Decentralized Evaluation of 2-DNF on Encrypted Data

Chloé Hébant - Duong Hieu Phan - David Pointcheval

Decentralized Evaluation of 2-DNF on Encrypted Data

Decentralized Evaluation of 2-DNF on Encrypted Data

Fully Homomorphic Encryption ?

Decentralized Evaluation of 2-DNF on Encrypted Data

Fully Homomorphic Encryption ?

- ✓ but not efficient

Decentralized

Evaluation of 2-DNF on Encrypted Data

Boneh, Goh, Nissim [TCC05]

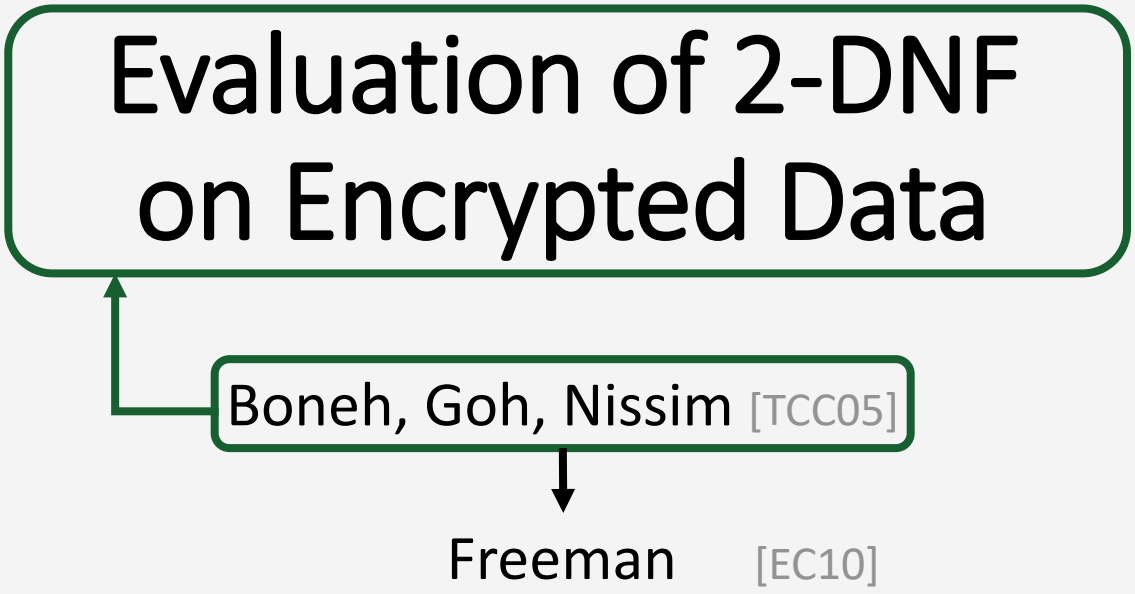
Decentralized

Evaluation of 2-DNF on Encrypted Data

Boneh, Goh, Nissim [TCC05]

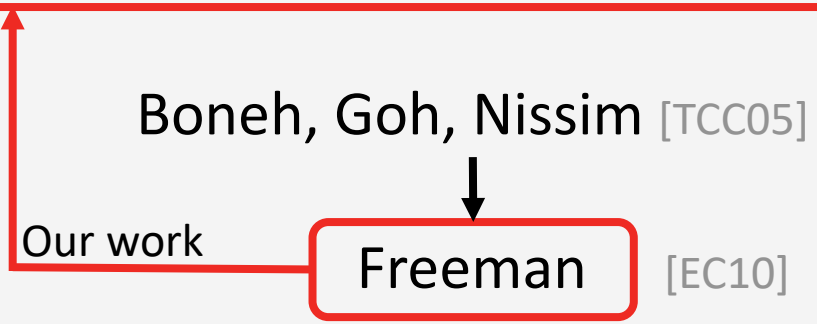
Multi-Users + Re-Encryption ⇒ Decentralized

Decentralized



Multi-Users + Re-Encryption ⇒ Decentralized

Decentralized Evaluation of 2-DNF on Encrypted Data



Multi-Users + Re-Encryption ⇒ Decentralized

2-DNF on Encrypted Data

$x_1, \dots, x_n \in \{0,1\}$

2-DNF:

$$\bigvee_{i=1}^{m} (\ell_{i,1} \wedge \ell_{i,2}) \qquad \ell_{i,1} \wedge \ell_{i,2} \in \{x_1, \dots, x_n\} \cup \{\overline{x_1}, \dots, \overline{x_n}\}$$

2-DNF on Encrypted Data

$$x_1, \dots, x_n \in \{0,1\}$$

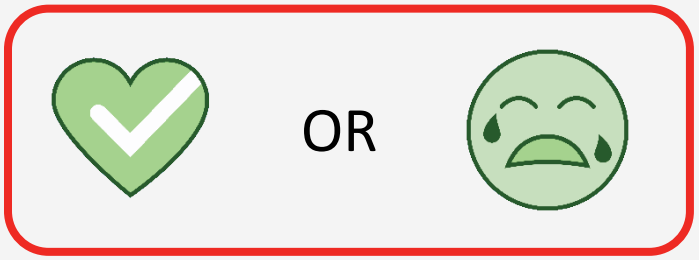
2-DNF:

$$\bigvee_{i=1}^{m} (\ell_{i,1} \wedge \ell_{i,2}) \qquad \ell_{i,1} \wedge \ell_{i,2} \in \{x_1, \dots, x_n\} \cup \{\overline{x_1}, \dots, \overline{x_n}\}$$

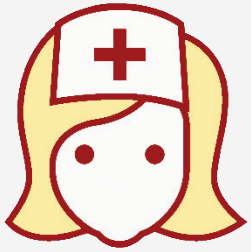
Multivariate polynomial degree 2:

$$\sum_{i=1}^{m} (y_{i,1} \cdot y_{i,2}) \qquad \begin{cases} y_{i,j} = \ell_{i,j} & \text{if } \ell_{i,j} \in \{x_1, \dots, x_n\} \\ y_{i,j} = 1 - \ell_{i,j} & \text{if } \ell_{i,j} \in \{\overline{x_1}, \dots, \overline{x_n}\} \end{cases}$$

Motivation: Group Testing

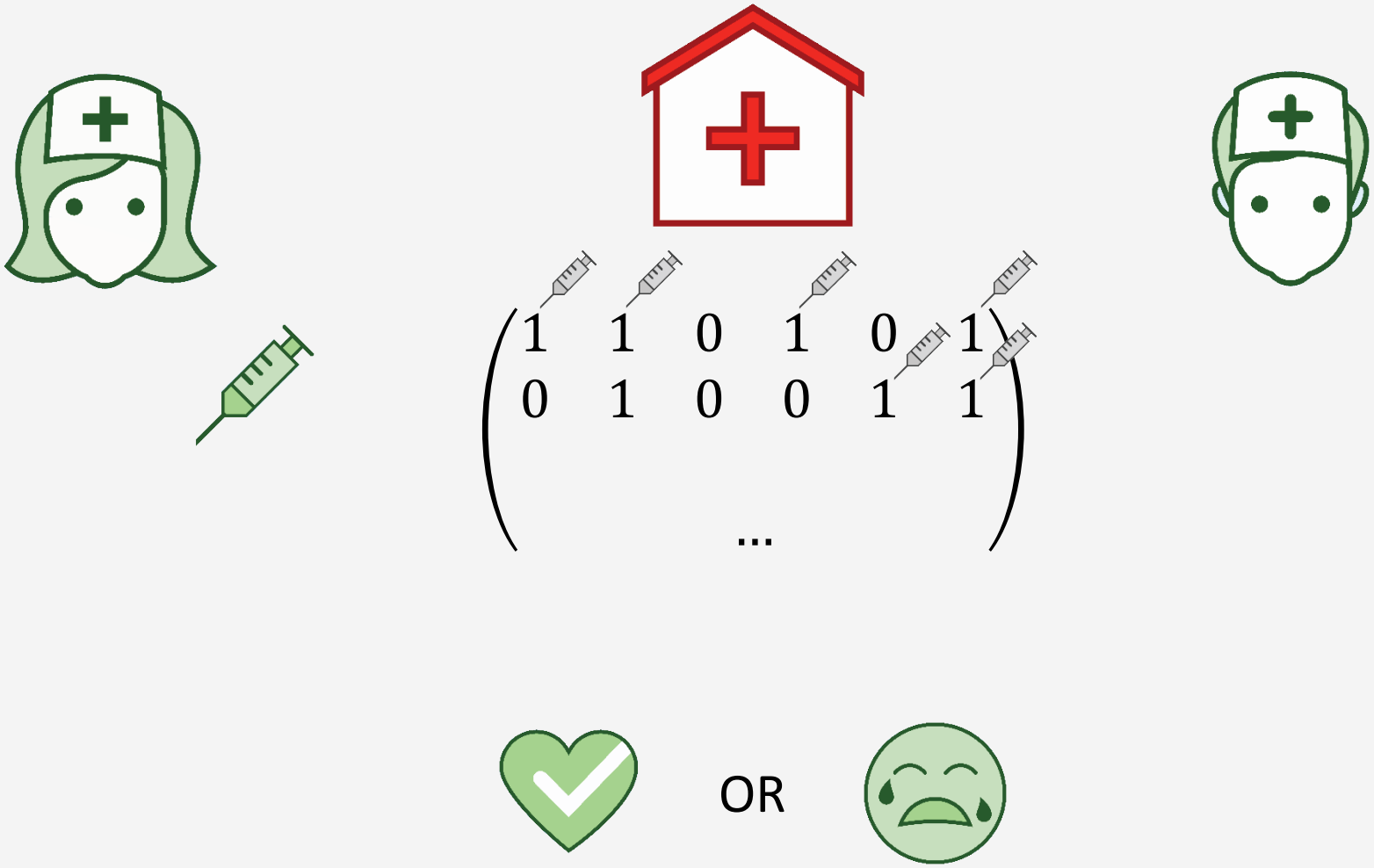


Motivation: Group Testing

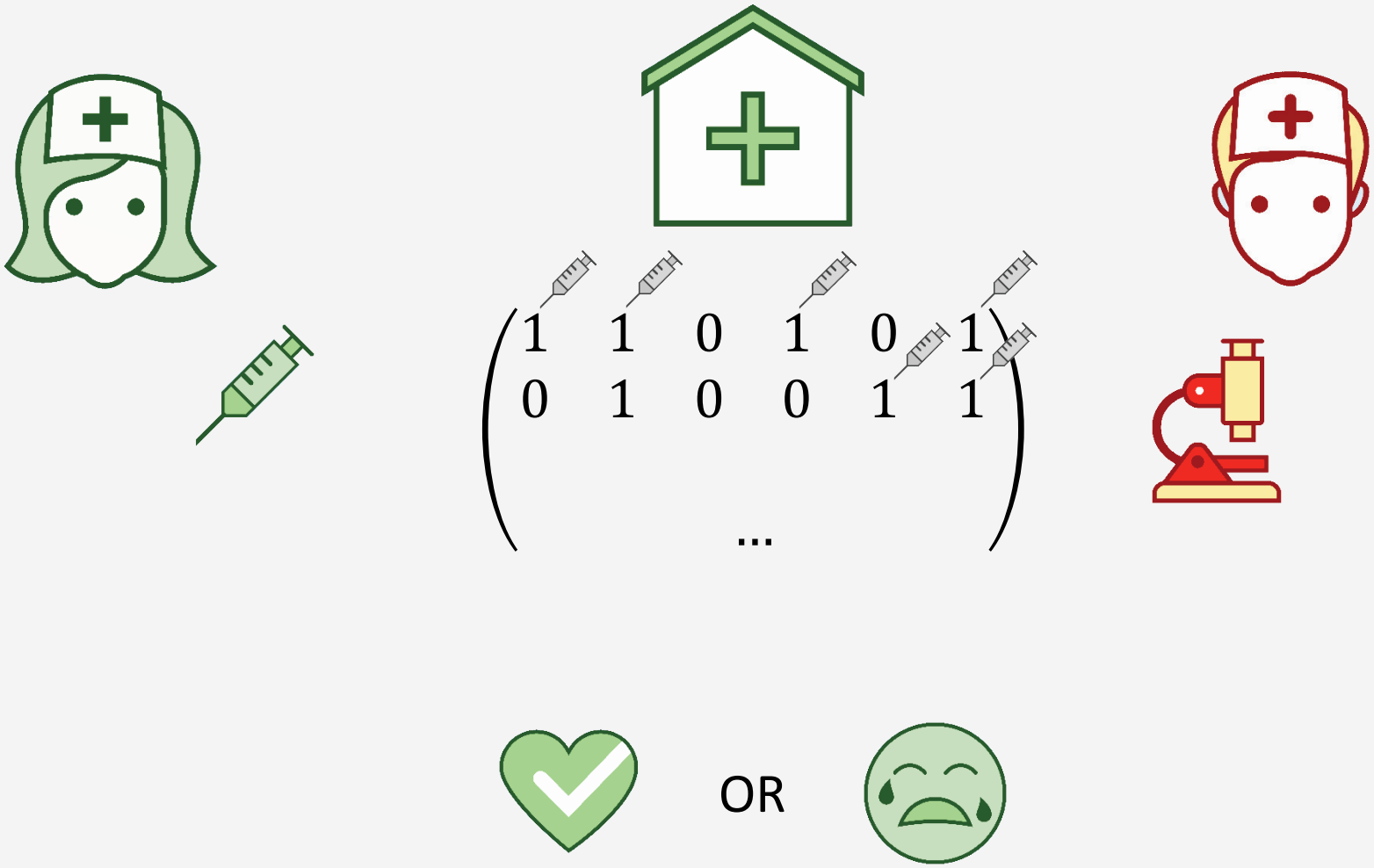


OR

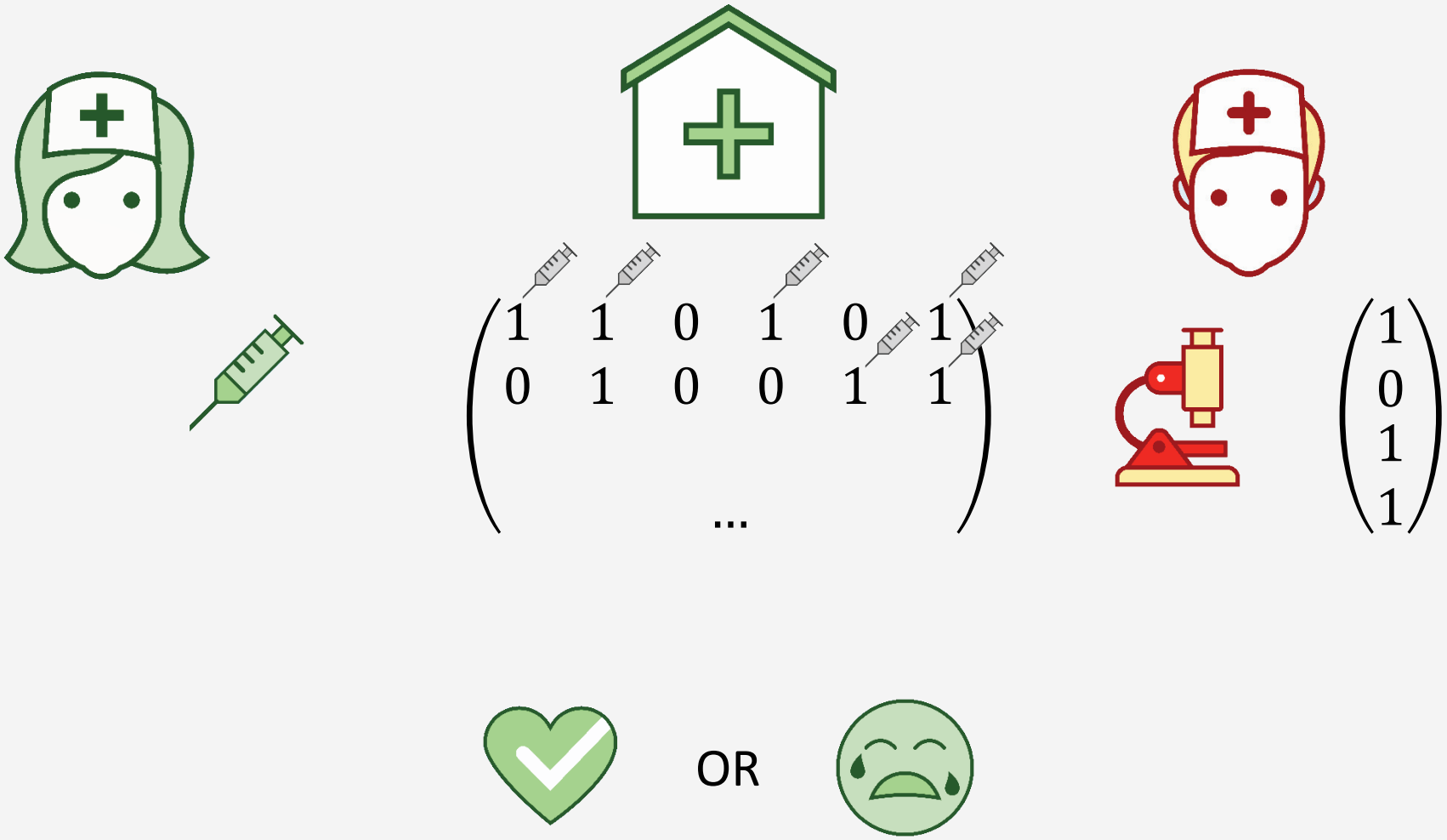
Motivation: Group Testing



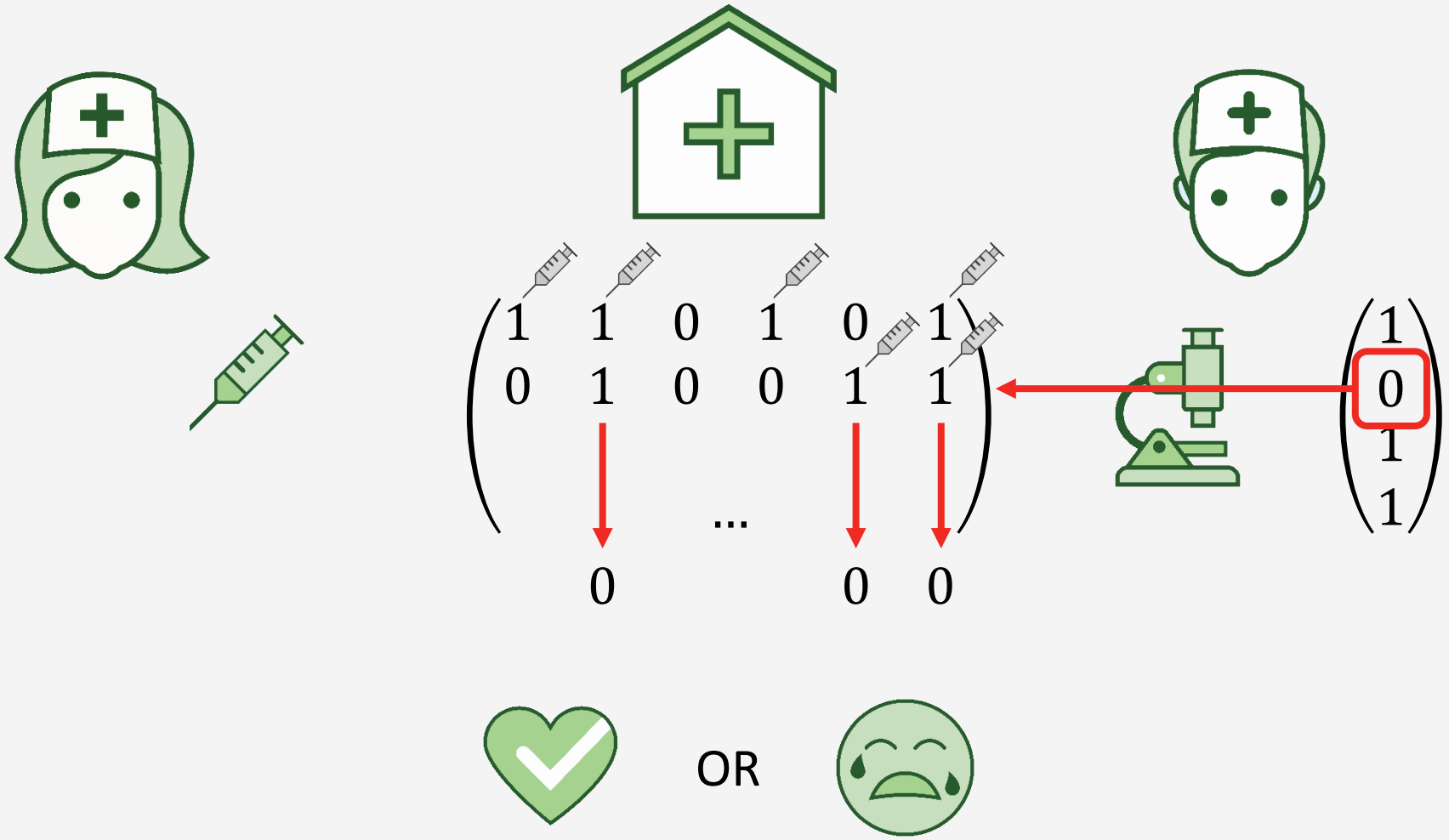
Motivation: Group Testing



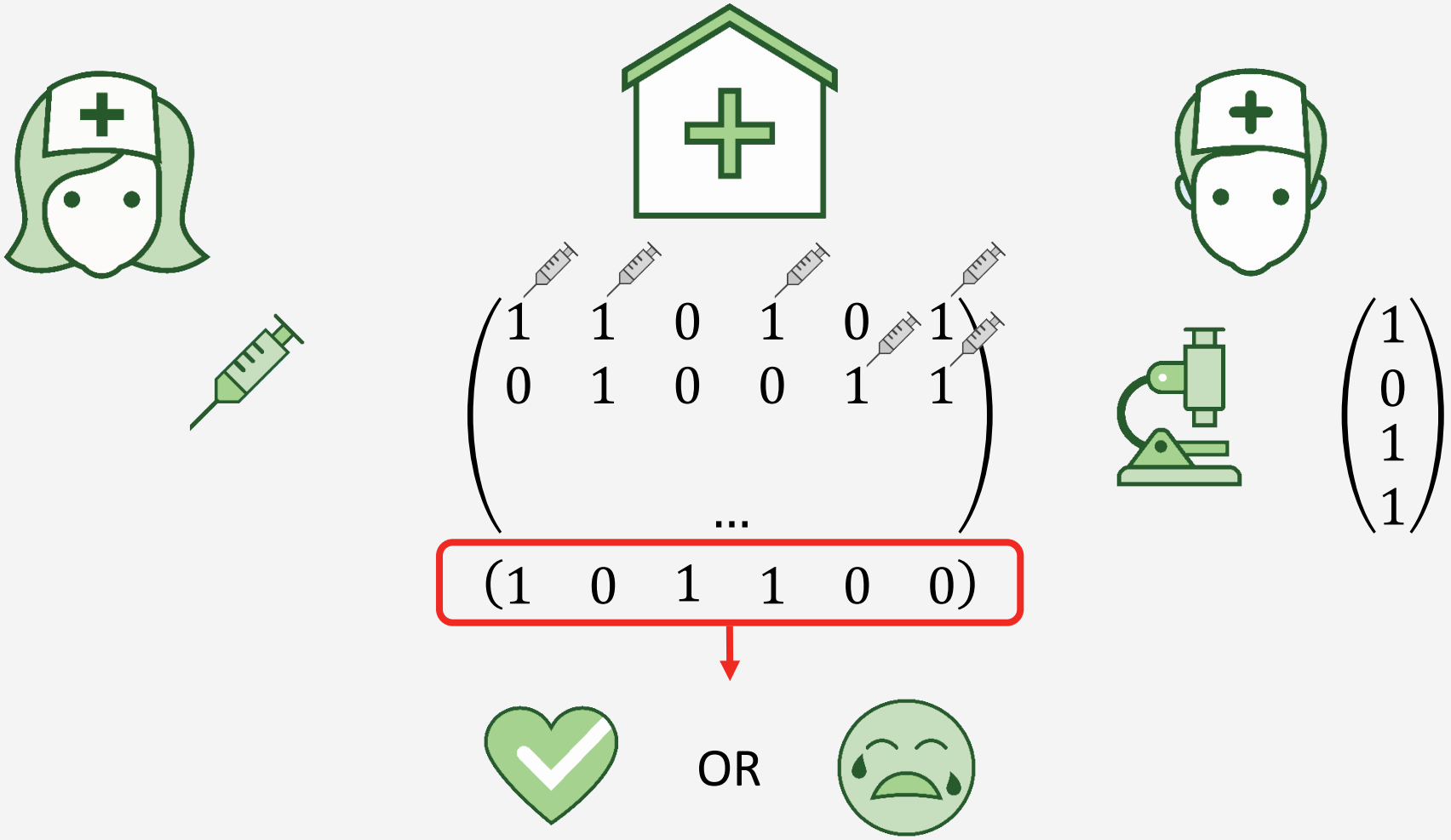
Motivation: Group Testing



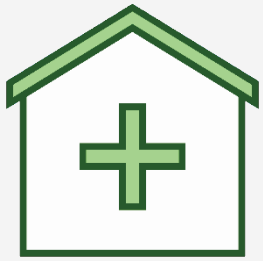
Motivation: Group Testing



Motivation: Group Testing



Motivation: Group Testing

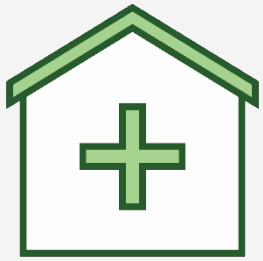


$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ & & \cdots & \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix} \qquad \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_m \end{pmatrix}$$

$$\bar{F}_j = \bigvee_i (x_{ij} \wedge \bar{y}_i)$$

OR

Motivation: Group Testing



$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ & & \cdots & \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix} \qquad \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_m \end{pmatrix}$$

$$\bar{F}_j = \sum_i (x_{ij} \cdot (1 - y_i))$$

OR

Notations

$\mathbb{G}_s = < g_s >$

$$a \in \mathbb{Z}_p, \qquad [a]_s = g_s^a$$

$$\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{Z}_p^n, \qquad [\boldsymbol{x}]_s = (g_s^{x_1}, \dots, g_s^{x_n})$$

Notations

$\mathbb{G}_s = < g_s >$

$$a \in \mathbb{Z}_p, \qquad [a]_s = g_s^a$$

$$\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{Z}_p^n, \qquad [\boldsymbol{x}]_s = (g_s^{x_1}, \dots, g_s^{x_n})$$

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$$[a]_1 \bullet [b]_2 = [a \otimes b]_T$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11} \cdot \boldsymbol{B} & a_{12} \cdot \boldsymbol{B} \\ a_{21} \cdot \boldsymbol{B} & a_{22} \cdot \boldsymbol{B} \end{pmatrix}$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen

$$\left(\boldsymbol{B}_s^{-1} \right) \left(\begin{matrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{matrix} \right) \left(\boldsymbol{B}_s \right) \in \mathrm{SL}_2(\mathbb{Z}_p)$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen

Projection

$\in \mathrm{SL}_2(\mathbb{Z}_p)$

$$\boldsymbol{P_s} = \left(\boldsymbol{B}_s^{-1} \right) \left(\begin{matrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{matrix} \right) \left(\boldsymbol{B}_s \right)$$

$$\mathrm{sk}_s$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen

Projection

$\in \mathrm{SL}_2(\mathbb{Z}_p)$

$$\boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1} \right) \begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix} \left(\boldsymbol{B}_s \right)$$

$$\mathrm{sk}_s$$

$$\ker(\boldsymbol{P}_s) = \{\boldsymbol{x} : \boldsymbol{x} \cdot \boldsymbol{P}_s = (0 \quad 0)\}$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen

Projection

$\in \mathrm{SL}_2(\mathbb{Z}_p)$

$$\boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1} \right) \begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix} \left(\boldsymbol{B}_s \right)$$

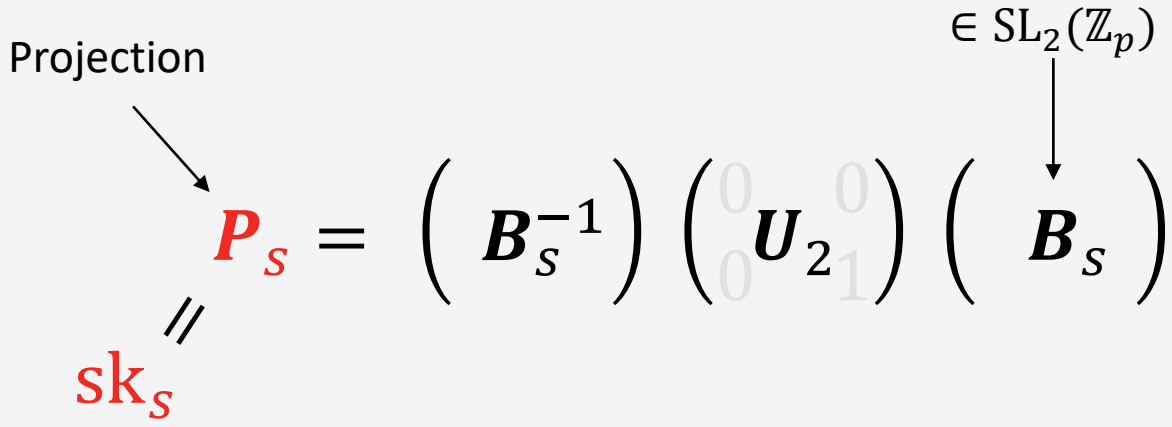
$$\mathrm{sk}_s = \boldsymbol{P}_s$$

$$\boldsymbol{p}_s \in \ker(\boldsymbol{P}_s) = \{\boldsymbol{x} : \boldsymbol{x} \cdot \boldsymbol{P}_s = (0 \quad 0)\}$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen



$$\boldsymbol{p}_s \in \ker(\boldsymbol{P}_s) = \{\boldsymbol{x}: \boldsymbol{x} \cdot \boldsymbol{P}_s = (0 \quad 0)\}$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [(0 \quad 0)]_s$$

The Encrytion Scheme for $m \in \{0,1\}$, $s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\mathbf{0}]_s$$

Encrypt

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

Encrypt

$$C_s = [\boldsymbol{c}_s]_s = m \cdot [(1 \quad 0)]_s + r \cdot [\boldsymbol{p}_s]_s \qquad r \in_\$ \mathbb{Z}_p$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

Encrypt

$$C_s = [\boldsymbol{c}_s]_s = m \cdot [(1 \quad 0)]_s + r \cdot [\boldsymbol{p}_s]_s \qquad r \in_\$ \mathbb{Z}_p$$

Decrypt

$$[\boldsymbol{c}_s]_s \cdot \boldsymbol{P}_s$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix}0 & 0\\ 0 & \boldsymbol{U}_2\end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

Encrypt

$$C_s = [\boldsymbol{c}_s]_s = m \cdot [(1 \quad 0)]_s + r \cdot [\boldsymbol{p}_s]_s \qquad r \in_\$ \mathbb{Z}_p$$

Decrypt

$$[\boldsymbol{c}_s]_s \cdot \boldsymbol{P}_s = m \cdot [(1 \quad 0)]_s \cdot \boldsymbol{P}_s + r \cdot [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix}0 & 0\\ 0 & \boldsymbol{U}_2\end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

Encrypt

$$C_s = [\boldsymbol{c}_s]_s = m \cdot [(1 \quad 0)]_s + r \cdot [\boldsymbol{p}_s]_s \qquad r \in_\$ \mathbb{Z}_p$$

Decrypt

$$[\boldsymbol{c}_s]_s \cdot \boldsymbol{P}_s = m \cdot [(1 \quad 0)]_s \cdot \boldsymbol{P}_s + \underbrace{r \cdot [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s}_{[\boldsymbol{0}]_s}$$

The Encrytion Scheme for $m \in \{0,1\}, s \in \{1,2\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix}0 & 0\\ 0 & \boldsymbol{U}_2\end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

Encrypt

$$C_s = [\boldsymbol{c}_s]_s = m \cdot [(1 \quad 0)]_s + r \cdot [\boldsymbol{p}_s]_s \qquad r \in_\$ \mathbb{Z}_p$$

Decrypt

$$[\boldsymbol{c}_s]_s \cdot \boldsymbol{P}_s = m \cdot [(1 \quad 0)]_s \cdot \boldsymbol{P}_s + \underbrace{r \cdot [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s}_{[\boldsymbol{0}]_s} = \begin{cases} [\boldsymbol{0}]_s \\ \neq [\boldsymbol{0}]_s \end{cases}$$

The Encrytion Scheme for $m \in \{0,1\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P_s} = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

$$\mathrm{sk}_T = (\mathrm{sk}_1, \mathrm{sk}_2)$$
$$\mathrm{pk}_T = (\mathrm{pk}_1, \mathrm{pk}_2)$$

The Encrytion Scheme for $m \in \{0,1\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

$$\mathrm{sk}_T = (\mathrm{sk}_1, \mathrm{sk}_2)$$
$$\mathrm{pk}_T = (\mathrm{pk}_1, \mathrm{pk}_2)$$

Encrypt $\quad [\boldsymbol{r}_1]_1 \in_\$ \mathbb{G}_1^2, [\boldsymbol{r}_2]_2 \in_\$ \mathbb{G}_2^2$

$$[\boldsymbol{c}_T]_T = m \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + [\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r}_2]_2 + [\boldsymbol{r}_1]_1 \bullet [\boldsymbol{p}_2]_2$$

The Encrytion Scheme for $m \in \{0,1\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

$$\mathrm{sk}_T = (\mathrm{sk}_1, \mathrm{sk}_2)$$
$$\mathrm{pk}_T = (\mathrm{pk}_1, \mathrm{pk}_2)$$

Encrypt $[\boldsymbol{r}_1]_1 \in_\$ \mathbb{G}_1^2, [\boldsymbol{r}_2]_2 \in_\$ \mathbb{G}_2^2$

$$[\boldsymbol{c}_T]_T = m \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + \underbrace{[\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r}_2]_2 + [\boldsymbol{r}_1]_1 \bullet [\boldsymbol{p}_2]_2}_{\in \ker(\boldsymbol{P}_1 \otimes \boldsymbol{P}_2)}$$

The Encrytion Scheme for $m \in \{0,1\}$

Keygen:

$$\mathrm{sk}_s = \boldsymbol{P}_s = \left(\boldsymbol{B}_s^{-1}\right)\begin{pmatrix} 0 & 0 \\ 0 & \boldsymbol{U}_2 \end{pmatrix}\left(\boldsymbol{B}_s\right)$$

$$\mathrm{pk}_s = [\boldsymbol{p}_s]_s \Rightarrow [\boldsymbol{p}_s]_s \cdot \boldsymbol{P}_s = [\boldsymbol{0}]_s$$

$$\mathrm{sk}_T = (\mathrm{sk}_1, \mathrm{sk}_2)$$
$$\mathrm{pk}_T = (\mathrm{pk}_1, \mathrm{pk}_2)$$

Encrypt $[\boldsymbol{r}_1]_1 \in_\$ \mathbb{G}_1^2, [\boldsymbol{r}_2]_2 \in_\$ \mathbb{G}_2^2$

$$[\boldsymbol{c}_T]_T = m \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + \underbrace{[\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r}_2]_2 + [\boldsymbol{r}_1]_1 \bullet [\boldsymbol{p}_2]_2}_{\in \ker(\boldsymbol{P}_1 \otimes \boldsymbol{P}_2)}$$

Decrypt

$$[\boldsymbol{c}_T]_T \cdot (\boldsymbol{P}_1 \otimes \boldsymbol{P}_2)$$

The Homomorphic Properties

Add

Many times

$$[\boldsymbol{c}_s]_s + [\boldsymbol{c'}_s]_s = (m + m') \cdot [(1 \quad 0)]_s + (r + r') \cdot [\boldsymbol{p}_s]_s$$

$$[\boldsymbol{c}_T]_T + [\boldsymbol{c}_T]_T =$$

$$(m + m') \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + [\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r}_2 + \boldsymbol{r'}_2]_2 + [\boldsymbol{r}_1 + \boldsymbol{r'}_1]_1 \bullet [\boldsymbol{p}_2]_2$$

The Homomorphic Properties

Add *Many times*

$$[\boldsymbol{c}_s]_s + [\boldsymbol{c'}_s]_s = (m + m') \cdot [(1 \quad 0)]_s + (r + r') \cdot [\boldsymbol{p}_s]_s$$

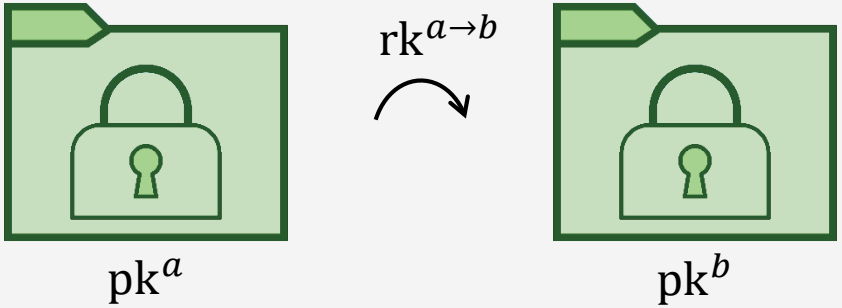
$$[\boldsymbol{c}_T]_T + [\boldsymbol{c}_T]_T = (m + m') \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + [\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r}_2 + \boldsymbol{r'}_2]_2 + [\boldsymbol{r}_1 + \boldsymbol{r'}_1]_1 \bullet [\boldsymbol{p}_2]_2$$

Multiply *Once*

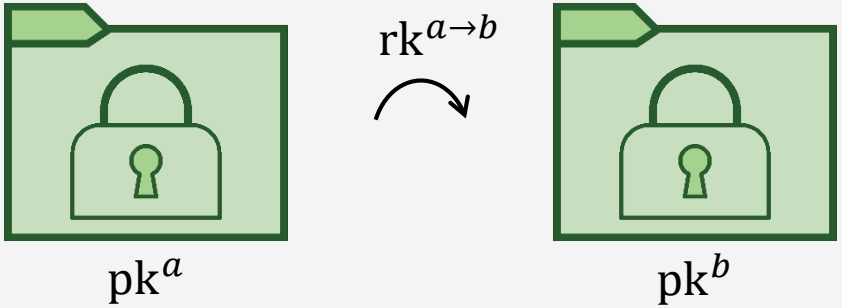
$$[\boldsymbol{c}_1]_1 \bullet [\boldsymbol{c}_2]_2 = (m_1 \cdot m_2) \cdot [(1 \quad 0 \quad 0 \quad 0)]_{\boldsymbol{T}} + [\boldsymbol{p}_1]_1 \bullet [\boldsymbol{r'}]_2 + [\boldsymbol{r}]_1 \bullet [\boldsymbol{p}_2]_2$$

$$[\boldsymbol{r}]_1 = m_1 r_2 (1 \quad 0)$$
$$[\boldsymbol{r'}]_2 = m_2 r_1 (1 \quad 0 \quad 0 \quad 0) + r_1 r_2 \boldsymbol{p}_2$$

Re-Encryption

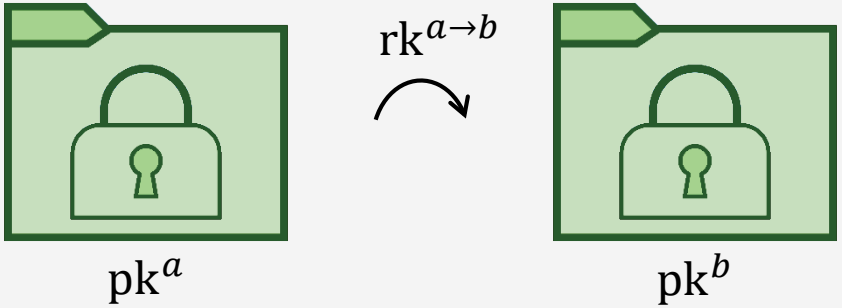


Re-Encryption



$$P = B^{-1}U_2B \quad \boxed{\mathrm{sk}^{a}} \quad \boxed{\mathrm{sk}^{b}} \quad P' = B'^{-1}U_2B'$$

Re-Encryption

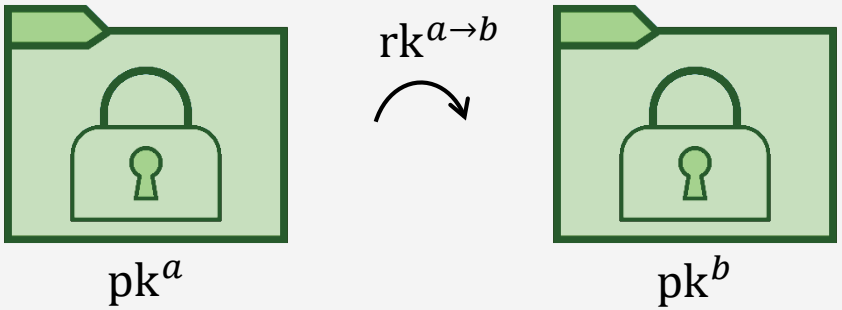


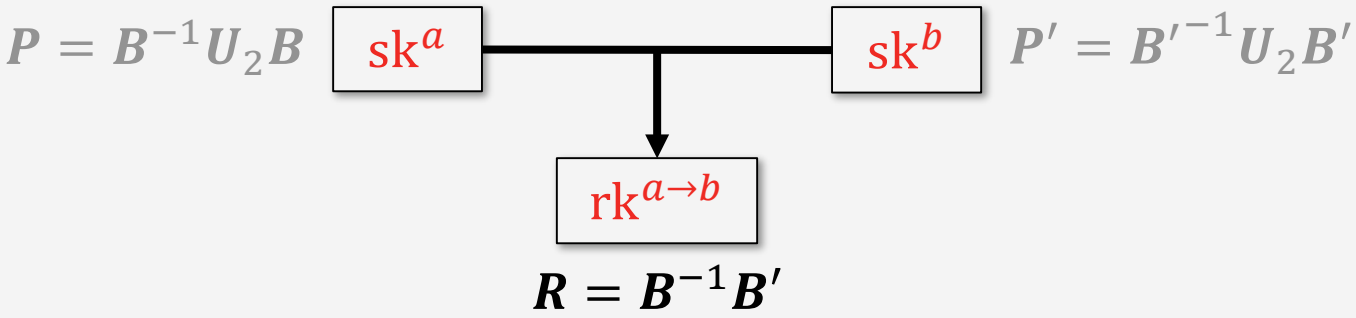
$P = B^{-1}U_2B$ sk^{a} sk^{b} $P' = B'^{-1}U_2B'$

$\mathrm{rk}^{a\to b}$

$\boldsymbol{R = B^{-1}B'}$

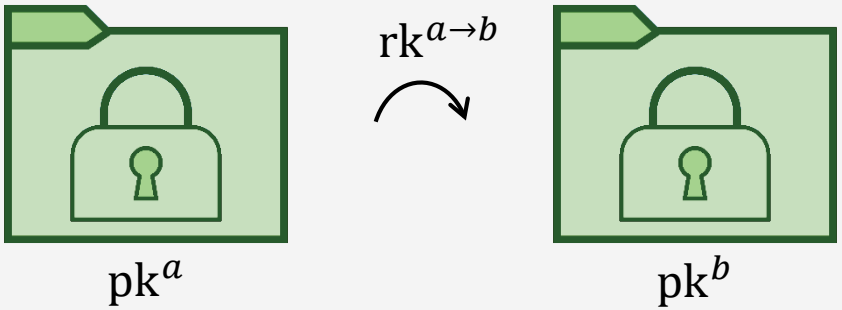
Re-Encryption





$$r \cdot [p_s]_s R_s = r' \cdot [p'_s]_s$$

Re-Encryption



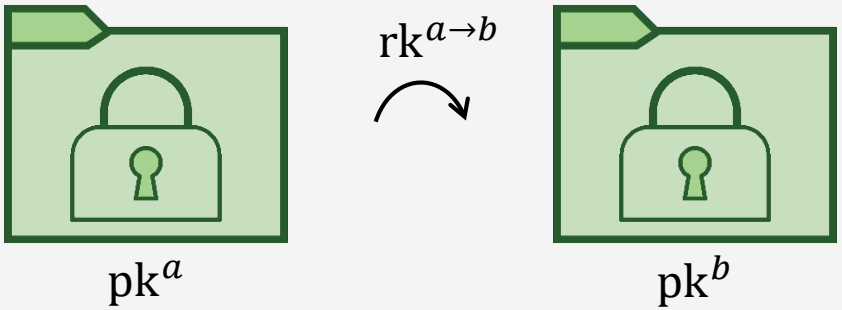
$P = B^{-1}U_2B$ sk^{a} sk^{b} $P' = B'^{-1}U_2B'$

$\mathrm{rk}^{a\to b}$

$$R = B^{-1}B'$$

$$m \cdot [(1 \quad 0)]_s R_s + r \cdot [p_s]_s R_s = r' \cdot [p'_s]_s + m \cdot [(1 \quad 0)]_s R_s$$

Re-Encryption



$P = B^{-1}U_2B$ sk^{a} sk^{b} $P' = B'^{-1}U_2B'$

rk$^{a\to b}$

$$R = B^{-1}B'$$

$$m \cdot [(1 \quad 0)]_s R_s + r \cdot [p_s]_s R_s = r' \cdot [p'_s]_s + m \cdot [(1 \quad 0)]_s R_s$$

$$[c_s]_s R_s = [c'_s]_s$$

Distributed Scheme

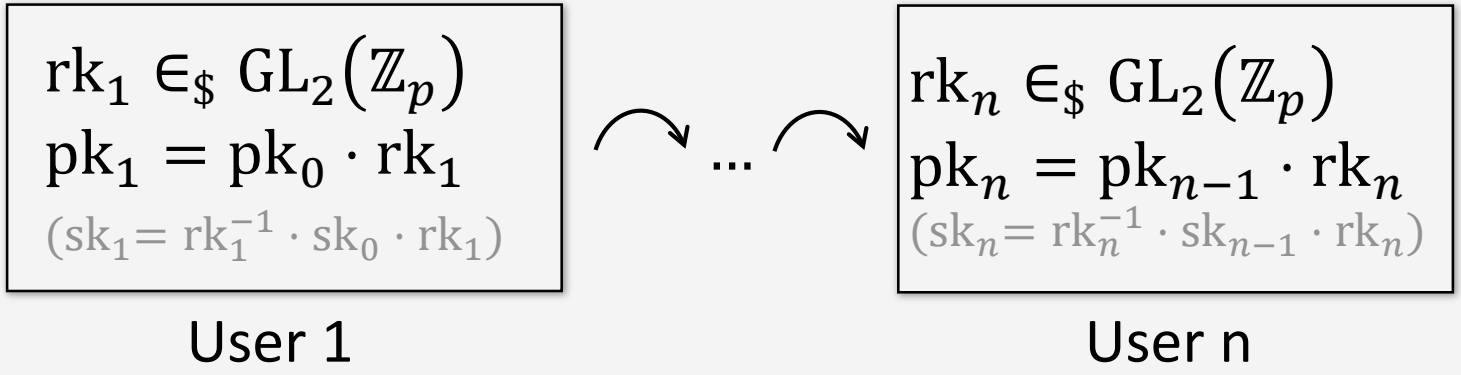
$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$

$$\mathrm{rk}_1 \in_{\$} \mathrm{GL}_2(\mathbb{Z}_p)$$
$$\mathrm{pk}_1 = \mathrm{pk}_0 \cdot \mathrm{rk}_1$$
$$(\mathrm{sk}_1 = \mathrm{rk}_1^{-1} \cdot \mathrm{sk}_0 \cdot \mathrm{rk}_1)$$

User 1

Distributed Scheme

$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$



Distributed Scheme

$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$

$\mathrm{rk}_1 \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_1 = \mathrm{pk}_0 \cdot \mathrm{rk}_1$
$(\mathrm{sk}_1 = \mathrm{rk}_1^{-1} \cdot \mathrm{sk}_0 \cdot \mathrm{rk}_1)$

User 1

...

$\mathrm{rk}_n \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_n = \mathrm{pk}_{n-1} \cdot \mathrm{rk}_n$
$(\mathrm{sk}_n = \mathrm{rk}_n^{-1} \cdot \mathrm{sk}_{n-1} \cdot \mathrm{rk}_n)$

User n

pk_n

Distributed Scheme

$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$

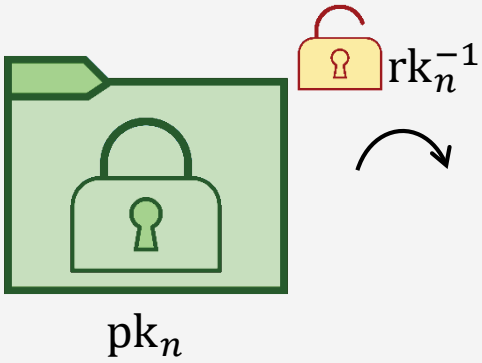
$\mathrm{rk}_1 \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_1 = \mathrm{pk}_0 \cdot \mathrm{rk}_1$
$(\mathrm{sk}_1 = \mathrm{rk}_1^{-1} \cdot \mathrm{sk}_0 \cdot \mathrm{rk}_1)$

User 1

...

$\mathrm{rk}_n \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_n = \mathrm{pk}_{n-1} \cdot \mathrm{rk}_n$
$(\mathrm{sk}_n = \mathrm{rk}_n^{-1} \cdot \mathrm{sk}_{n-1} \cdot \mathrm{rk}_n)$

User n



Distributed Scheme

$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$

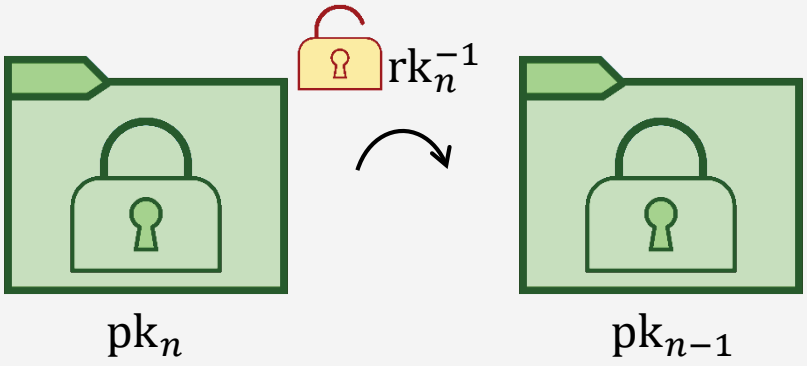
$\mathrm{rk}_1 \in_{\$} \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_1 = \mathrm{pk}_0 \cdot \mathrm{rk}_1$
$(\mathrm{sk}_1 = \mathrm{rk}_1^{-1} \cdot \mathrm{sk}_0 \cdot \mathrm{rk}_1)$

User 1

...

$\mathrm{rk}_n \in_{\$} \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_n = \mathrm{pk}_{n-1} \cdot \mathrm{rk}_n$
$(\mathrm{sk}_n = \mathrm{rk}_n^{-1} \cdot \mathrm{sk}_{n-1} \cdot \mathrm{rk}_n)$

User n



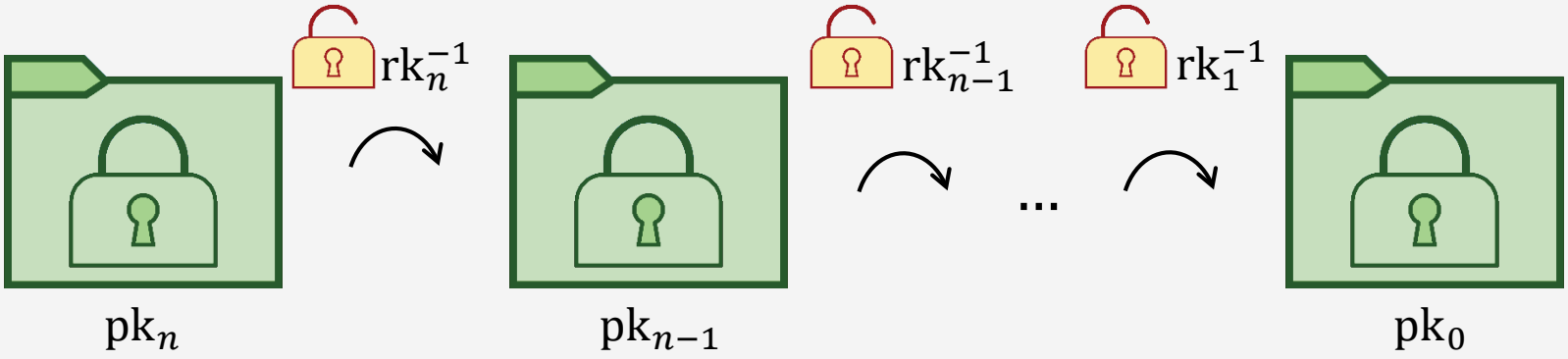
Distributed Scheme

$sk_0 = \boldsymbol{U}_2$
$pk_0 = ([\mathbf{1}], [\mathbf{0}])$

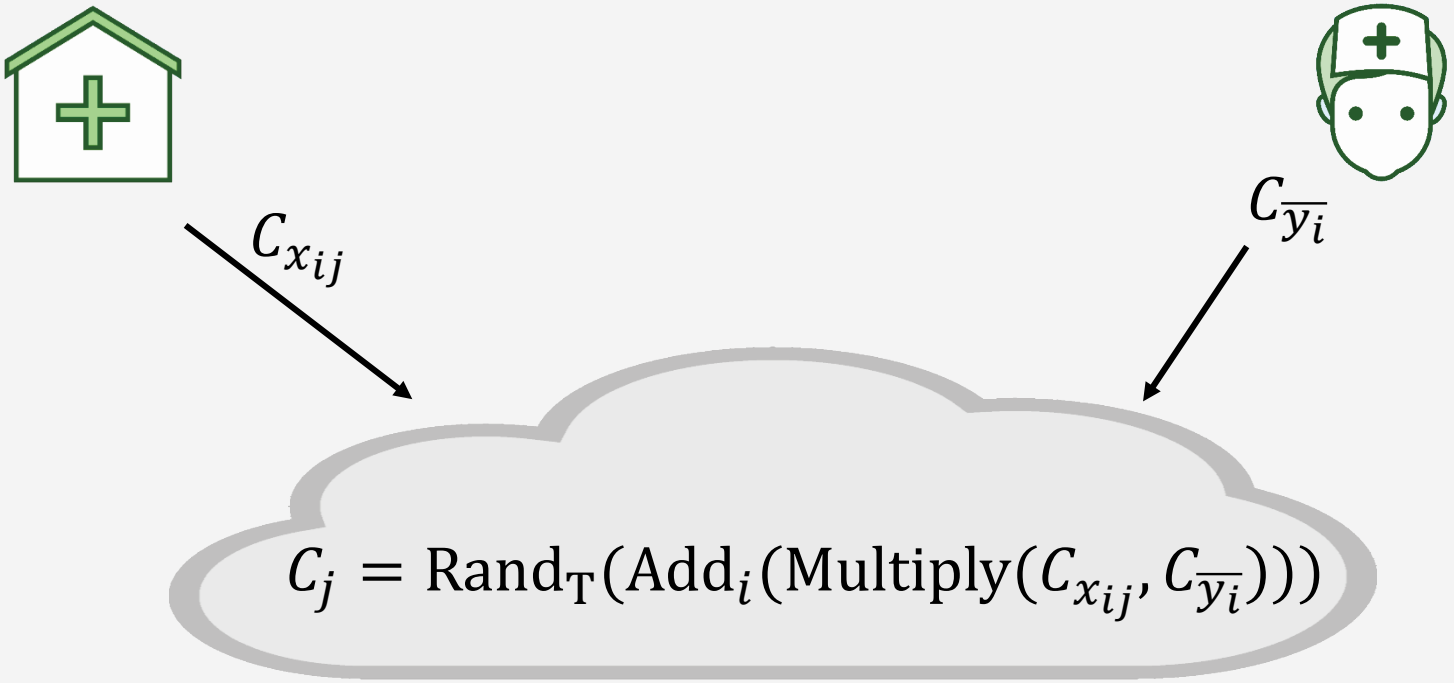
$\mathrm{rk}_1 \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_1 = \mathrm{pk}_0 \cdot \mathrm{rk}_1$
$(\mathrm{sk}_1 = \mathrm{rk}_1^{-1} \cdot \mathrm{sk}_0 \cdot \mathrm{rk}_1)$

User 1 ... User n

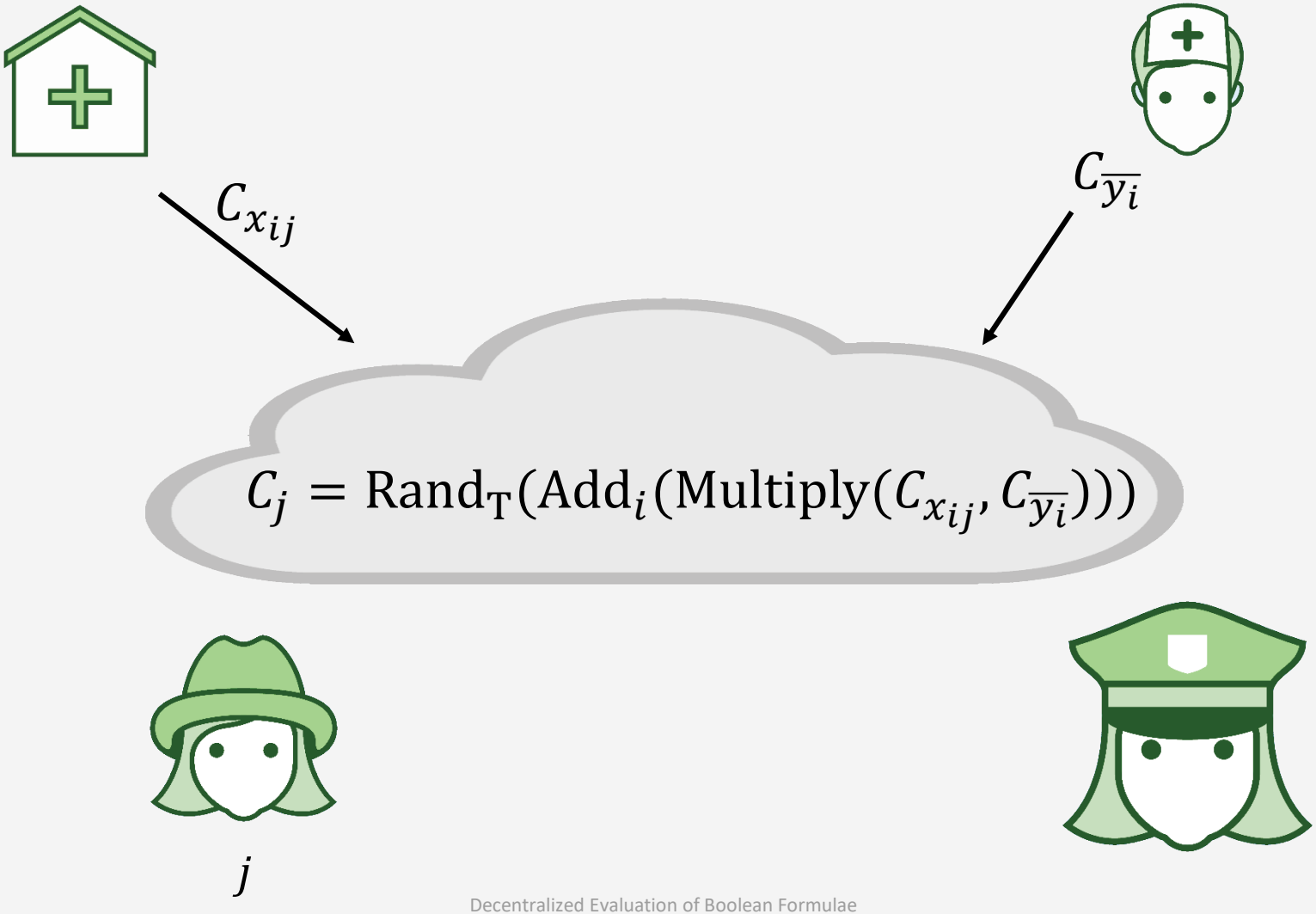
$\mathrm{rk}_n \in_\$ \mathrm{GL}_2(\mathbb{Z}_p)$
$\mathrm{pk}_n = \mathrm{pk}_{n-1} \cdot \mathrm{rk}_n$
$(\mathrm{sk}_n = \mathrm{rk}_n^{-1} \cdot \mathrm{sk}_{n-1} \cdot \mathrm{rk}_n)$



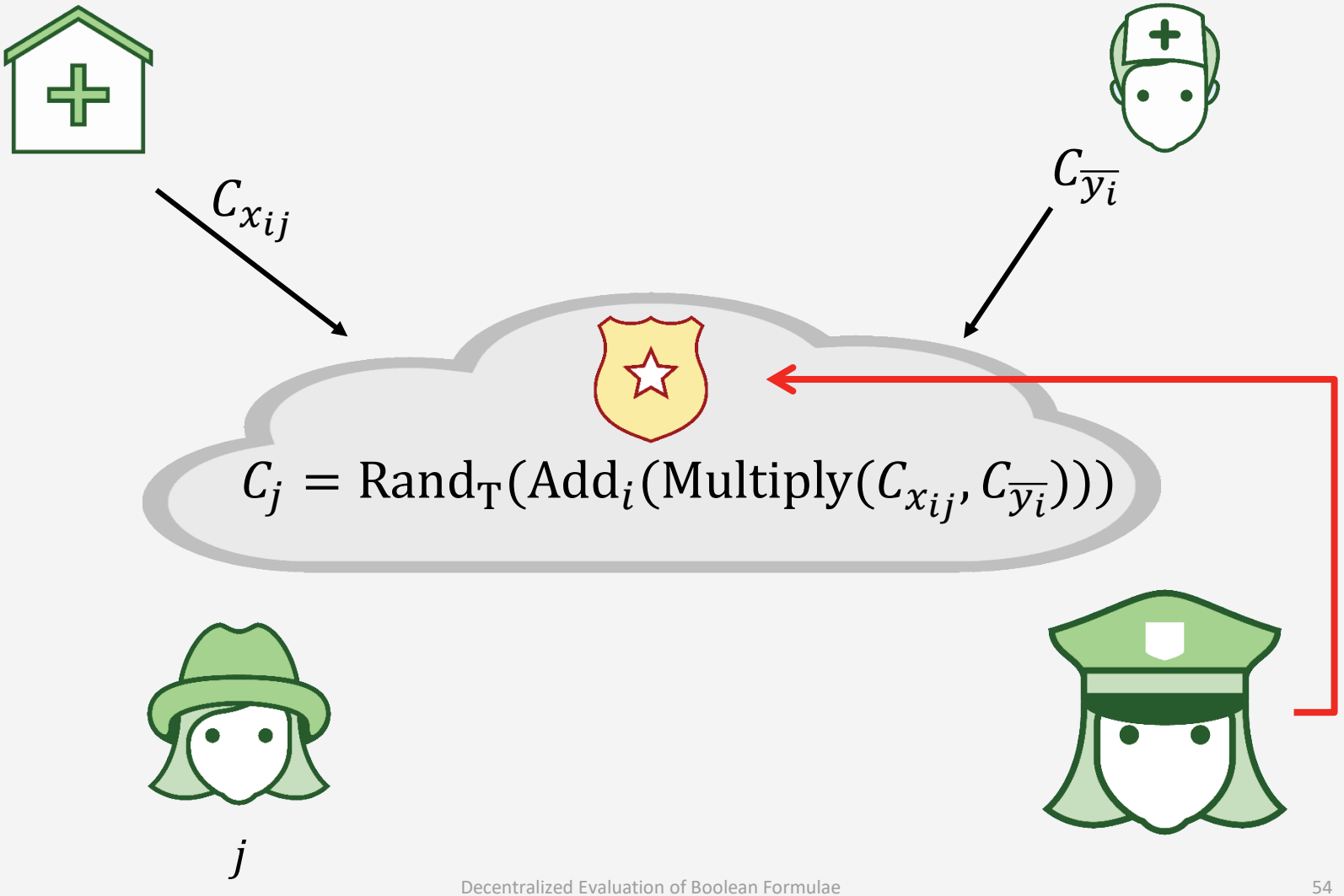
Solution: Group Testing



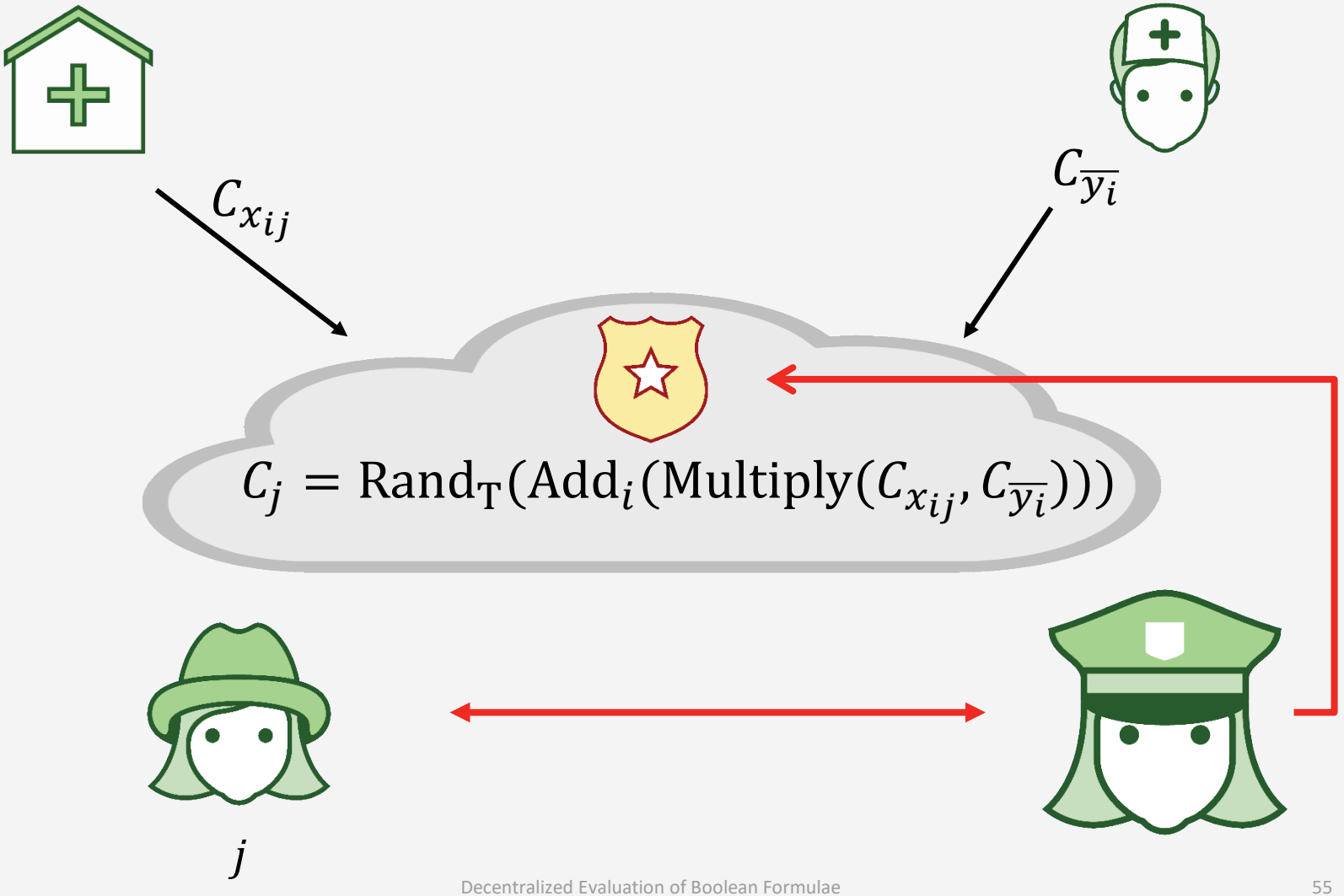
Solution: Group Testing



Solution: Group Testing



Solution: Group Testing



Thank you