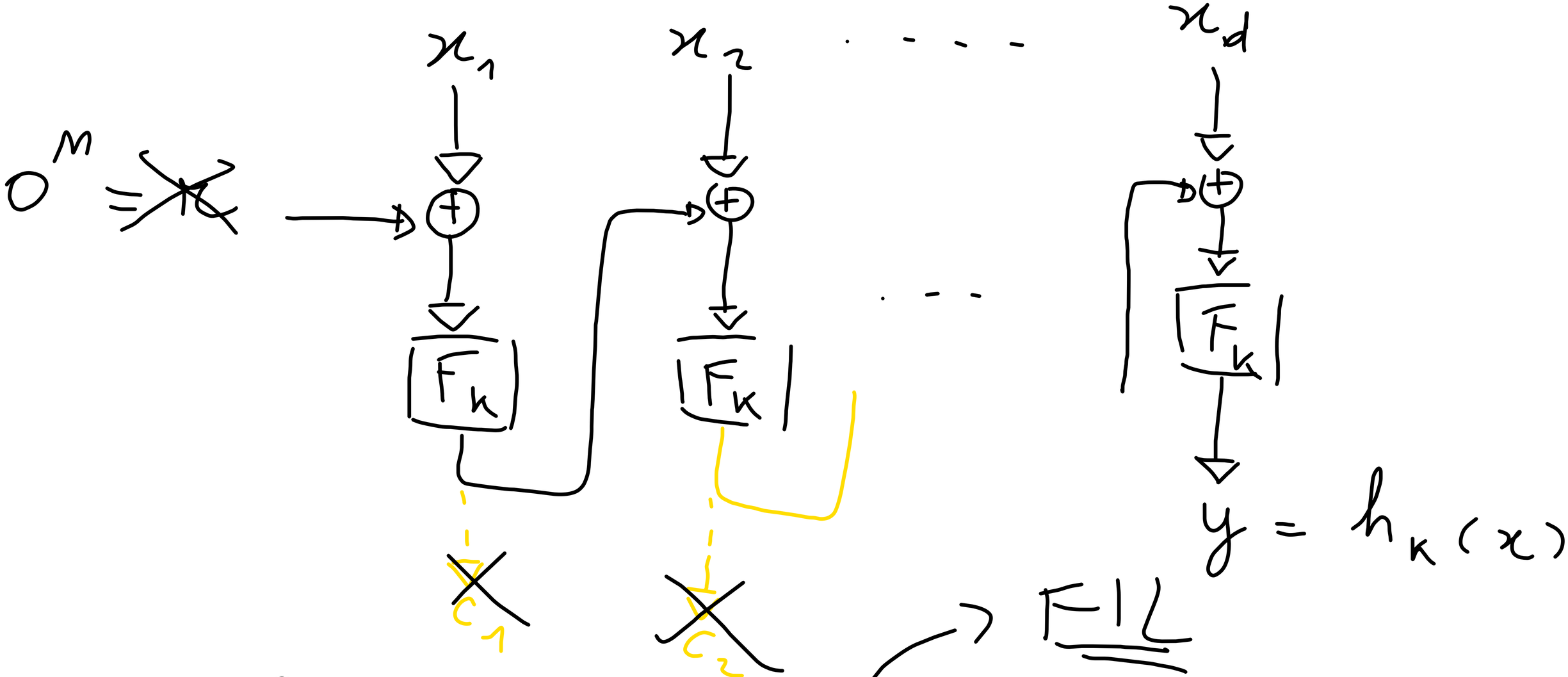
$$\Pr_s\left[q_{x-x'}(s) = 0 \right] = \frac{d-1}{\underbrace{|F|}_{2^n}} \approx \frac{N}{N \cdot 2^n} = d$$

$$= negl(n).$$

In practice: Practitioners construct COMPUTATIONAL ac

H is based on any PRF (AES).

CBC - MAC



Ex. CBC-MAC not secure if:

1) * All blocks are output; OR

2) * r is RANDOM (part of the tag)

FACT. $h_k(\cdot) \equiv$ CBC-MAC is AU.

$\Rightarrow$ CBC-MAC is directly UF-CMA for FIL.

$\Rightarrow$ $F_{k'}(\underbrace{CBCMAC_k(m)}_{h_k(m)})$ UF-CMA for VIL!

Encrypted CBC-MAC

Ex. CBC-MAC not UF-CMA for VIL.