Functional Encryption Without Obfuscation

OR: How to Have a TCC Paper with Broken Assumptions

Sanjam Garg – UC Berkeley

Craig Gentry – IBM Research

Shai Halevi – IBM Research

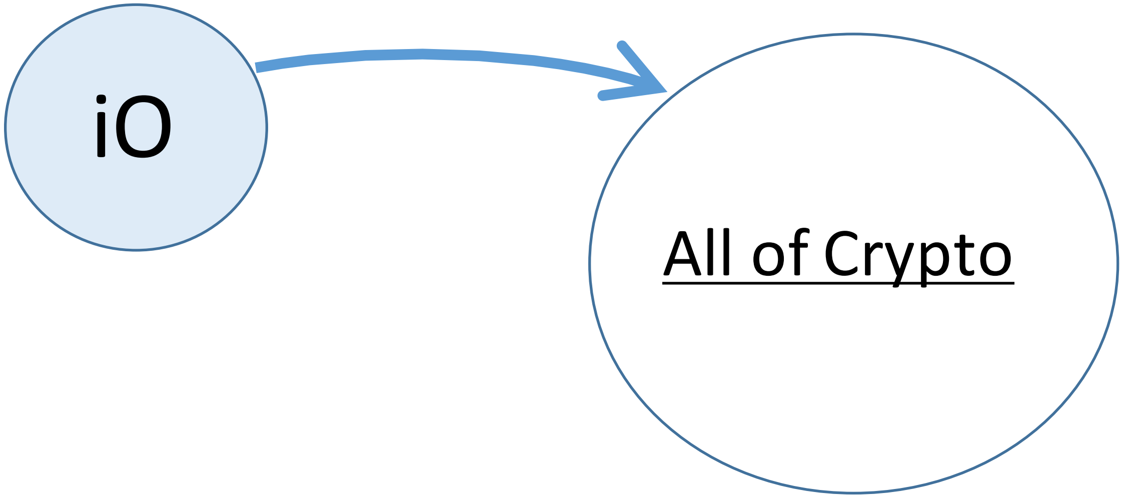
Mark Zhandry – MIT → Princeton

Program Obfuscation

“Scramble” a program

- Hide implementation details
- Maintain functionality
- Formal security notion: iO [BGIRSVY’01]

Golden goose of crypto, nearly “crypto complete”



iO

All of Crypto

Functional Encryption

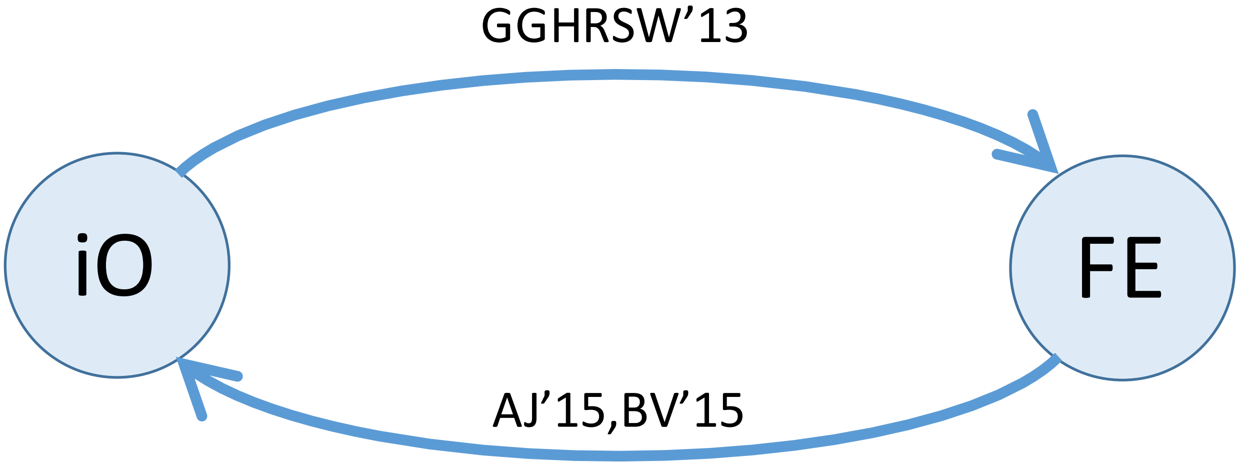
Generalizes IBE, ABE, PE, etc

Can give out partially functional decryption key

- Can learn function **f** of message
- Learn nothing else about message

Formalish defs later…

Relation Between FE and iO



Case closed, right?

FE, IO, and Complexity Leveraging

AJ’15,BV’15 involve complexity leveraging

Break iO with prob ε $\Rightarrow$ break FE with prob $\varepsilon/2^n$

Complexity leveraging inherent to iO? [GGSW’13]

- **iO** = exp many assumptions, one per circuit pair

Assumption(C_0,C_1): $iO(C_0) \approx iO(C_1)$

- Assumption(C_0,C_1) clearly false for inequivalent circuits
- Reduction from Assumption(C_0,C_1) to single hard problem must distinguish equivalent from inequivalent (NP-hard)

FE, IO, and Complexity Leveraging

Complexity leveraging does **NOT** appear inherent to FE

- But who really knows?

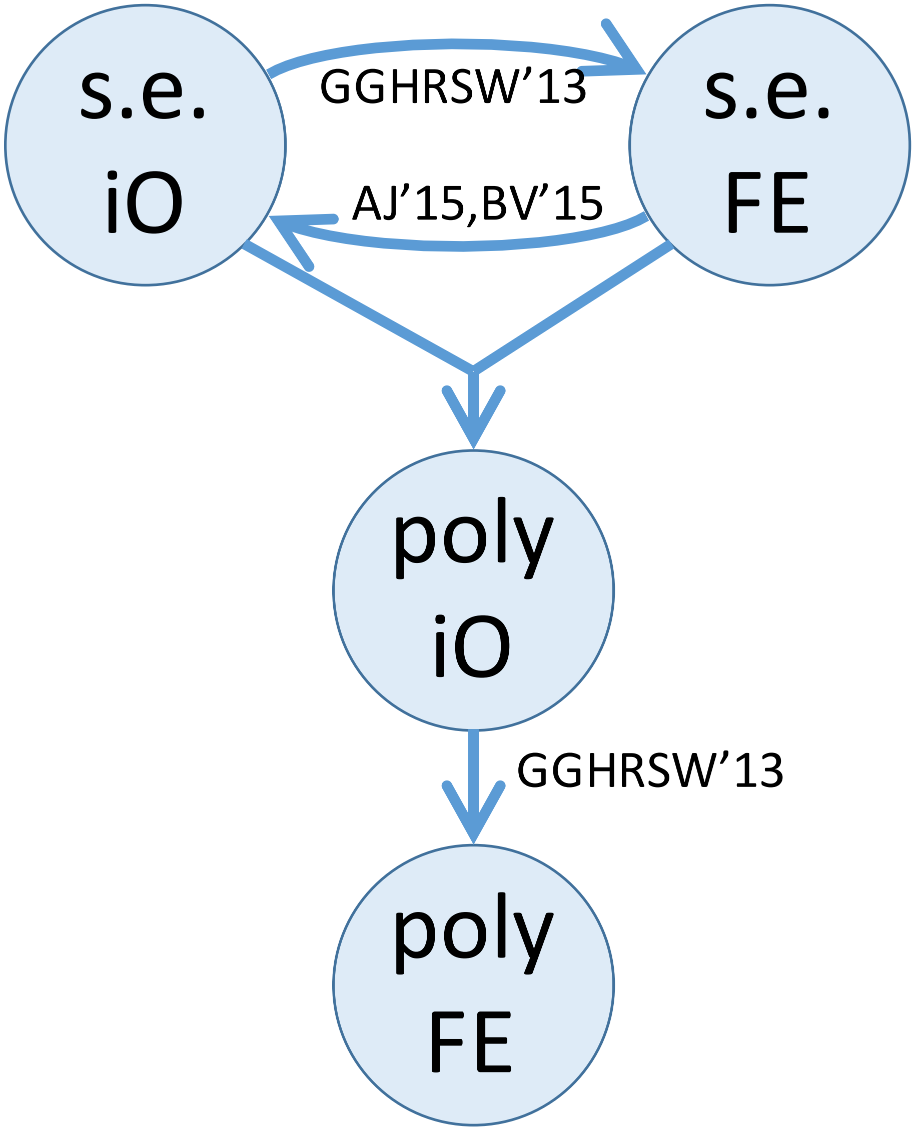
This work:

FE from POLY hardness of 2 complexity assumptions on MMAPs

Implications:

- Complexity leveraging **NOT** inherent to FE
- Leveraging **IS LIKELY** inherent in FE→iO transformation

A More Refined View



Caveat

Unfortunately, none of the current MMaps support our assumptions

- Nor any “nice” assumptions used to build iO

Hopefully a temporary issue

- Our assumptions are generic

Still compelling evidence that FE does not need complexity leveraging

- Provides route to achieve this

Motivation for finding new MMaps

Outline of Construction

Build “slotted” FE

- More expressive than FE
- Initially much weaker security properties

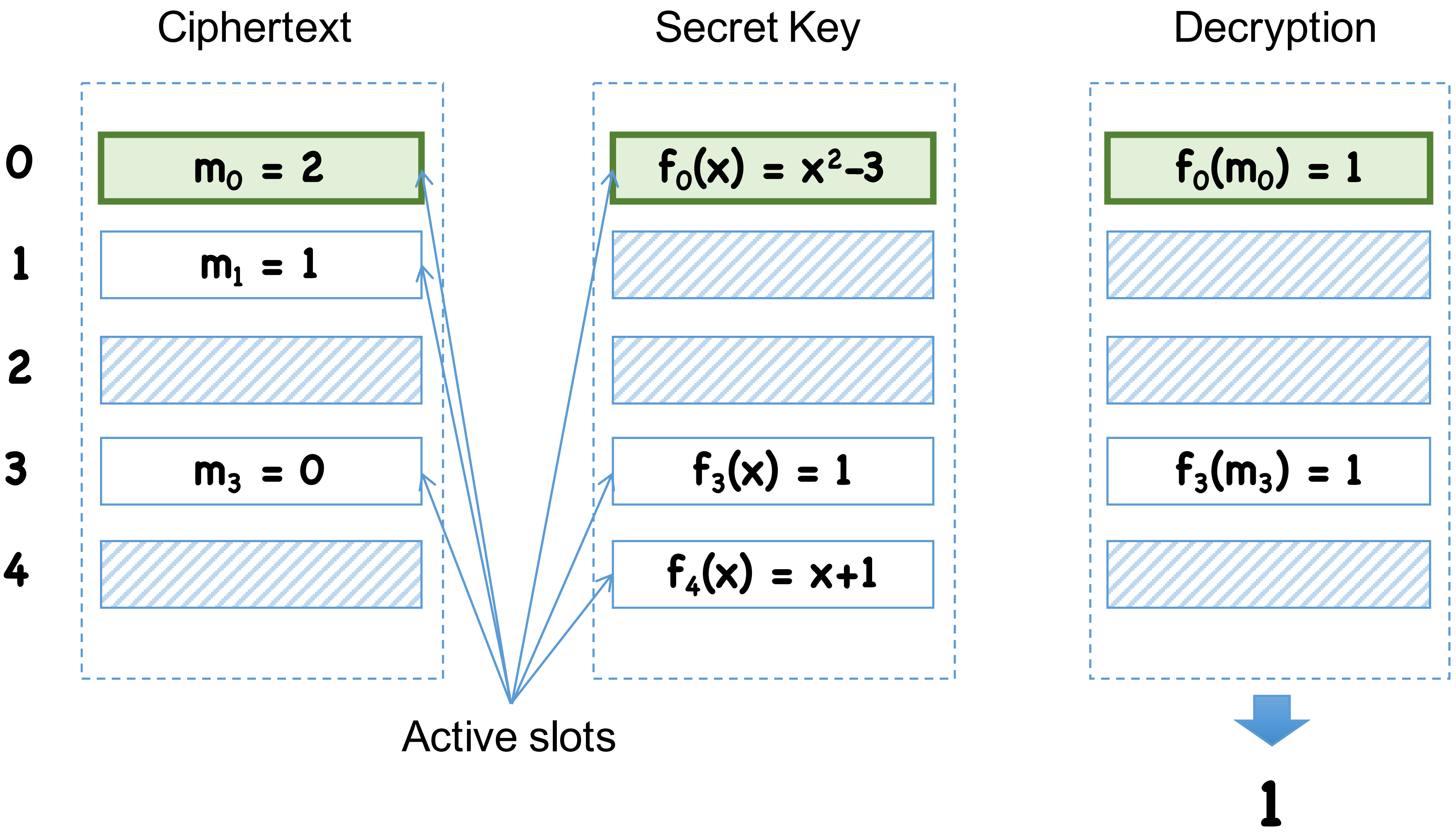
$\Rightarrow$ directly mapped to multilinear map assumptions

Boost weaker security properties to full security

- Use up slots in the process
- Arrive at plain FE

Focus of this talk

Slotted Functional Encryption



Ciphertext

Secret Key

Decryption

0 $m_0 = 2$ $f_0(x) = x^2-3$ $f_0(m_0) = 1$

1 $m_1 = 1$

2

3 $m_3 = 0$ $f_3(x) = 1$ $f_3(m_3) = 1$

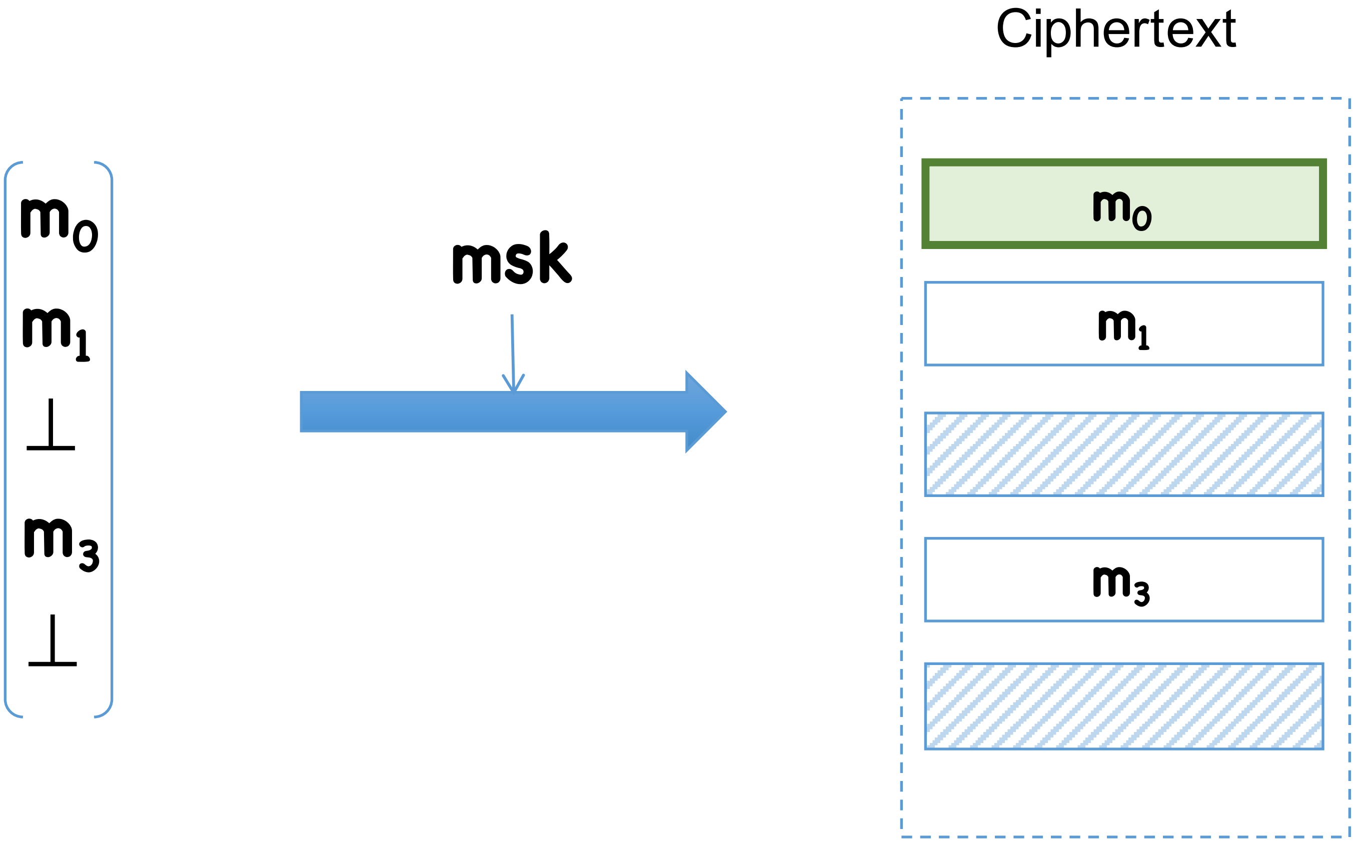
4 $f_4(x) = x+1$

Active slots

1

Slotted Functional Encryption

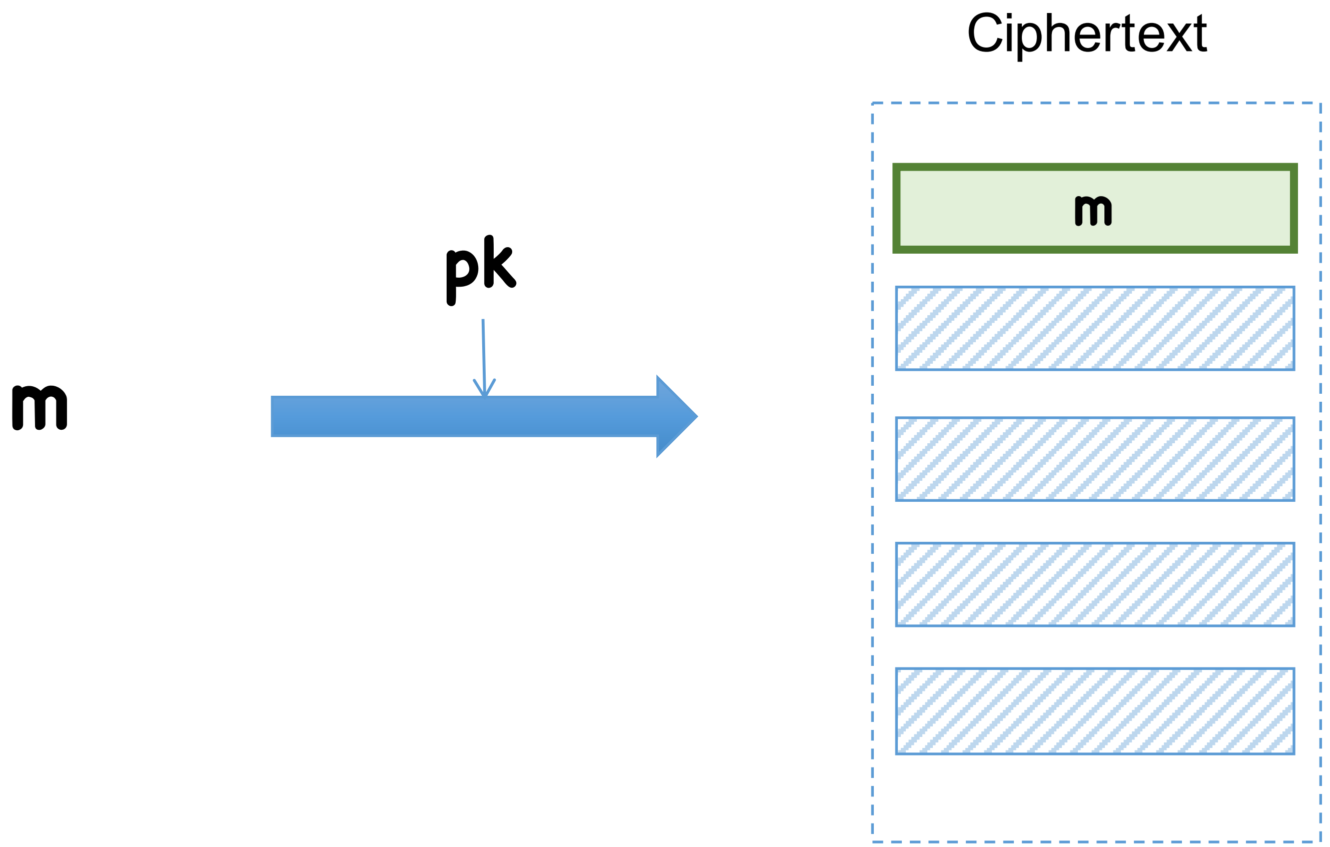
Private (slotted) encryption: encrypt in all slots



$\begin{pmatrix} m_0 \\ m_1 \\ \perp \\ m_3 \\ \perp \end{pmatrix}$
msk
Ciphertext
m_0
m_1
m_3

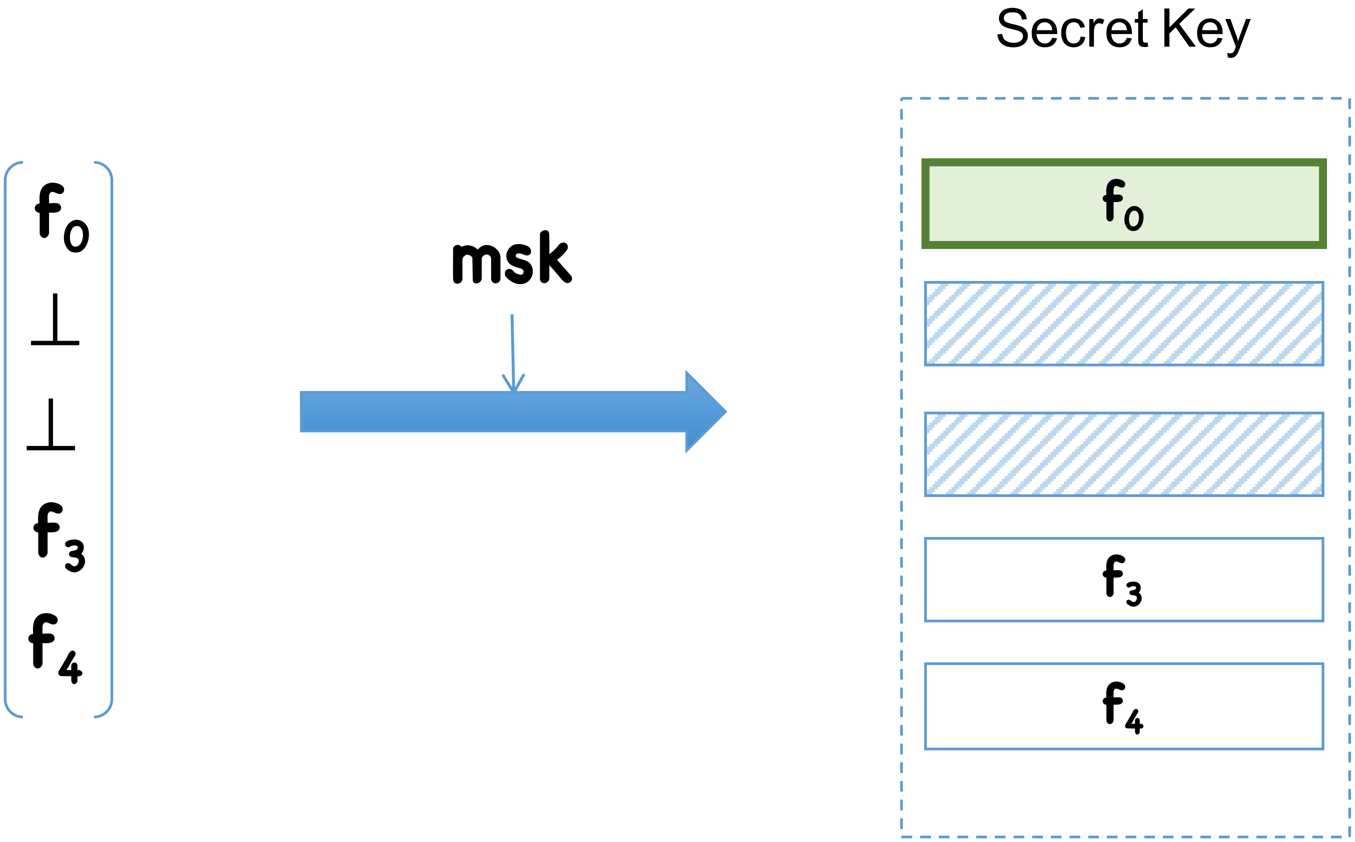
Slotted Functional Encryption

Public (unslotted) encryption: encrypt in slot 0



Slotted Functional Encryption

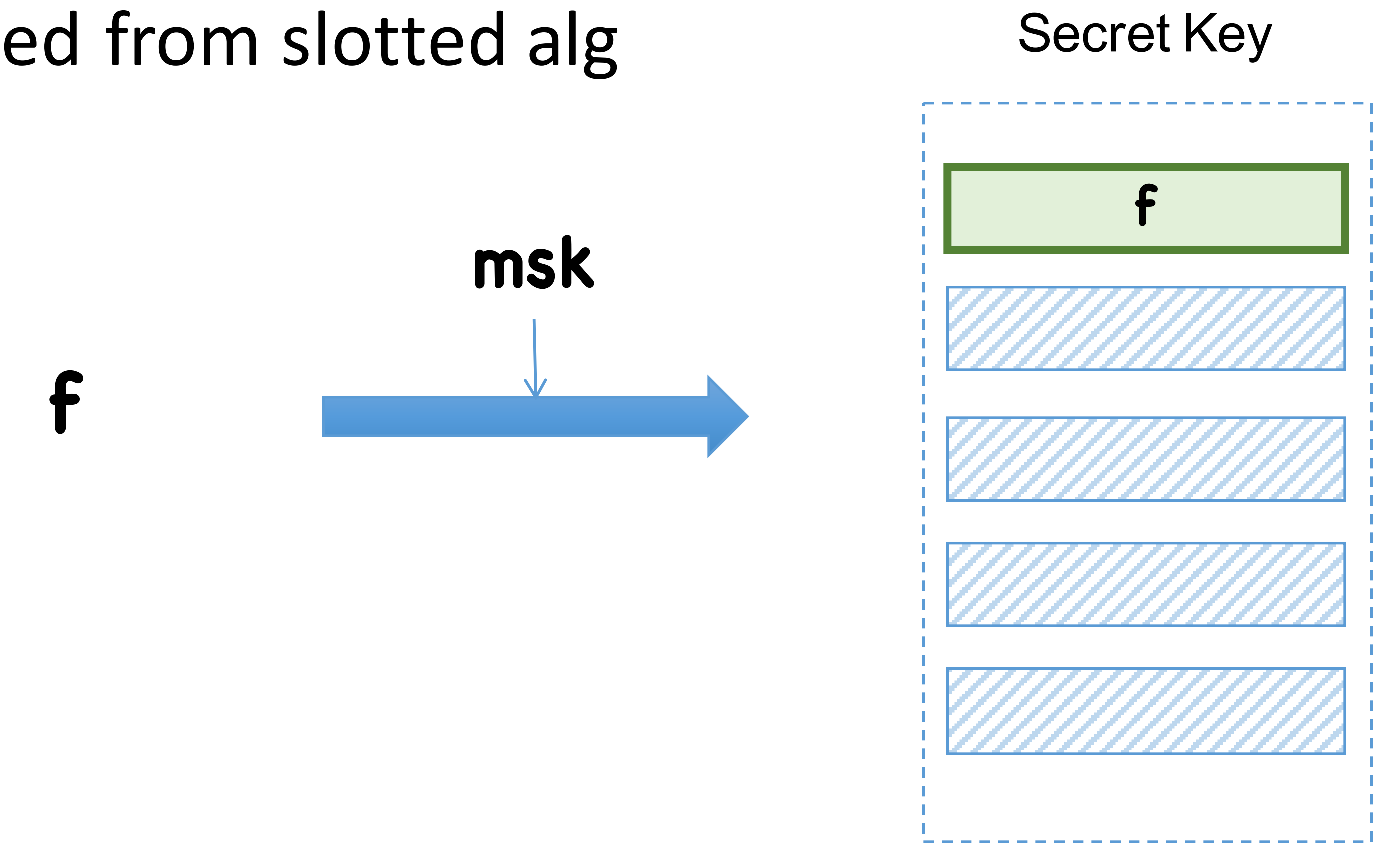
Slotted keygen: secret keys in all slots


$\begin{bmatrix} f_0 \\ \perp \\ \perp \\ f_3 \\ f_4 \end{bmatrix}$
msk
Secret Key
f_0
f_3
f_4

Slotted Functional Encryption

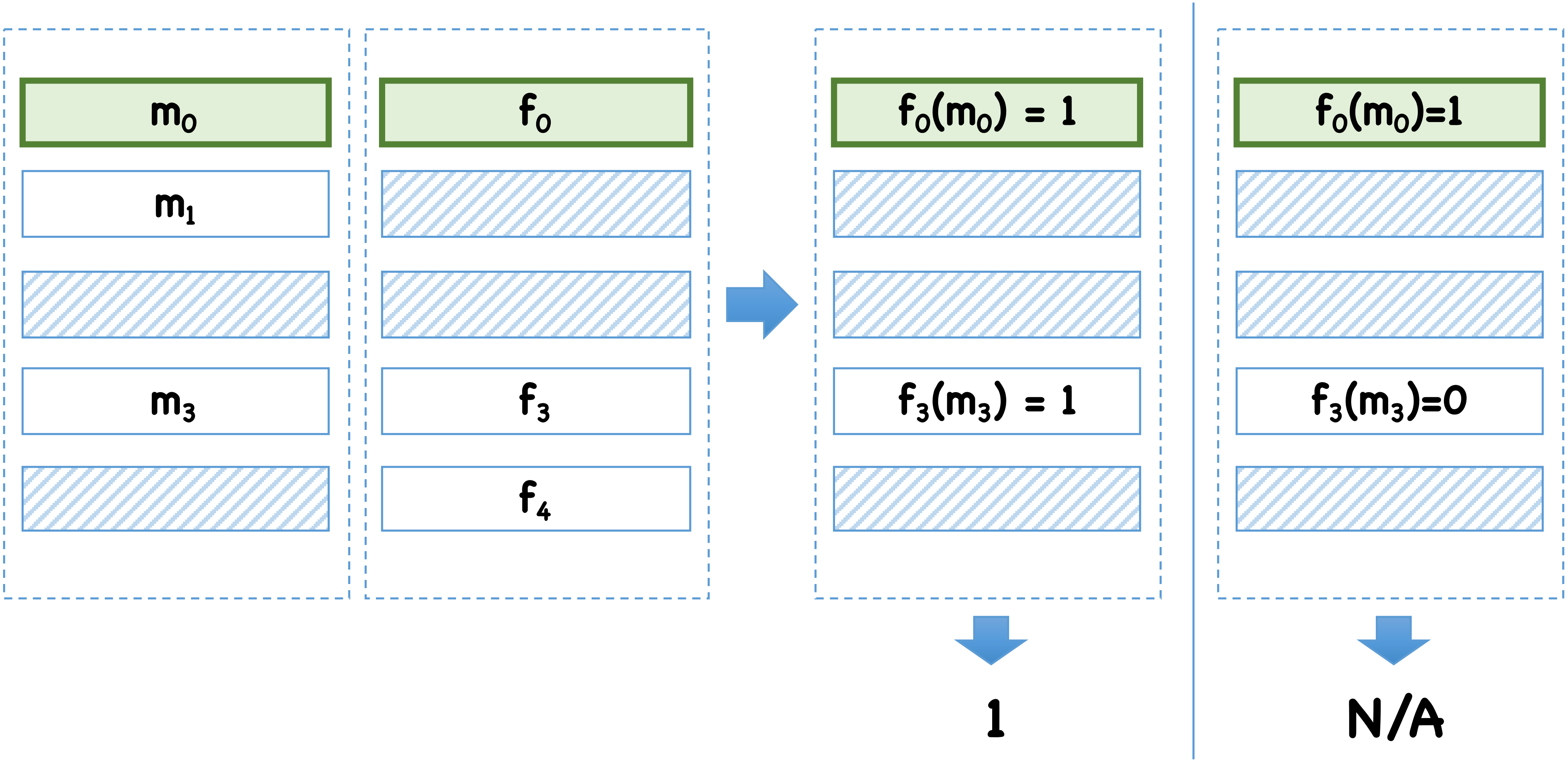
Unslotted keygen: secret keys in slot 0

- Derived from slotted alg



Slotted Functional Encryption

Decryption: decrypt all active slots, output result if agree



Slotted FE to (Unslotted) FE

Throw away slotted algorithms

Enc(msk, (m_0, m_1, m_2, …))

Enc(pk, m)

KeyGen(msk, (f_0, f_1, f_2, …)

KeyGen(msk, f)

→

Enc(pk, m)

KeyGen(msk, f)

Slotted Functional Encryption

Slot **0** acts as a public key FE scheme

Slots **1,…** act as secret key FE schemes

“Best possible” security notion:

- Can change ctxt/sk without detection as long as output of decryption unaffected
- EXCEPT: cannot change function in slot **0** (message ok)

Crucial: without it, notion implies iO

Security of Slotted Functional Encryption

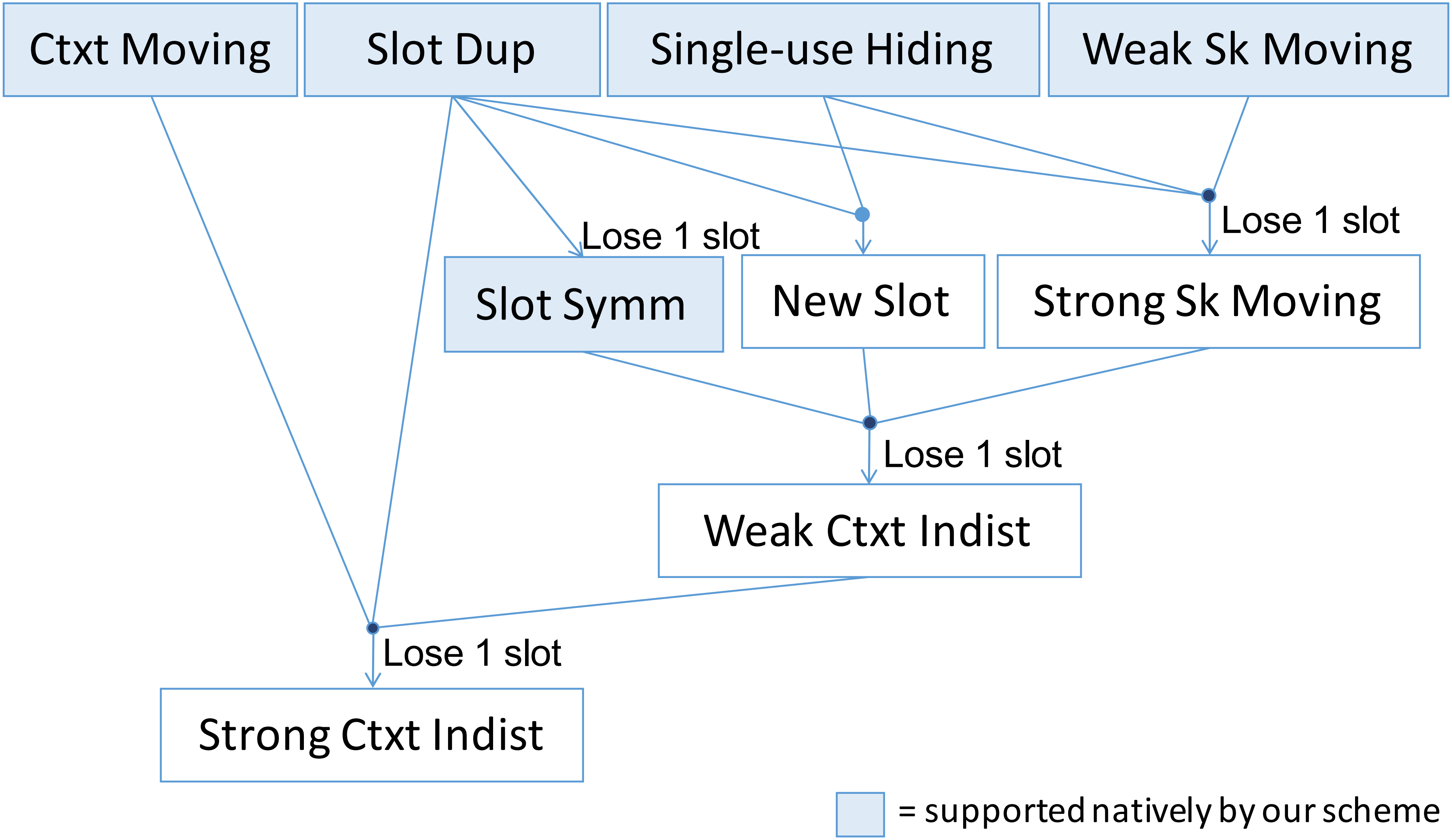
Strategy: define desired security property:

- Strong ciphertext indistinguishability $\Rightarrow$ security of derived FE

Derive from other simpler properties:

- Slot Duplication
- Slot symmetry
- Single use hiding
- Ciphertext moving
- Weak key moving
- Strong key moving
- New slot
- Weak ciphertext indistinguishability

Reductions!



Ctxt Moving

Slot Dup

Single-use Hiding

Weak Sk Moving

Lose 1 slot

Lose 1 slot

Slot Symm

New Slot

Strong Sk Moving

Lose 1 slot

Weak Ctxt Indist

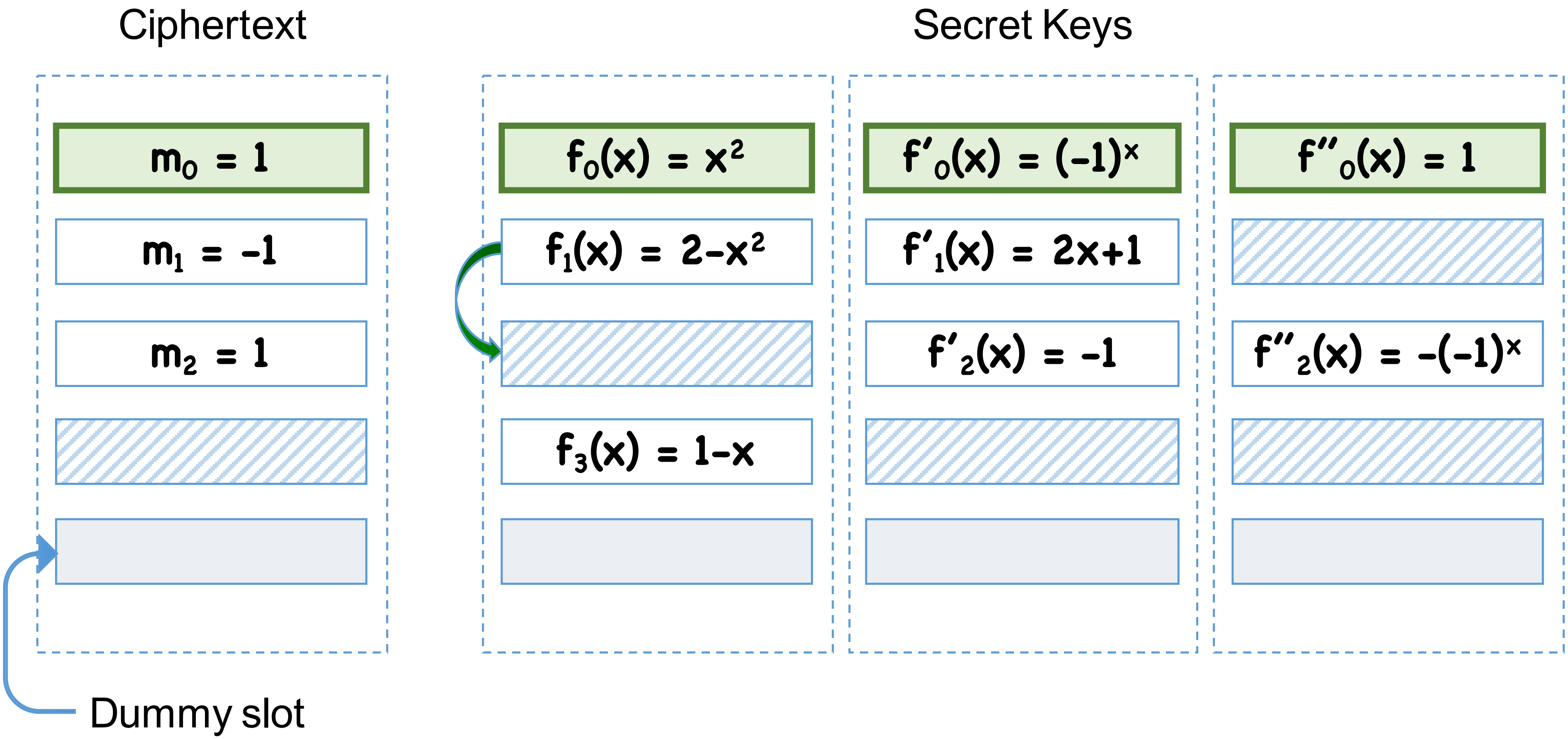
Lose 1 slot

Strong Ctxt Indist

▨ = supported natively by our scheme

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

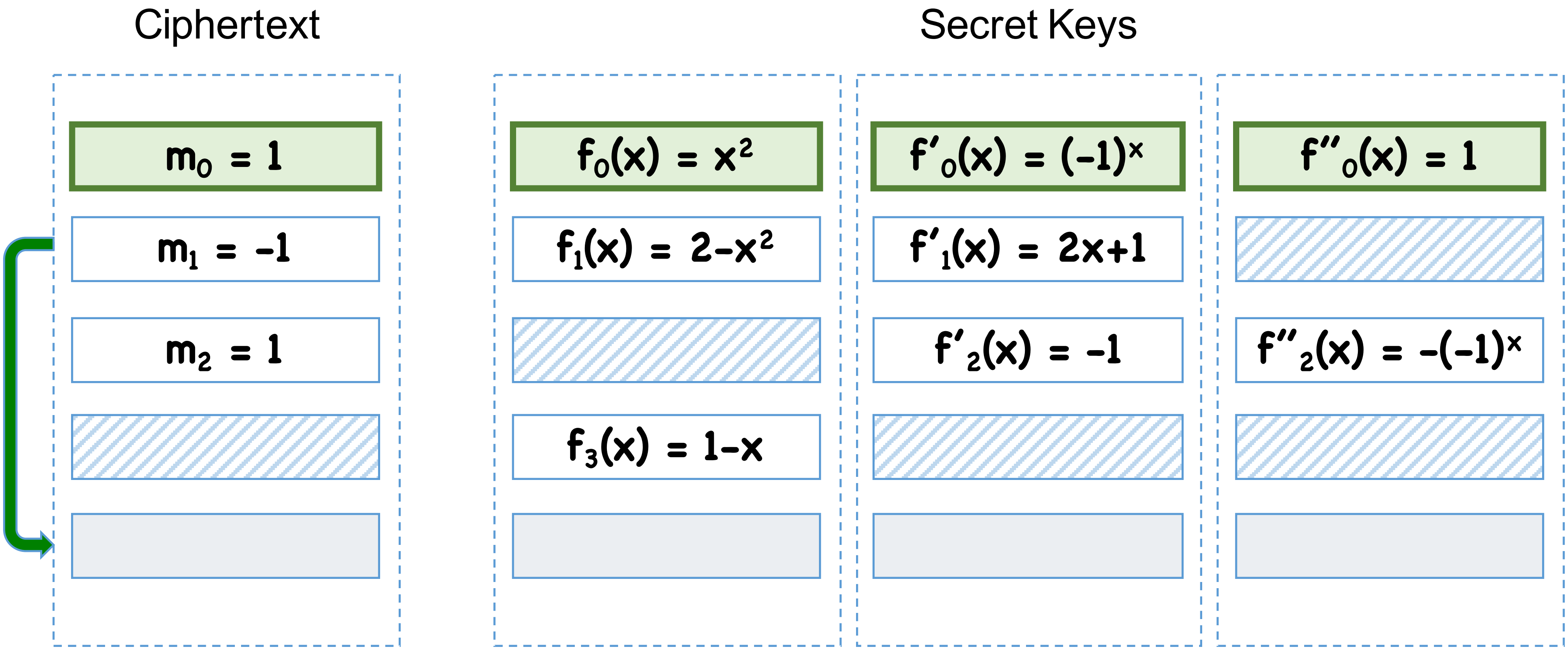


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Dummy slot

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

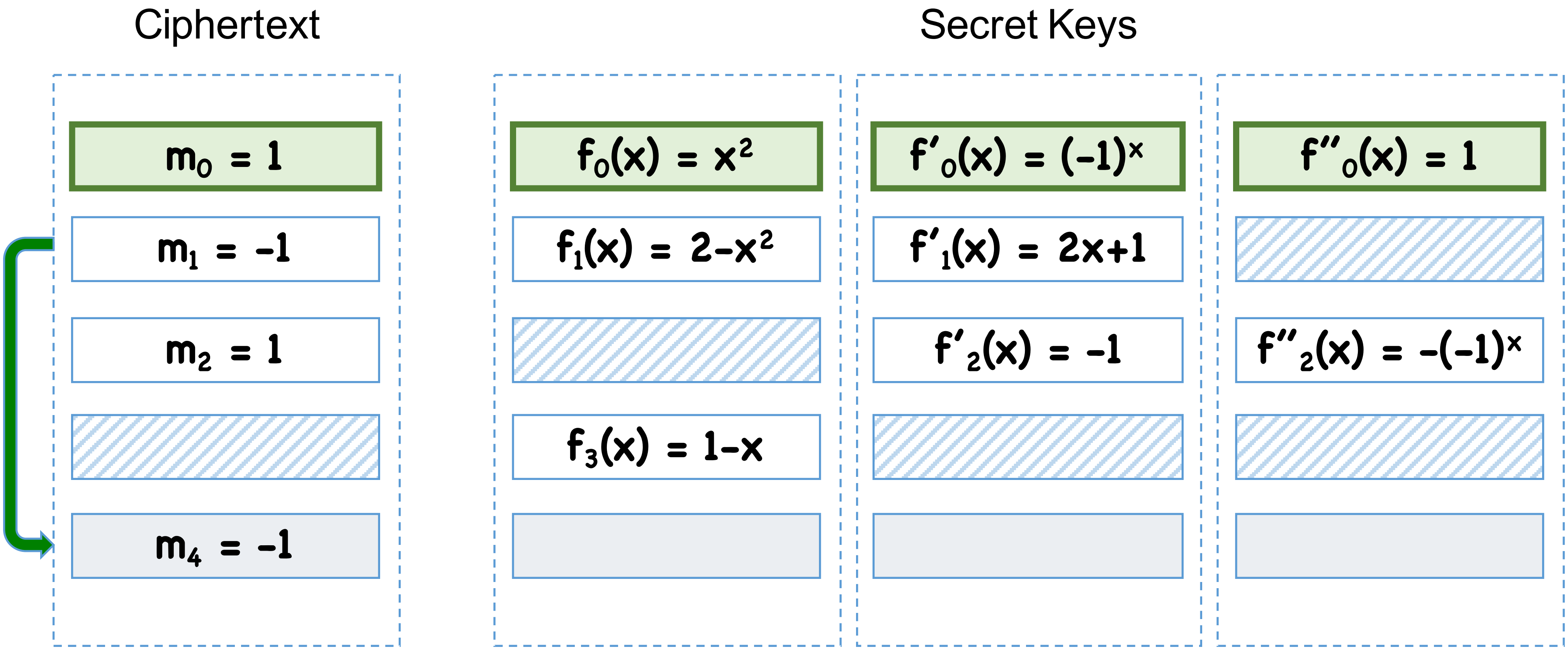


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

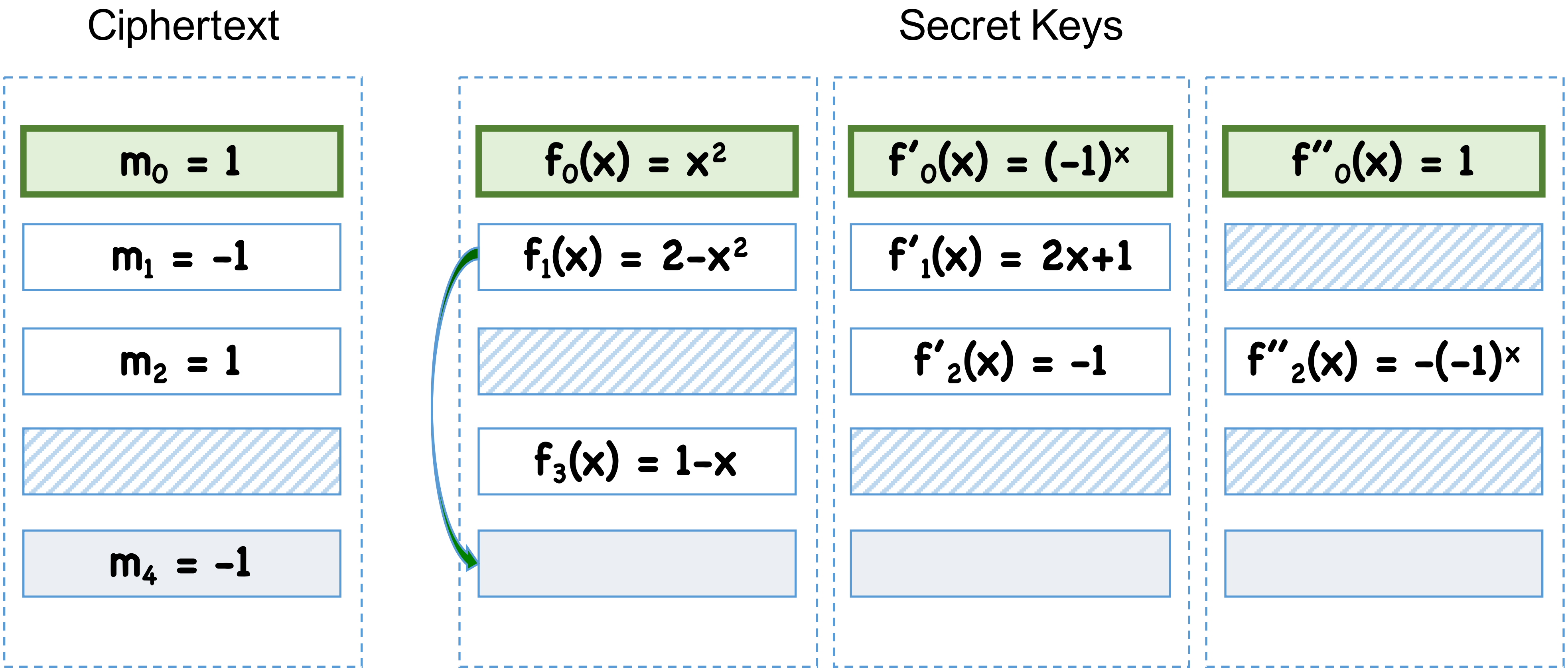


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$			

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

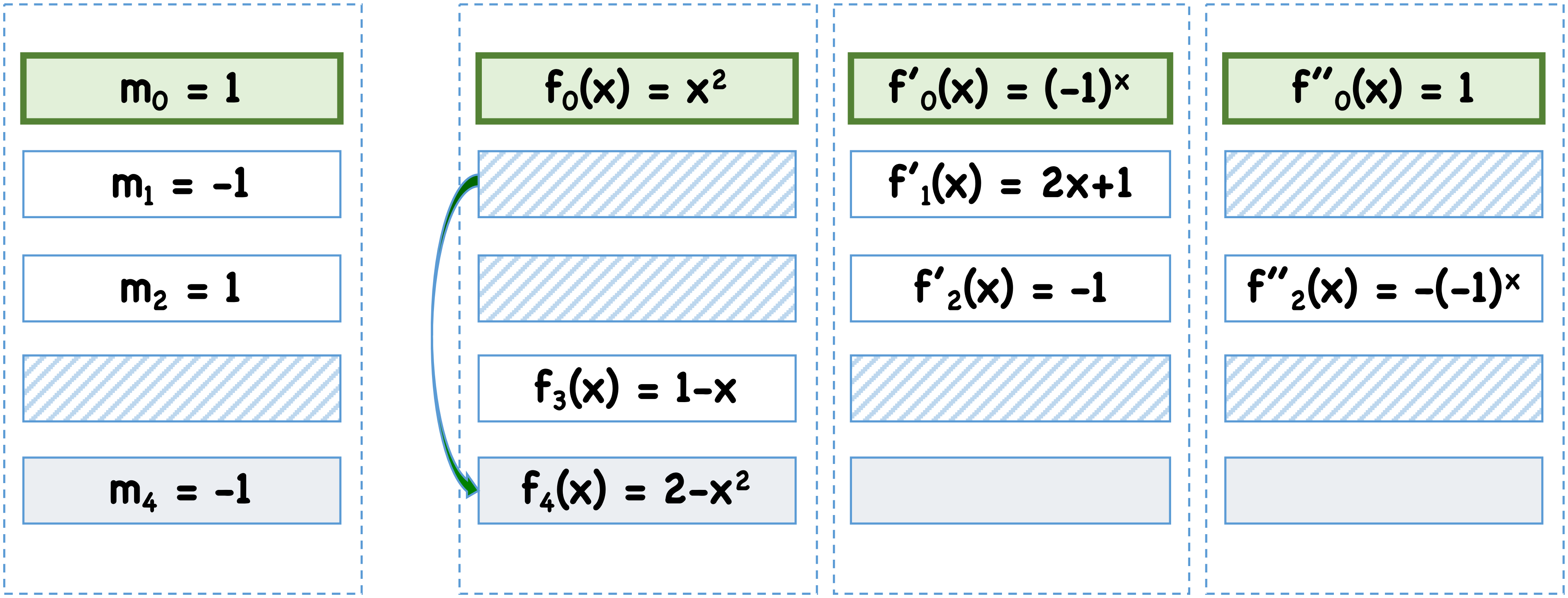


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$			

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

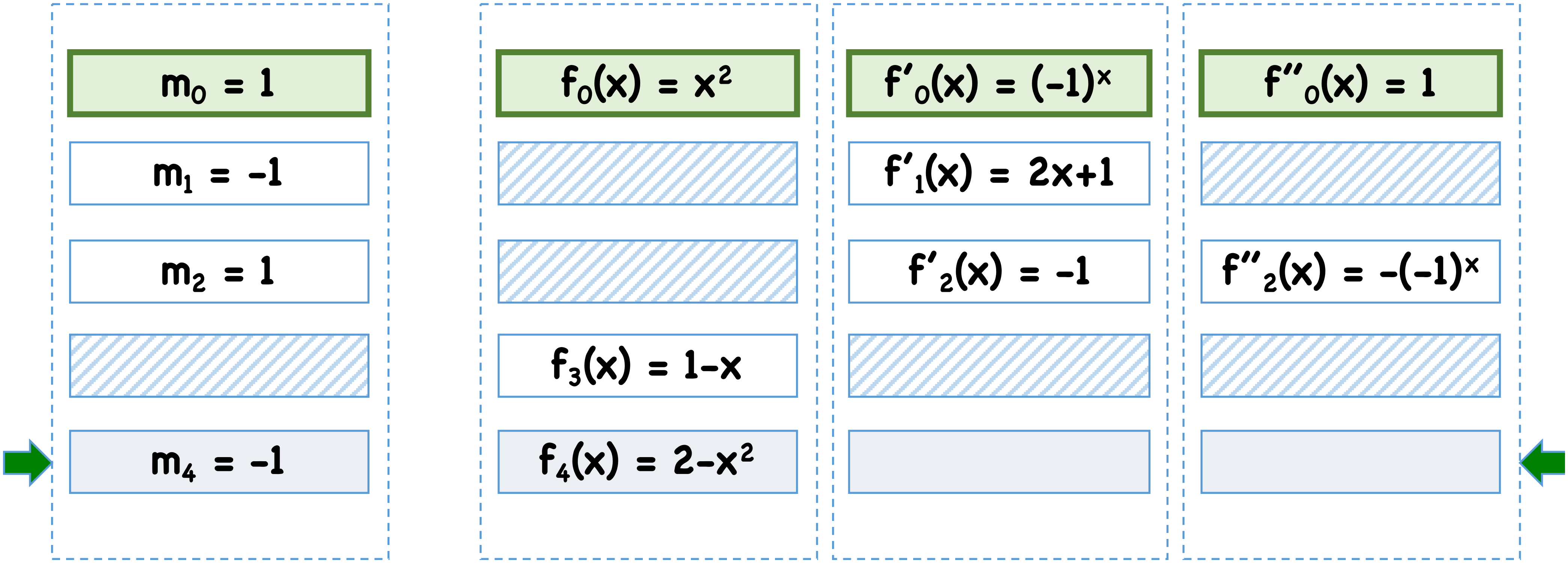


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

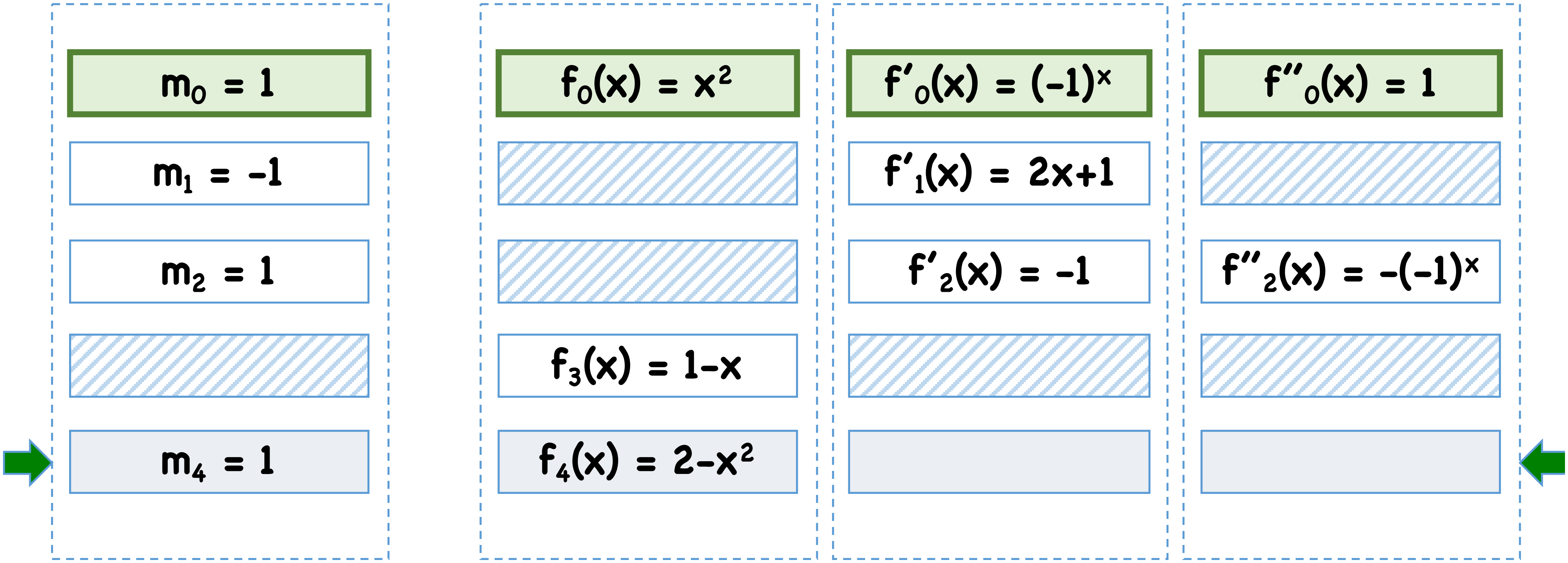


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Single Use Hiding

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

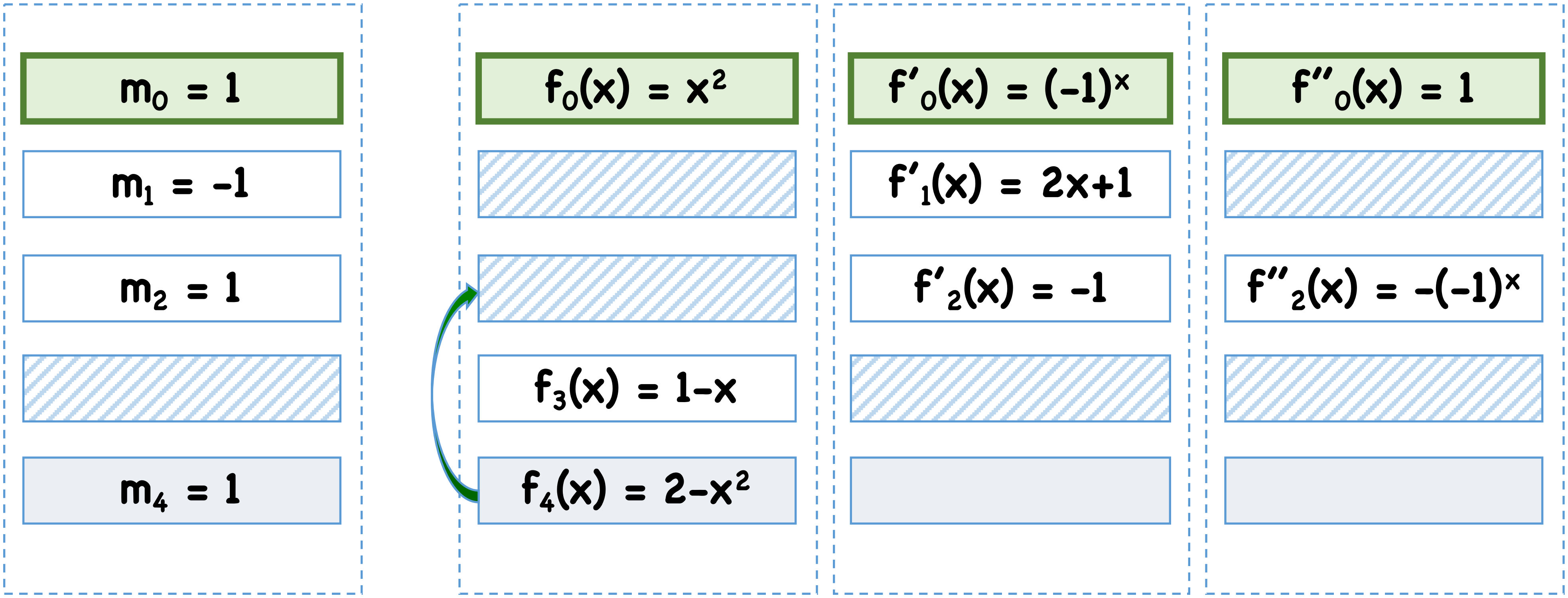


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$	$f_4(x) = 2-x^2$		

Single Use Hiding

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

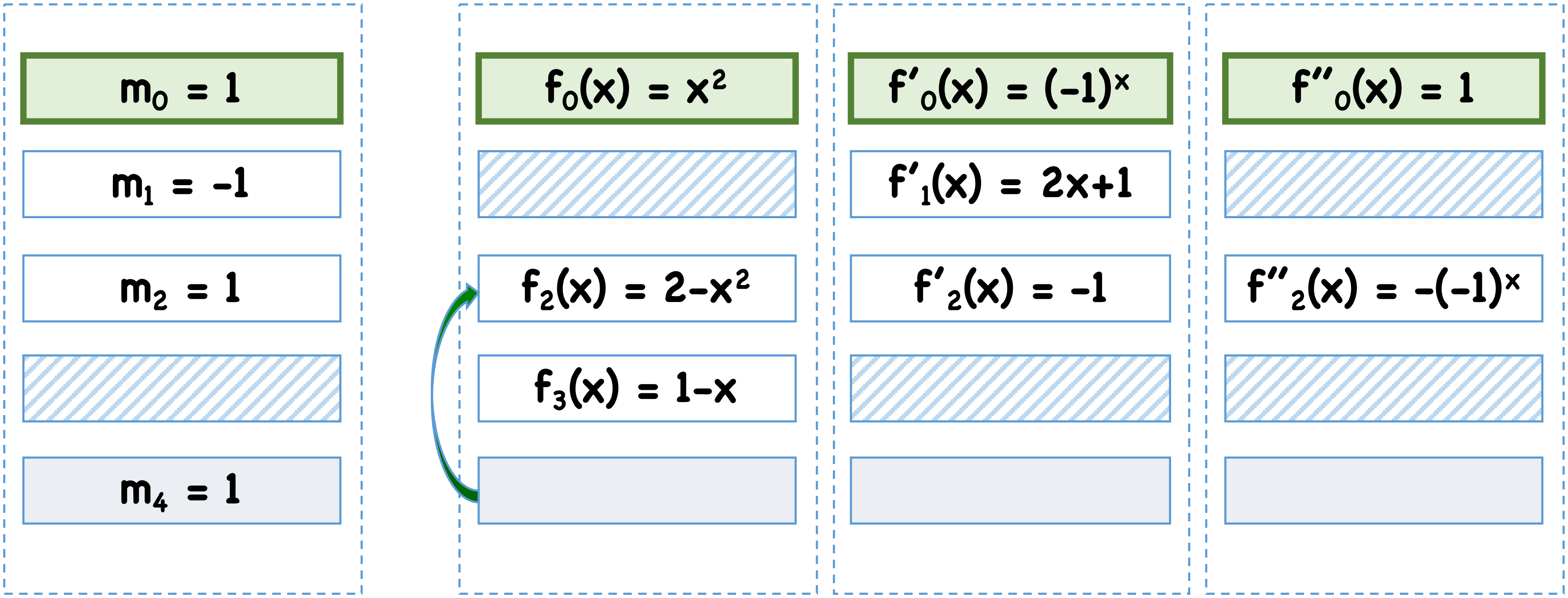


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$	$f_4(x) = 2-x^2$		

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

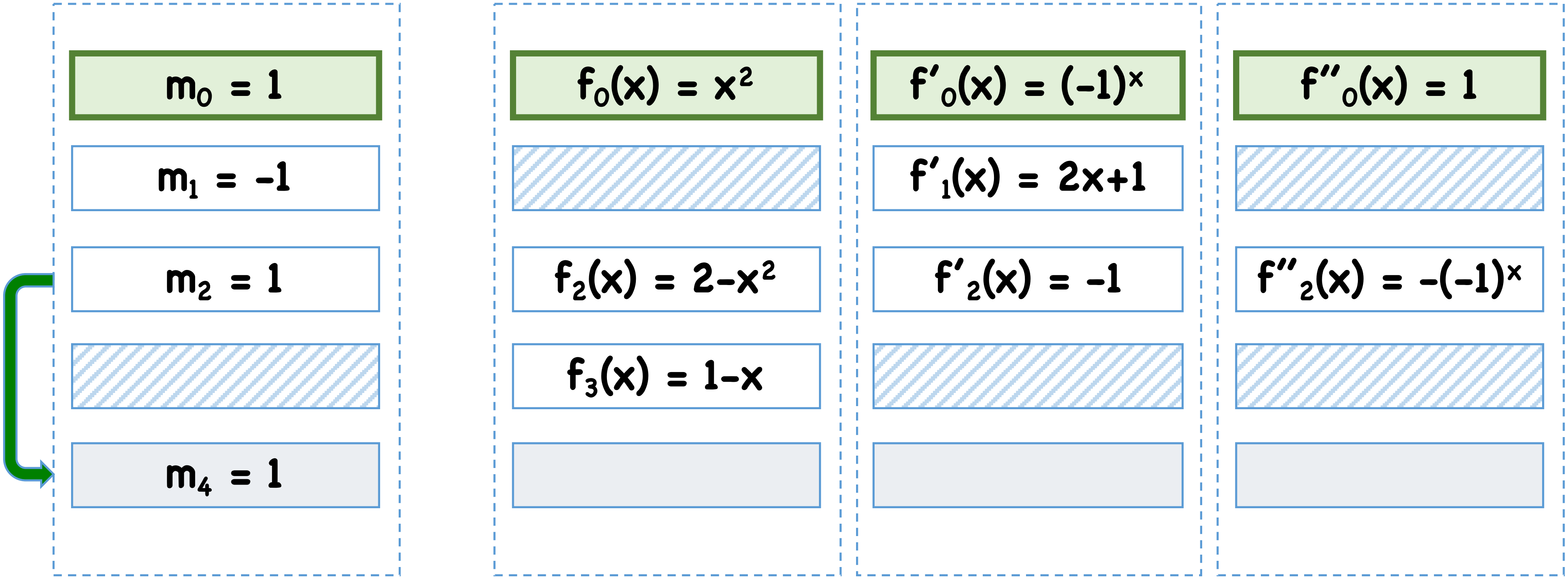


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$			

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

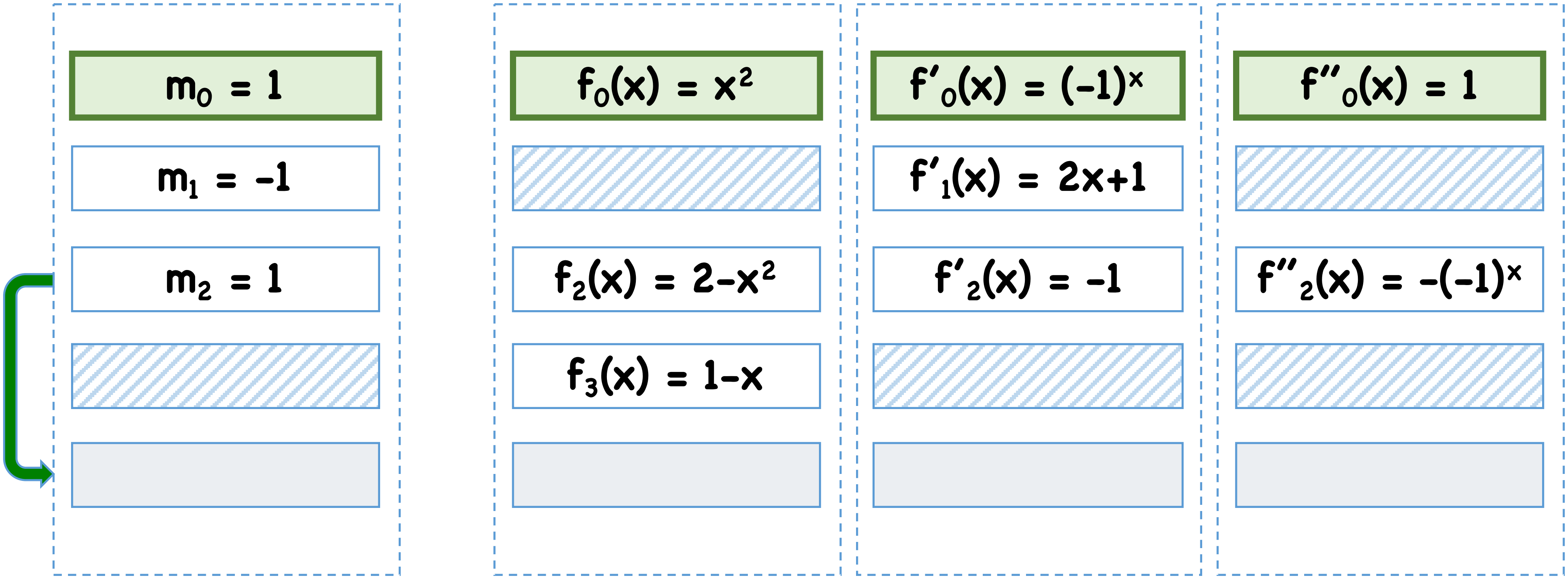


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$			

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot

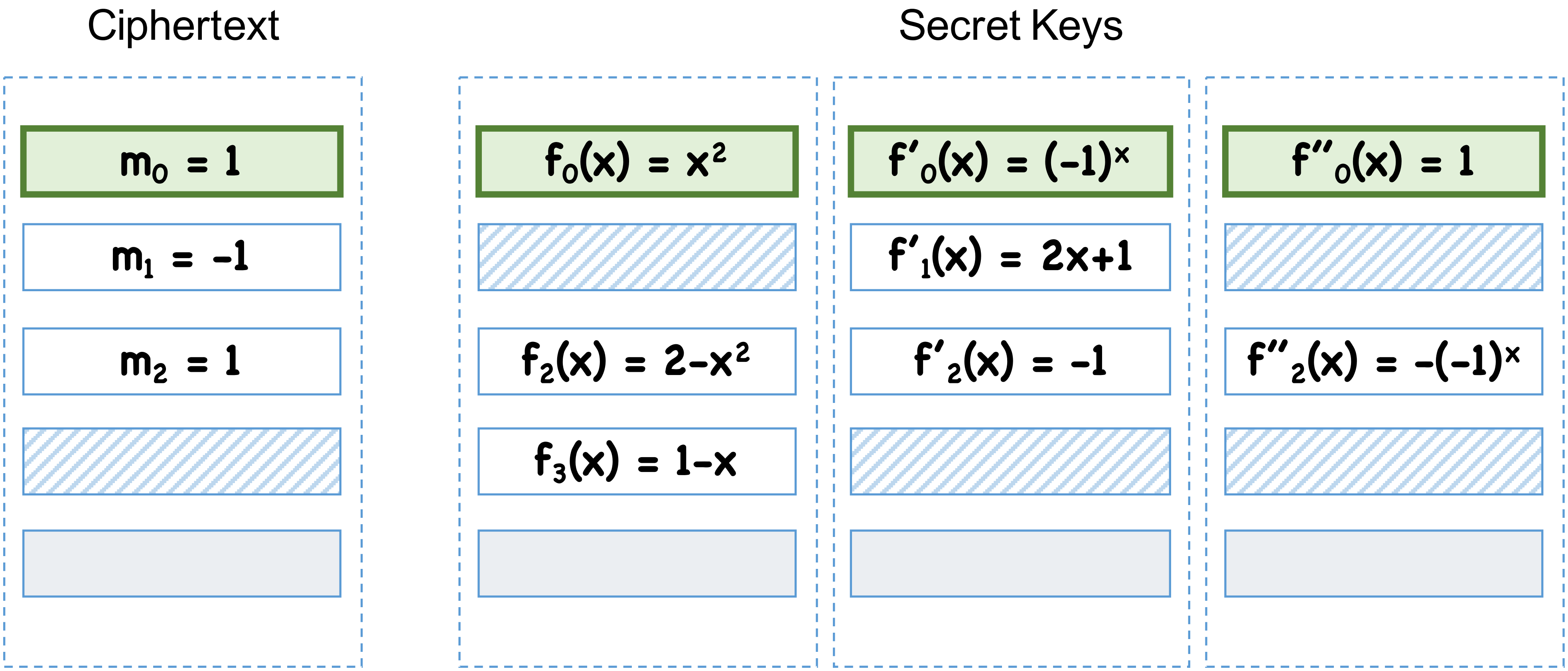


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to third slot



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

More on Slotted FE

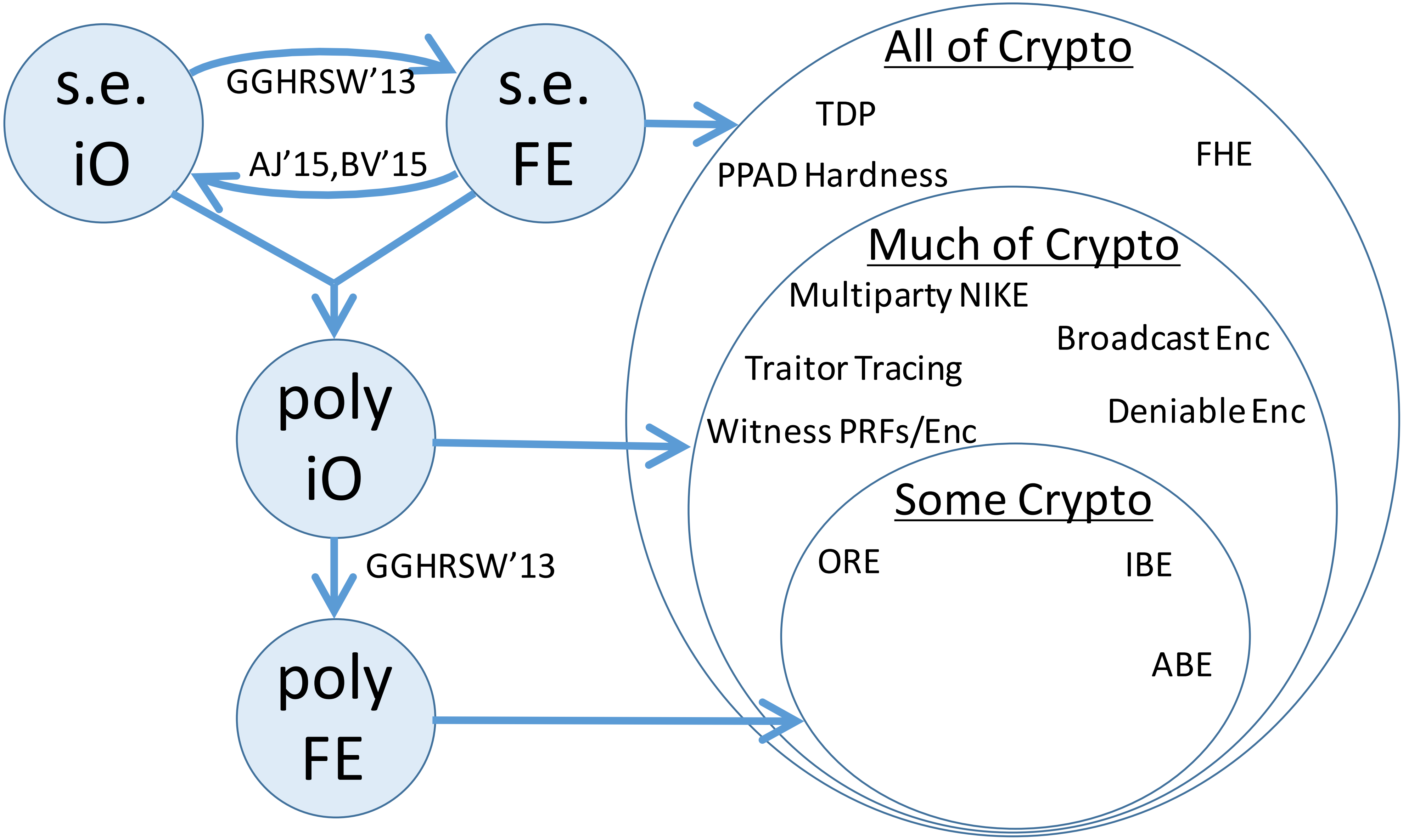
Can extend reductions to get “best possible” security

Alternate view of several other works
([CIJOPP’13,GHRW’14,BS’15,ABSV’15,NWZ’15]):

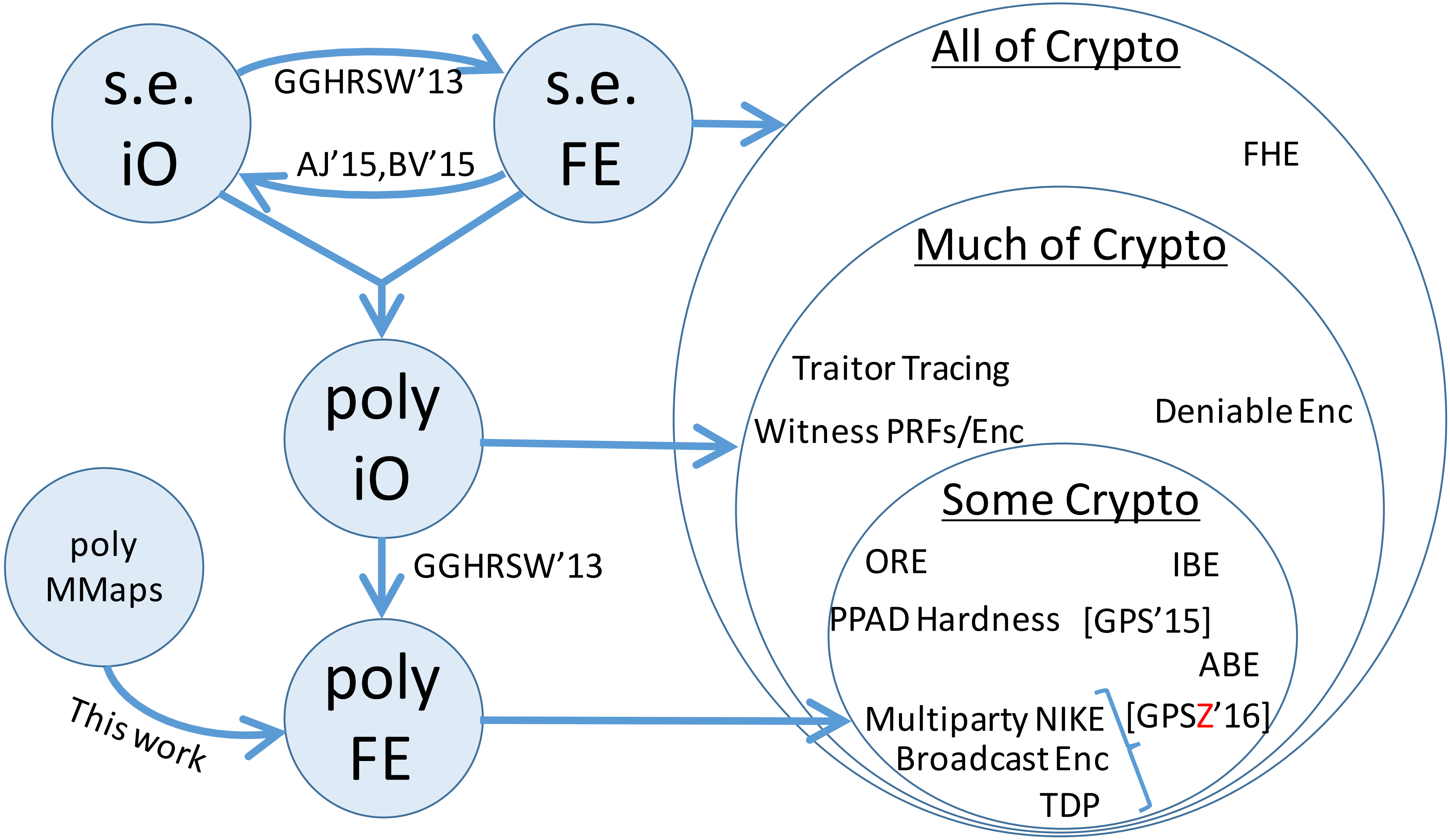
FE $\Rightarrow$ Slotted FE $\Rightarrow$ Cool stuff

Takeaway: slotted FE is useful abstraction in its own right

A New Crypto Landscape



A New Crypto Landscape



THANKS!