Indistinguishability Obfuscation from Well-Founded Assumptions

Tutorial, Part 1

Aayush Jain
UCLA

Huijia (Rachel) Lin
UW

Amit Sahai
UCLA

Center *for* Encrypted Functionalities
An NSF Frontier Center

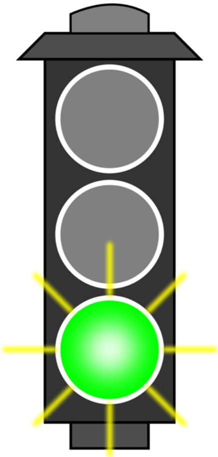
Simons Institute: New Developments in Obfuscation 12/10/2020

Today

- We will establish that iO exists, assuming sub-exponential hardness holds for **all** of the following assumptions:
  - **LPN over $\mathbb{Z}_p$**
  - LWE
  - PRG in NC^0
  - SXDH

Constructing iO: Today

iO



New Pseudorandom Object

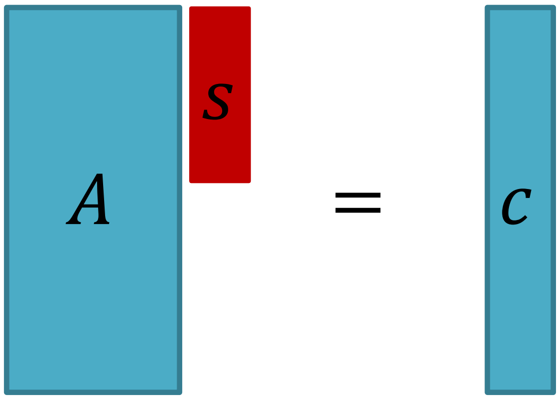
[JLS20], building upon many prior works

LPN over $\mathbb{Z}_p$ + SXDH (bilinear maps) + PRG in NC^0 + LWE

Well-Founded Assumptions

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

Random Linear Codes over $\mathbb{Z}_p$ [Hamming, 1950]



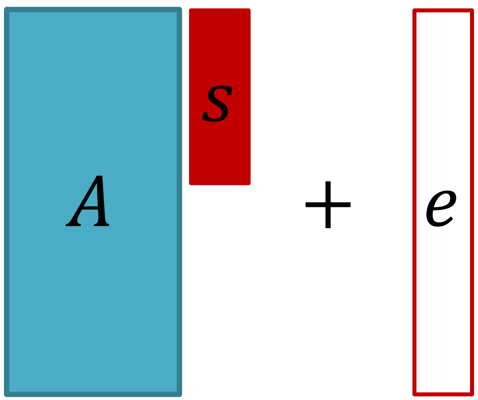
$\{a_i\}_{i\in[n]}, s \leftarrow \mathbb{Z}_p^{\ell}$

$n = \mathrm{poly}(\ell)$

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

Random Linear Codes over $\mathbb{Z}_p$

$$\{e_i\}_{i\in[n]} : \begin{cases} e_i \leftarrow \mathbb{Z}_p & \text{with prob. } 1/\ell^\delta \\ e_i = 0 & \text{otherwise} \end{cases}$$



$$\{a_i\}_{i\in[n]}, s \leftarrow \mathbb{Z}_p^\ell$$

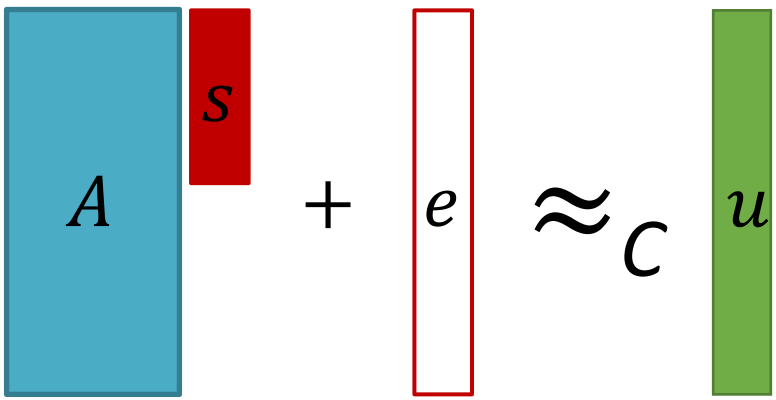
$$n = \text{poly}(\ell)$$

- Random Linear Codes exhibit strong *combinatorial* error-correction capabilities vs. **sparse error** [Gilbert 1952, Varshamov 1957, …]
- However, no efficient (sub-exponential in ℓ) decoding algorithms known despite decades of study

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

LPN over $\mathbb{Z}_p$ Assumption:

$$\{e_i\}_{i\in[n]} : \begin{cases} e_i \leftarrow \mathbb{Z}_p & \text{with prob. } 1/\ell^\delta \\ e_i = 0 & \text{otherwise} \end{cases}$$



$$\{a_i\}_{i\in[n]}, s \leftarrow \mathbb{Z}_p^\ell$$

$$\{u_i\}_{i\in[n]} \leftarrow \mathbb{Z}_p$$

$$n = \mathrm{poly}(\ell)$$

- We assume there exist (arbitrary) constants $\varepsilon, \delta > 0$, such that this holds for all Time 2^{ℓ^ε} adversaries.
- Follows from hardness of decoding – recovering s from $(A, As + e)$ – via search-to-decision reduction [AIK 07].
- Best known attack is $2^{O\left(\ell^{1-\delta}\right)}$ [EKM 17,BCGI 18]

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

δ

More details:

We set $p = 2^{\ell^{\varepsilon'}}$ for tiny constant $\varepsilon' < \varepsilon$

This allows for search-to-decision reduction, which runs in time polynomial in p.

If we want $\varepsilon' > \varepsilon$, (i.e. p larger than running time of LPN adversary) then that's fine, but make decisional assumption directly.

- We assume there exist (arbitrary) constants $\varepsilon, \delta > 0$, such that this holds for all Time $2^{\ell^{\varepsilon}}$ adversaries.
- Follows from hardness of decoding – recovering s from $(A, As + e)$ – via search-to-decision reduction [AIK 07].
- Best known attack is $2^{O\left(\ell^{1-\delta}\right)}$ [EKM 17,BCGI 18]

Slide from: **Geoffroy Couteau**

Security of LPN over Large Fields

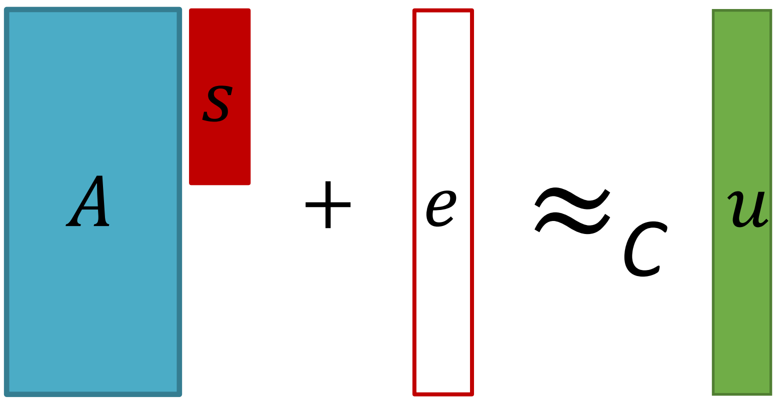
A tremendous number of attacks on LPN has been published in the literature

- **Statistical Decoding Attacks**
  - Jabri's attack [ICCC:Jab01]
  - Overbeck's variant [ACISP:Ove06]
  - FKI's variant [Trans.IT:FKI06]
  - Debris-Tillich variant [ISIT:DT17]
- **Information Set Decoding Attacks**
  - Prange's algorithm [Prange62]
  - Stern's variant [ICIT:Stern88]
  - Finiasz and Sendrier's variant [AC:FS09]
  - BJMM variant [EC:BJMM12]
  - May-Ozerov variant [EC:MO15]
  - Both-May variant [PQC:BM18]
  - MMT variant [AC:MMT11]
  - Well-pooled MMT [CRYPTO:EKM17]
  - BLP variant [CRYPTO:BLP11]
- **Classical Techniques**
  - Low-deg approx [ITCS:ABGKR17]
- **Gaussian Elimination attacks**
  - Standard gaussian elimination
  - Blum-Kalai-Wasserman [J.ACM:BKW03]
  - Sample-efficient BKW [A-R:Lyu05]
  - Pooled Gauss [CRYPTO:EKM17]
  - Well-pooled Gauss [CRYPTO:EKM17]
  - Leviel-Fouque [SCN:LF06]
  - Covering codes [JC:GJL19]
  - Covering codes+ [BTV15]
  - Covering codes++ [BV:AC16]
  - Covering codes+++ [EC:ZJW16]
- **Other Attacks**
  - Generalized birthday [CRYPTO:Wag02]
  - Improved GBA [Kirchner11]
  - Linearization [EC:BM97]
  - Linearization 2 [INDO:Saa07]
  - Low-weight parity-check [Zichron17]

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

LPN over $\mathbb{Z}_p$ Assumption:

$$\{e_i\}_{i\in[n]} : \begin{cases} e_i \leftarrow \mathbb{Z}_p & \text{with prob. } 1/\ell^{\delta} \\ e_i = 0 & \text{otherwise} \end{cases}$$



$$\{a_i\}_{i\in[n]}, s \leftarrow \mathbb{Z}_p^{\ell}$$

$$\{u_i\}_{i\in[n]} \leftarrow \mathbb{Z}_p$$

$$n = \mathrm{poly}(\ell)$$

$$\{a_i, \langle a_i, s\rangle + e_i\}_{i=1,\ldots,n} \approx_C \{a_i, u_i\}_{i=1,\ldots,n}$$

- We assume there exist (arbitrary) constants $\varepsilon, \delta > 0$, such that this holds for all Time $2^{\ell^{\varepsilon}}$ adversaries.
- Follows from hardness of decoding – recovering s from $(A, As + e)$ – via search-to-decision reduction [AIK 07].
- Best known attack is $2^{O\left(\ell^{1-\delta}\right)}$ [EKM 17,BCGI 18]

LPN over $\mathbb{Z}_p$ [BFKL'93, IPS 2009]

LPN over $\mathbb{Z}_p$ Assumption:

$e_i \leftarrow \mathbb{Z}_p \quad \text{with prob. } 1/\ell^{\delta}$

LPN with $\delta > 0$ is not known to imply PKE.

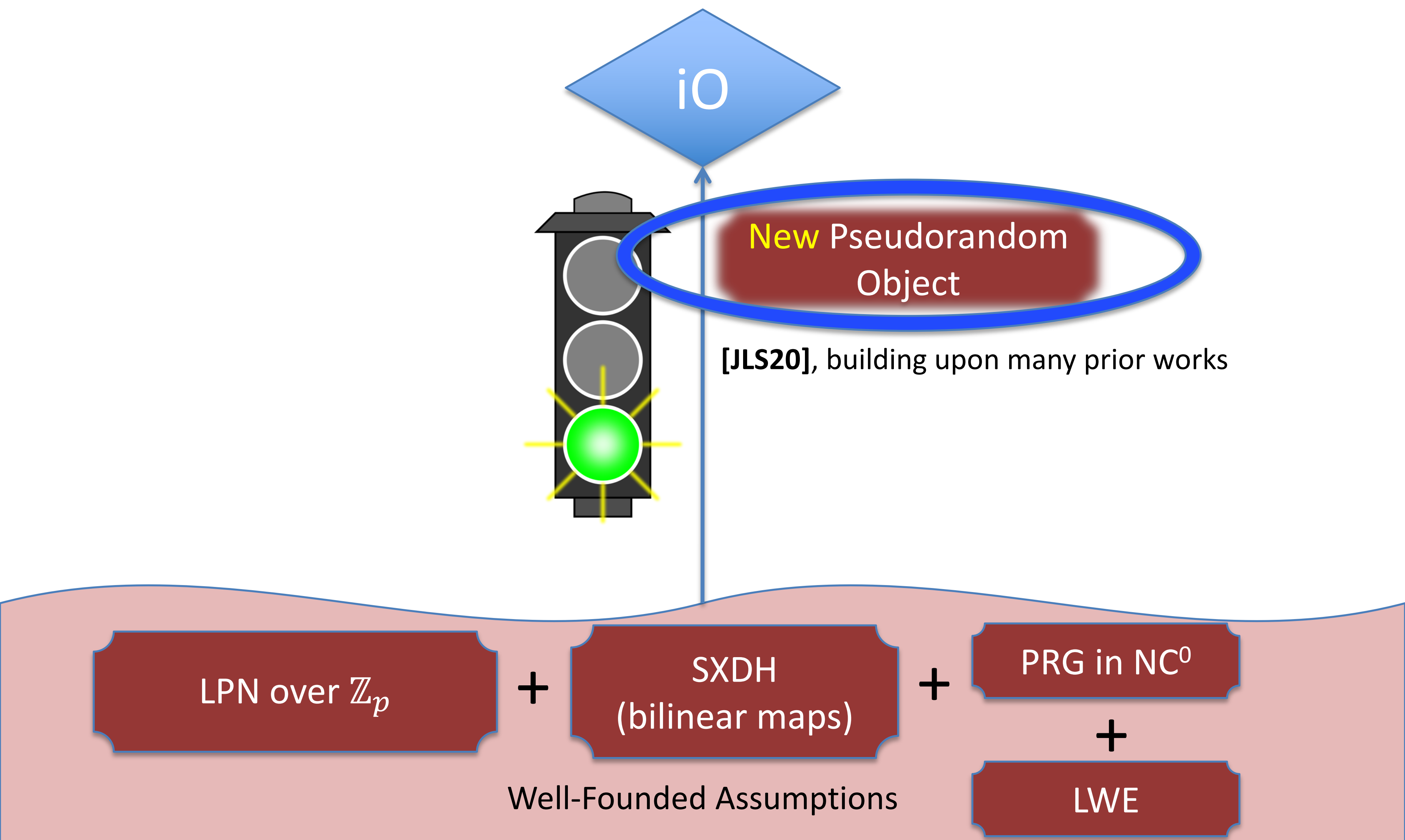
(Need $\delta > 1/2$ to imply PKE [Ale 03, AAB15].)

As far as we know,
this is a "minicrypt" assumption, unlike LWE.

$$\{a_i, \langle a_i, s\rangle + e_i\}_{i=1,\ldots,n} \approx_C \{a_i, u_i\}_{i=1,\ldots,n}$$

- We assume there exist (arbitrary) constants $\varepsilon, \delta > 0$, such that this holds for all Time $2^{\ell^{\varepsilon}}$ adversaries.
- Follows from hardness of decoding – recovering s from $(A, As + e)$ – via search-to-decision reduction [AIK 07].
- Best known attack is $2^{O(\ell^{1-\delta})}$ [EKM 17,BCGI 18]

Constructing iO: Today



Preview: Why LPN over $\mathbb{Z}_p$?

- Using LPN over $\mathbb{Z}_p$ to build a **key pseudorandom object** is at the heart of our new work: a "structured-seed PRG" (**sPRG**).
- **sPRG** has both a "public seed" and "secret seed", following our previous work from [AJS18, LM18, AJLMS19, JLMS19, JLS19, GJLS20].
- **sPRG** has three main requirements:
  - (1) "Degree-2 efficiency": very roughly speaking, the output is a degree-2 polynomial in the secret seed
  - (2) Expansion: The length of the structured seed is $m^{1-\epsilon}$, where the **sPRG** outputs m bits.
  - **(3) Pseudorandomness**
- Talk Part 2 (Rachel) will tell us why **sPRG** is enough to build iO
- Talk Part 3 (Aayush) will tell us how to achieve (1) and (2)

Preview: Why LPN over $\mathbb{Z}_p$?

- **sPRG** output has two parts, that are (unfortunately) correlated:
  - First, a part that looks like distribution from LPN over $\mathbb{Z}_p$:

    $$\{a_i, \langle a_i, s\rangle + e_i + x_i\}_{i=1,\ldots,n},$$
    where each $x_i \leftarrow \{0,1\}$
  - Second, a correlated output:

    $$PRG(x_1, \ldots, x_n)$$
- We want to show these are (jointly) pseudorandom, despite this correlation: x_i used in both outputs.
- Simple insight (of [JLS20] over [AJS18,LM18,…]):
  We separate the "error" into two components: $e_i + x_i$
- In earlier works, there was no LPN error e_i.
  The entire error in the first component was x_i.

Preview: Why LPN over $\mathbb{Z}_p$?

- LPN over $\mathbb{Z}_p$ allows a simple pseudo-randomness analysis:

$$\{a_i, \langle a_i, s\rangle + e_i + x_i\}_{i=1,\dots,n}, PRG(x_1, \dots, x_n)$$

- By LPN over $\mathbb{Z}_p$, this is indistinguishable from:

$$\{a_i, u_i + x_i\}_{i=1,\dots,n}, PRG(x_1, \dots, x_n)$$
$$\approx_S \{a_i, u_i\}_{i=1,\dots,n}, PRG(x_1, \dots, x_n)$$

- Finally, by the pseudo-randomness of PRG, this is indistinguishable from:

$$\{a_i, u_i\}_{i=1,\dots,n}, R$$

- In this simple way, LPN over $\mathbb{Z}_p$ is used to “break up” a dependency – we can prove pseudo-randomness even though $x_1, \dots, x_n$ is used both as input to PRG, and as “noise”

Other Well-Founded Assumptions

- We assume LWE (which is just like LPN, but with small Gaussian error e_i instead of sparse error) with sub-exponential modulus-to-noise ratio.
  - Known to be true if the Shortest Vector Problem over general lattices is worst-case hard to approximate to any sub-exponential factor [Reg 05, Pei 09, BLPRS 12].
  - Search-to-decision reduction also for LWE [MM 11].
  - LWE has turned out to be a remarkably versatile assumption in cryptography, most famously used for constructing Fully Homomorphic Encryption [BV 11, BGV 11, GSW 13]

Preview: Why LPN over $\mathbb{Z}_p$?

- LPN over $\mathbb{Z}_p$ allows a simple pseudo-randomness analysis:

$$\{a_i, \langle a_i, s\rangle + e_i + x_i\}_{i=1,\ldots,n}, PRG(x_1, \ldots, x_n)$$

- By LPN over $\mathbb{Z}_p$, this is indistinguishable from:

$$\{a_i, u_i + x_i\}_{i=1,\ldots,n}, PRG(x_1, \ldots, x_n)$$
$$\approx_S \{a_i, u_i\}_{i=1,\ldots,n}, PRG(x_1, \ldots, x_n)$$

Note: the analysis so far could have worked just as well using LWE, where the errors e_i are small.

The fact that LPN errors are ***sparse*** is crucial for suitably ***computing*** the sPRG.
(Stay tuned for details in Part 3!)

Other Well-Founded Assumptions

- We assume LWE (which is just like LPN, but with small Gaussian error e_i instead of sparse error) with sub-exponential modulus-to-noise ratio.
  - Known to be hard if SVP is worst-case hard to approximate to any sub-exponential factor [Reg 05, Pei 09, BLPRS 12].
- We assume the existence of PRGs computable by constant-depth (NC^0) circuits, with stretch $n^{1+\epsilon}$, for any constant $\epsilon > 0$.
  - Extensively studied [Gol 00, CM 01, MST 03, IKOS 08, …].
  - Follows from one-way-ness conjectures [App13, AK19].
- We assume the SXDH assumption over bilinear maps.
  - Extensively studied and used since [BdGMM 05].
- All assumptions made vs. sub-exponential time adversaries.

Parts 2 and 3

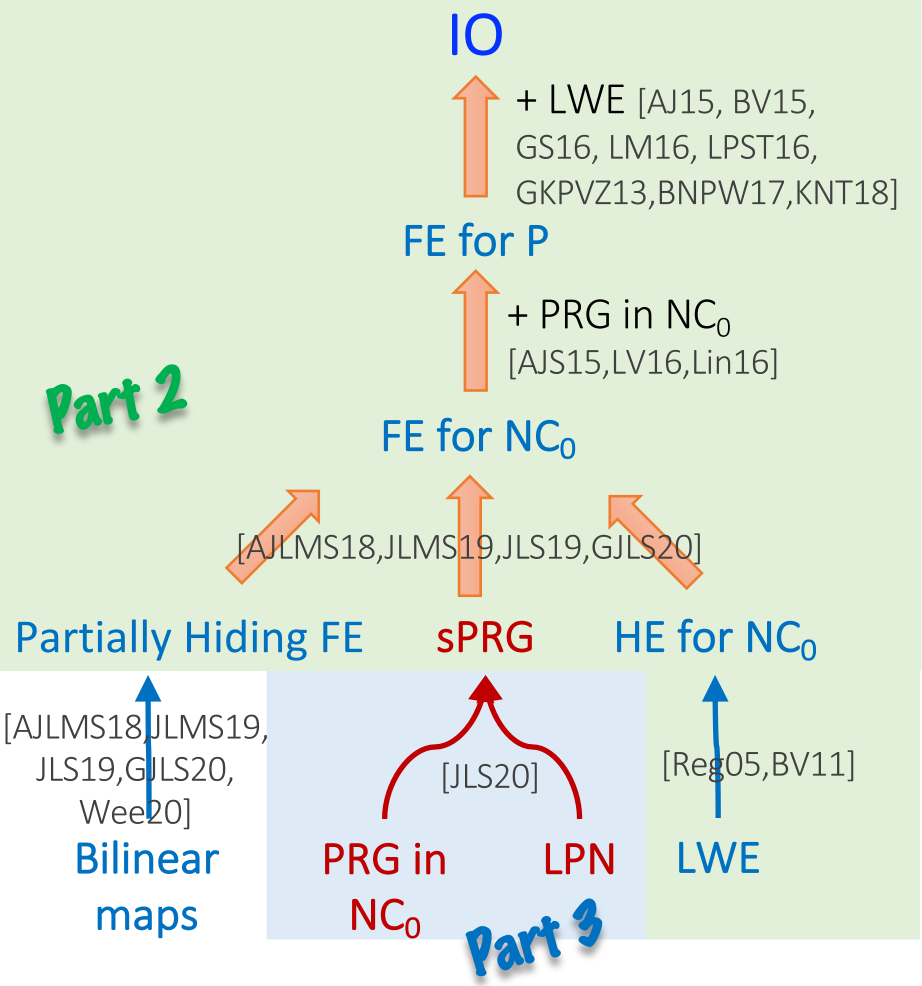


Image credit: Rachel Lin