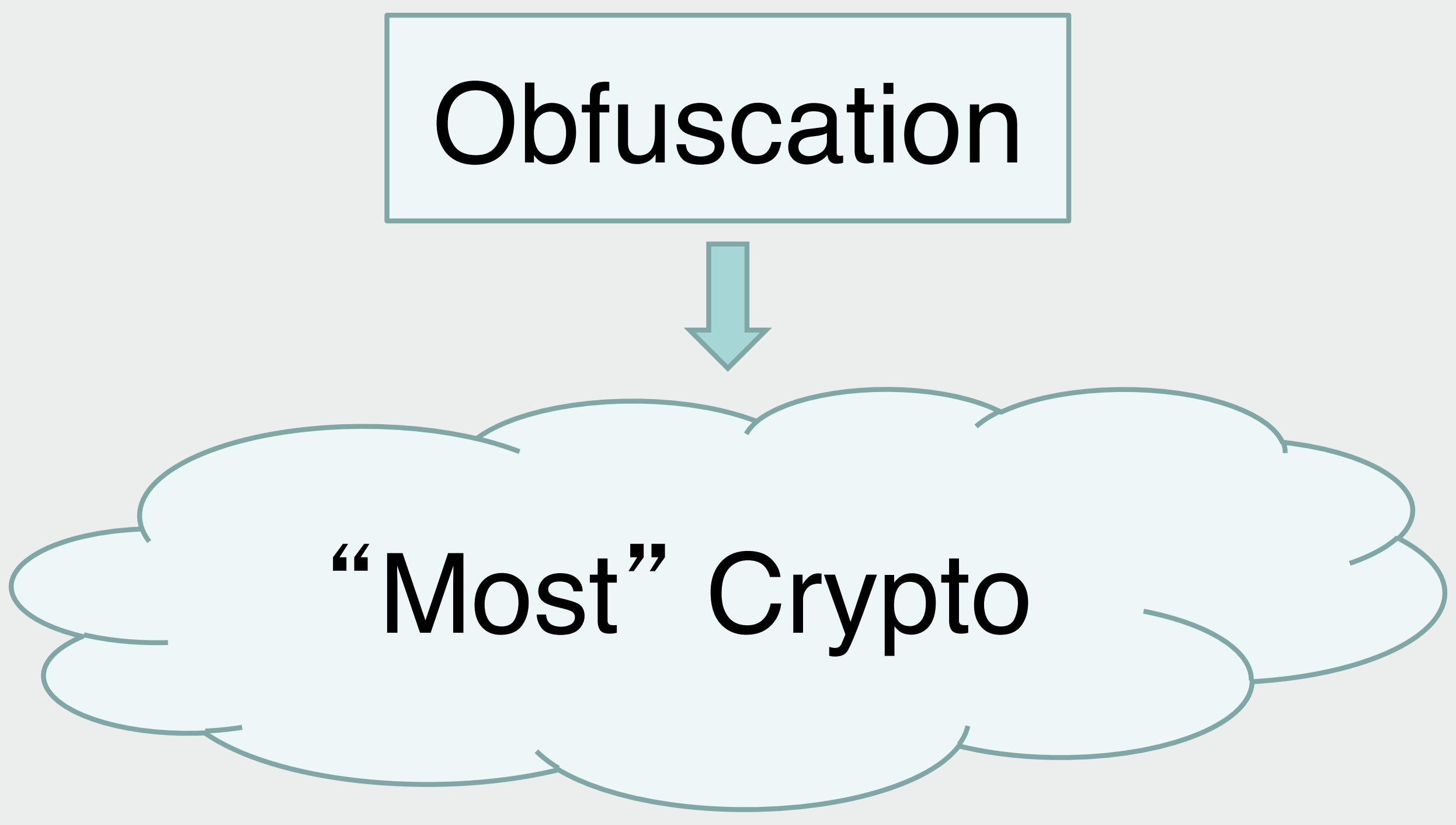
Encryptor Combiners

PI: Mark Zhandry – Princeton University

Introduction



Obfuscation

“Most” Crypto

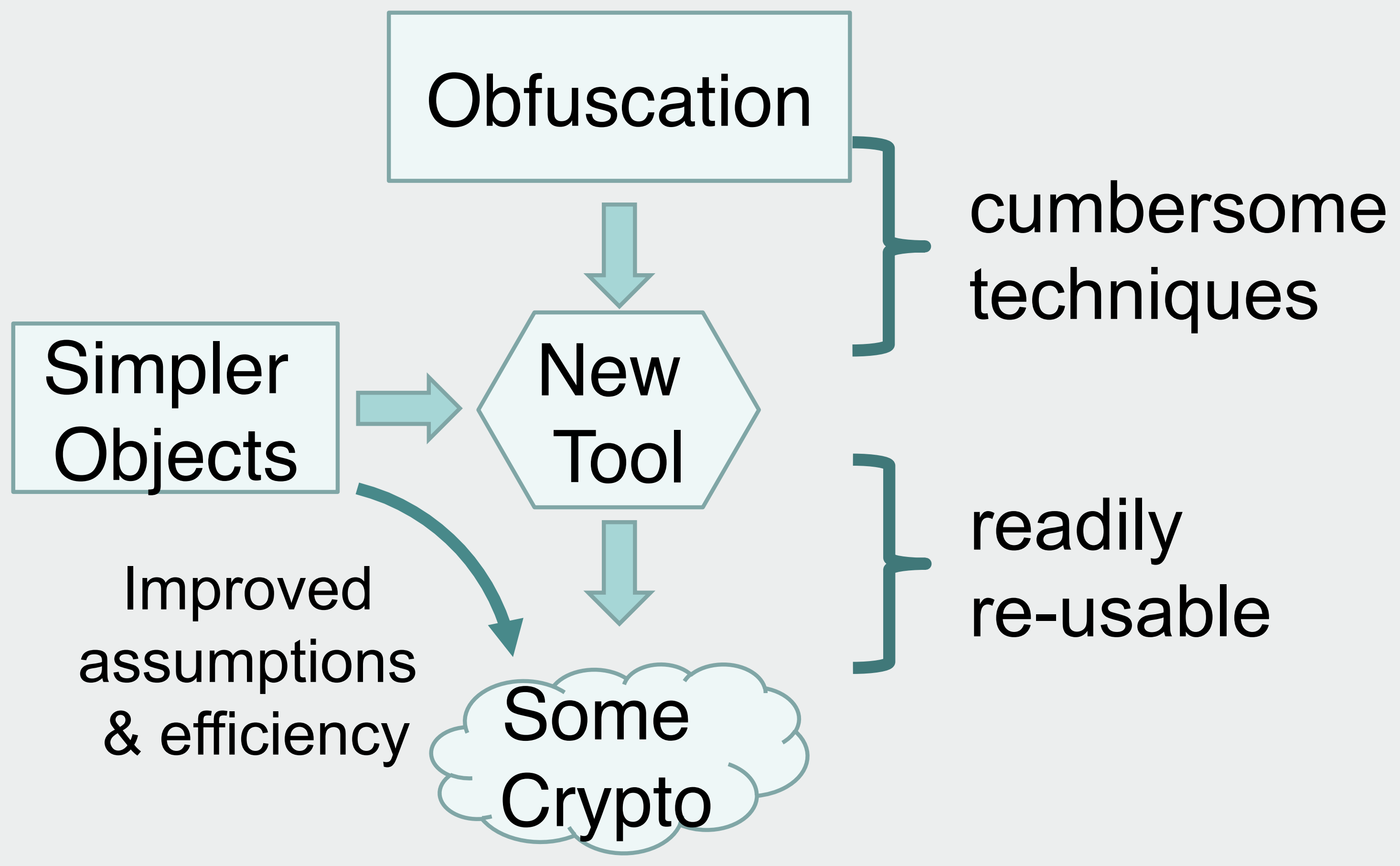
But…

Obfuscation is unnecessarily powerful for most applications → Applications extremely impractical

Obfuscation rests on new, unvetted security assumptions → Tenuous security for applications

Techniques can be very cumbersome → Hard to re-use for other applications

High Level Approach



Obfuscation

New Tool

Some Crypto

Simpler Objects

Improved assumptions & efficiency

cumbersome techniques

readily re-usable

Terminology

Encryptor: $c \leftarrow E(m)$ (randomized)

Decryptor: $m \leftarrow D(c)$ (deterministic)

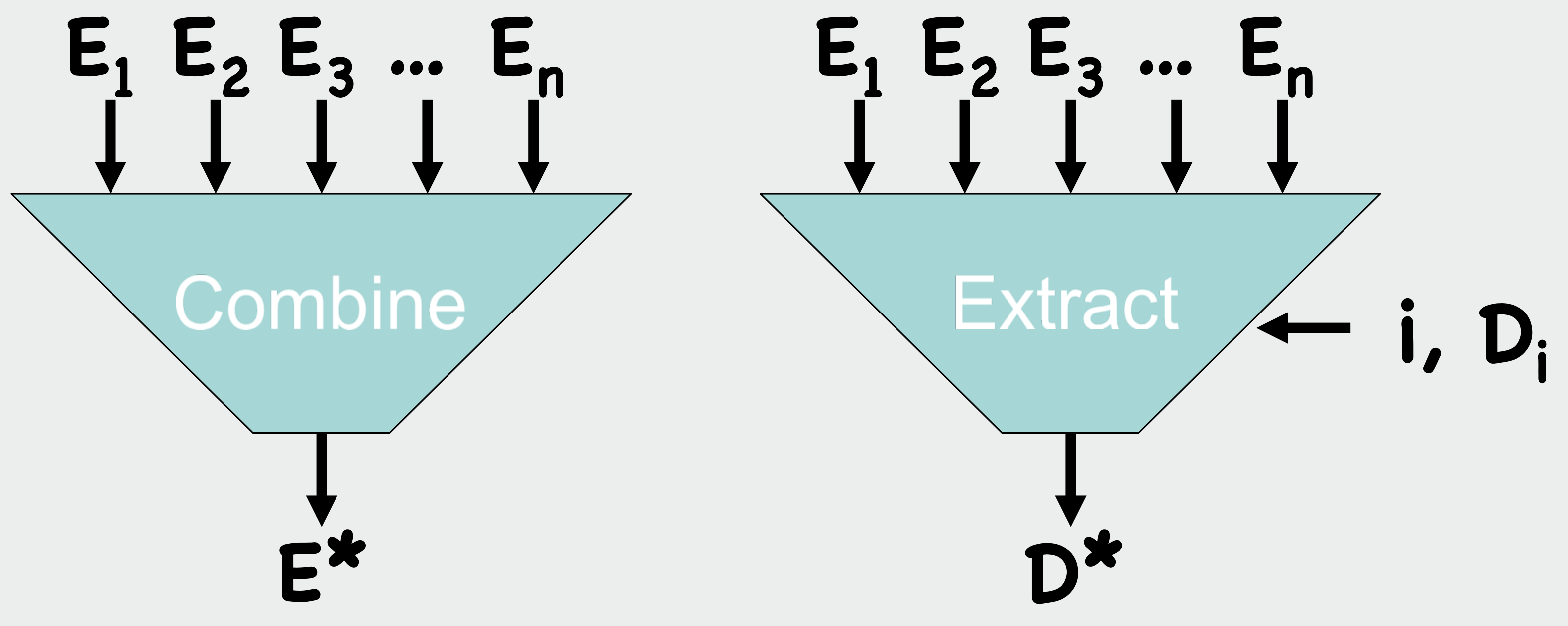
D is **valid** for E if, for any m,

$\Pr[D(E(m))=m] > 1 - \mathrm{negl}$

Ex: PKE: $E(m) = \mathrm{Enc}(pk,m)$, $D(c) = \mathrm{Dec}(sk,c)$

IBE: $E_{id}(m) = \mathrm{Enc}(mpk,id,m)$, $D_{id}(c) = \mathrm{Dec}(sk_{id},c)$

New Tool: Encryptor Combiners



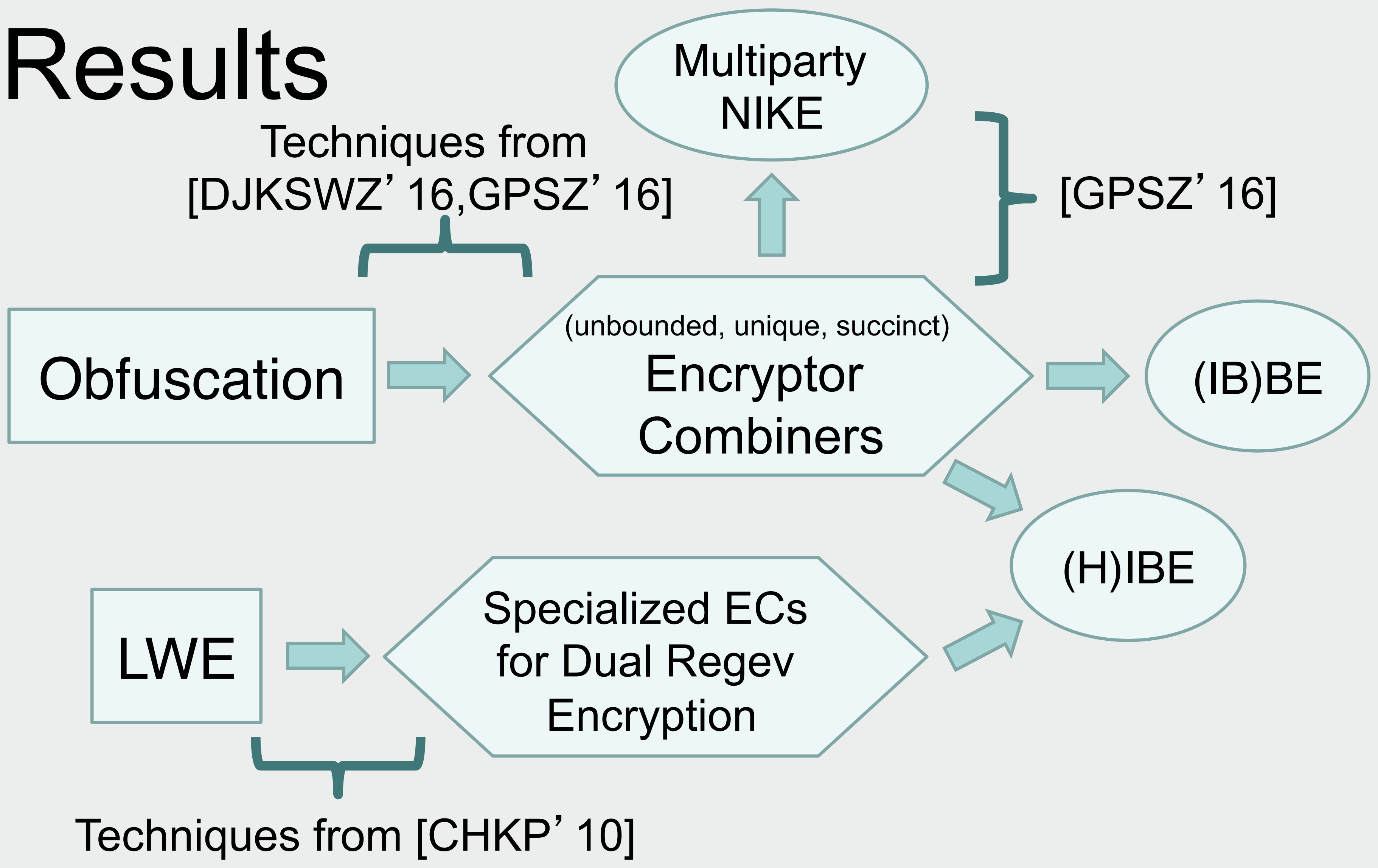
Correctness: D_i valid for $E_i \Rightarrow D^*$ valid for E^*

Security: If adversary can decrypt E^*, then it can decrypt at least one E_i

Variants:

- Unbounded vs Bounded n
- Unique D^* vs Many D^*
- Compact $|ctxt|$ vs $|ctxt|$ grows with n

Results



Multiparty NIKE

Techniques from [DJKSWZ’ 16,GPSZ’ 16]

[GPSZ’ 16]

Obfuscation

(unbounded, unique, succinct) Encryptor Combiners

(IB)BE

(H)IBE

LWE

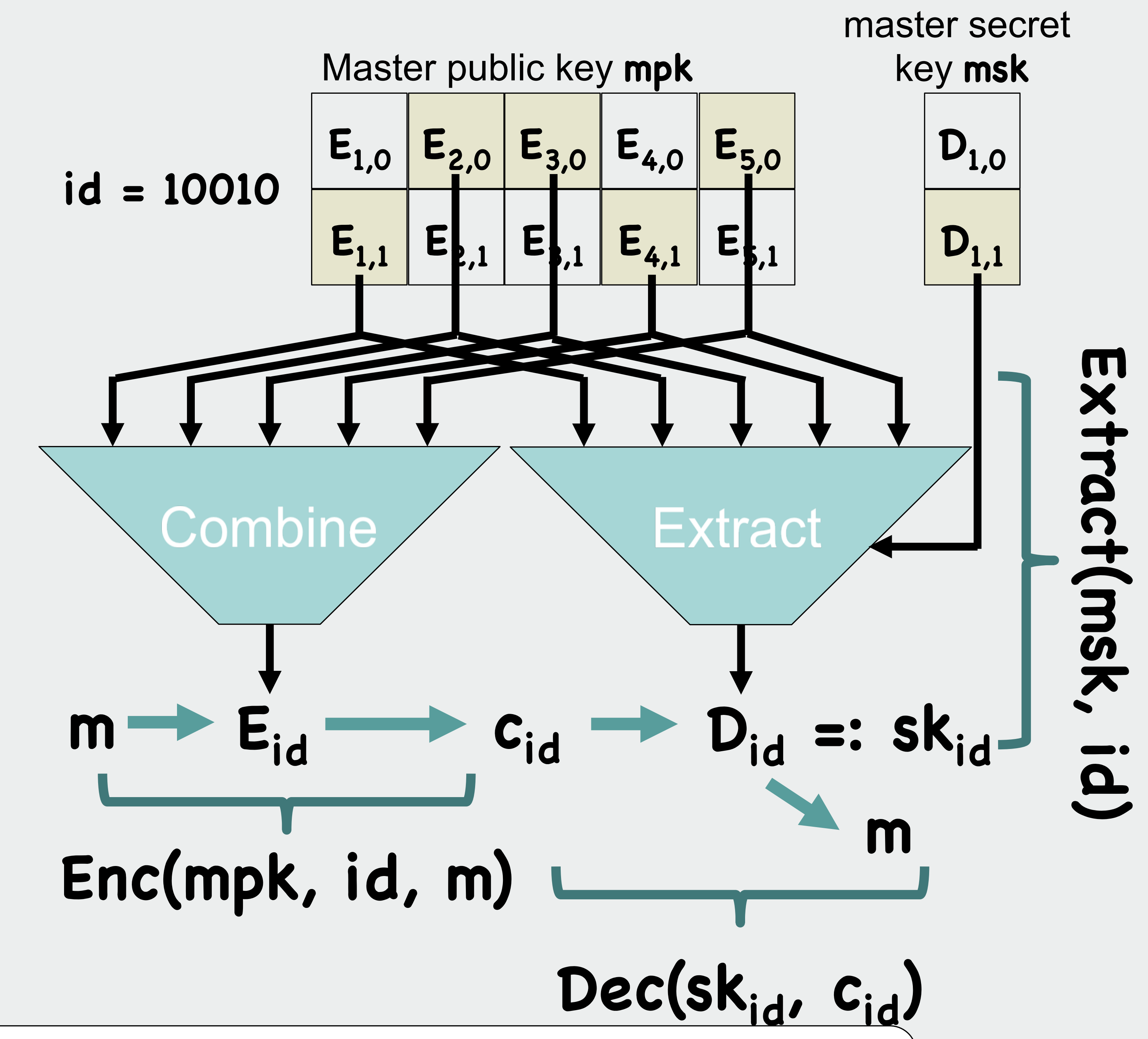
Specialized ECs for Dual Regev Encryption

Techniques from [CHKP’ 10]

Notes:

- New way to view existing applications of obfuscation, LWE
- Our LWE-based (H)IBE scheme is reminiscent of early schemes [CHKP’ 10]
- Identify concrete features needed from LWE to obtain BE (compactness) and multiparty NIKE (uniqueness)

Example: Identity-based Encryption



Master public key **mpk**
master secret key **msk**
id = 10010
$E_{1,0}$ $E_{2,0}$ $E_{3,0}$ $E_{4,0}$ $E_{5,0}$
$E_{1,1}$ $E_{2,1}$ $E_{3,1}$ $E_{4,1}$ $E_{5,1}$
$D_{1,0}$
$D_{1,1}$
Combine
Extract
$m \rightarrow E_{id} \rightarrow c_{id} \rightarrow D_{id} =: sk_{id}$
m
$\mathrm{Enc}(mpk, id, m)$
$\mathrm{Dec}(sk_{id}, c_{id})$
$\mathrm{Extract}(msk, id)$

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9 -11th 2017
Arlington, VA