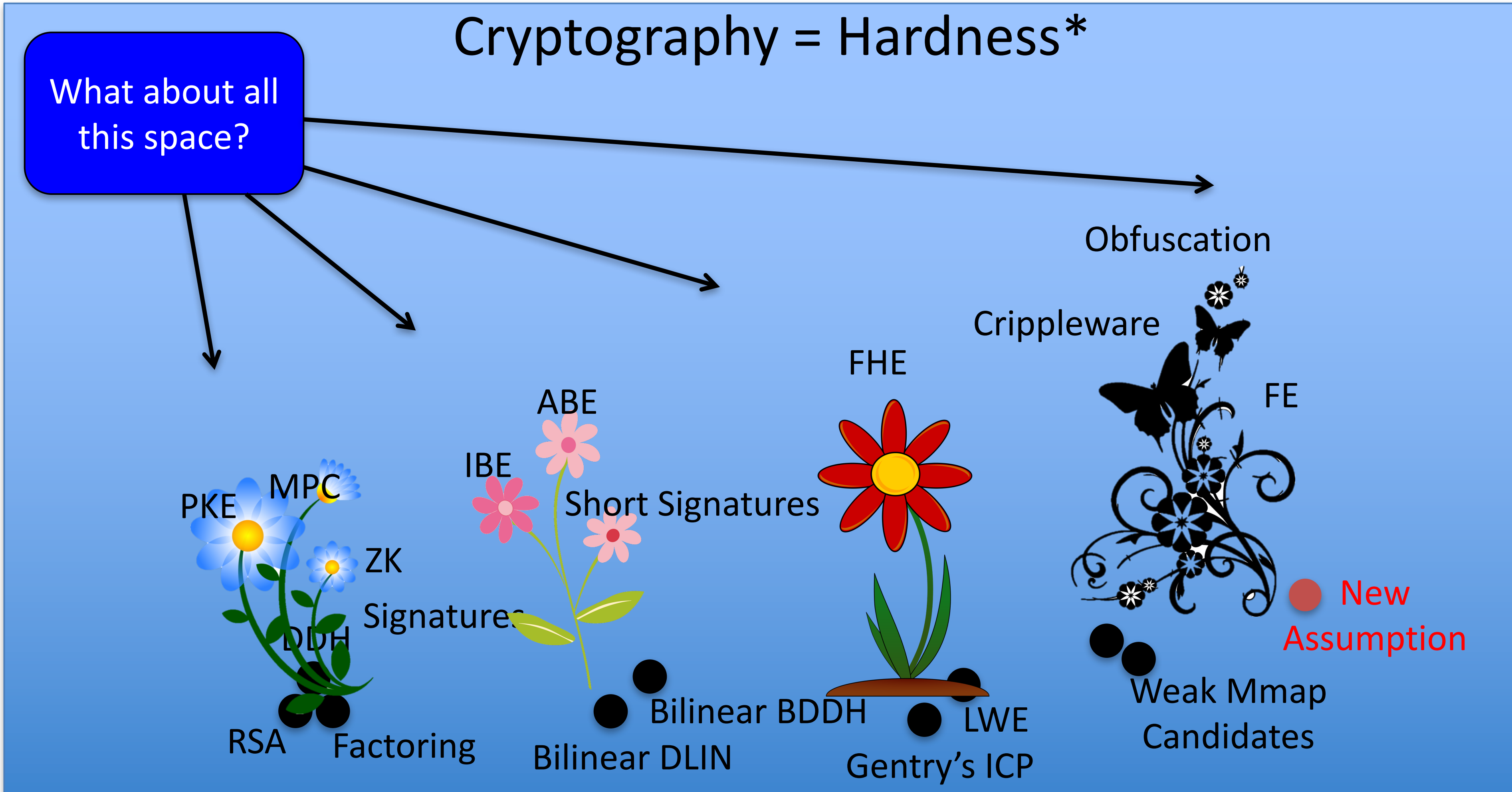
New Roads to Cryptopia

Amit Sahai
UCLA

Center *for* Encrypted Functionalities
An NSF Frontier Center

OPACity Panel, May 19, 2019

New Roads to Cryptopia



*Let's ignore information-theoretic cryptography for now.

Starting from LWE
[AJS18,Agr18,LM18,JLMS19]

- Let p be a λ-bit prime; χ be a poly-bounded error distribution for LWE; n is poly(λ).

1. Sample $s \leftarrow \mathbb{Z}_p^\lambda$
2. Sample $e_i \leftarrow \chi$ for $i \in [n]$
3. Sample random vectors $a_i \leftarrow \mathbb{Z}_p^\lambda$ f

We add "leakage" on e

$$\{q_\ell(\vec{e}, \vec{y}, \vec{z})\}_{\ell \in [n^{1+\epsilon}]}$$

$$\{a_i, \langle a_i, s\rangle + e_i \bmod p\}_{i \in [n]}$$

The Actual N

this version fro

- Here: $s \leftarrow \mathbb{Z}_p^{\lambda}$; e_i $\leftarrow$

$\{q_i\}$ sampled by efficient randomized algorithm.
Each monomial has:

- Poly(λ) bounded coefficients
- Degree-1 in $\vec{y}$ and $\vec{z}$
- Constant Degree d in $\vec{e}$

- Now consider distributions:
- Distribution D1:

$$\{a_i, \langle a_i, s\rangle + e_i \bmod p\}_{i\in[n]}, \quad \{q_\ell(\vec{e},\vec{y},\vec{z}) + \delta_\ell\}_{\ell\in[n^{1+\epsilon}]}$$

- Distribution D2:

$$\{a_i, \langle a_i, s\rangle + e_i \bmod p\}_{i\in[n]}, \quad \{q_\ell(\vec{e},\vec{y},\vec{z})\}_{\ell\in[n^{1+\epsilon}]}$$

- Assumption: No efficient adversary can distinguish D1 and D2 with advantage > 1-1/poly(λ)
- Can hold even if Adversary can distinguish with probability 99%!

The Road Ahead

- How do we deal with new assumptions?
  - Simplicity (first and foremost?)
  - Cryptanalysis
  - Lower bounds
  - Relations with existing assumptions
- Fundamental issue: We don't know where/how/why structured hardness arises.
- This is the **only** way for crypto to progress. iO gives us the "excuse" to investigate new assumptions.
- Even without iO – Crypto Dark Matter (TCC 2018)