SUCCINCT HOMOMORPHIC SECRET-SHARING

DAMIANO ABRAM

LANCE ROY

PETER SCHOLL

AARHUS UNIVERSITY

BOCCONI UNIVERSITY

HALF-CHOSEN VECTOR-OLE

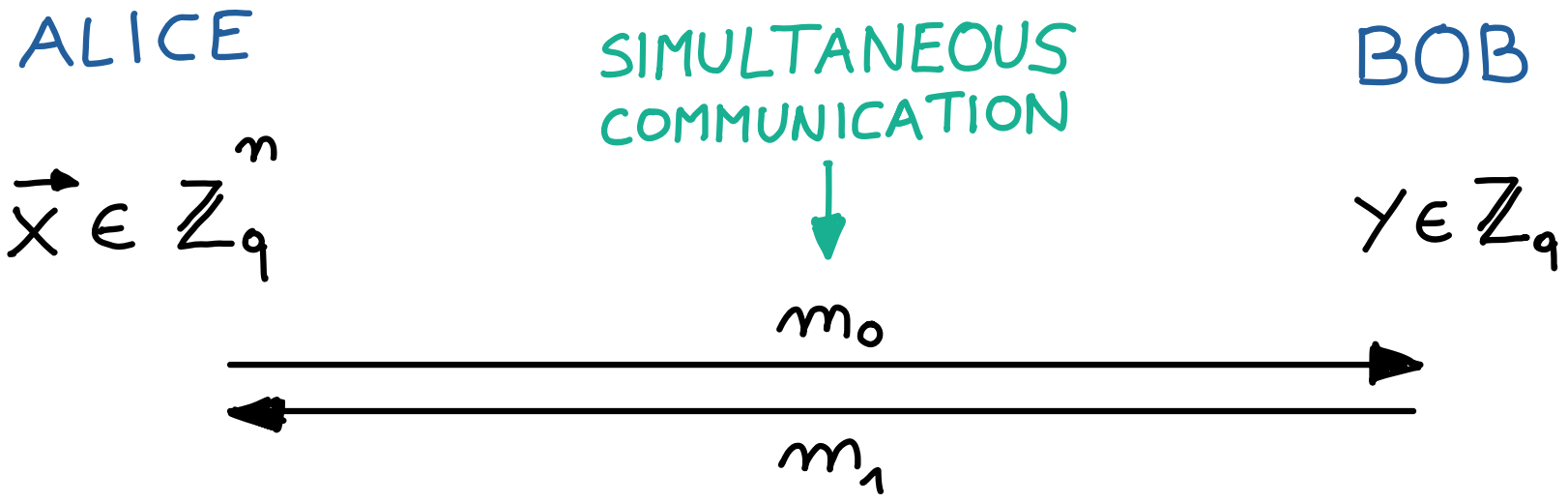
ALICE

$\vec{x} \in \mathbb{Z}_q^n$

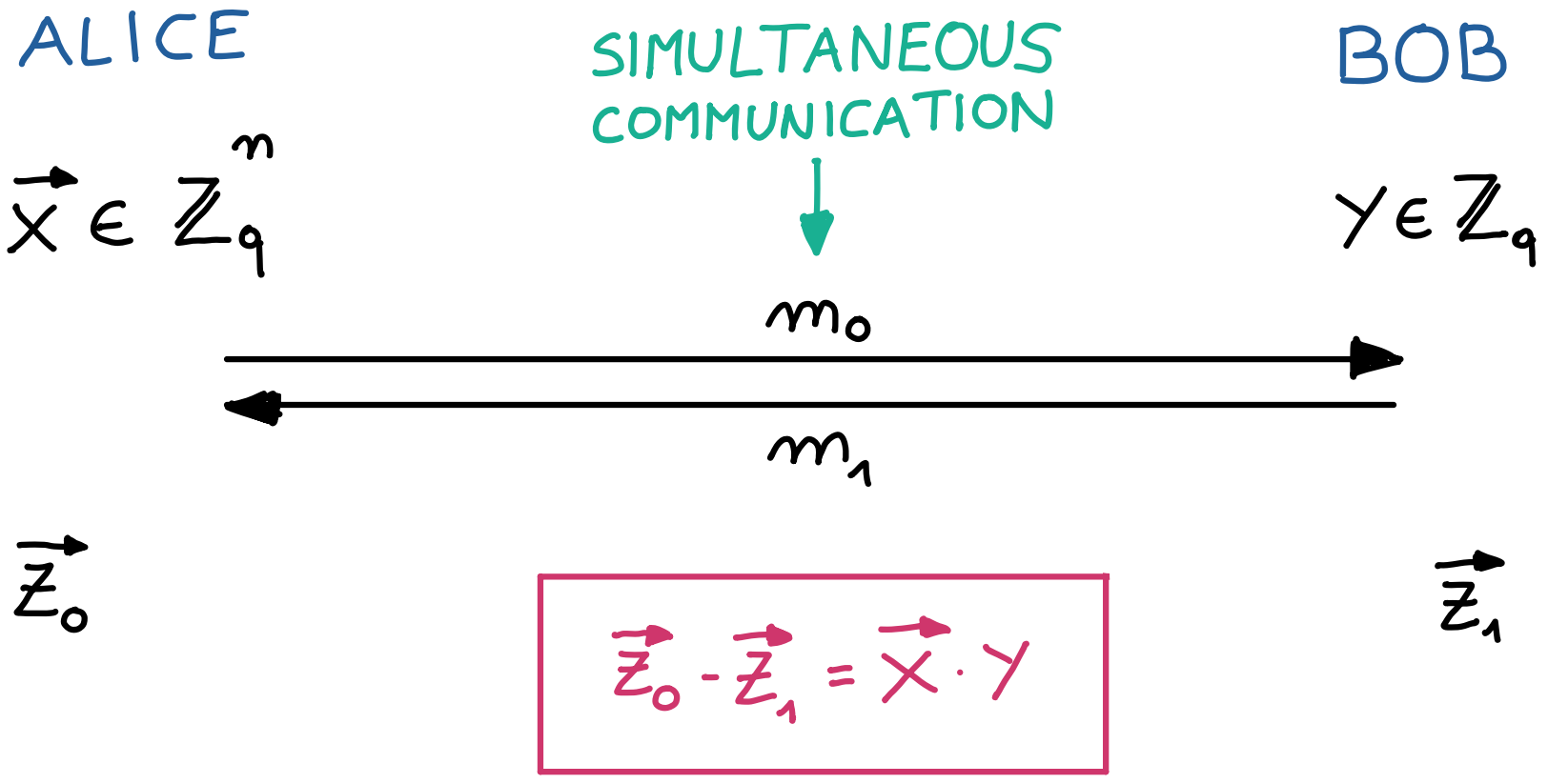
BOB

$y \in \mathbb{Z}_q$

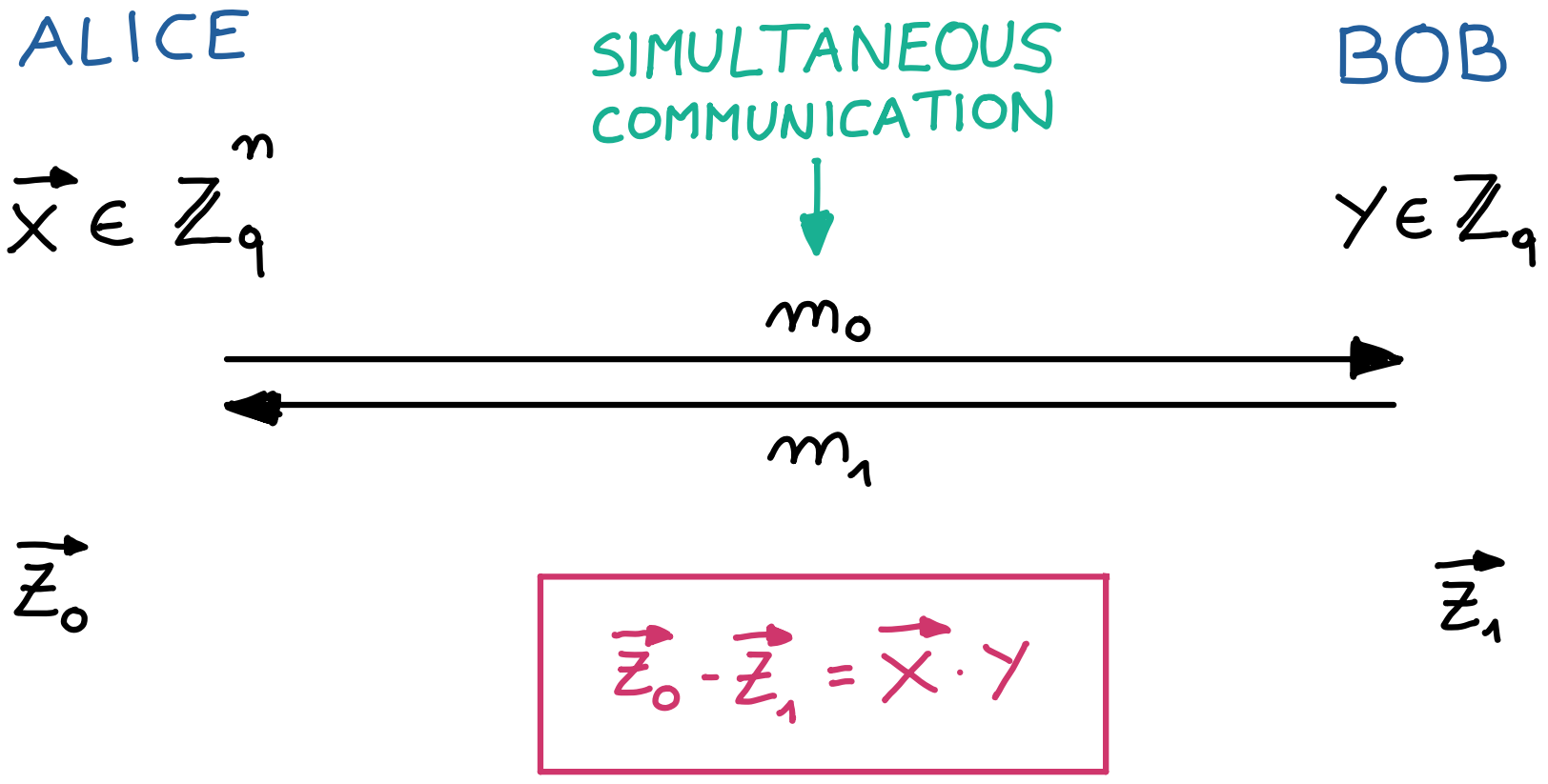
HALF-CHOSEN VECTOR-OLE



HALF-CHOSEN VECTOR-OLE

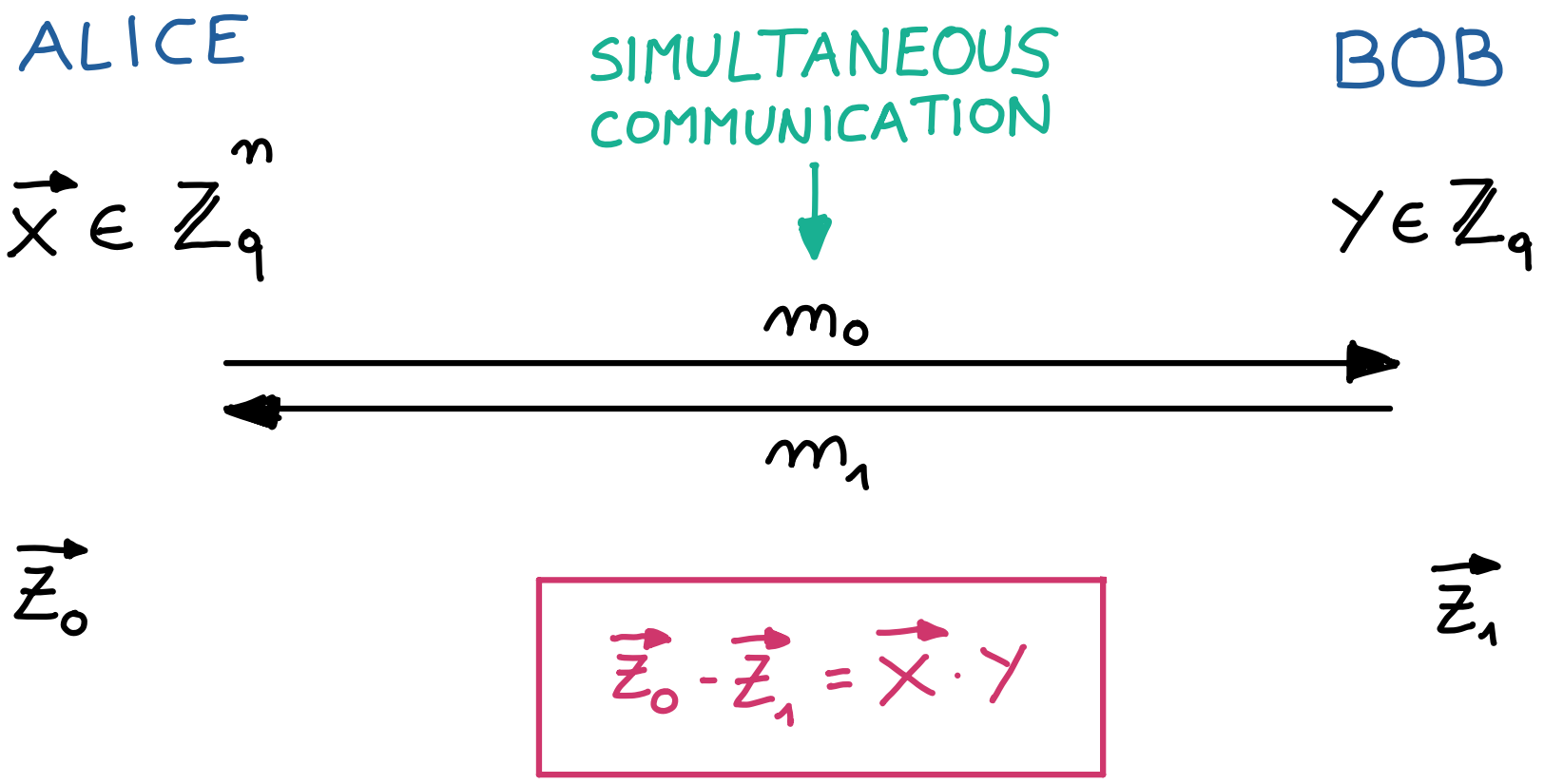


HALF-CHOSEN VECTOR-OLE



What's the minimal communication complexity?

HALF-CHOSEN VECTOR-OLE



What's the minimal communication complexity?

$\leq n^{\alpha} \cdot \text{poly}\,\lambda$ for $\alpha < 1$

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
DCR	$q = N$, RSA modulus	$O(n^{2/3})$

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
DCR	$q = N$, RSA modulus	$O(n^{2/3})$
DDH-like assumption over CLASS GROUPS	$q =$ any prime	$O(n^{2/3})$

trustless setup →

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
DCR	$q = N$, RSA modulus	$O(n^{2/3})$
DDH-like assumption over CLASS GROUPS	$q =$ any prime	$O(n^{2/3})$
QR	$q = 2$	$O(n^{2/3})$

trustless setup →

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
DCR	$q = N$, RSA modulus	$O(n^{2/3})$
DDH-like assumption over CLASS GROUPS	$q =$ any prime	$O(n^{2/3})$
QR	$q = 2$	$O(n^{2/3})$
LWE (with $\lambda^{\omega(1)}$ modulus-noise ratio)	any q	$O(n^{2/3})$

trustless setup →

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
POWER DDH over Paillier groups	$q = N$ or $q = 2$ RSA modulus	$O(n^{1/2})$

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
POWER DDH over Paillier groups	$q = N$ or $q = 2$ RSA modulus	$O(n^{1/2})$
POWER DDH over CLASS GROUPS	$q =$ any prime	$O(n^{1/2})$

SUCCINCT HALF-CHOSEN VECTOR-OLE

ASSUMPTION	$\mathbb{Z}_q$	COMMUNICATION COMPLEXITY
POWER DDH over Paillier groups	$q = N$ or $q=2$ RSA modulus	$O(n^{1/2})$
POWER DDH over CLASS GROUPS	$q =$ any prime	$O(n^{1/2})$
POWER - RING LWE (with $\lambda^{\omega(1)}$ modulus-noise ratio)	any q	$O(n^{1/2})$

trustless setup →

↑ new assumption!

APPLICATIONS

SUCCINCT HSS

secure 2-round computation of $\langle C(x), y \rangle$ ($C \in NC_1$)

with $(|x| + |y|^{\alpha}) \cdot \text{poly}(\lambda)$ communication $(\alpha < 1)$

APPLICATIONS

SUCCINCT HSS

secure 2-round computation of $\langle C(x), y \rangle$ ($C \in NC_1$)

with $(|x| + |y|^{\alpha}) \cdot \text{poly}(\lambda)$ communication $(\alpha < 1)$

PCG FOR N-PARTY DISTRIBUTED POINT FUNCTIONS

communication $(L \cdot T)^{\alpha} \cdot \text{poly}\,\lambda$ $(\alpha < 1)$

L: #DPFs; T: DOMAIN SIZE

APPLICATIONS

SUCCINCT HSS

secure 2-round computation of $\langle C(x), y \rangle$ ($C \in NC_1$)

with $(|x| + |y|^{\alpha}) \cdot \text{poly}(\lambda)$ communication $(\alpha < 1)$

PCG FOR N-PARTY DISTRIBUTED POINT FUNCTIONS

communication $(L \cdot T)^{\alpha} \cdot \text{poly}\,\lambda$ $(\alpha < 1)$

L: #DPFs, T: DOMAIN SIZE

N-PARTY COMPUTATION FOR LAYERED CIRCUITS WITH SUBLINEAR COMMUNICATION IN THE CIRCUIT SIZE

APPLICATIONS

SUCCINCT HSS

secure 2-round computation of $\langle C(x), y \rangle$ ($C \in NC_1$)

with $(|x| + |y|^{\alpha}) \cdot \text{poly}(\lambda)$ communication $(\alpha < 1)$

PCG FOR N-PARTY DISTRIBUTED POINT FUNCTIONS

communication $(L \cdot T)^{\alpha} \cdot \text{poly}\,\lambda$ $(\alpha < 1)$

L: #DPFs, T: DOMAIN SIZE

N-PARTY COMPUTATION FOR LAYERED CIRCUITS WITH SUBLINEAR COMMUNICATION IN THE CIRCUIT SIZE

1st construction

$O\left(N \cdot \frac{s}{\log \log s}\right)$ $s \leftarrow$ size of the circuit

APPLICATIONS

SUCCINCT HSS

secure 2-round computation of $\langle C(x), y \rangle$ ($C \in NC_1$)

with $(|x| + |y|^{\alpha}) \cdot \text{poly}(\lambda)$ communication $(\alpha < 1)$

PCG FOR N-PARTY DISTRIBUTED POINT FUNCTIONS

communication $(L \cdot T)^{\alpha} \cdot \text{poly}\,\lambda$ $(\alpha < 1)$

L: #DPFs, T: DOMAIN SIZE

N-PARTY COMPUTATION FOR LAYERED CIRCUITS WITH SUBLINEAR COMMUNICATION IN THE CIRCUIT SIZE

1st construction

$O\left(N \cdot \frac{s}{\log \log s}\right)$ $s \leftarrow$ size of the circuit

2nd construction

$O\left(N \cdot \frac{s}{\log s}\right)$ only for sufficiently wide circuits

BILINEAR HSS

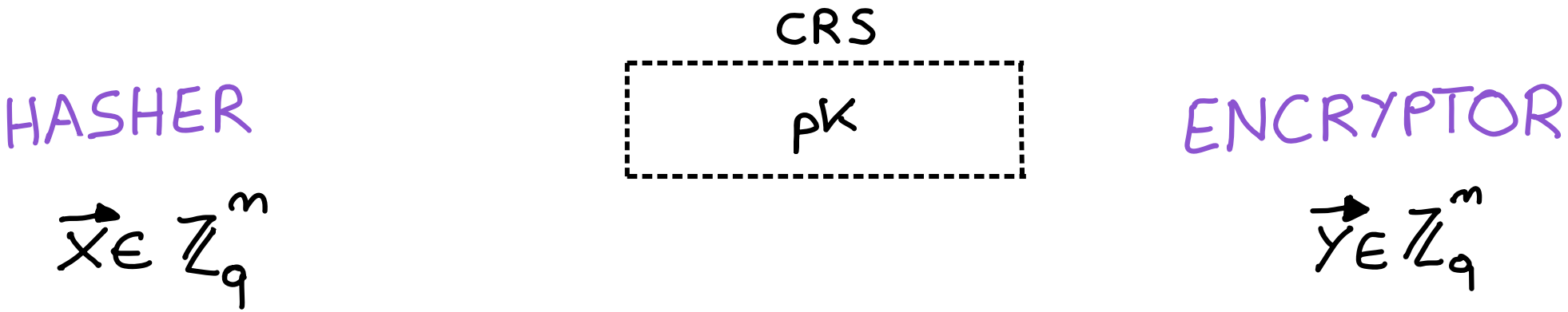
HASHER

$\vec{x} \in \mathbb{Z}_q^n$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

BILINEAR HSS



BILINEAR HSS

CRS

pk

HASHER

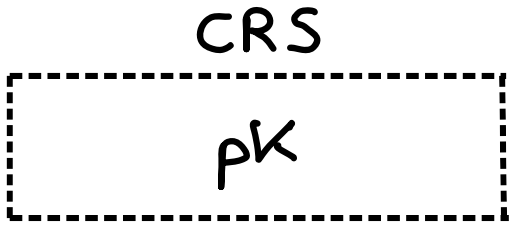
$\vec{x} \in \mathbb{Z}_q^n$

$(d, \pi) \xleftarrow{\$} \mathrm{Hash}(pk, \vec{x})$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

BILINEAR HSS



HASHER

$\vec{x} \in \mathbb{Z}_q^n$

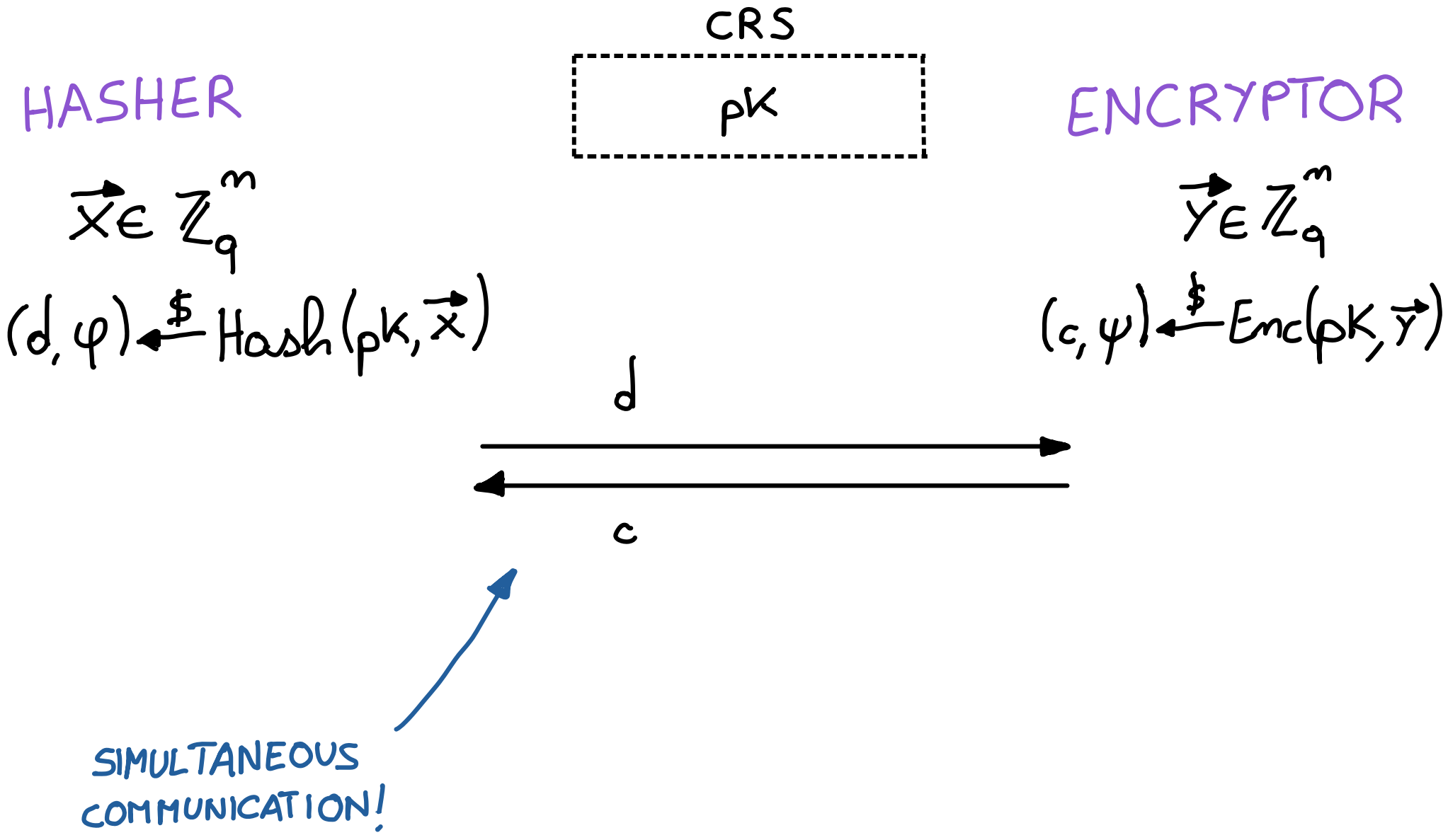
$(d, \pi) \xleftarrow{\$} \mathrm{Hash}(pk, \vec{x})$

ENCRYPTOR

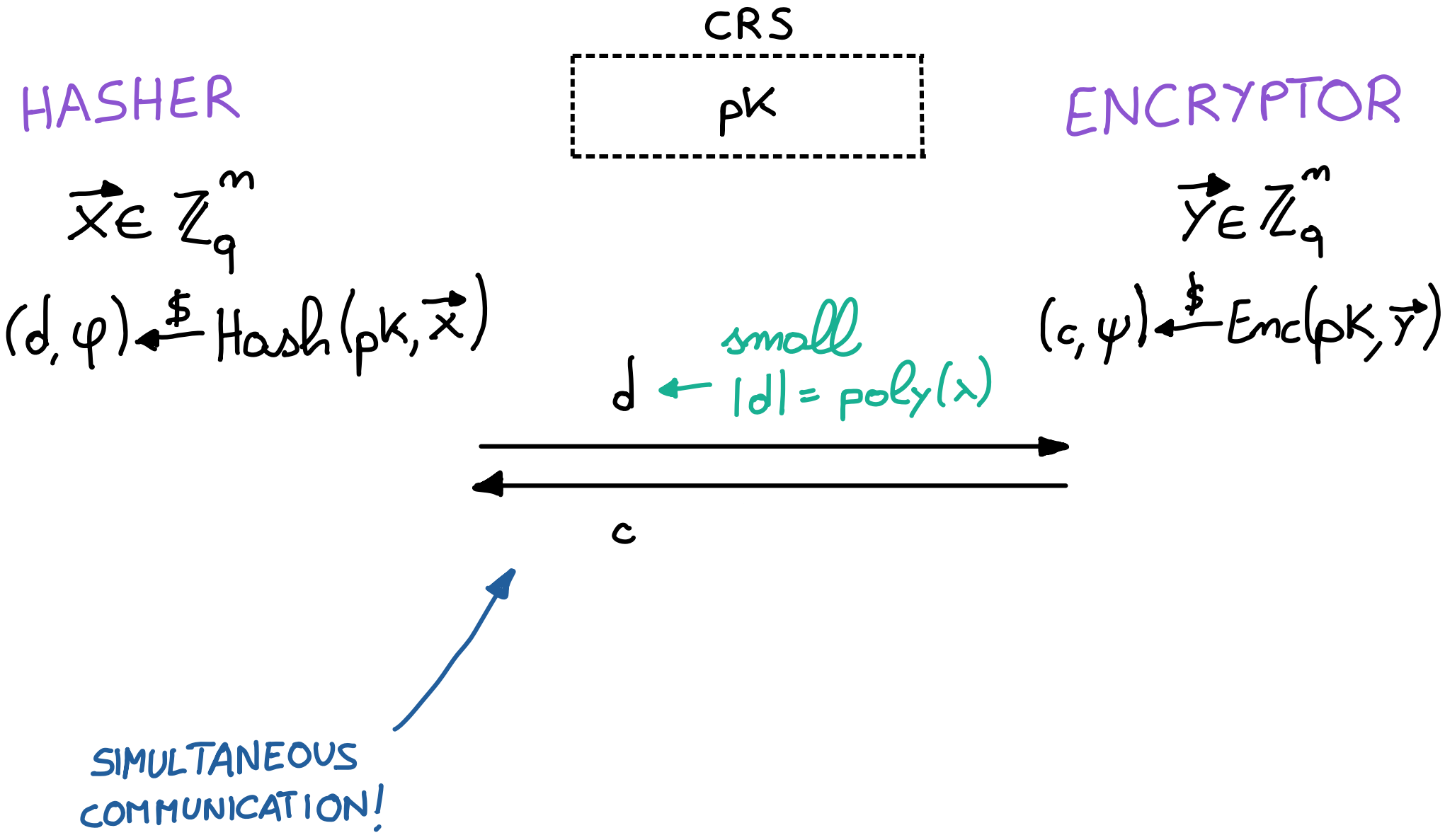
$\vec{y} \in \mathbb{Z}_q^n$

$(c, \psi) \xleftarrow{\$} \mathrm{Enc}(pk, \vec{y})$

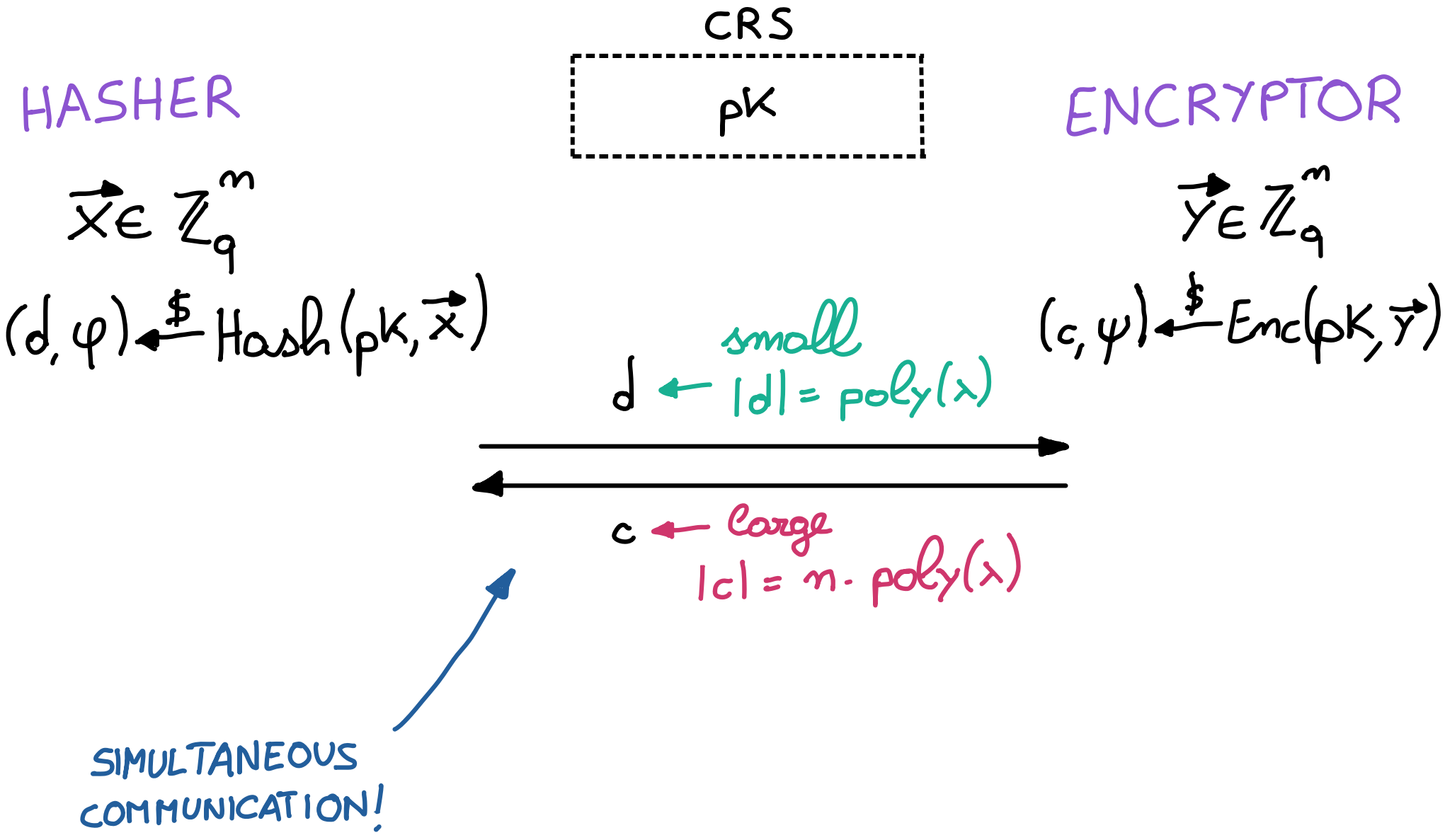
BILINEAR HSS



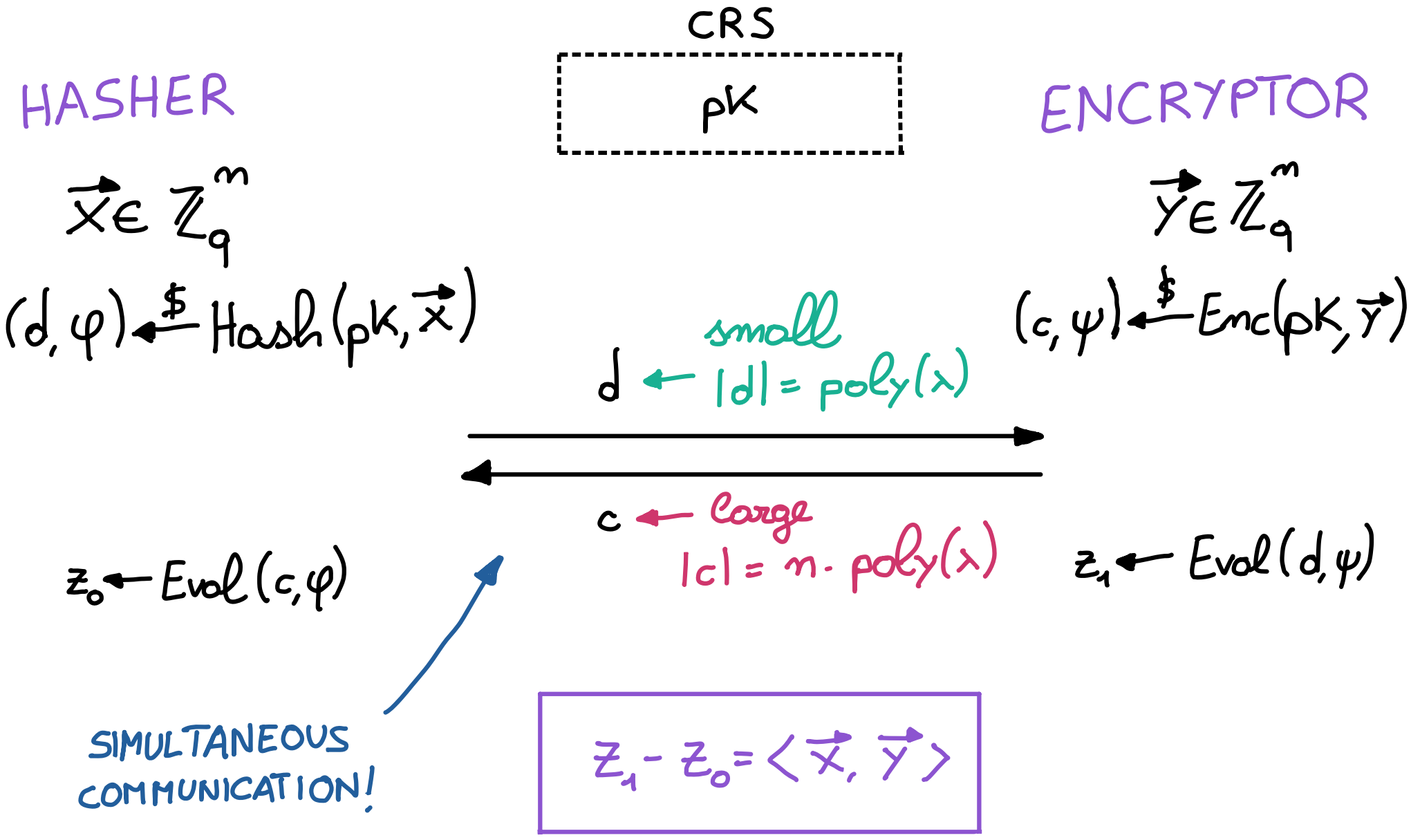
BILINEAR HSS



BILINEAR HSS



BILINEAR HSS



FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE

ALICE

$\vec{x} \in \mathbb{Z}_q^n$

BOB

$y \in \mathbb{Z}_q$

FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE

ALICE

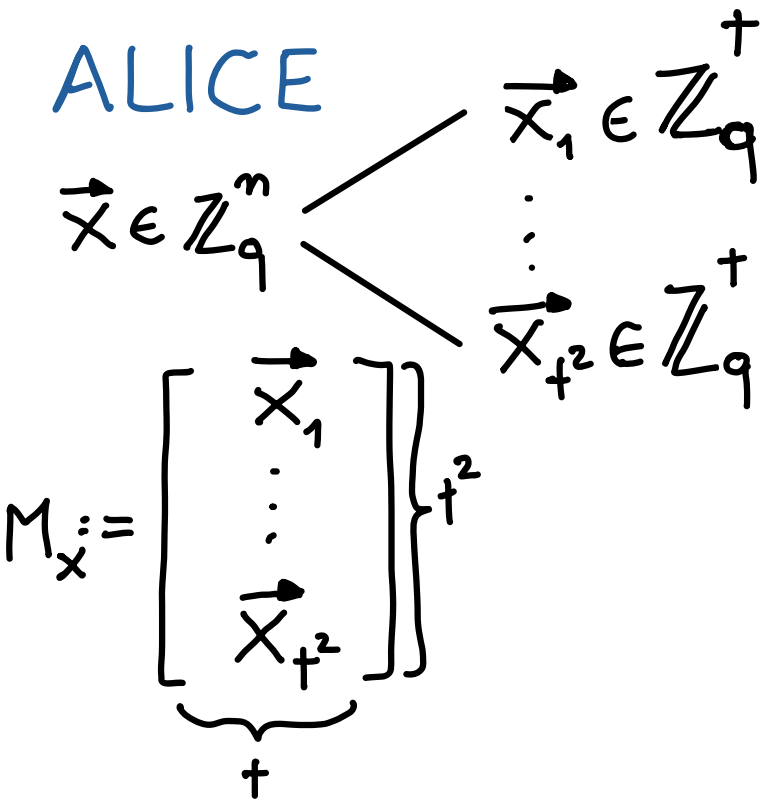
$\vec{x} \in \mathbb{Z}_q^n$

$t = n^{\frac{1}{3}}$

BOB

$y \in \mathbb{Z}_q$

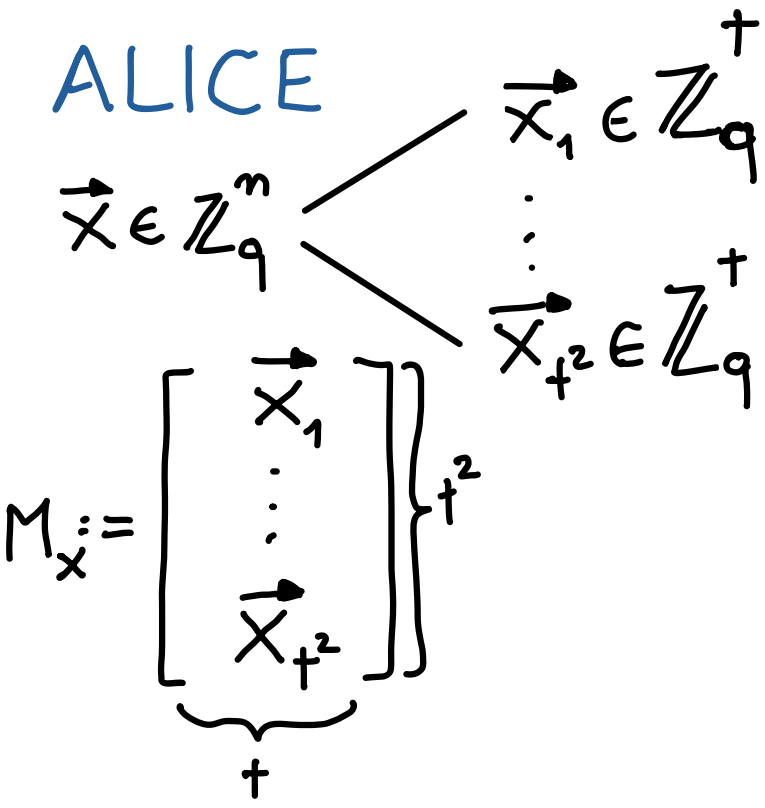
FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE



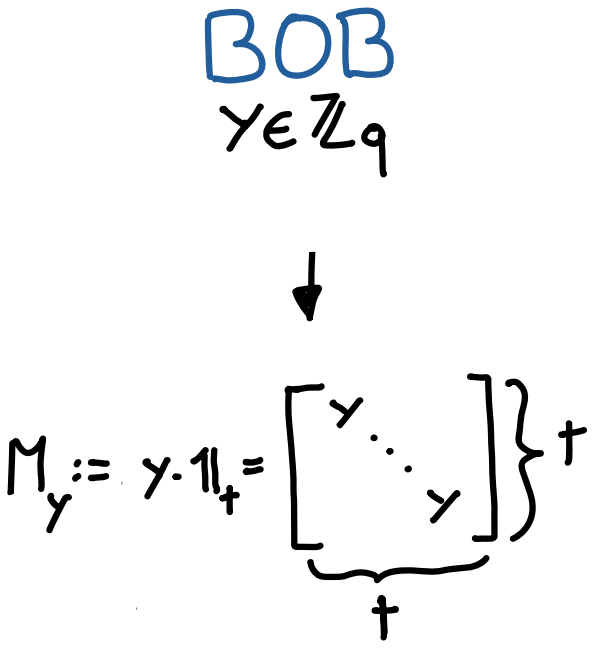
$t = n^{\frac{1}{3}}$

BOB
$y \in \mathbb{Z}_q$

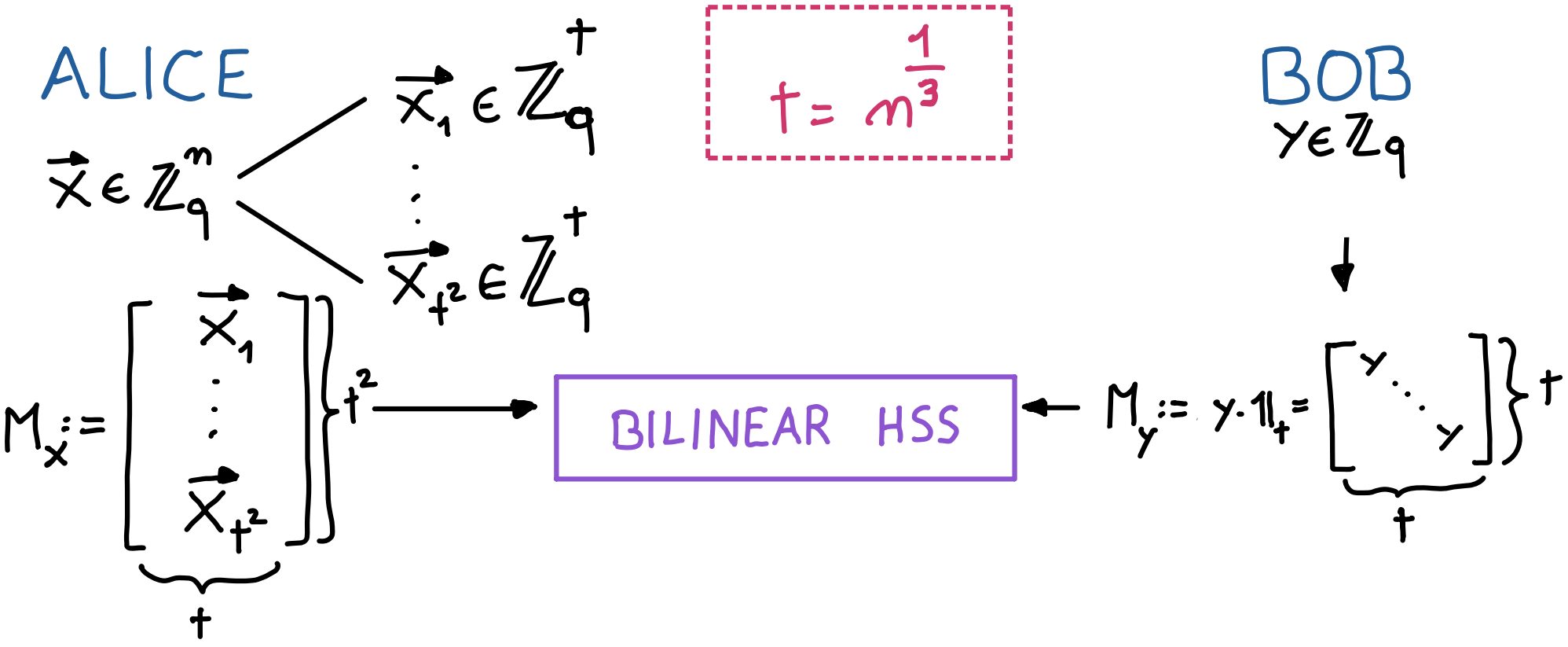
FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE



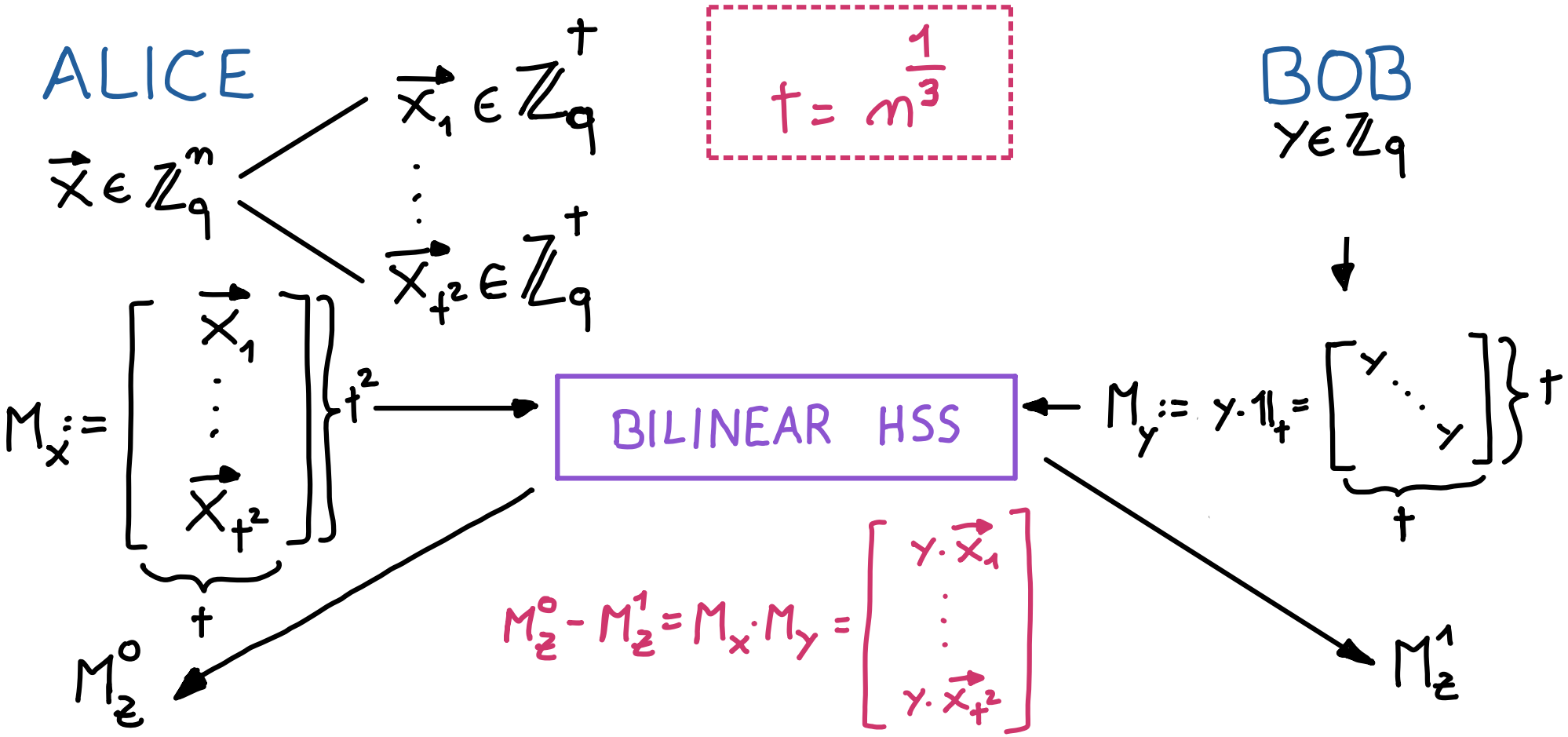
$t = n^{\frac{1}{3}}$



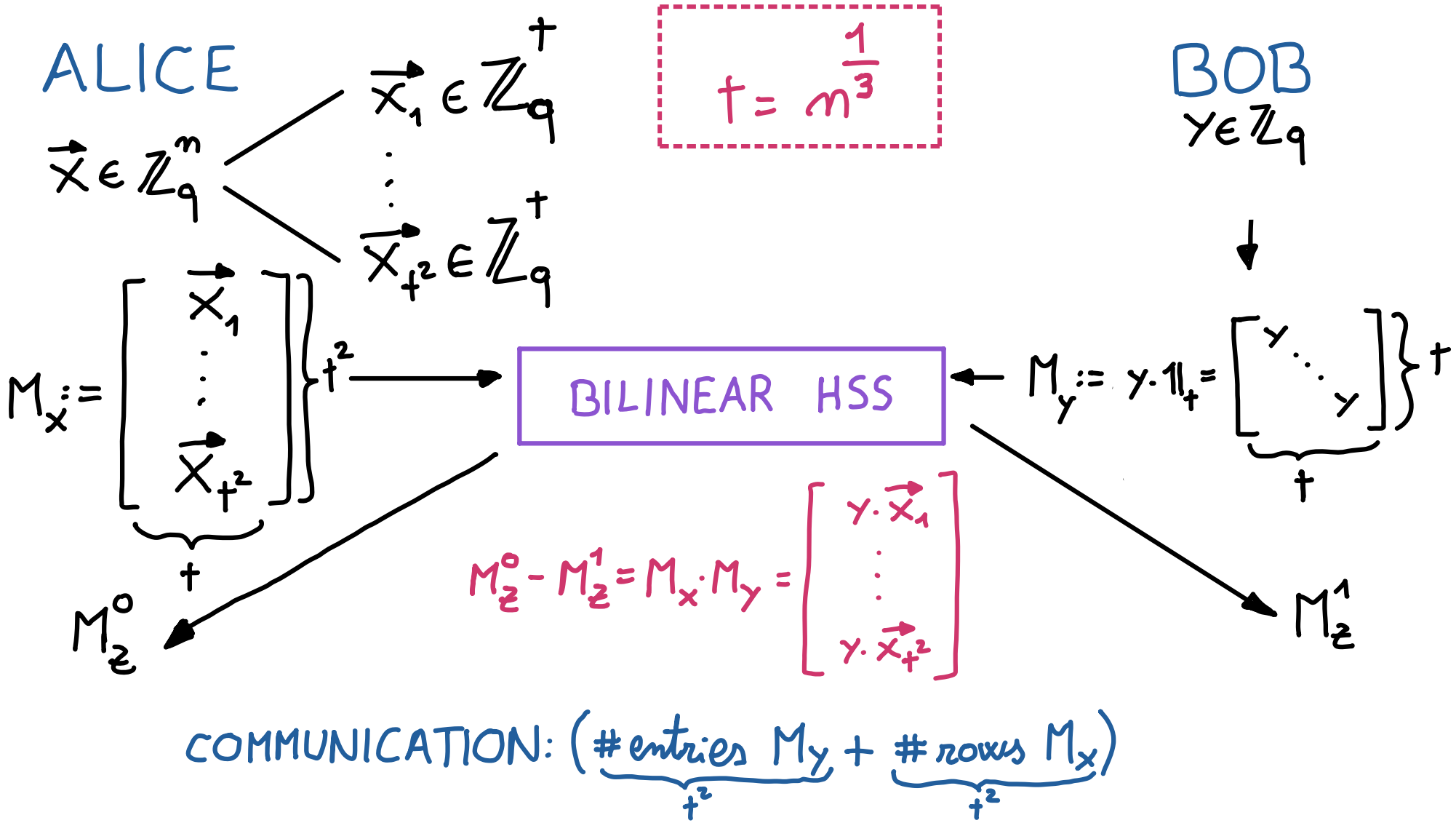
FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE



FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE

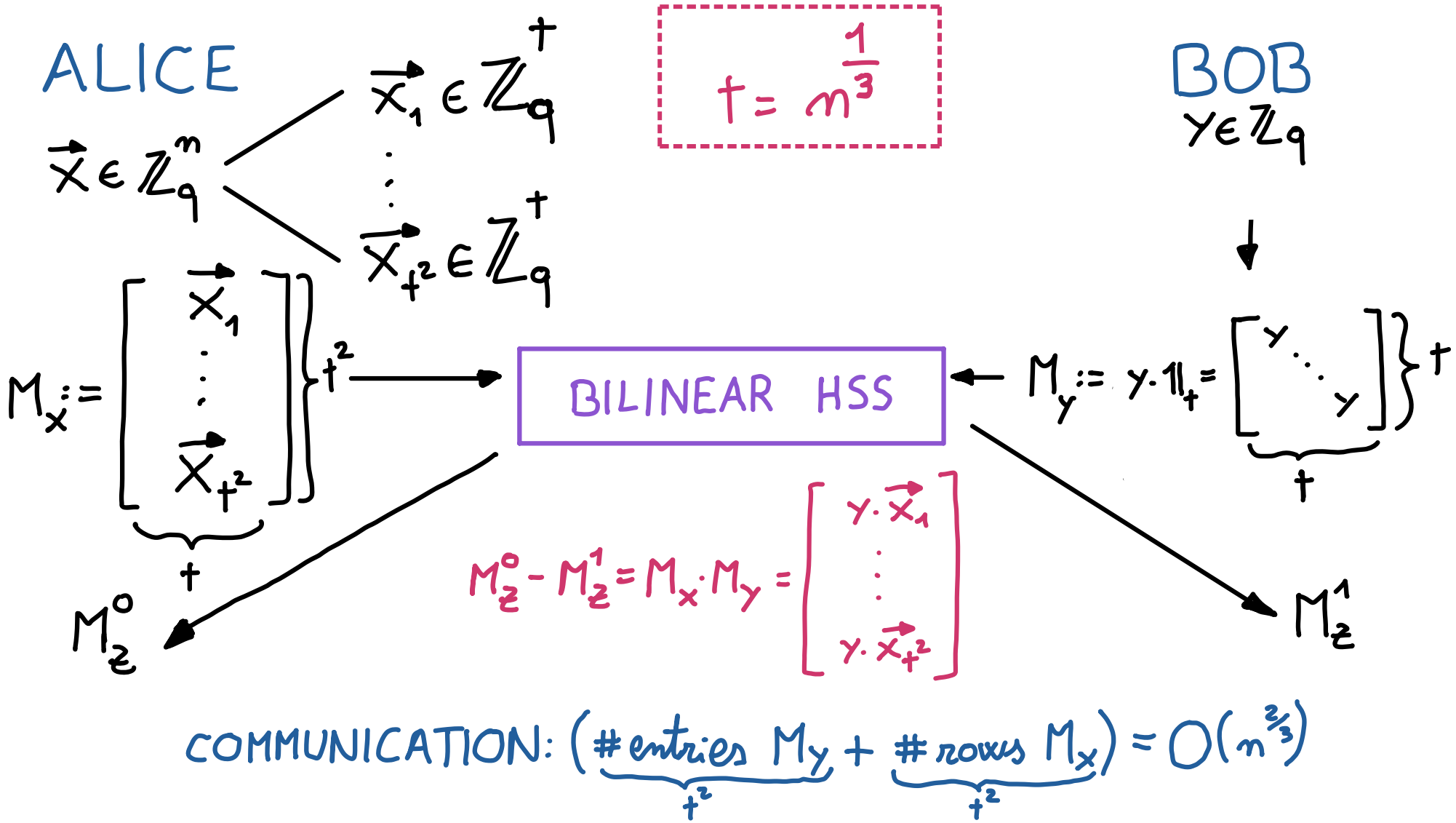


FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE



COMMUNICATION: $(\underbrace{\#\text{entries } M_y}_{t^2} + \underbrace{\#\text{rows } M_x}_{t^2})$

FROM BILINEAR HSS TO HALF-CHOSEN VECTOR-OLE



COMMUNICATION: $(\underbrace{\#\text{entries } M_y}_{t^2} + \underbrace{\#\text{rows } M_x}_{t^2}) = O(n^{2/3})$

DISTRIBUTED DLOG

DISTRIBUTED DLOG

$$G = F \times H$$

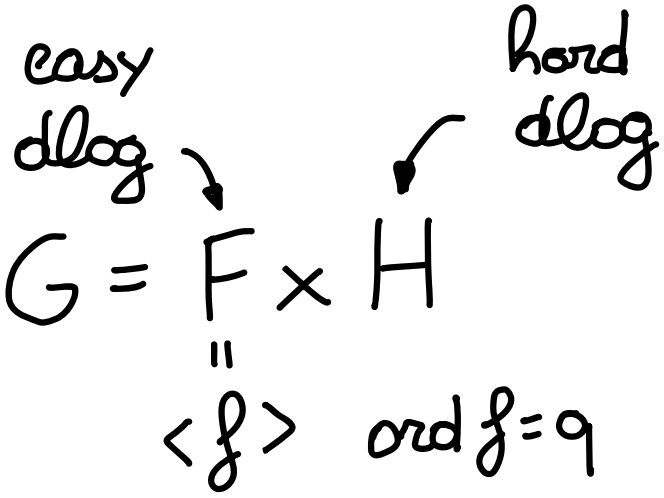
DISTRIBUTED DLOG

$$G = F \times H$$

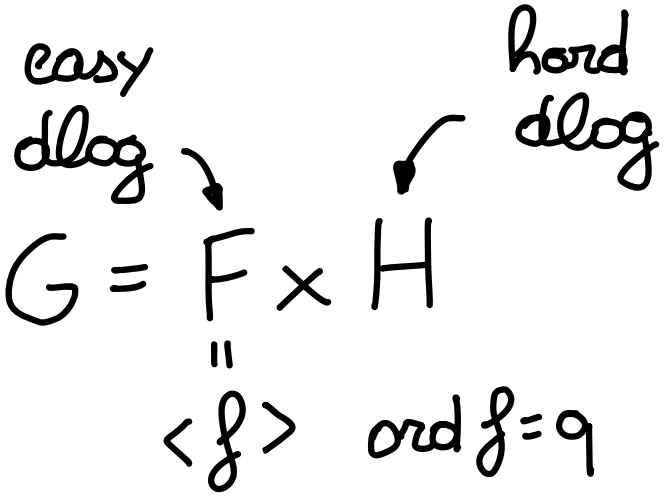
$$\| \quad \text{ord } f = q$$

$$\langle f \rangle$$

DISTRIBUTED DLOG



DISTRIBUTED DLOG



ALICE

u_0

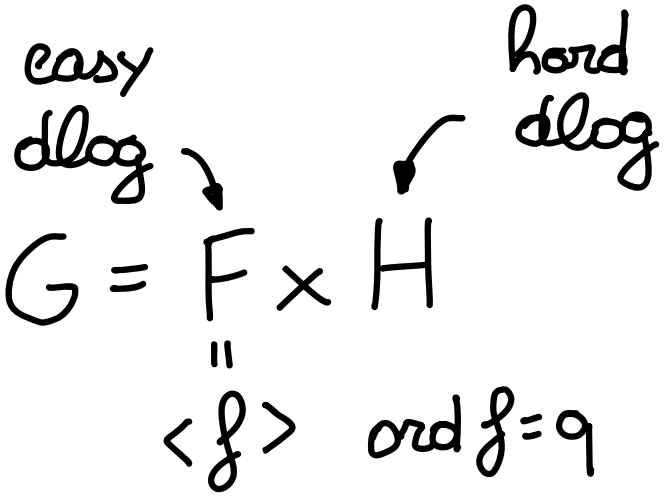
BOB

u_1

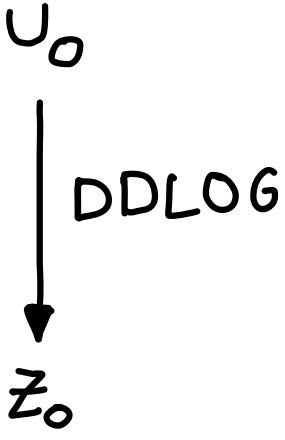
PROMISE

$$\frac{u_0}{u_1} = f^z$$

DISTRIBUTED DLOG



ALICE

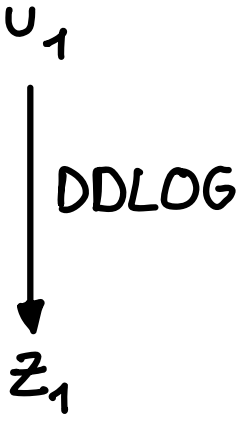


PROMISE

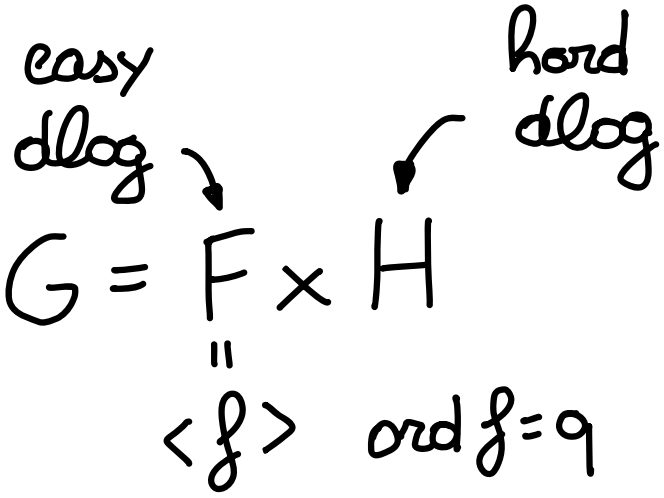
$$\frac{u_0}{u_1} = f^z$$

$$z_0 - z_1 = z \mod q$$

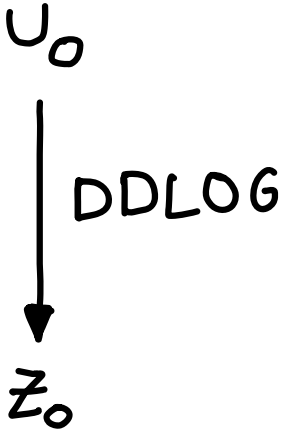
BOB



DISTRIBUTED DLOG



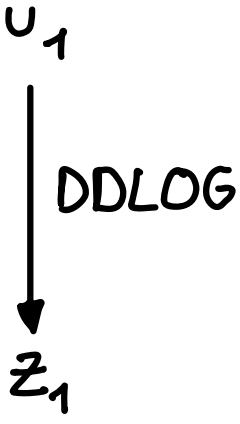
ALICE



PROMISE

$$\frac{u_0}{u_1} = f^z$$

BOB



$$z_0 - z_1 = z \mod q$$

NO INTERACTION!

BILINEAR HSS FROM DDLOG

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

BILINEAR HSS FROM DDLOG

$$G = F \times H$$

$F = \langle g \rangle$ $q = \operatorname{ord} g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \ldots, g_n \in G$

$F = \langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$\uparrow$ $\langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\longrightarrow$

$\longleftarrow$ $c_0 := g_0^s,\ c_1 := g^{y_1} \cdot g_1^s,\ \dots,\ c_n := g^{y_n} \cdot g_n^s$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle f \rangle$ $\quad q = \text{ord}\, f$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

$\frac{U_0}{U_1} =$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := g^{y_1} \cdot g_1^s,\ \dots,\ c_n := g^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

$$\frac{U_0}{U_1} = \frac{c_0^r \cdot \prod_{i=1}^{n} c_i^{x_i}}{d^s}$$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$\langle f \rangle$ $\quad q = \text{ord}\, f$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

$$\frac{U_0}{U_1} = \frac{g_0^{r \cdot s} \cdot \prod_{i=1}^{n} c_i^{x_i}}{d^s}$$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle f \rangle \quad q = \text{ord}\, f$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

$$\frac{U_0}{U_1} = \frac{g_0^{r \cdot s} \cdot \prod_{i=1}^{n} f^{x_i \cdot y_i} \cdot g_i^{s \cdot x_i}}{d^s}$$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$\uparrow$ $\langle g \rangle$ $\quad q = \text{ord}\, g$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\longrightarrow$

$\longleftarrow$ $c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$U_1 := d^s$

$$\frac{U_0}{U_1} = \frac{g_0^{r \cdot s} \cdot \prod_{i=1}^{n} f^{x_i \cdot y_i} \cdot g_i^{s \cdot x_i}}{g_0^{r \cdot s} \cdot g_1^{s \cdot x_1} \cdot \dots \cdot g_n^{s \cdot x_n}}$$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \ldots, g_n \in G$

$\langle f \rangle$ $\quad q = \text{ord}\, f$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \ldots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \ldots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \ldots \cdot c_n^{x_n}$

$U_1 := d^s$

$$\frac{U_0}{U_1} = \frac{g_0^{r \cdot s} \cdot \prod_{i=1}^{n} f^{x_i \cdot y_i} \cdot g_i^{s \cdot x_i}}{g_0^{r \cdot s} \cdot g_1^{s \cdot x_1} \cdot \ldots \cdot g_n^{s \cdot x_n}} = f^{\langle \vec{x}, \vec{y} \rangle}$$

BILINEAR HSS FROM DDLOG

$G = F \times H$ $\quad pk = g_0, \dots, g_n \in G$

$F = \langle f \rangle$ $\quad q = \text{ord}\, f$

HASHER

$\vec{x} \in \mathbb{Z}_q^n$

$r \xleftarrow{\$} [\ell]$

ENCRYPTOR

$\vec{y} \in \mathbb{Z}_q^n$

$s \xleftarrow{\$} [\ell]$

$d := g_0^r \cdot g_1^{x_1} \cdot \dots \cdot g_n^{x_n}$ $\quad \longrightarrow$

$\longleftarrow$ $\quad c_0 := g_0^s,\ c_1 := f^{y_1} \cdot g_1^s,\ \dots,\ c_n := f^{y_n} \cdot g_n^s$

$U_0 := c_0^r \cdot c_1^{x_1} \cdot \dots \cdot c_n^{x_n}$

$\downarrow$ DDLOG

z_0

$$\frac{U_0}{U_1} = \frac{g_0^{r \cdot s} \cdot \prod_{i=1}^{n} f^{x_i \cdot y_i} \cdot g_i^{s \cdot x_i}}{g_0^{r \cdot s} \cdot g_1^{s \cdot x_1} \cdot \dots \cdot g_n^{s \cdot x_n}} = f^{\langle \vec{x}, \vec{y} \rangle}$$

$U_1 := d^s$

$\downarrow$ DDLOG

z_1

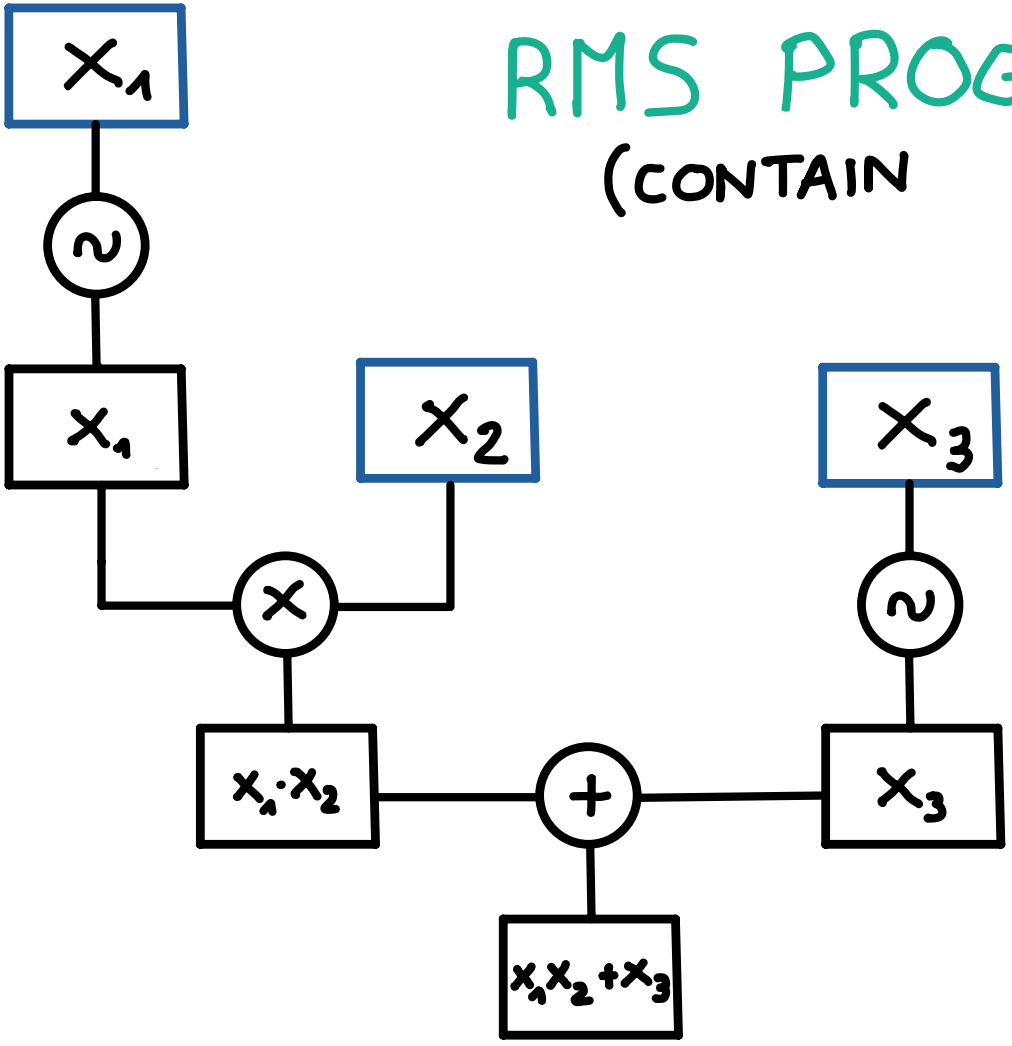
$$z_0 - z_1 = \langle \vec{x}, \vec{y} \rangle$$

SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE

RMS PROGRAMS

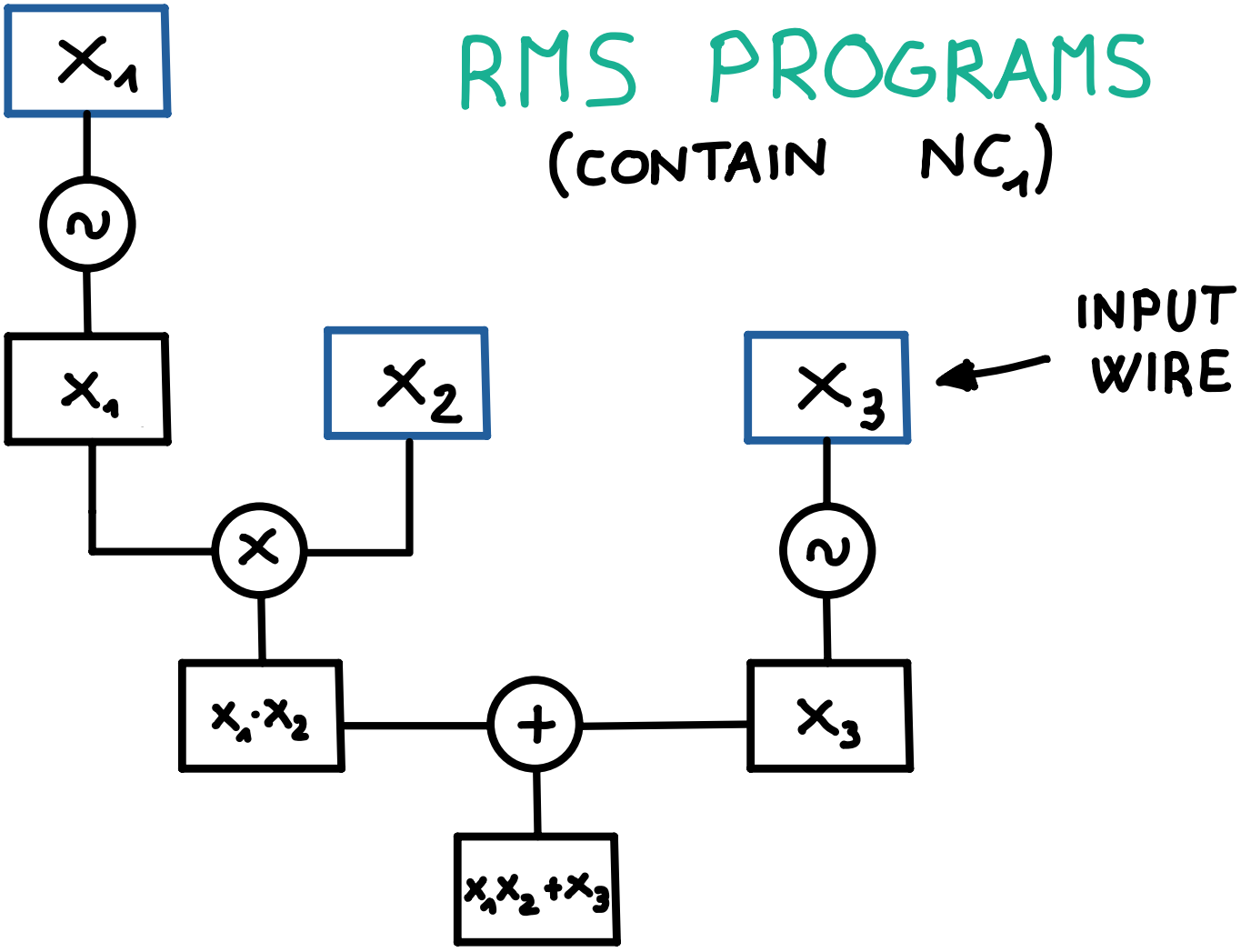
(CONTAIN NC^1)

SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE

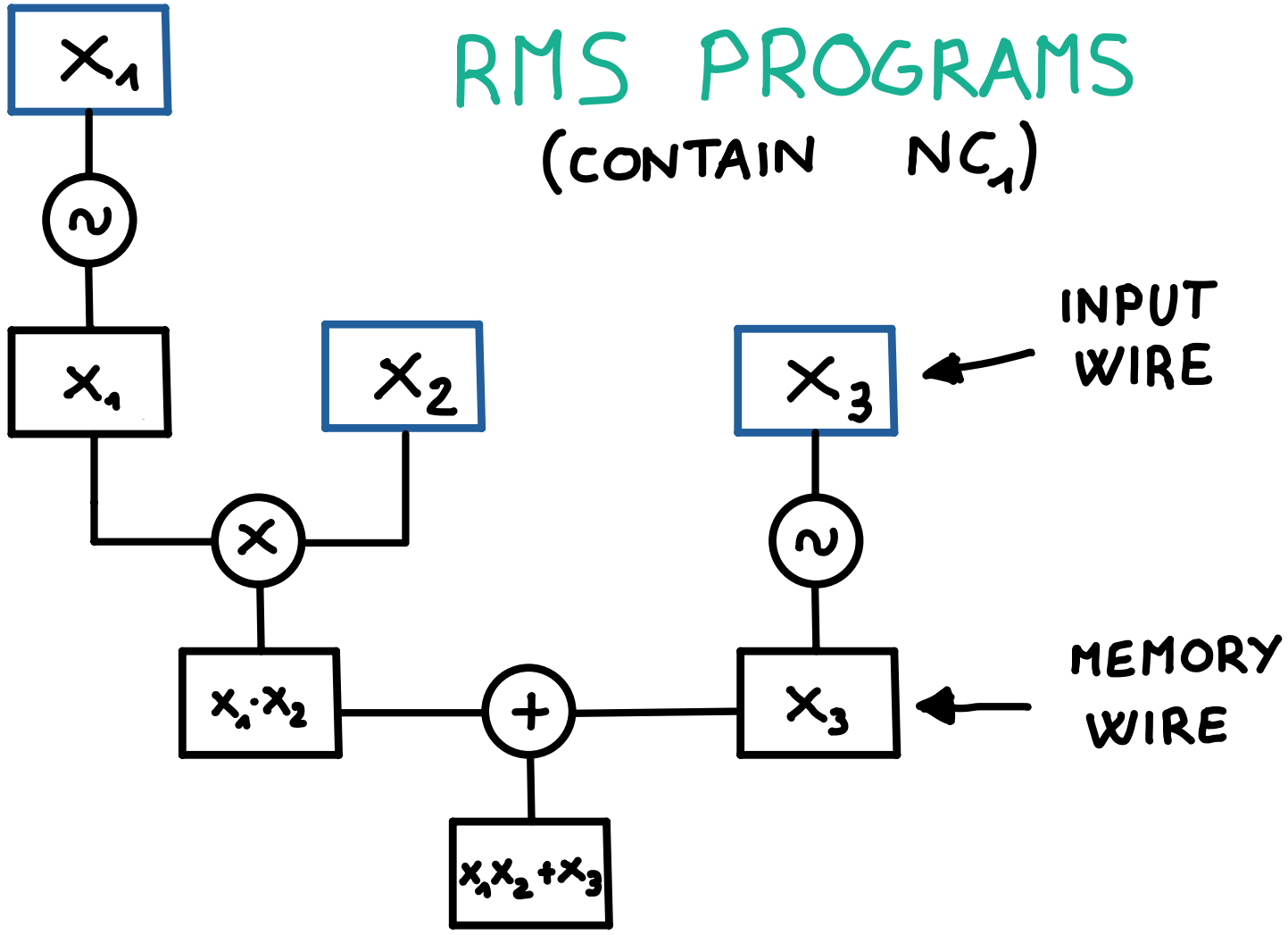


RMS PROGRAMS
(CONTAIN NC_1)

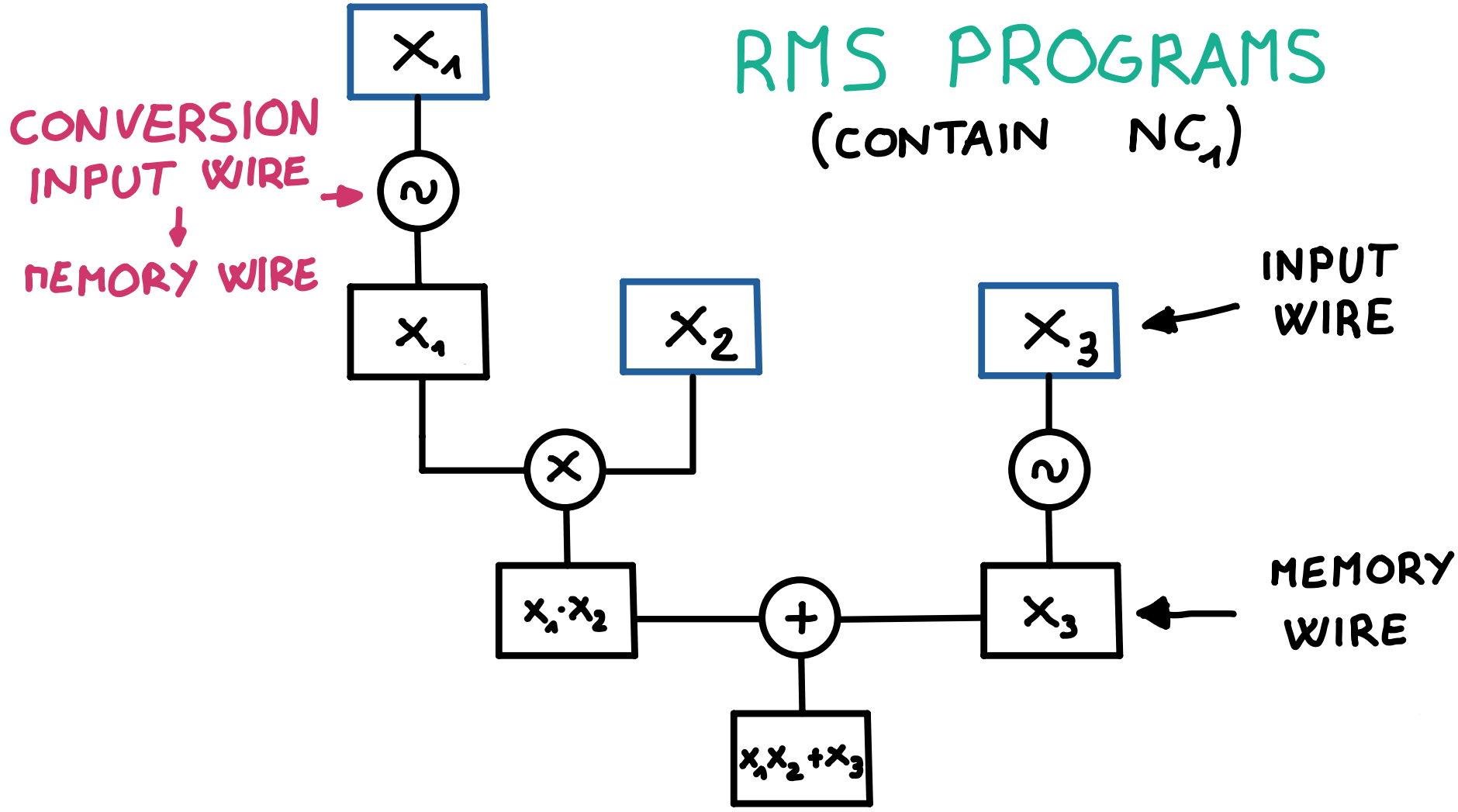
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



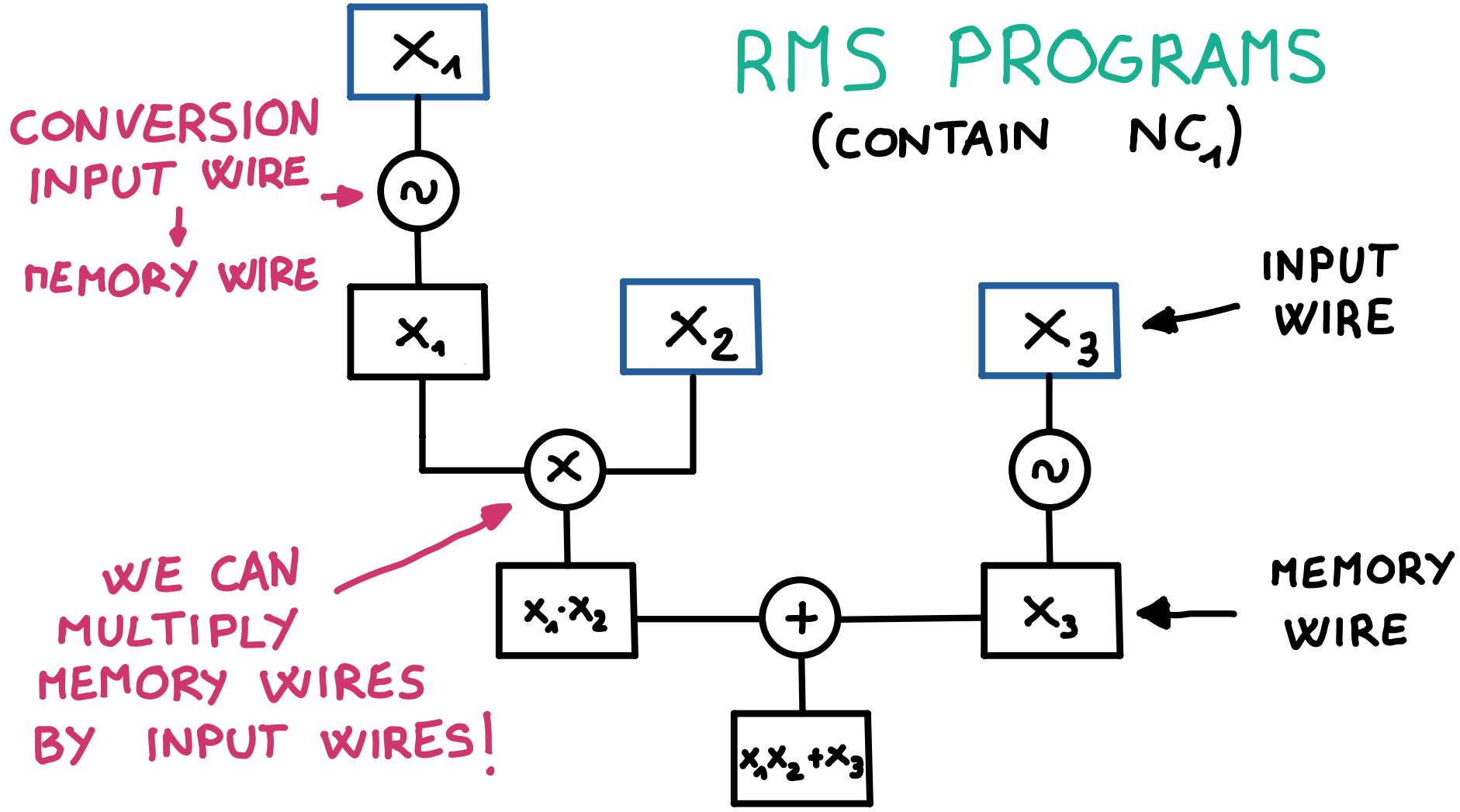
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



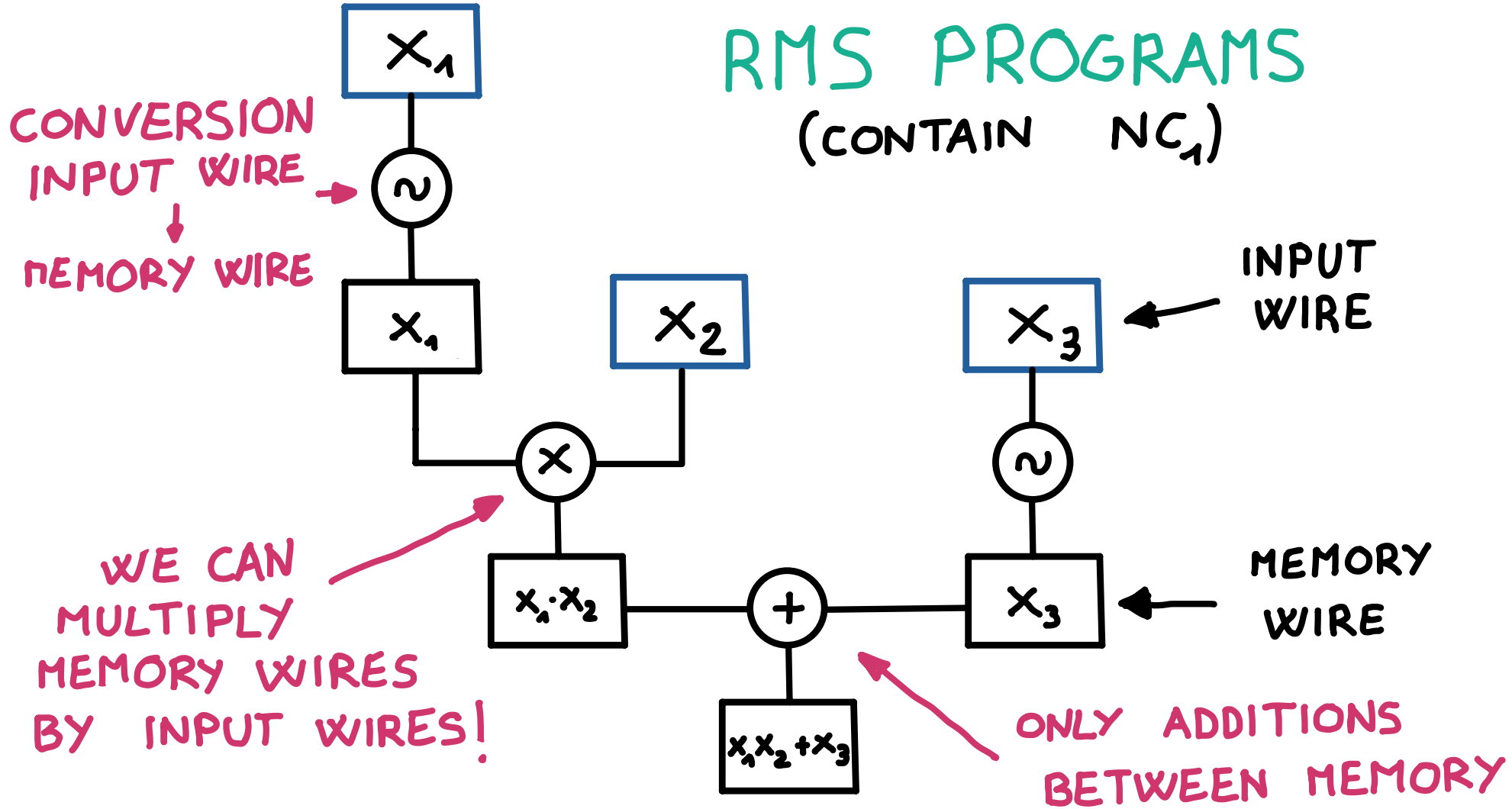
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



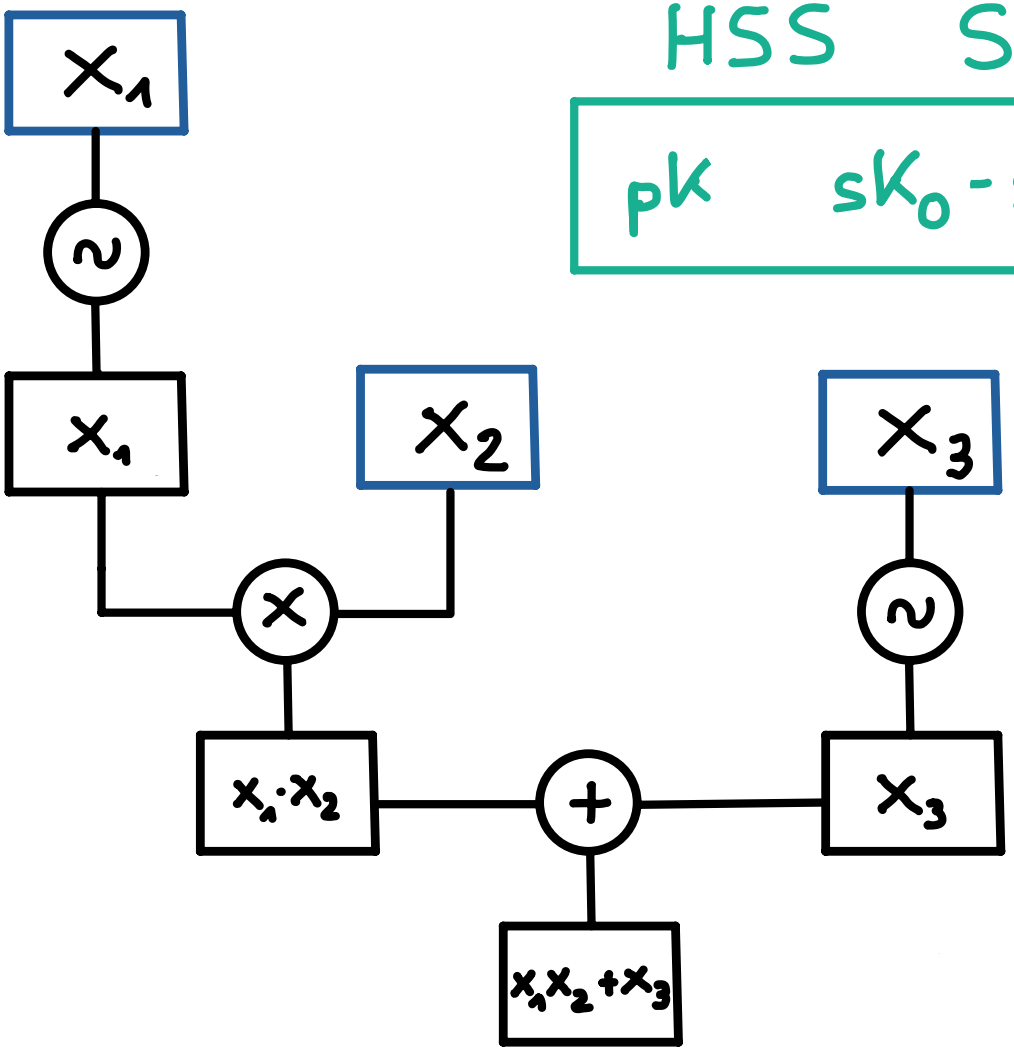
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



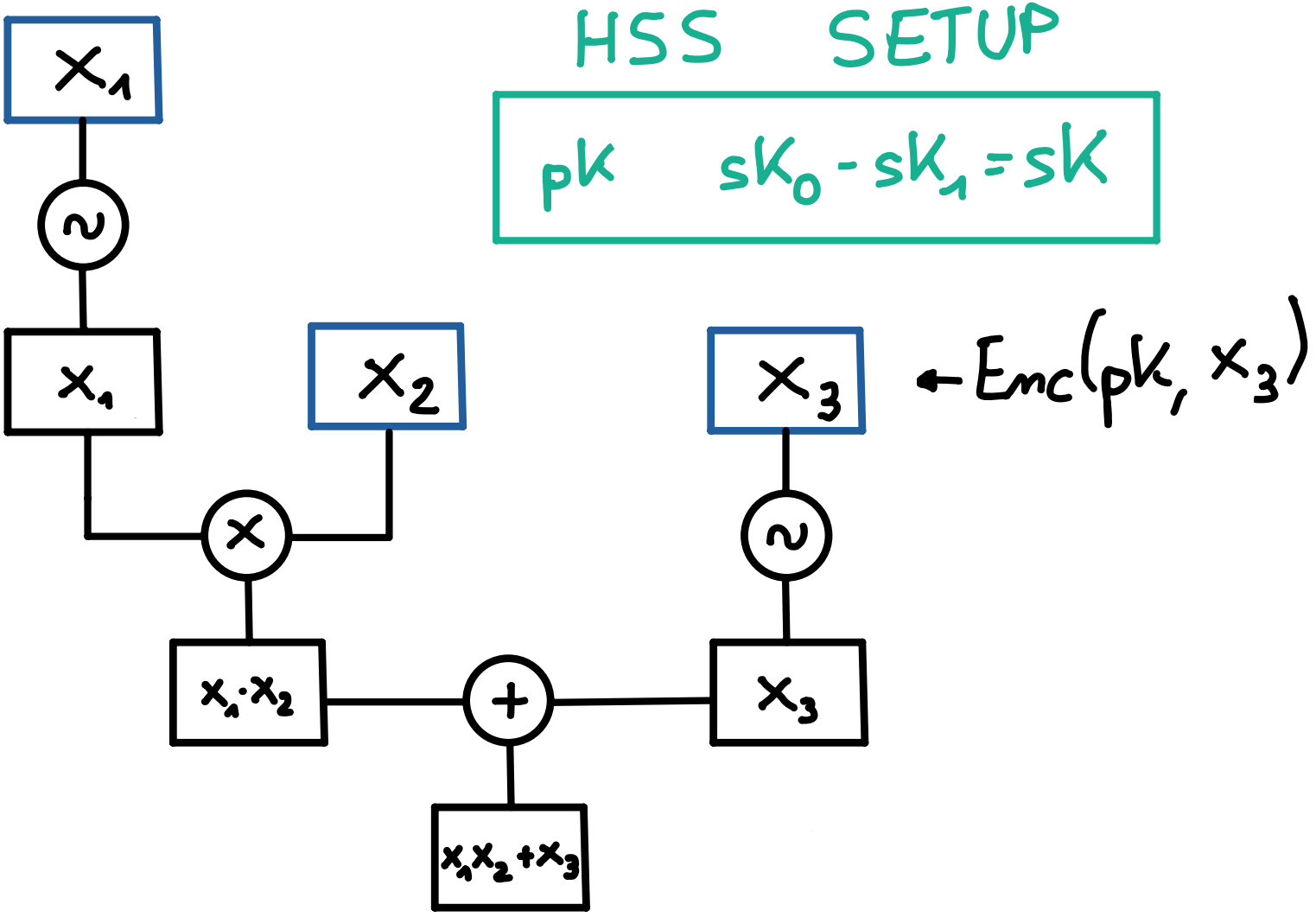
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



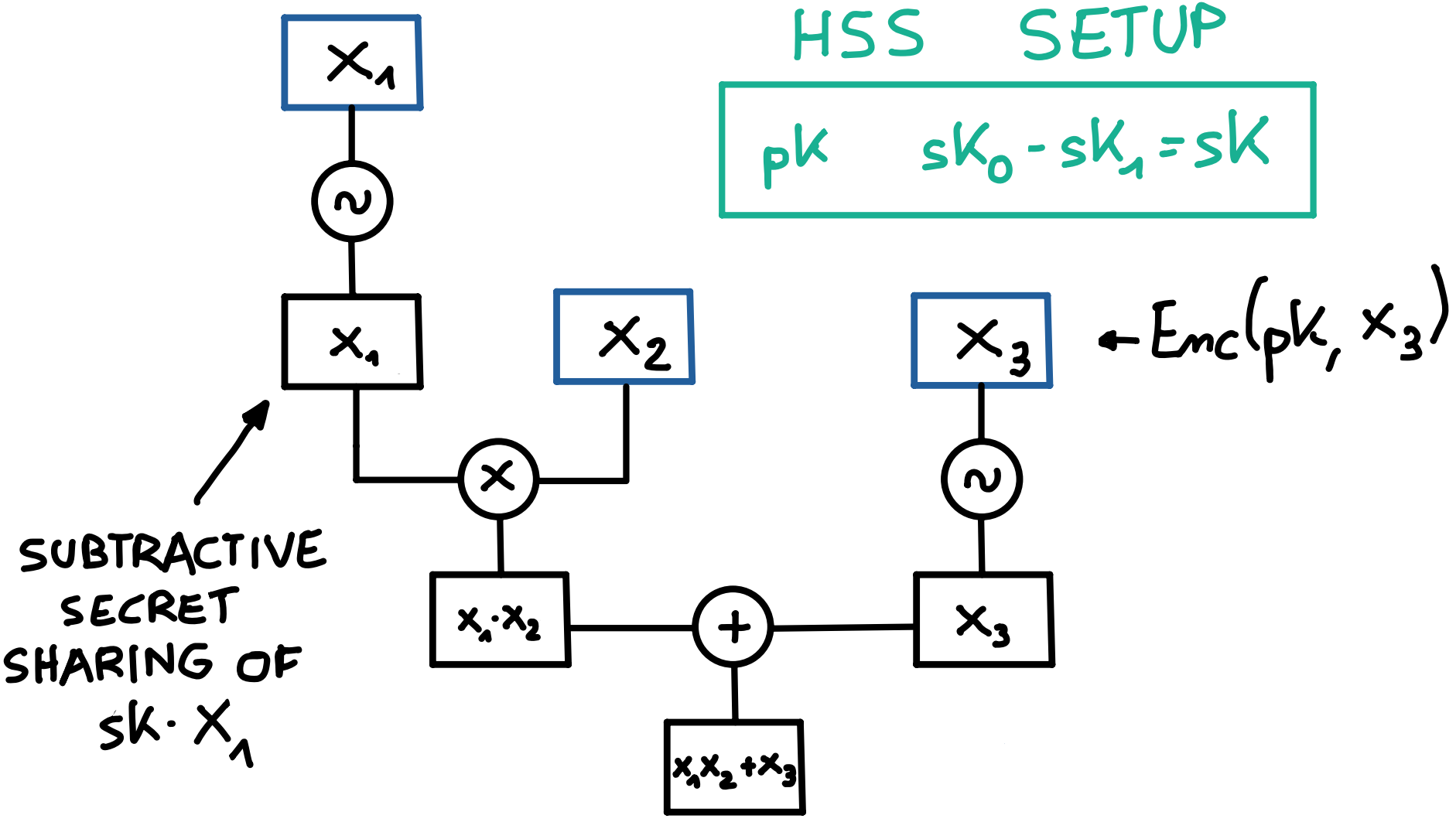
HSS SETUP

$pk \quad sk_0 - sk_1 = sk$

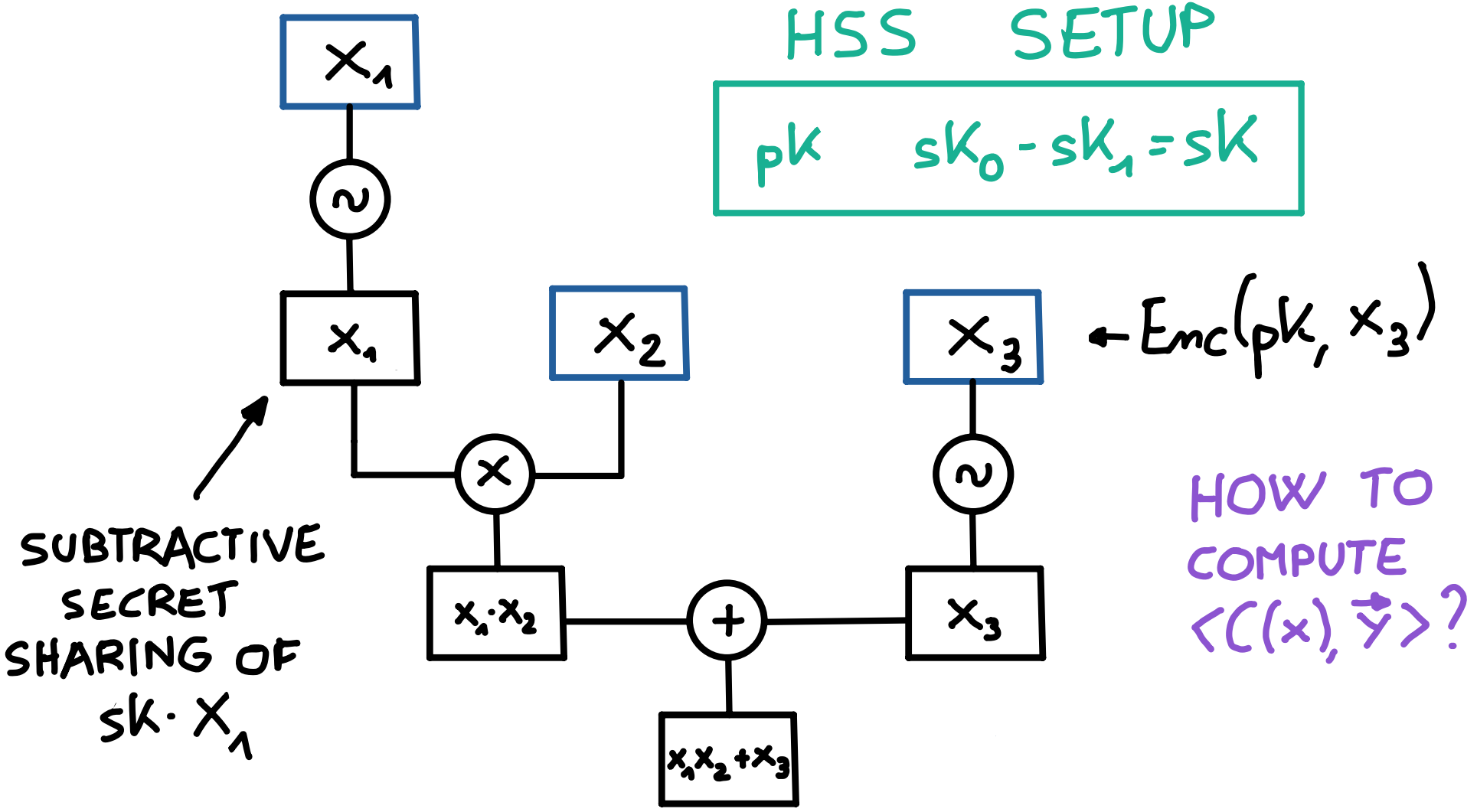
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



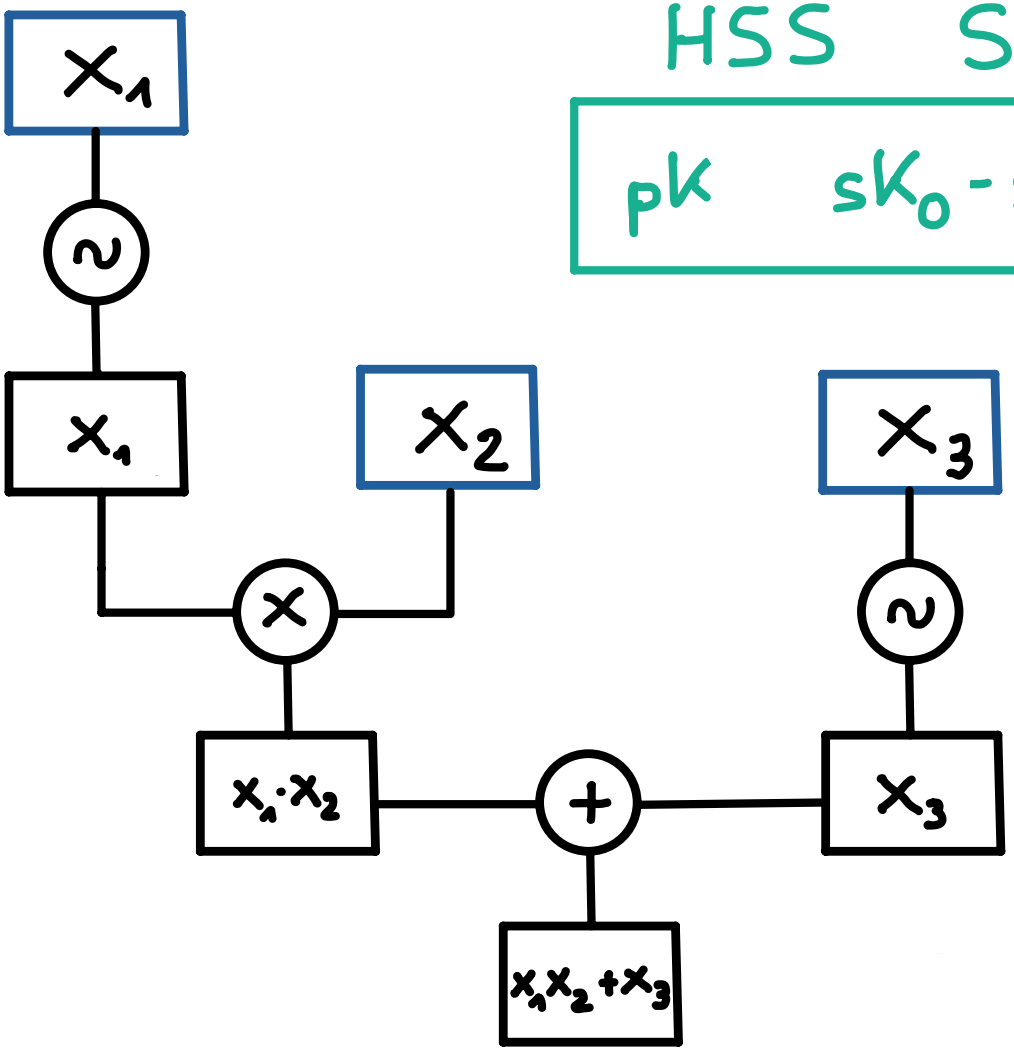
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



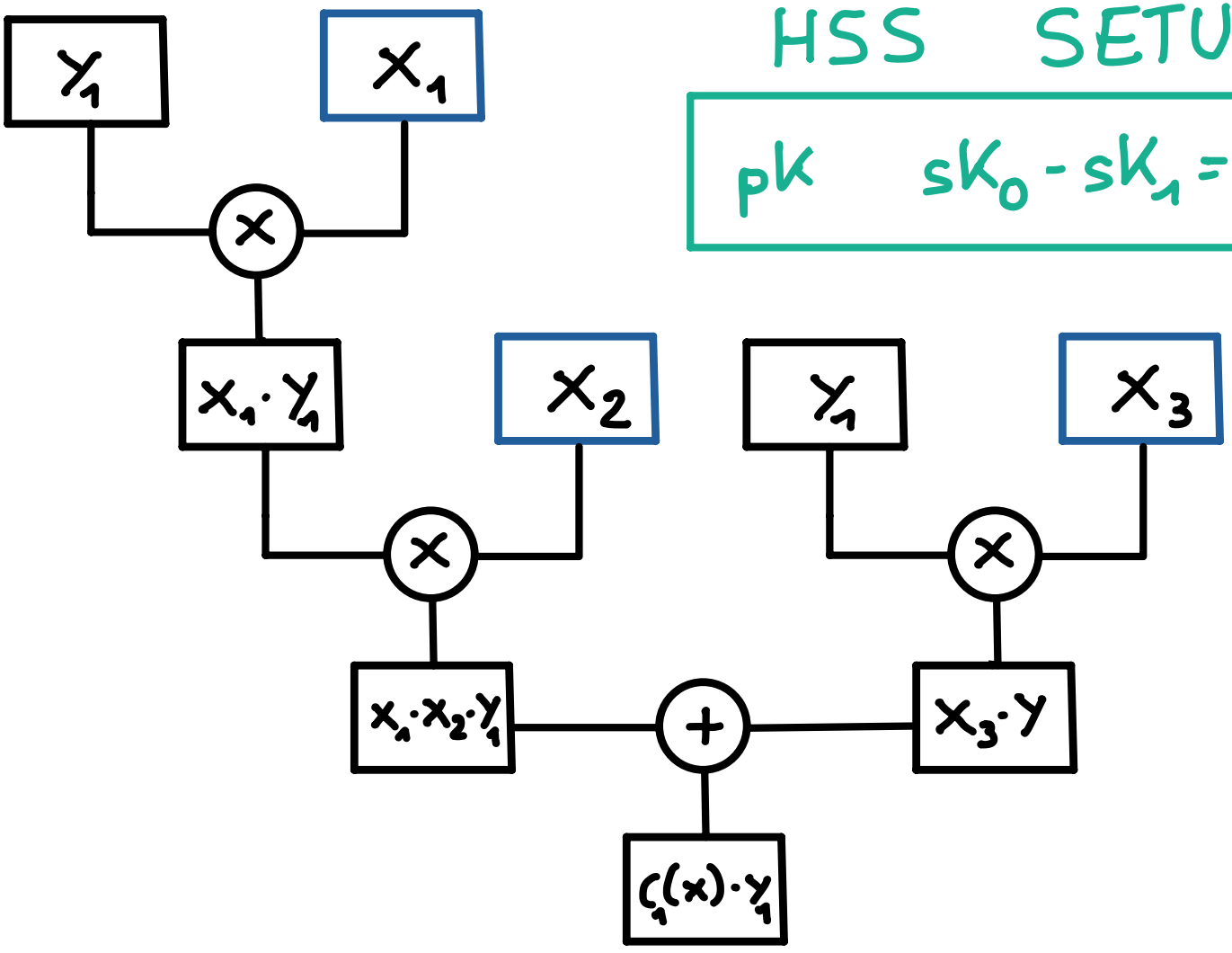
HSS SETUP

$pk \quad sk_0 - sk_1 = sk$

← circuit for C_1

HOW TO COMPUTE $\langle C(x), \vec{y} \rangle$?

SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE

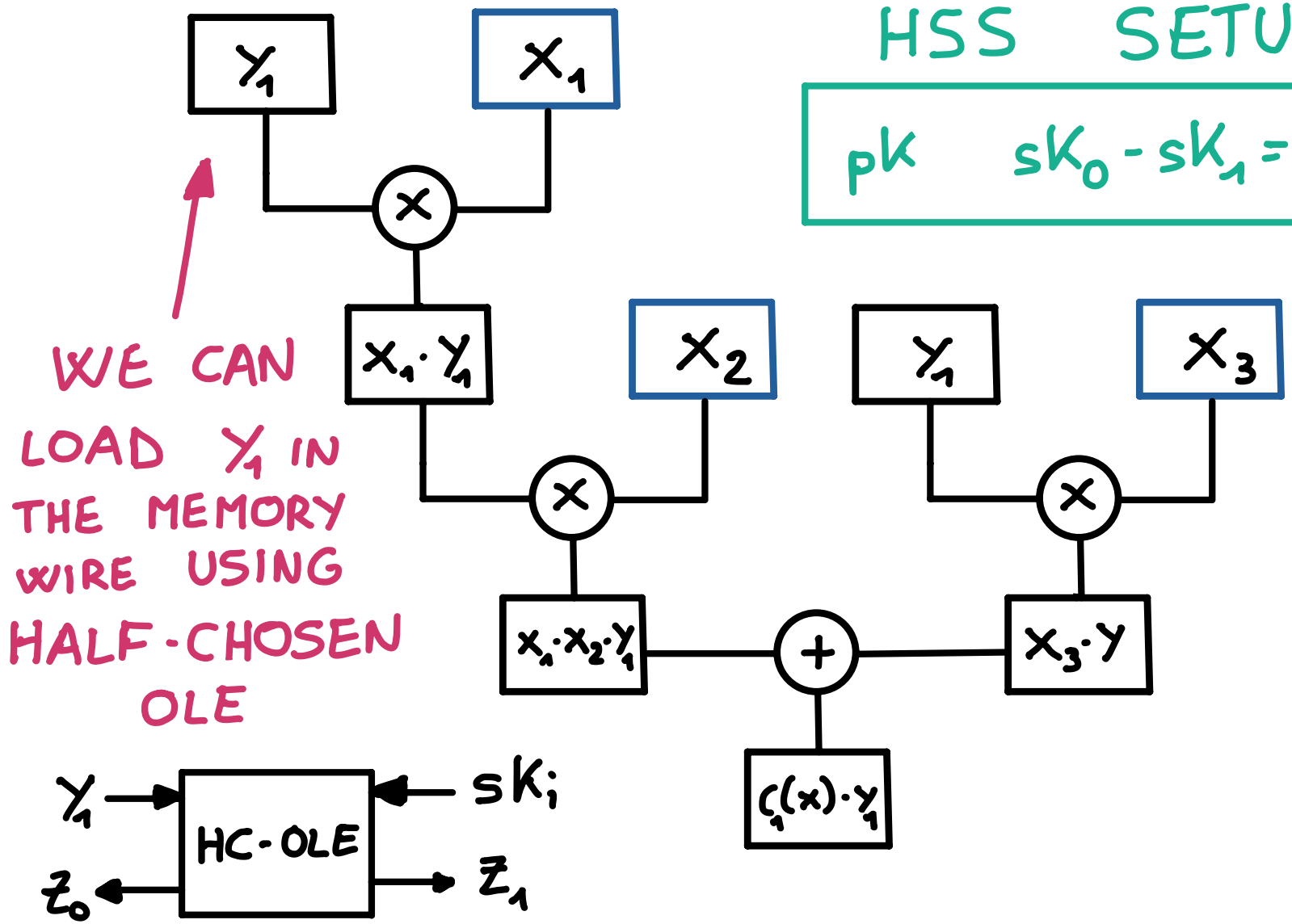


HSS SETUP

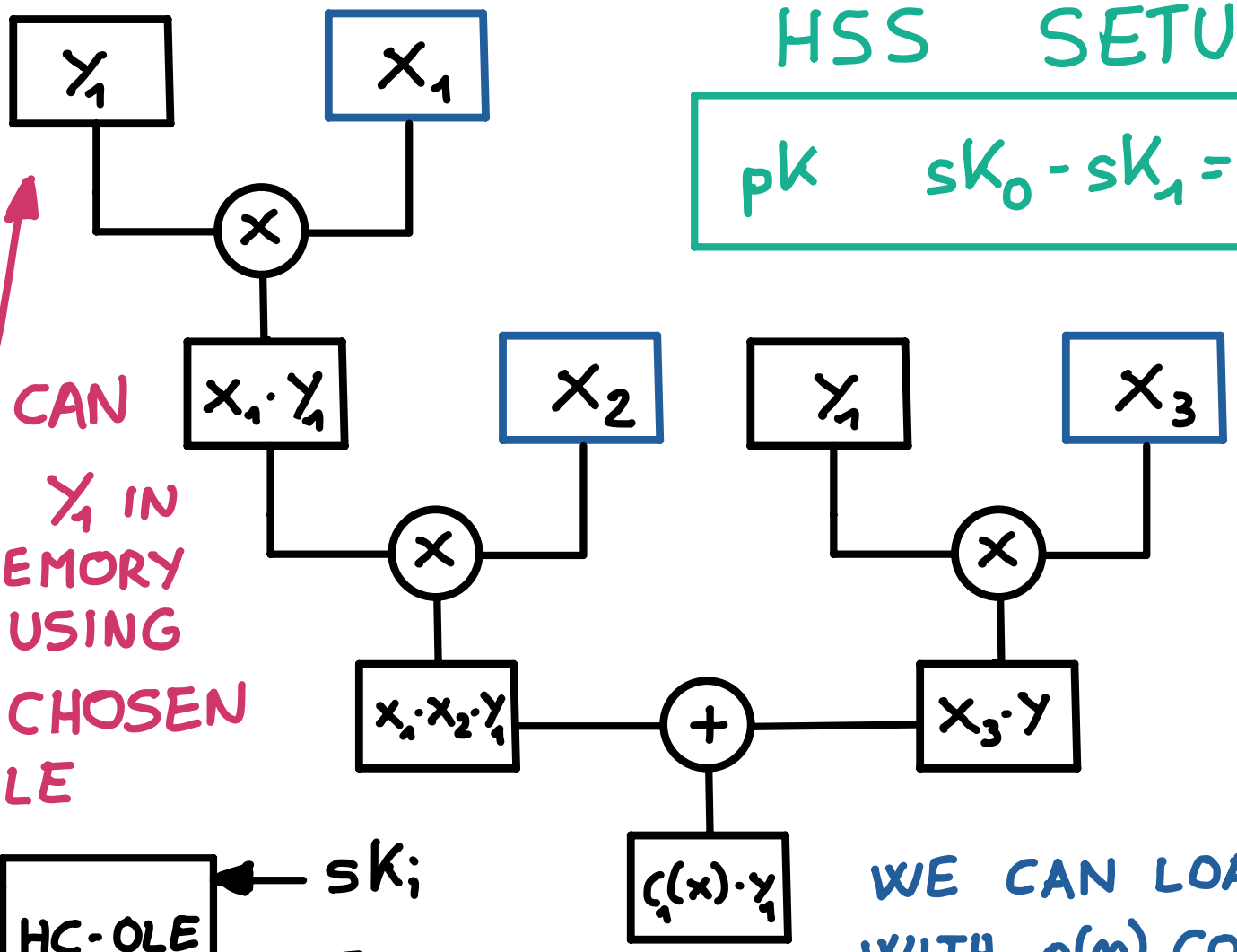
$pk \quad sk_0 - sk_1 = sk$

HOW TO COMPUTE $\langle C(x), \vec{y} \rangle$?

SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



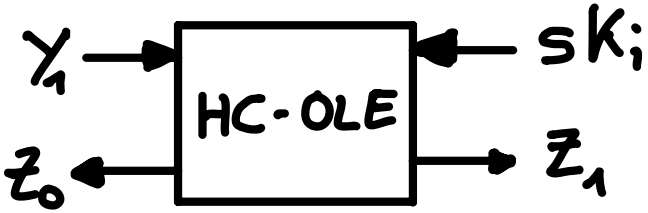
SUCCINCT HSS FROM HALF-CHOSEN VECTOR-OLE



HSS SETUP

$pk \quad sk_0 - sk_1 = sk$

WE CAN LOAD Y_1 IN THE MEMORY WIRE USING HALF-CHOSEN OLE



HOW TO COMPUTE $\langle C(x), \vec{y} \rangle$?

WE CAN LOAD $\vec{y} = (y_1, \ldots, y_m)$ WITH $o(m)$ COMMUNICATION!

N-PARTY DPF

$$P_i \leftarrow \alpha_i \in \{0,1\}^n, \ \beta_i \in \mathbb{Z}_q^*$$

N-PARTY DPF

$$P_i \leftarrow \alpha_i \in \{0,1\}^n, \ \beta_i \in \mathbb{Z}_q^*$$

GENERATE AN ADDITIVE SECRET-SHARING OF

$$(0, \ldots, 0, \prod_i \beta_i, 0, \ldots, 0) \in \mathbb{Z}_q^{2^n}$$

position $\bigoplus_i \alpha_i$

N-PARTY DPF

$P_i \leftarrow \alpha_i \in \{0,1\}^n, \ \beta_i \in \mathbb{Z}_q^*$

GENERATE AN ADDITIVE SECRET-SHARING OF

$$(0, \ldots, 0, \underset{i}{\Pi} \beta_i, 0, \ldots, 0) \in \mathbb{Z}_q^{2^n}$$

position $\underset{i}{\oplus} \alpha_i$

WITH $o(2^n)$ COMMUNICATION

N-PARTY DPF

INVARIANT:

At step j, we obtain an additive secret-sharing $\vec{s}^{\,j}_1, \ldots, \vec{s}^{\,j}_j$ of $(0, \ldots, 0, \prod_{i=1}^{j} \beta_i, 0, \ldots, 0)$ between $P_1, \ldots, P_j$

position $\bigoplus_{i=1}^{j} \alpha_i$

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{S} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{s} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta')) \cdot \vec{s} = (0, \ldots 0, \beta \cdot \beta', 0, \ldots, 0)$$

position $\alpha \oplus \alpha'$

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{s} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s}) = (0, \ldots 0, \beta \cdot \beta', 0, \ldots, 0)$$

now a matrix

position $\alpha \oplus \alpha'$

N-PARTY DPF

PROBLEM:

Given $\vec{s} := (0, \ldots 0, \underset{\text{position } \alpha \in \{0,1\}^n}{\beta}, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s} = (0, \ldots 0, \underset{\text{position } \alpha \oplus \alpha'}{\beta \cdot \beta'}, 0, \ldots, 0)$$

((α', β'): now a matrix)

$$\delta_\gamma(\alpha') = \prod_{i=1}^{n} (\alpha'_i \oplus \gamma_i \oplus 1)$$

N-PARTY DPF

PROBLEM:

Given $\vec{s} := (0, \ldots 0, \underset{\text{position } \alpha \in \{0,1\}^n}{\beta}, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s}) = (0, \ldots 0, \underset{\text{position } \alpha \oplus \alpha'}{\beta \cdot \beta'}, 0, \ldots, 0)$$

($C((\alpha', \beta'))$: now a matrix)

$$\delta_\gamma(\alpha') = \prod_{i=1}^{n} (\alpha'_i \oplus \gamma_i \oplus 1)$$

$\forall \gamma$ this is a polynomial in α': we can compute it using RMS programs

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{s} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s} = (0, \ldots 0, \beta \cdot \beta', 0, \ldots, 0) \leftarrow \vec{s}'$$

(α', β'): now a matrix

$\beta \cdot \beta'$: position $\alpha \oplus \alpha'$

$$\vec{s}'_i = \sum_\gamma \vec{s}_\gamma \cdot \delta_{\gamma \oplus i}(\alpha') \cdot \beta'$$

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{s} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s} = (0, \ldots 0, \beta \cdot \beta', 0, \ldots, 0) \leftarrow \vec{s}'$$

$C((\alpha', \beta')$: now a matrix

$\beta \cdot \beta'$: position $\alpha \oplus \alpha'$

$$\vec{s}'_i = \sum_\gamma \vec{s}_\gamma \cdot \underbrace{\delta_{\gamma \oplus i}(\alpha') \cdot \beta'}_{\text{computable by RMS program}}$$

N-PARTY DPF

PROBLEM:

position $\alpha \in \{0,1\}^n$

Given $\vec{s} := (0, \ldots 0, \beta, 0, \ldots, 0)$ and $\alpha' \in \{0,1\}^n$ and $\beta' \in \mathbb{Z}_q^*$,

find RMS program C such that

$$C((\alpha', \beta') \cdot \vec{s} = (0, \ldots 0, \beta \cdot \beta', 0, \ldots, 0) \leftarrow \vec{s}'$$

$C((\alpha', \beta')$: now a matrix

$\beta \cdot \beta'$: position $\alpha \oplus \alpha'$

$$\vec{s}'_i = \sum_\gamma \vec{s}_\gamma \cdot \underbrace{\delta_{\gamma \oplus i}(\alpha') \cdot \beta'}_{\text{computable by RMS program}} = \langle \vec{s}, C_i(\alpha', \beta') \rangle$$

$C_i(\alpha', \beta')$: RMS PROGRAM

N-PARTY DPF

position α_1

STEP 1: P_1 sets $\vec{S}_1^1 := (0, \ldots, 0, \beta_1, 0, \ldots, 0)$

N-PARTY DPF

STEP 1: P_1 sets $\vec{S}_1^1 := (0, \ldots, 0, \underset{\text{position } \alpha_1}{\beta_1}, 0, \ldots, 0)$

STEP 2: P_1 and P_2 run succinct HSS to get additive secret-sharing

$$\vec{S}_1^2 + \vec{S}_2^2 = (0, \ldots, 0, \underset{\text{position } \alpha_1 \oplus \alpha_2}{\beta_1 \cdot \beta_2}, 0, \ldots, 0)$$

N-PARTY DPF

STEP 1: P_1 sets $\vec{s}_1^{\,1} := (0, \ldots, 0, \underset{\text{position } \alpha_1}{\beta_1}, 0, \ldots, 0)$

STEP 2: P_1 and P_2 run succinct HSS to get additive secret-sharing

$$\vec{s}_1^{\,2} + \vec{s}_2^{\,2} = (0, \ldots, 0, \underset{\text{position } \alpha_1 \oplus \alpha_2}{\beta_1 \cdot \beta_2}, 0, \ldots, 0)$$

i) hash $\vec{s}_1^{\,1} = (0, \ldots, 0, \beta_1, 0, \ldots, 0)$

N-PARTY DPF

STEP 1: P_1 sets $\vec{s}_1^{\,1} := (0, \ldots, 0, \underset{\text{position } \alpha_1}{\beta_1}, 0, \ldots, 0)$

STEP 2: P_1 and P_2 run succinct HSS to get additive secret-sharing

$$\vec{s}_1^{\,2} + \vec{s}_2^{\,2} = (0, \ldots, 0, \underset{\text{position } \alpha_1 \oplus \alpha_2}{\beta_1 \cdot \beta_2}, 0, \ldots, 0)$$

i) hash $\vec{s}_1^{\,1} = (0, \ldots, 0, \beta_1, 0, \ldots, 0)$

ii) input β_2 and bits of α_2

N-PARTY DPF

STEP 1: P_1 sets $\vec{s}_1^{\,1} := (0, \ldots, 0, \underset{\text{position } \alpha_1}{\beta_1}, 0, \ldots, 0)$

STEP 2: P_1 and P_2 run succinct HSS to get additive secret-sharing

$$\vec{s}_1^{\,2} + \vec{s}_2^{\,2} = (0, \ldots, 0, \underset{\text{position } \alpha_1 \oplus \alpha_2}{\beta_1 \cdot \beta_2}, 0, \ldots, 0)$$

i) hash $\vec{s}_1^{\,1} = (0, \ldots, 0, \beta_1, 0, \ldots, 0)$

ii) input β_2 and bits of α_2

iii) compute $C(\alpha_2, \beta_2) \cdot \vec{s}_1^{\,1}$

N-PARTY DPF

STEP i-1: $P_1, \ldots, P_{i-1}$ hold $\vec{S}_1^{i-1} + \ldots + \vec{S}_{i-1}^{i-1} = (0, \ldots, 0, \underset{\text{position } \alpha_1 \oplus \ldots \oplus \alpha_{i-1}}{\beta_1 \ldots \beta_{i-1}}, 0, \ldots, 0)$

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1})$$

($C(\alpha_i, \beta_i)$: MATRIX)

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1}) \rightsquigarrow \sum_{j=1}^{i-1} C(\alpha_i, \beta_i) \cdot \vec{S}_j^{i-1}$$

MATRIX

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1}) \rightsquigarrow \sum_{j=1}^{i-1} C(\alpha_i, \beta_i) \cdot \vec{S}_j^{i-1}$$

($C(\alpha_i, \beta_i)$: MATRIX)

P_i just runs succinct HSS with P_j $\forall j < i$

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{s}_1^{\,i-1} + \dots + \vec{s}_{i-1}^{\,i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{s}_1^{\,i-1} + \dots + \vec{s}_{i-1}^{\,i-1}) \rightsquigarrow \sum_{j=1}^{i-1} C(\alpha_i, \beta_i) \cdot \vec{s}_j^{\,i-1}$$

MATRIX

P_i just runs succinct HSS with P_j $\forall j < i$

i) hash $\vec{s}_j^{\,i-1}$

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{s}_1^{\,i-1} + \dots + \vec{s}_{i-1}^{\,i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{s}_1^{\,i-1} + \dots + \vec{s}_{i-1}^{\,i-1}) \rightsquigarrow \sum_{j=1}^{i-1} C(\alpha_i, \beta_i) \cdot \vec{s}_j^{\,i-1}$$

MATRIX

P_i just runs succinct HSS with P_j $\forall j<i$

i) hash $\vec{s}_j^{\,i-1}$

ii) input β_i and bits of α_i

N-PARTY DPF

STEP i-1: $P_1, \dots, P_{i-1}$ hold $\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1} = (0, \dots, 0, \underset{\text{position } \alpha_1 \oplus \dots \oplus \alpha_{i-1}}{\beta_1}, \dots, \beta_{i-1}, 0, \dots, 0)$

STEP i: We want to compute

$$C(\alpha_i, \beta_i) \cdot (\vec{S}_1^{i-1} + \dots + \vec{S}_{i-1}^{i-1}) \rightsquigarrow \sum_{j=1}^{i-1} C(\alpha_i, \beta_i) \cdot \vec{S}_j^{i-1}$$

($C(\alpha_i, \beta_i)$: MATRIX)

P_i just runs succinct HSS with P_j $\forall j < i$

i) hash $\vec{S}_j^{i-1}$

ii) input β_i and bits of α_i

iii) compute $C(\alpha_i, \beta_i) \cdot \vec{S}_j^{i-1}$

POWER RING LWE

$R_q \leftarrow$ ring $\quad\quad$ $\chi \leftarrow$ error distribution

POWER RING LWE

$R_q \leftarrow$ ring $\qquad \chi \leftarrow$ error distribution

$$\left\{ a,\ \begin{array}{r} s + e_0 \\ a \cdot s + e_1 \\ a^2 \cdot s + e_2 \\ \vdots \\ a^m \cdot s + e_m \end{array} \;\middle|\; \begin{array}{l} a \xleftarrow{\$} R_q \\ s \xleftarrow{\$} R_q \\ e_0, \ldots, e_m \xleftarrow{\$} \chi \end{array} \right\} \approx_c U_{R_q}^{m+2}$$

POWER RING LWE

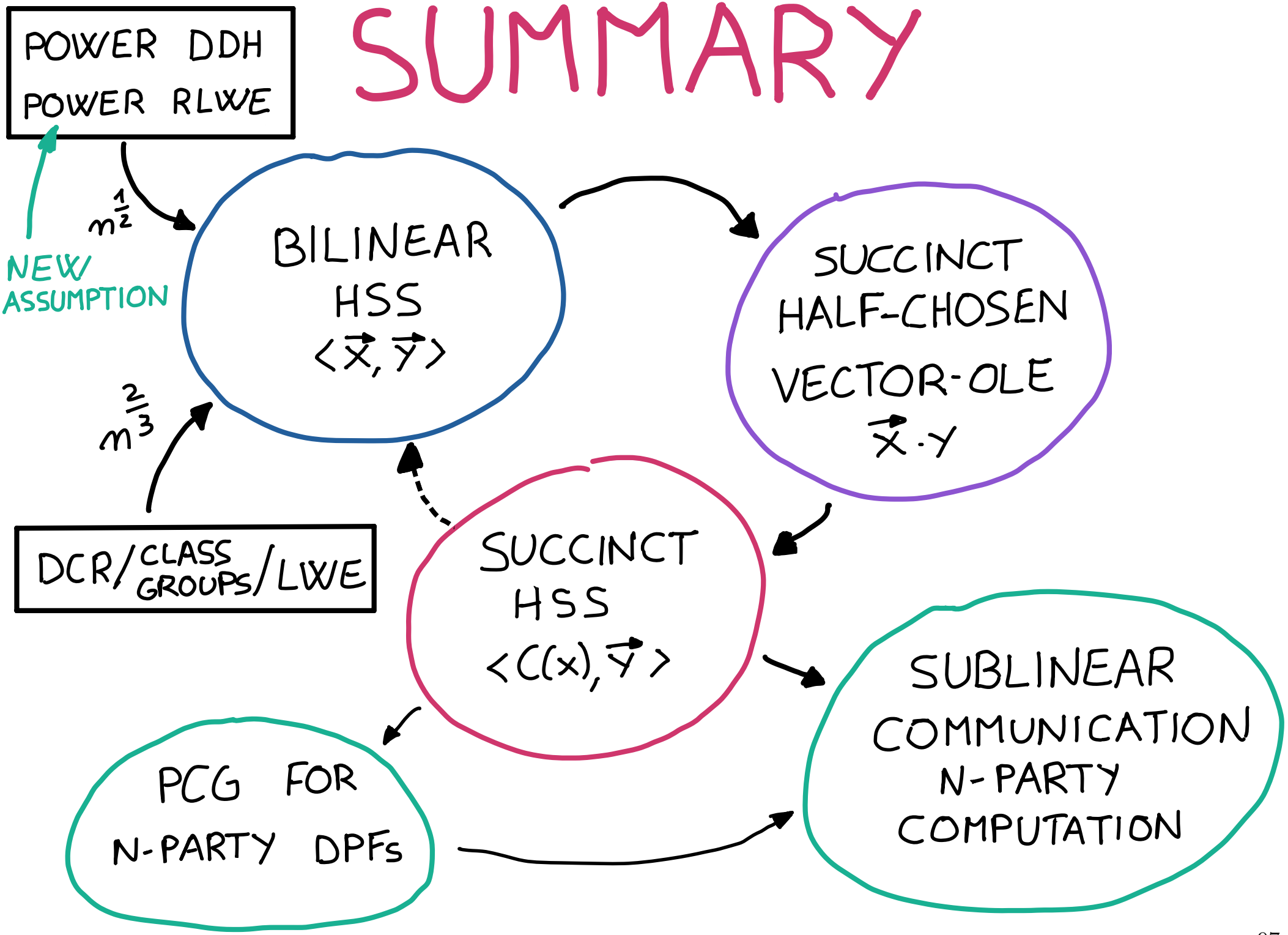
$R_q \leftarrow$ ring $\qquad \chi \leftarrow$ error distribution

$$\left\{ a,\ \begin{array}{r} s + e_0 \\ a \cdot s + e_1 \\ a^2 \cdot s + e_2 \\ \vdots \\ a^m \cdot s + e_m \end{array} \;\middle|\; \begin{array}{l} a \xleftarrow{\$} R_q \\ s \xleftarrow{\$} R_q \\ e_0, \ldots, e_m \xleftarrow{\$} \chi \end{array} \right\} \approx_c \mathcal{U}_{R_q^{m+2}}$$

DUAL SIS PROBLEM HAS ALREADY BEEN STUDIED!

VANISHING SIS [CINI, LAI, MALAVOLTA 2023]

SUMMARY


POWER DDH
POWER RLWE
NEW ASSUMPTION
$m^{\frac{1}{2}}$
$m^{\frac{2}{3}}$
DCR/CLASS GROUPS/LWE
BILINEAR HSS
$\langle \vec{x}, \vec{y} \rangle$
SUCCINCT HALF-CHOSEN VECTOR-OLE
$\vec{x} \cdot y$
SUCCINCT HSS
$\langle C(x), \vec{y} \rangle$
PCG FOR N-PARTY DPFs
SUBLINEAR COMMUNICATION N-PARTY COMPUTATION