Fully Secure Functional Encryption Without Obfuscation

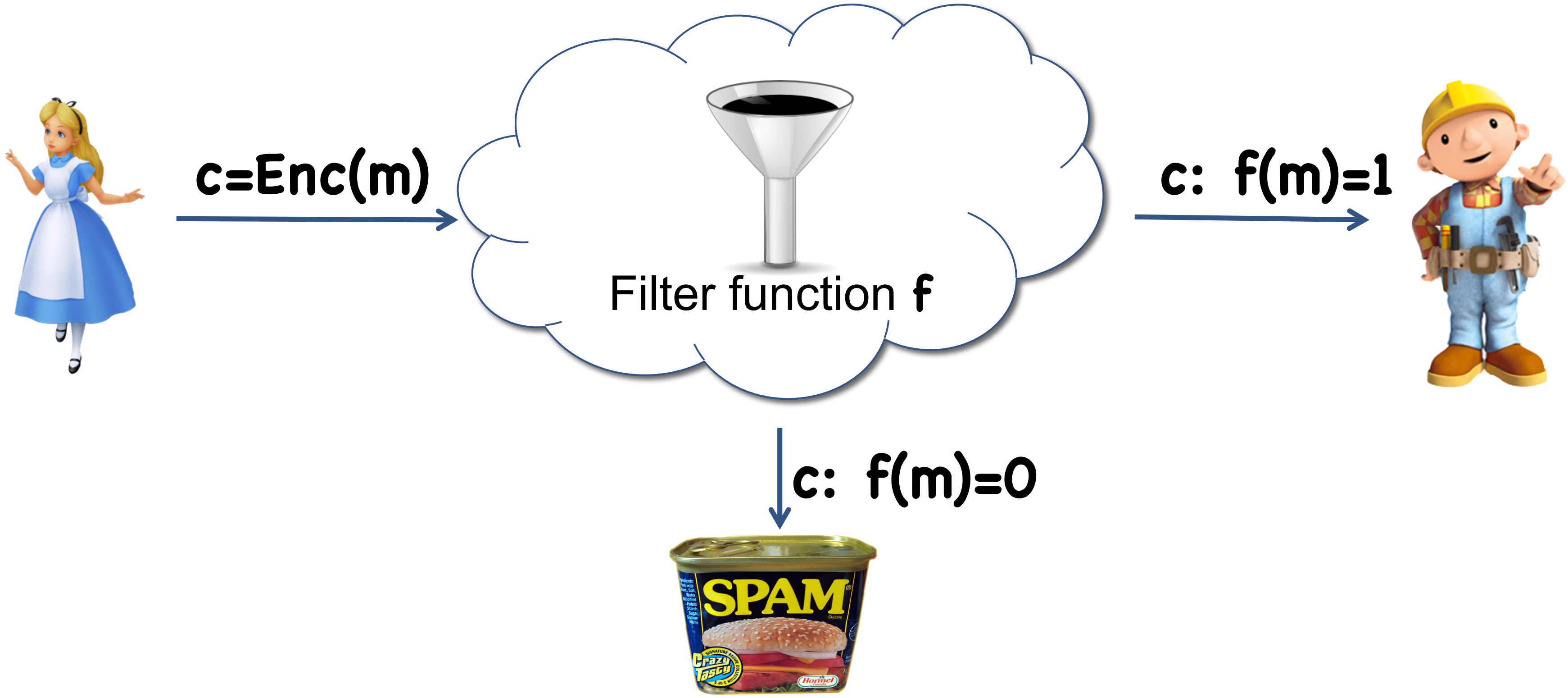
Sanjam Garg (IBM Research and UC Berkeley)

Craig Gentry (IBM Research)

Shai Halevi (IBM Research)

Mark Zhandry (Stanford University)

Example: Spam Filter



c=Enc(m)

Filter function **f**

c: f(m)=1

c: f(m)=0

Solution 0: Give cloud **sk** ⇒ cloud learns entire message ✗

Solution 1: Use FHE ⇒ cloud only learns **Enc(f(m))** ✗

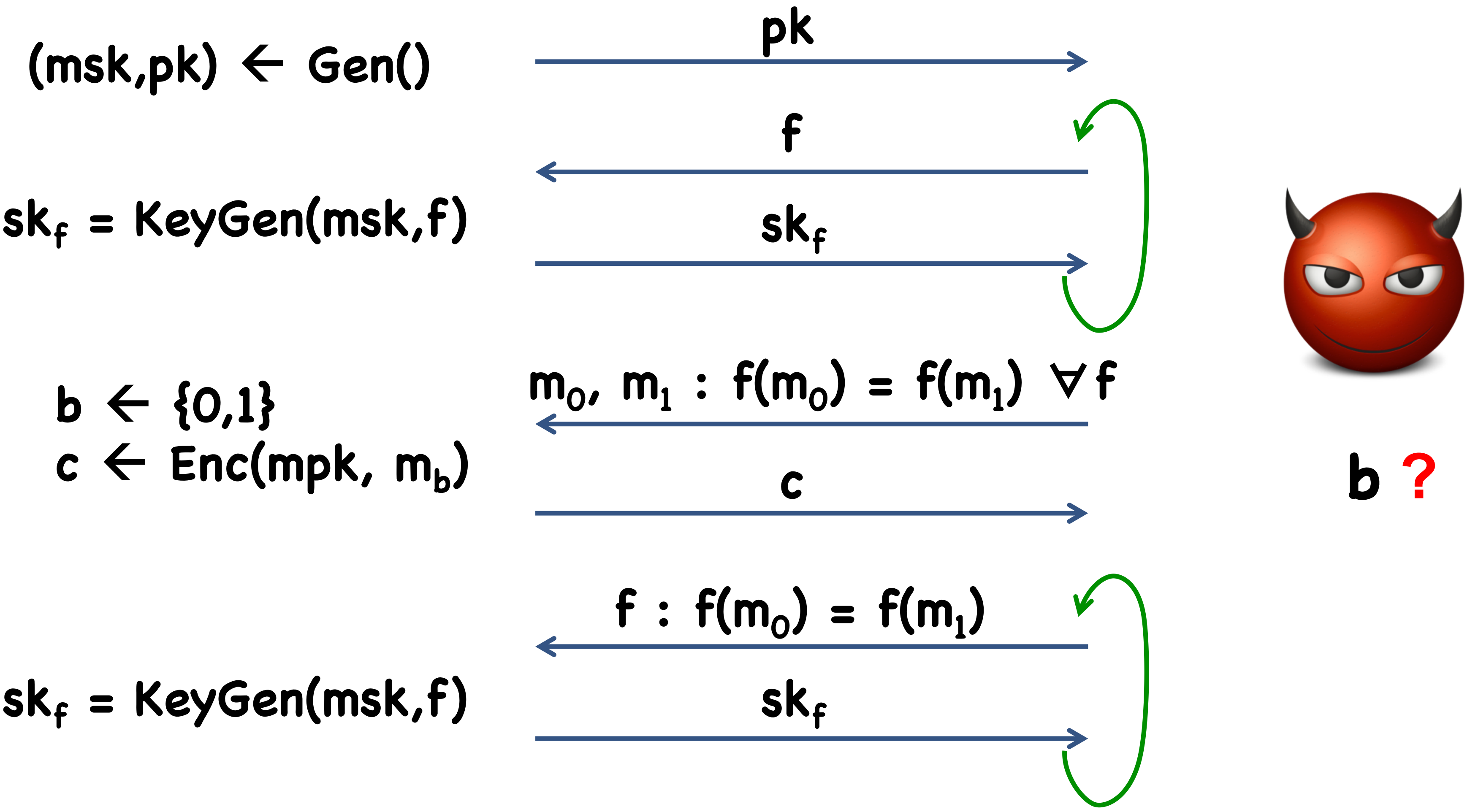
Solution 2: Functional encryption: cloud learns **f(m)**, nothing else ✓

Functional Encryption: Semantics [BSW'11]

Gen():	Output keys **(msk, pk)**
Enc(pk, m):	Output ciphertext **c**
KeyGen(msk, f):	Output decryption key **sk_f**
Dec(sk_f, c):	Output **f(m)**

Functional Encryption: Security [BSW'10,O'N'10]

Unbounded full adaptive game-based security:



$(msk,pk) \leftarrow Gen()$

pk

f

$sk_f = KeyGen(msk,f)$

sk_f

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(mpk, m_b)$

$m_0, m_1 : f(m_0) = f(m_1) \ \forall f$

c

b ?

$f : f(m_0) = f(m_1)$

$sk_f = KeyGen(msk,f)$

sk_f

Before Obfuscation

Tons of work on special cases: IBE, ABE, PE…

[SW’05, BSW’10,O’N’10]: Definitions

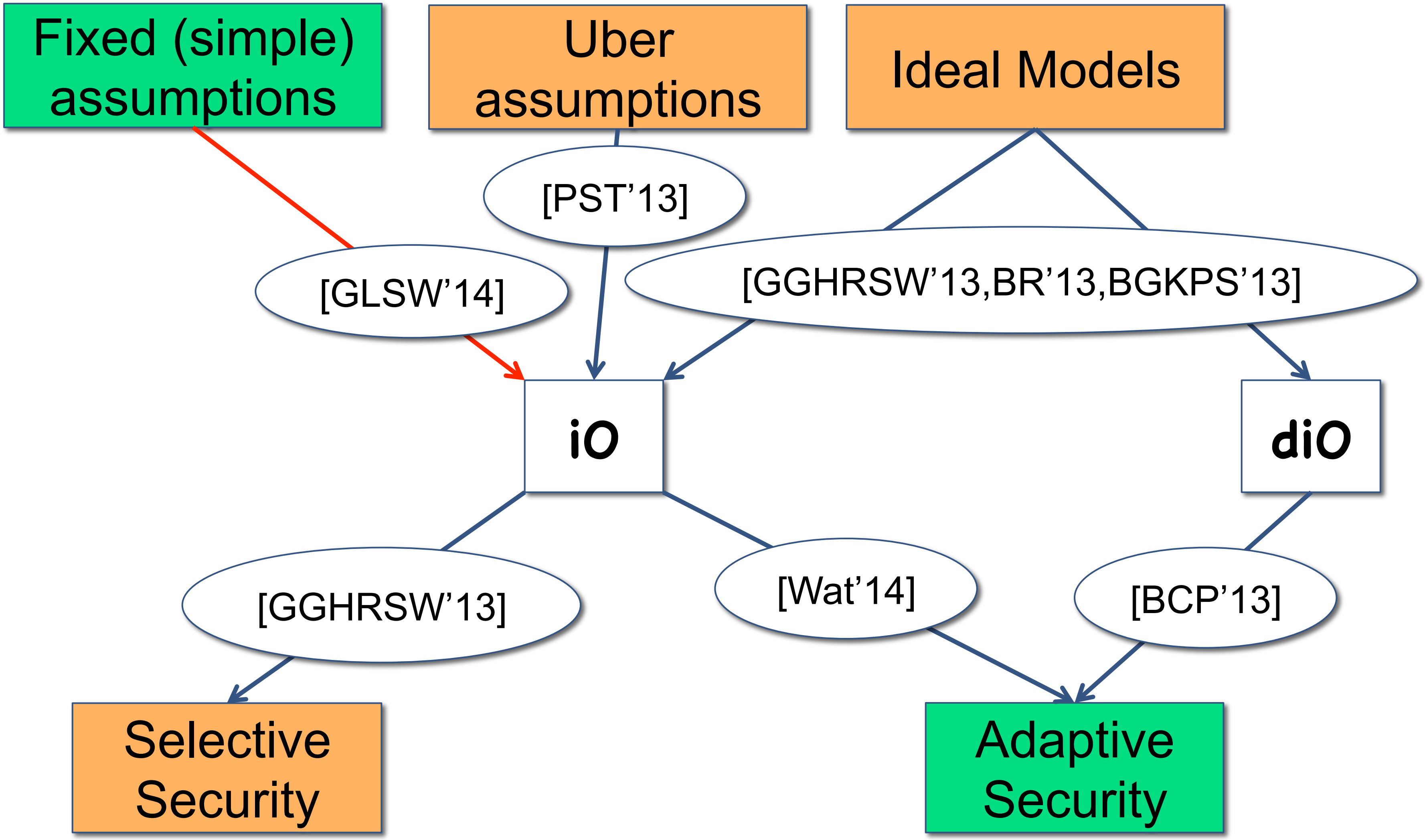
[BW’07,KSW’08,AFV’11,SSW’09]: Simple functions

[SS10,GVW’12,GKPVZ’12]: Bounded number of secret keys

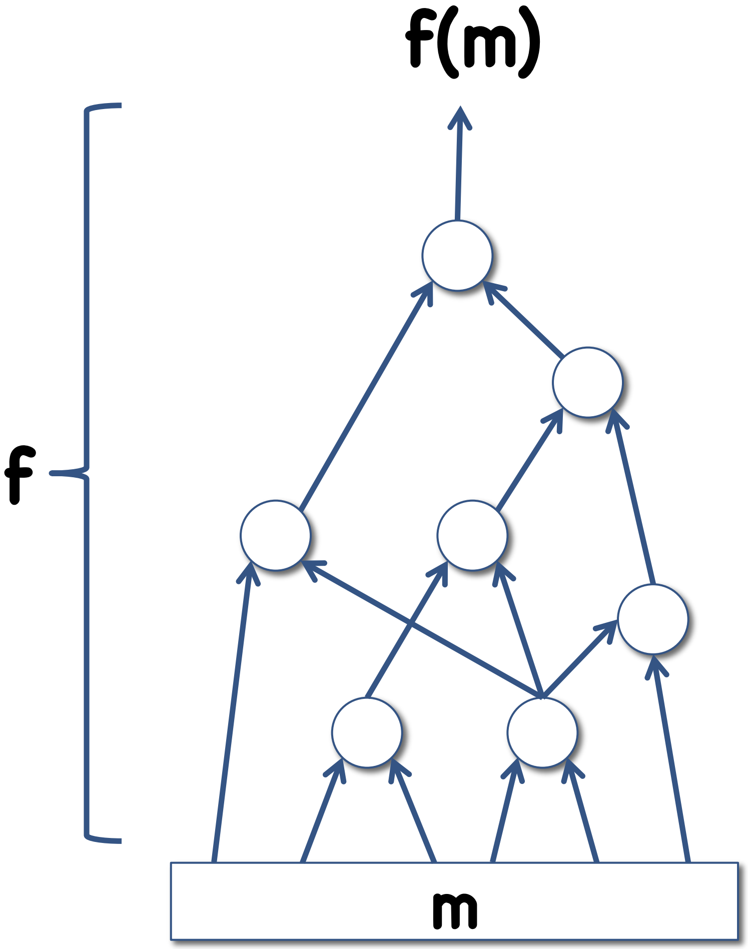
[AGVW’12]: Impossibility of unbounded simulation-based def

No unbounded constructions until…

After Obfuscation: First Unbounded Constructions

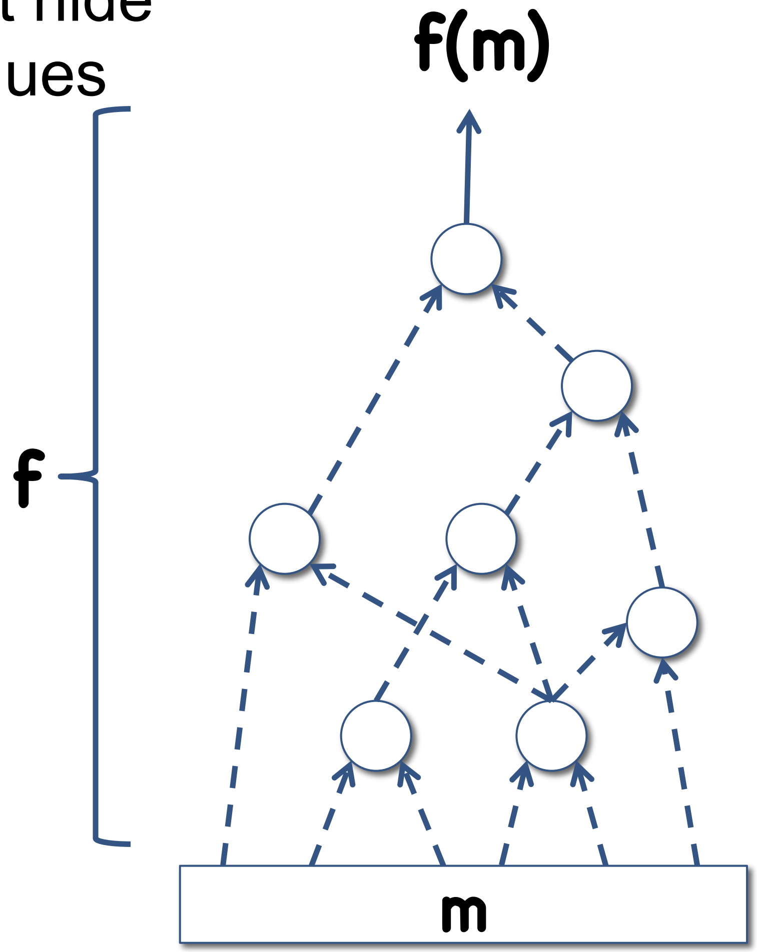


Why Obfuscation Seems Inherent



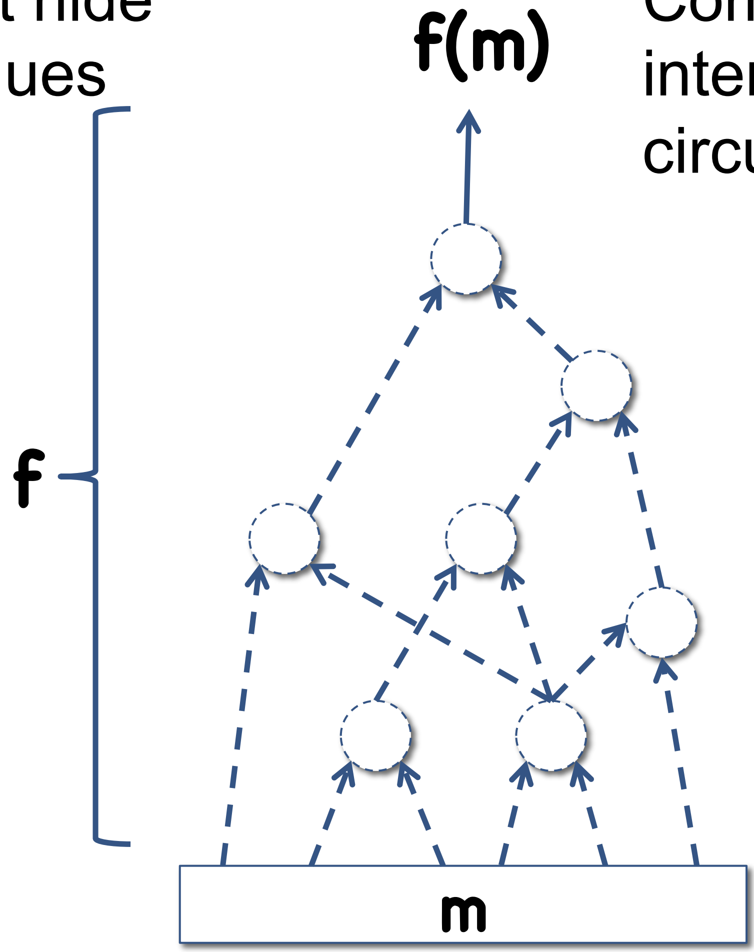
Why Obfuscation Seems Inherent

Decryption must hide intermediate values



Why Obfuscation Seems Inherent

Decryption must hide intermediate values



Common ways to hide intermediate values hide circuit too. E.g.

- garbled circuits
- branching progs
- obfuscation

f is now hidden

Note: [BCP'13] does **not** have function hiding

Function Hiding ⇒ IO

```
iO(C):               (msk,pk) ← Gen()
                     sk ← KeyGen(msk,C)
                     Output (pk,sk)

Eval( (pk,sk), x):   e = Enc(pk,x)
                     y = Dec(sk,e)
```

sk hides **C** → indistinguishability obfuscation

Takeaway: FE with function hiding implies iO

Question 1:

Can we build FE without iO?

Why avoid Obfuscation?

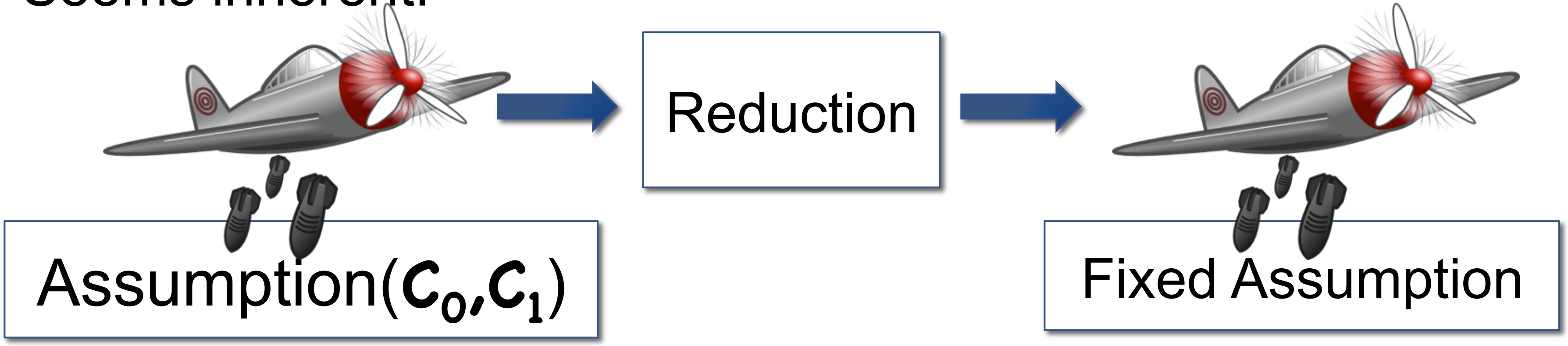
iO = exponentially many assumptions

- One per pair of circuits

Assumption(C_0,C_1):

$$iO(C_0) \approx iO(C_1)$$

Seems inherent:



Assumption(C_0,C_1)

Reduction

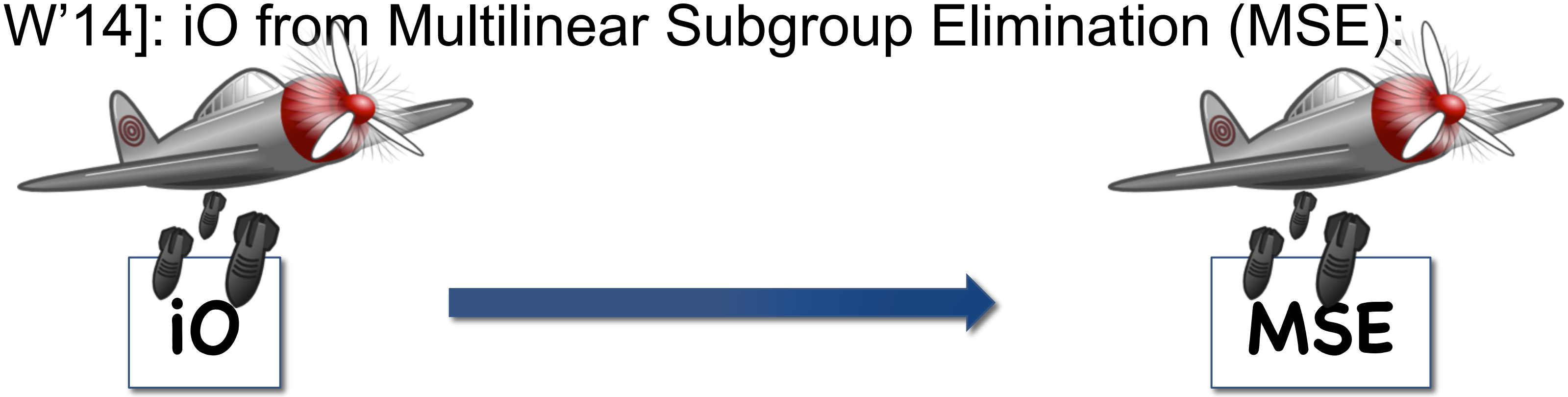
Fixed Assumption

Reduction can only work for equiv C_0, C_1

⇒ must somehow decide equivalence (NP-hard)

What about GLSW?

[GLSW’14]: iO from Multilinear Subgroup Elimination (MSE):

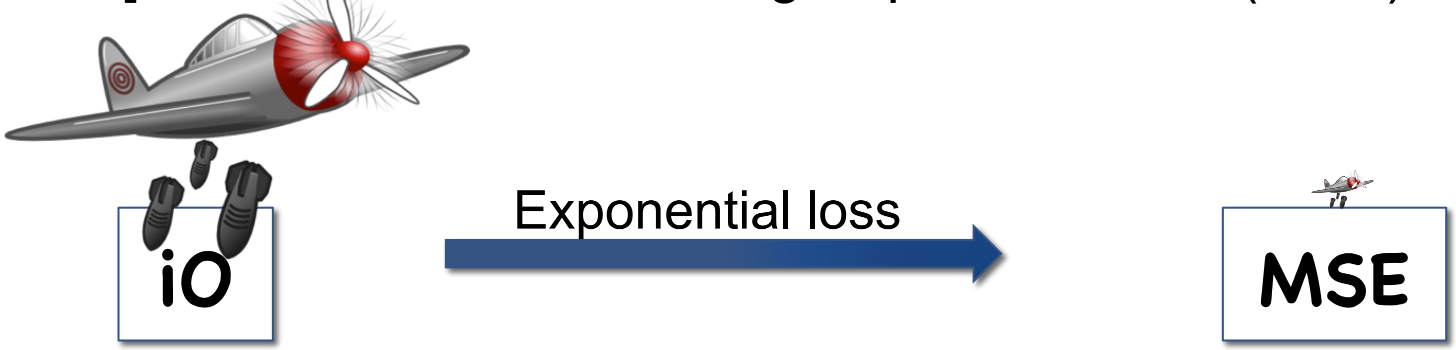


iO

MSE

What about GLSW?

[GLSW’14]: iO from Multilinear Subgroup Elimination (MSE):



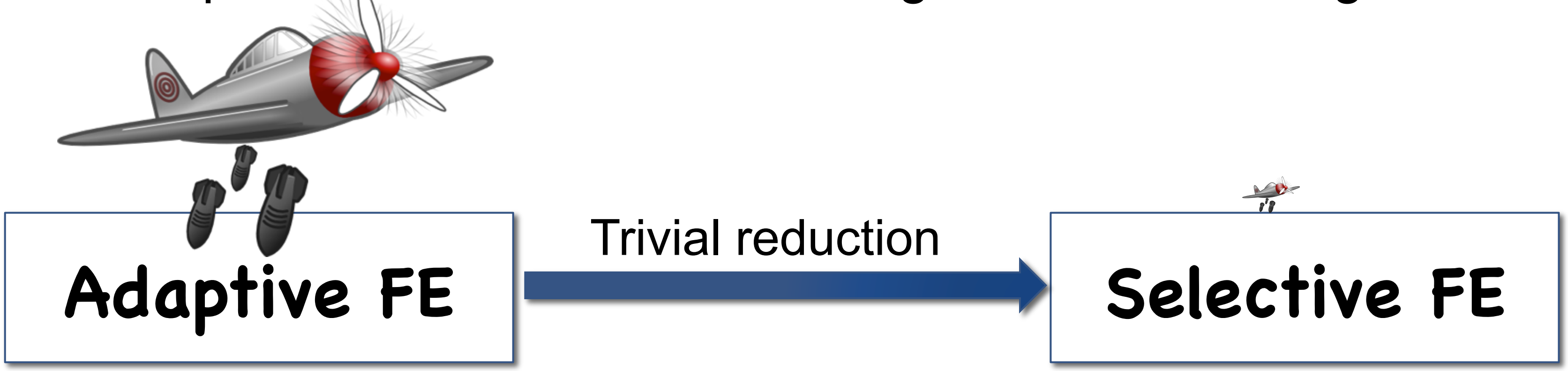
iO

Exponential loss

MSE

- Need to assume MSE **really** hard (complexity leveraging)

Note: Adaptive vs selective FE meaningless in this setting



Adaptive FE

Trivial reduction

Selective FE

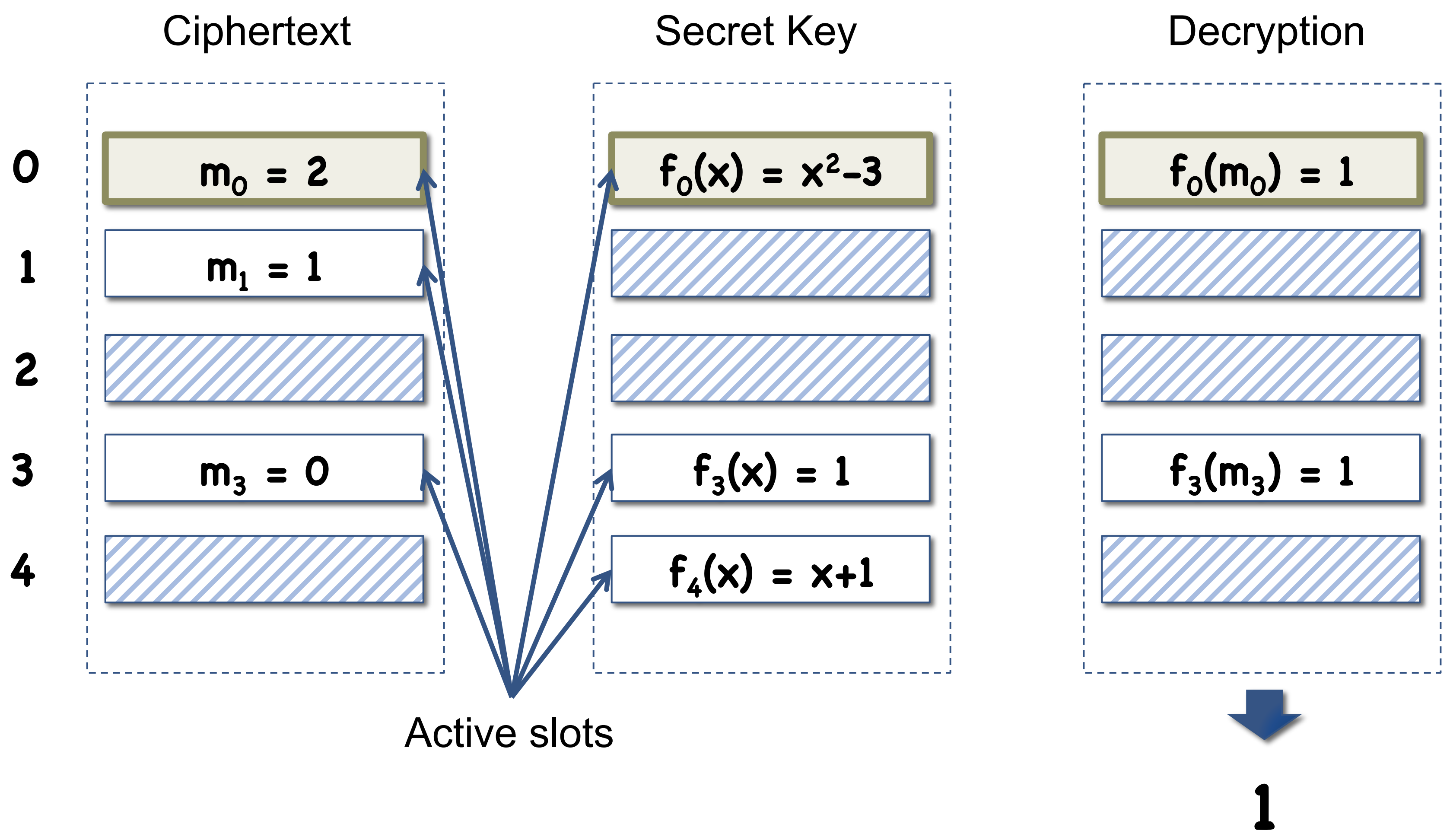
Question 2:

Can we build (adaptive) FE from fixed assumptions w/o complexity leveraging?

Our answer to questions 1 & 2:

YES!

Generalization: Slotted Functional Encryption



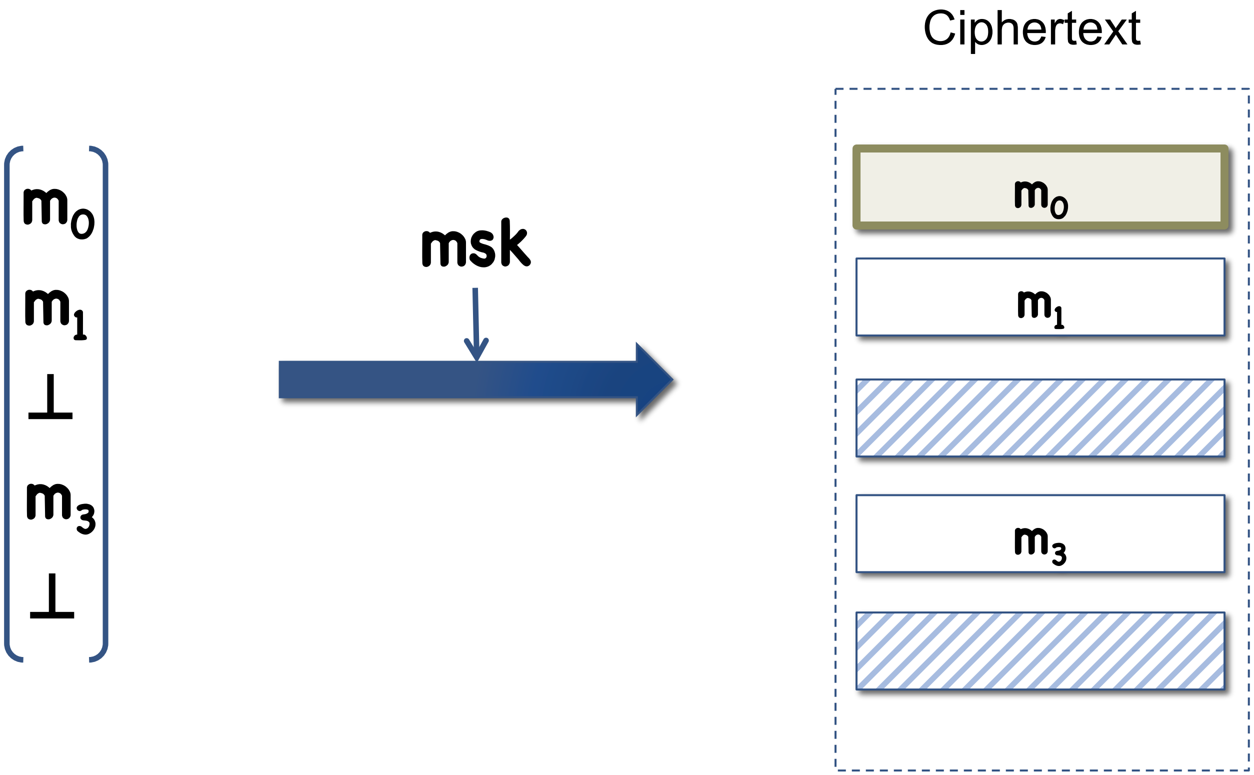
	Ciphertext	Secret Key	Decryption
0	$m_0 = 2$	$f_0(x) = x^2-3$	$f_0(m_0) = 1$
1	$m_1 = 1$	▨	▨
2	▨	▨	▨
3	$m_3 = 0$	$f_3(x) = 1$	$f_3(m_3) = 1$
4	▨	$f_4(x) = x+1$	▨

Active slots

1

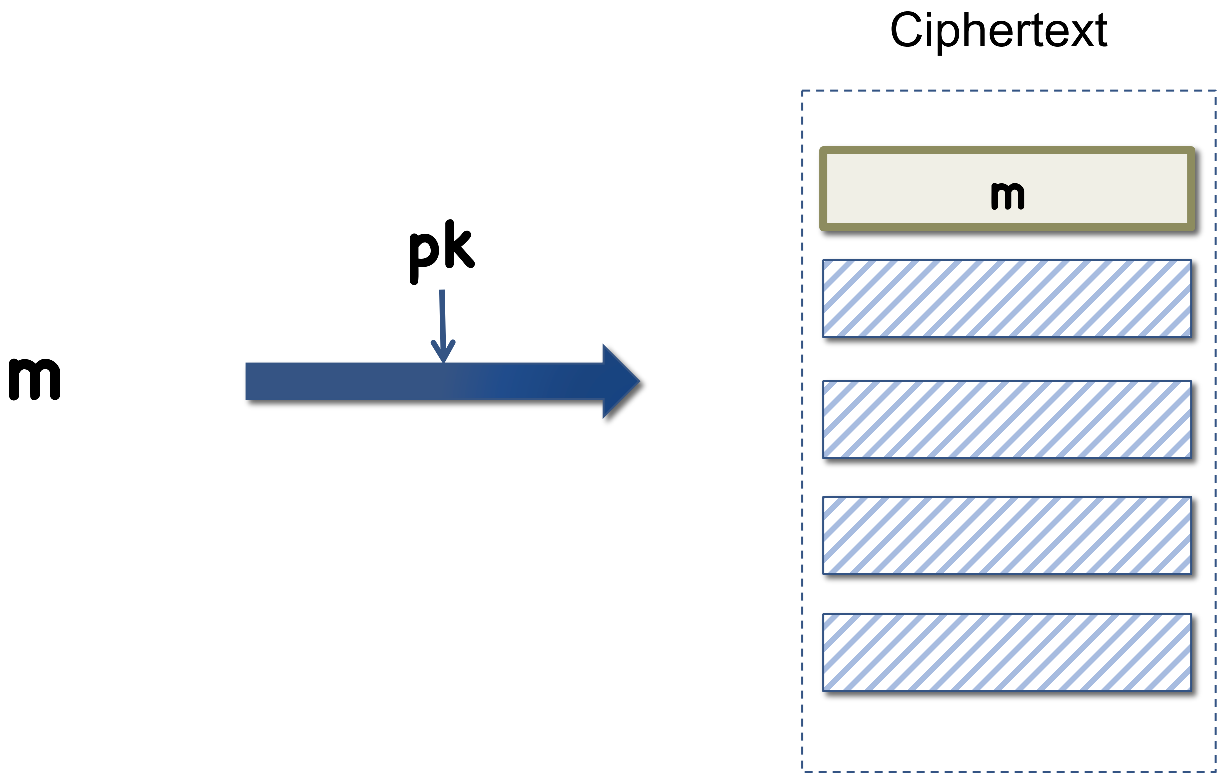
Slotted Functional Encryption

Private (slotted) encryption: encrypt in all slots


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

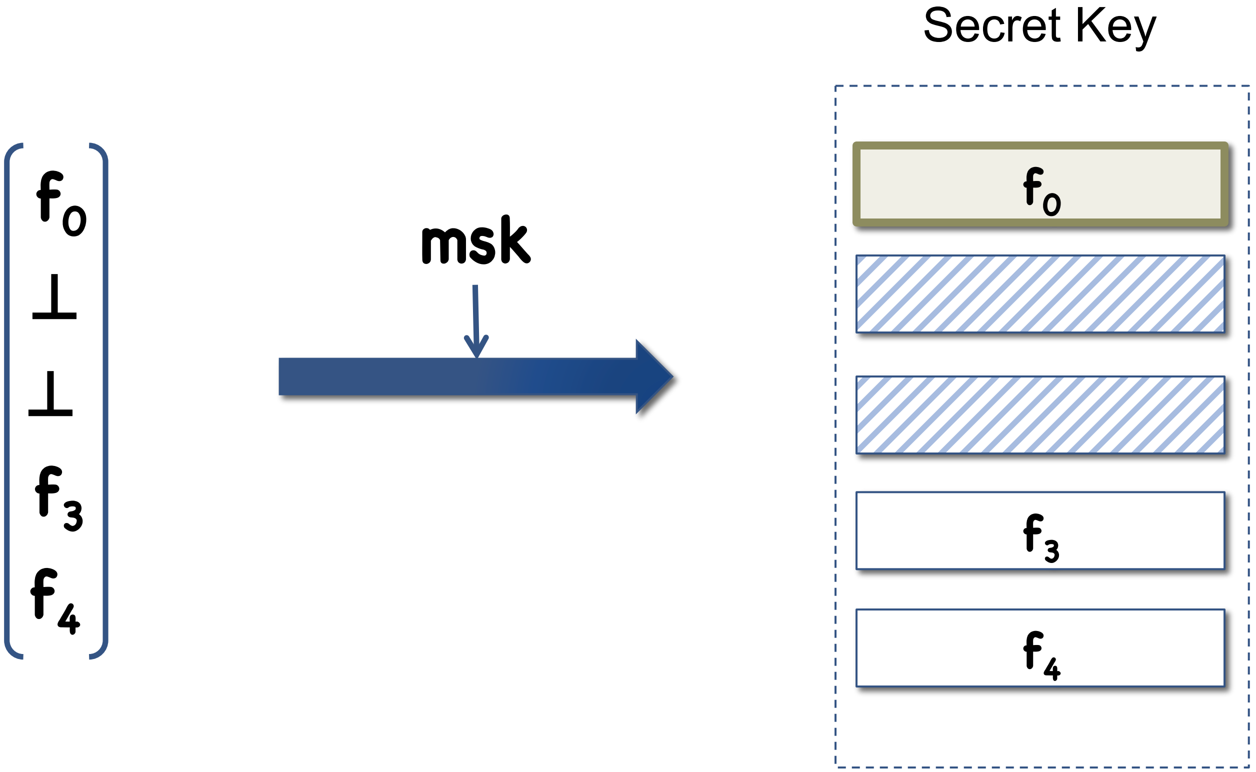
Slotted Functional Encryption

Public (unslotted) encryption: encrypt in slot 0



Slotted Functional Encryption

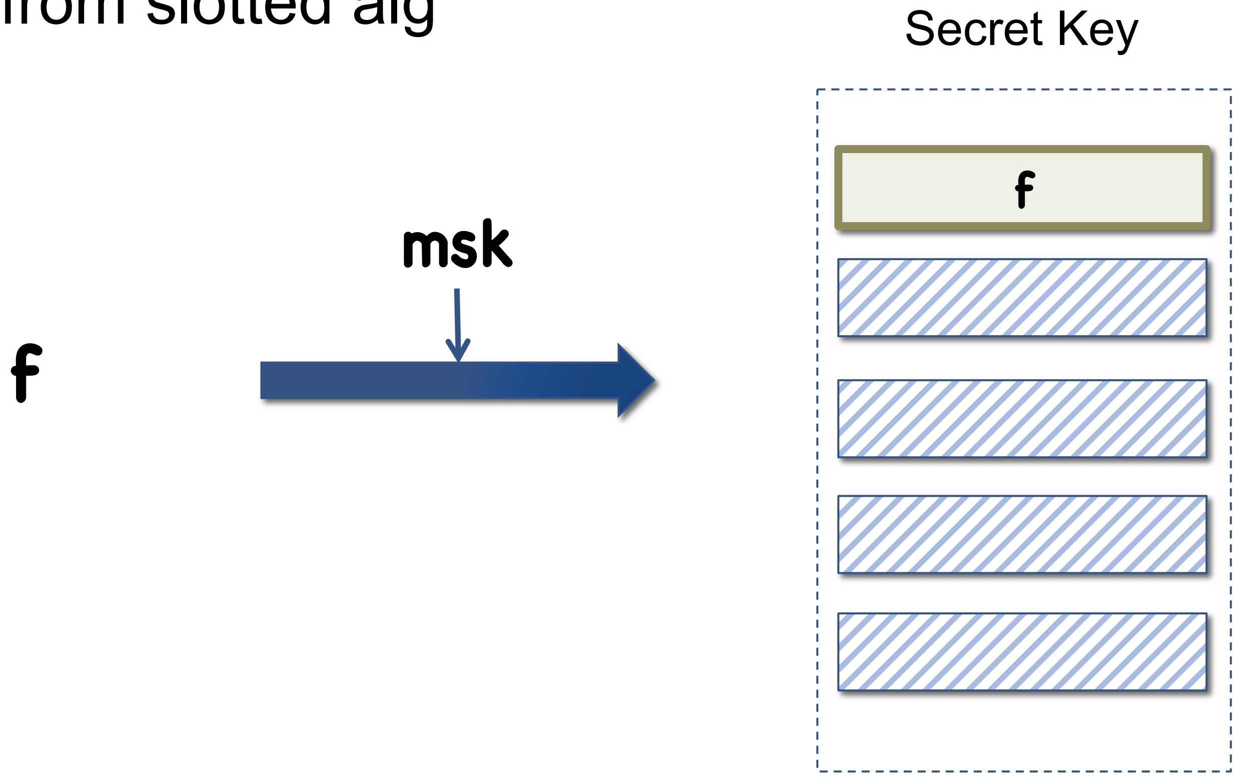
Slotted keygen: secret keys in all slots



Slotted Functional Encryption

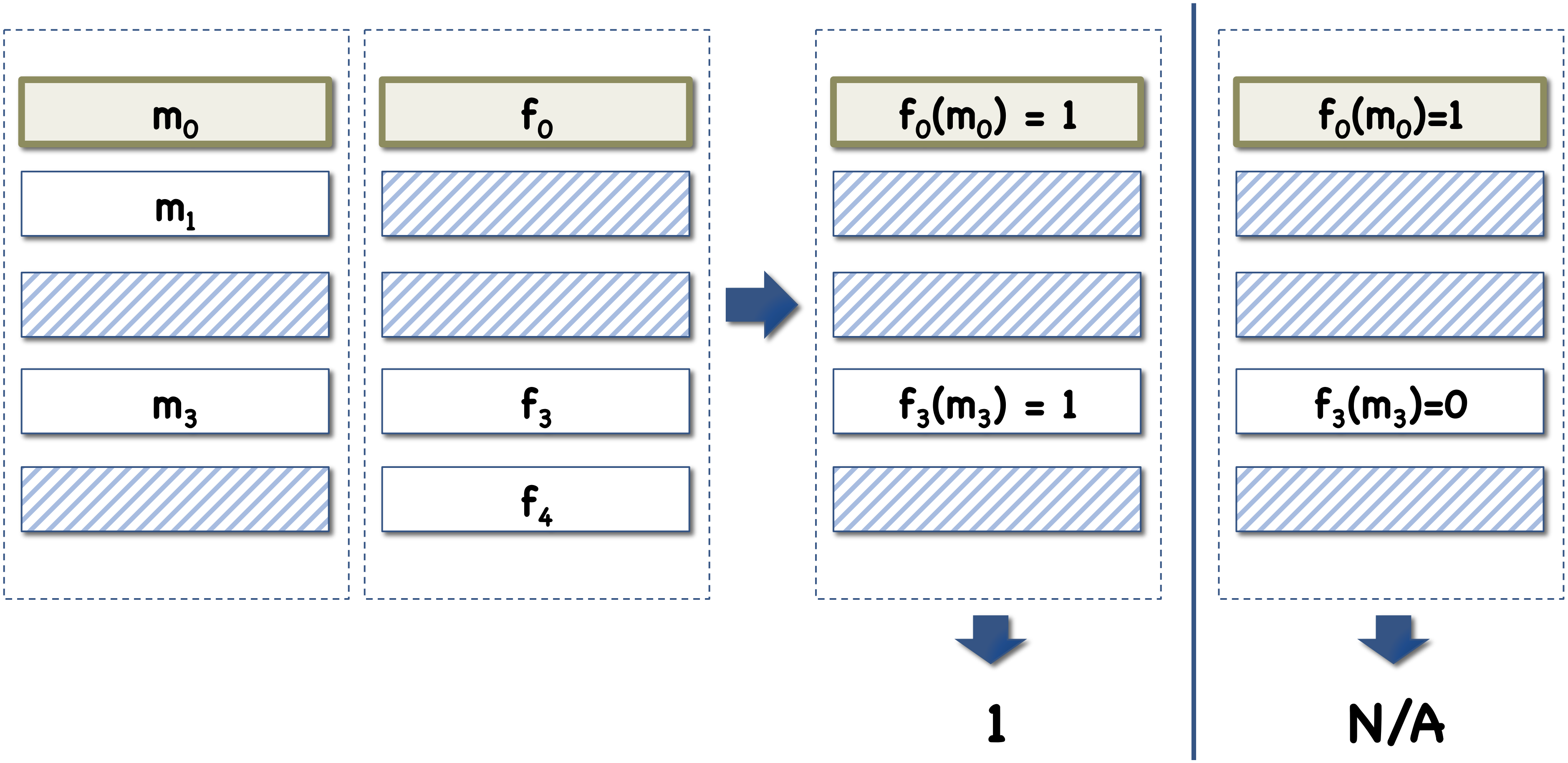
Unslotted keygen: secret keys in slot 0

- 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)

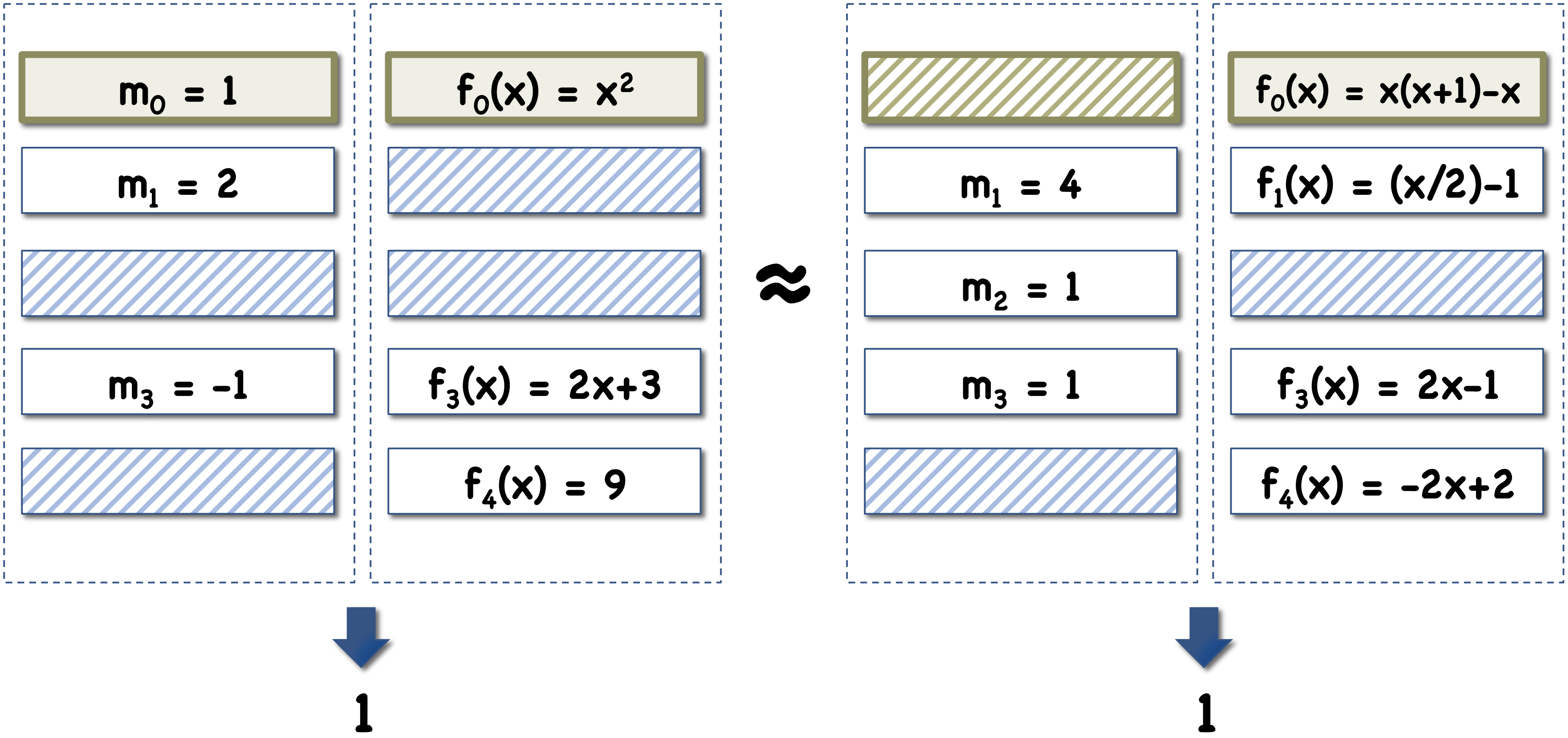
→

Enc(pk, m)

KeyGen(msk, f)

Security of Slotted Functional Encryption

Ideal: can’t learn anything except through decryption



$m_0 = 1$

$m_1 = 2$

$m_3 = -1$

$f_0(x) = x^2$

$f_3(x) = 2x+3$

$f_4(x) = 9$

$\approx$

$m_1 = 4$

$m_2 = 1$

$m_3 = 1$

$f_0(x) = x(x+1)-x$

$f_1(x) = (x/2)-1$

$f_3(x) = 2x-1$

$f_4(x) = -2x+2$

1

1

Too strong: implies function hiding in unslotted scheme

Security of Slotted Functional Encryption

Strategy: define desired property:

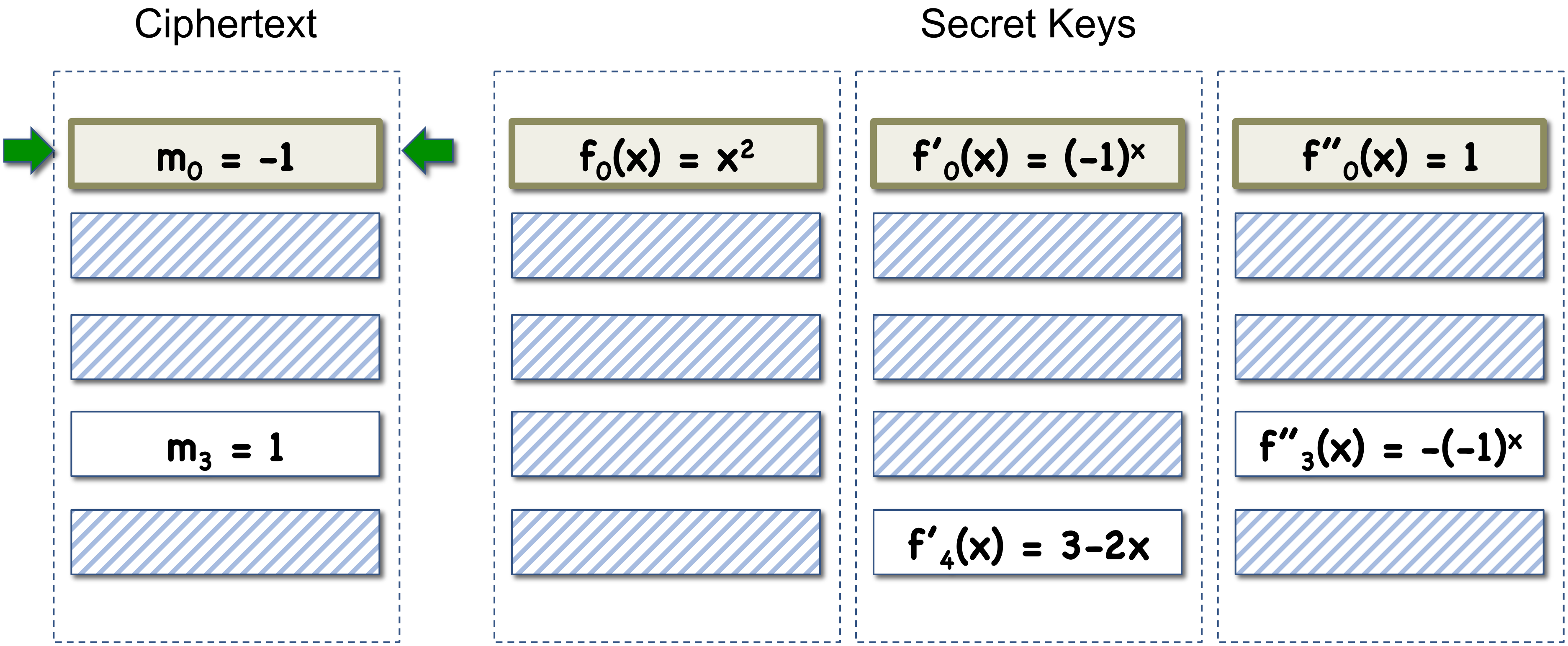
- Strong ciphertext indistinguishability

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

Security of Slotted Functional Encryption

Strong Ciphertext Indistinguishability: change ciphertext slot (possibly in slot **0**) as long as decryption unaffected



Ciphertext

Secret Keys

$m_0 = -1$

$m_3 = 1$

$f_0(x) = x^2$

$f'_0(x) = (-1)^x$

$f'_4(x) = 3-2x$

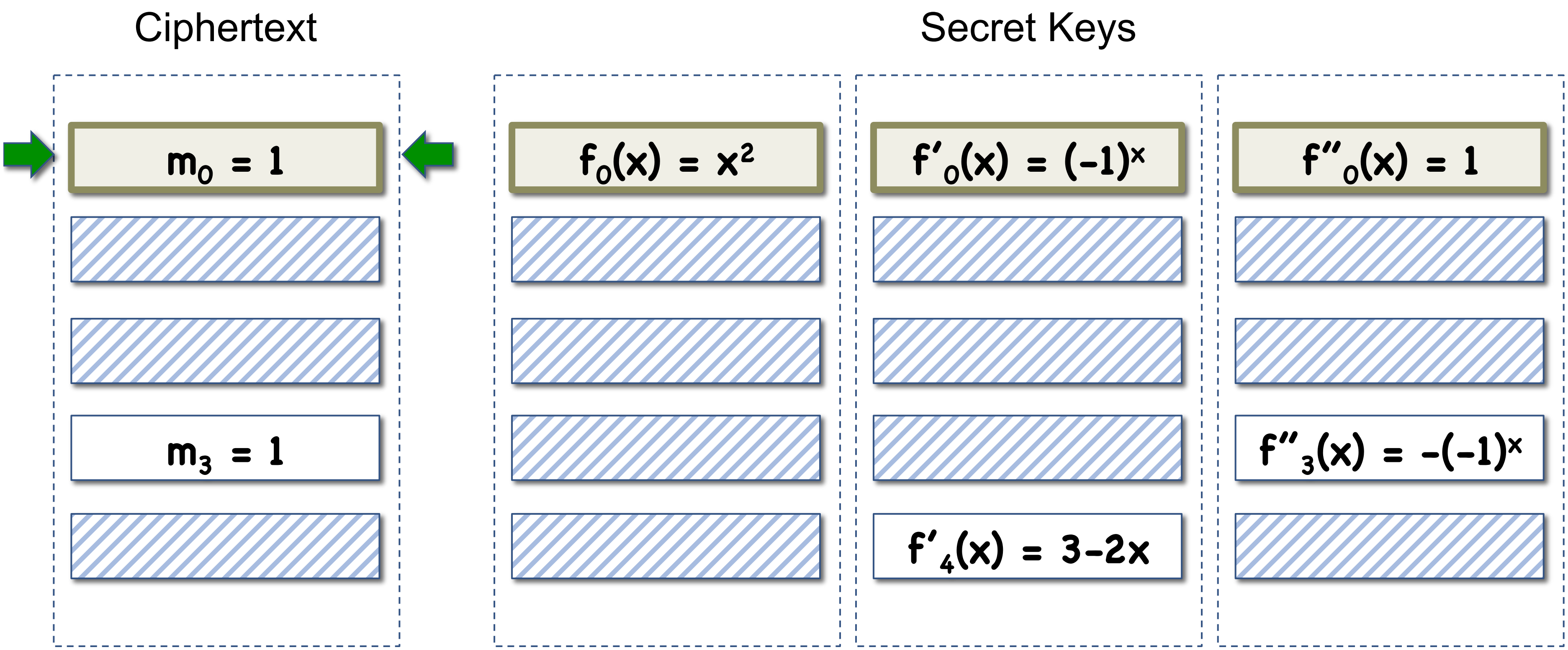
$f''_0(x) = 1$

$f''_3(x) = -(-1)^x$

$m_0 = -1 \rightarrow m_0 = 1$ does not affect decryption

Security of Slotted Functional Encryption

Strong Ciphertext Indistinguishability: change ciphertext slot (possibly in slot **0**) as long as decryption unaffected



Ciphertext

$m_0 = 1$

$m_3 = 1$

Secret Keys

$f_0(x) = x^2$

$f'_0(x) = (-1)^x$

$f'_4(x) = 3-2x$

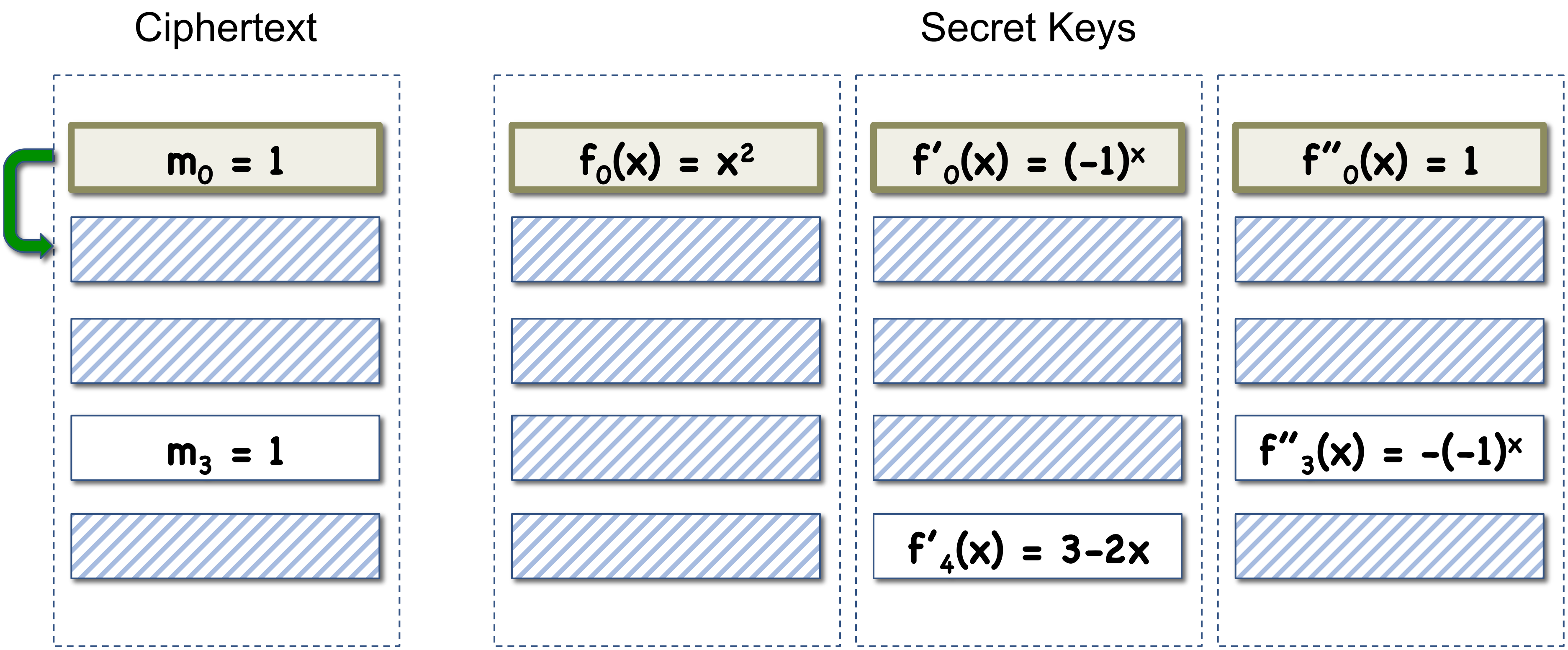
$f''_0(x) = 1$

$f''_3(x) = -(-1)^x$

$m_0 = -1 \rightarrow m_0 = 1$ does not affect decryption

Security of Slotted Functional Encryption

Slot Duplication: Copy any slot (inc. slot **0**) into unused slot (except slot **0**) (don't have to copy everything)



Ciphertext

Secret Keys

$m_0 = 1$

$m_3 = 1$

$f_0(x) = x^2$

$f'_0(x) = (-1)^x$

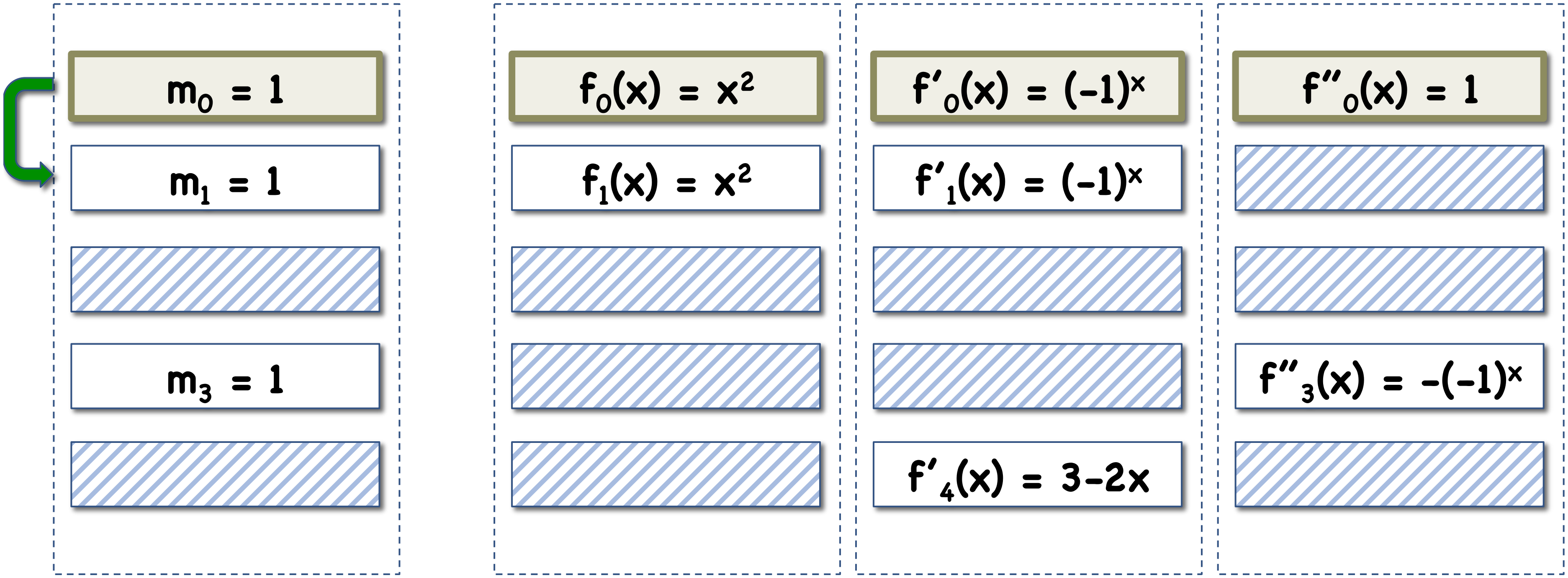
$f'_4(x) = 3-2x$

$f''_0(x) = 1$

$f''_3(x) = -(-1)^x$

Security of Slotted Functional Encryption

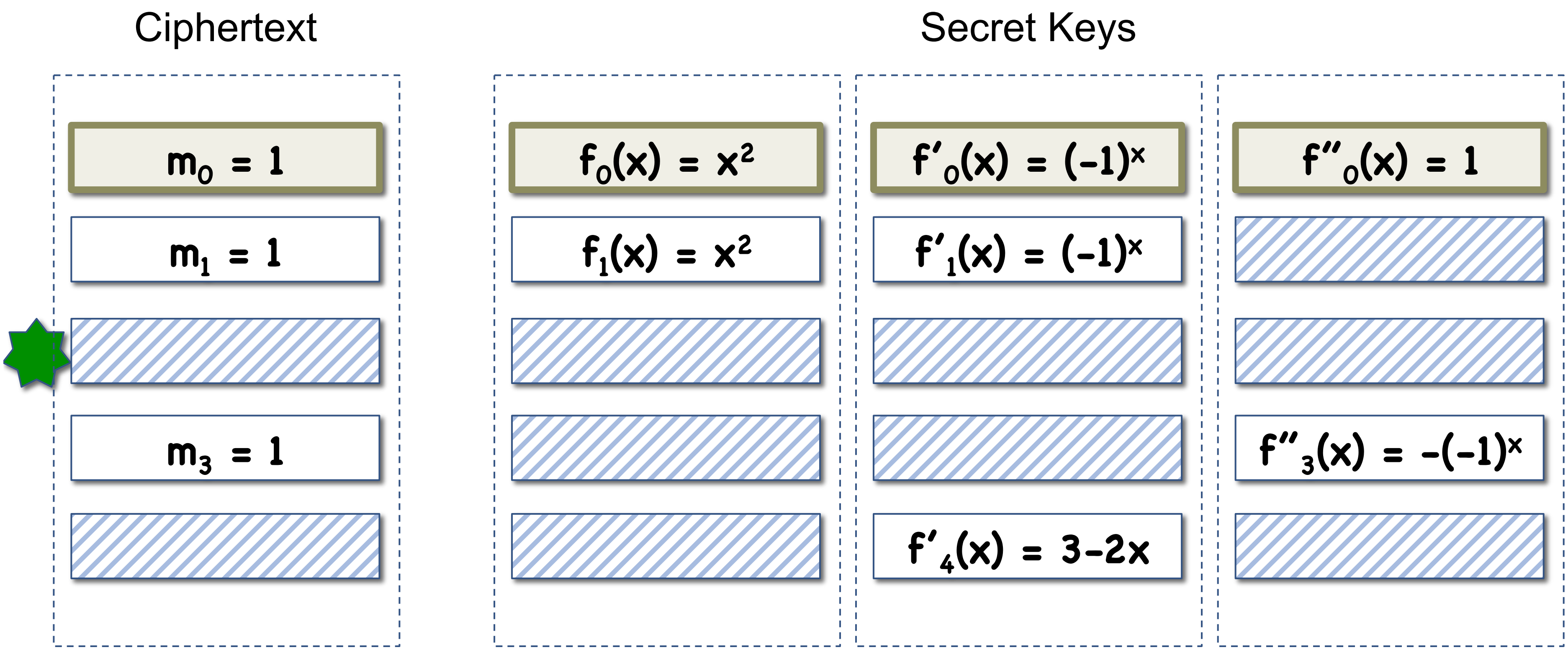
Slot Duplication: Copy any slot (inc. slot **0**) into unused slot (except slot **0**) (don’t have to copy everything)



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 1$	$f_1(x) = x^2$	$f'_1(x) = (-1)^x$	▨
▨	▨	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

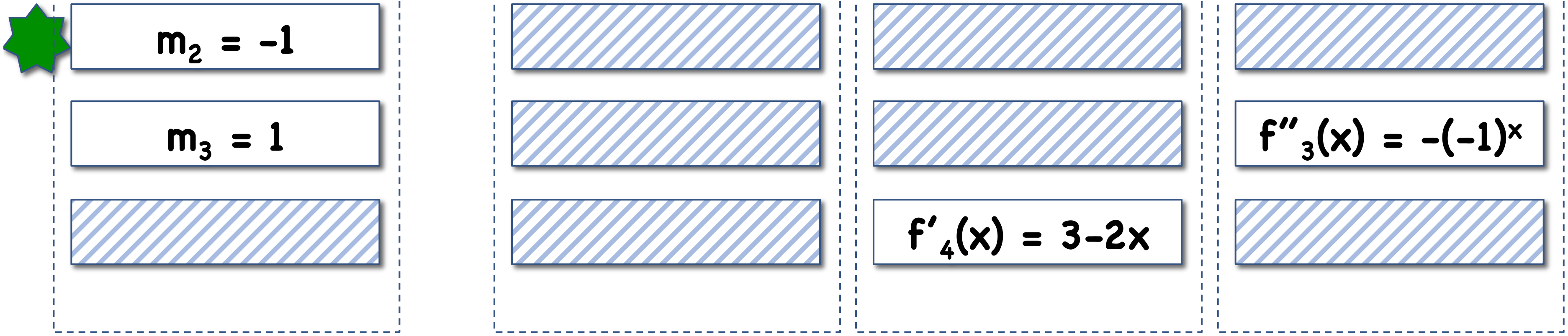
New Slot: In unused slot (except slot **0**), put any ciphertext val



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 1$	$f_1(x) = x^2$	$f'_1(x) = (-1)^x$	▨
▨	▨	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

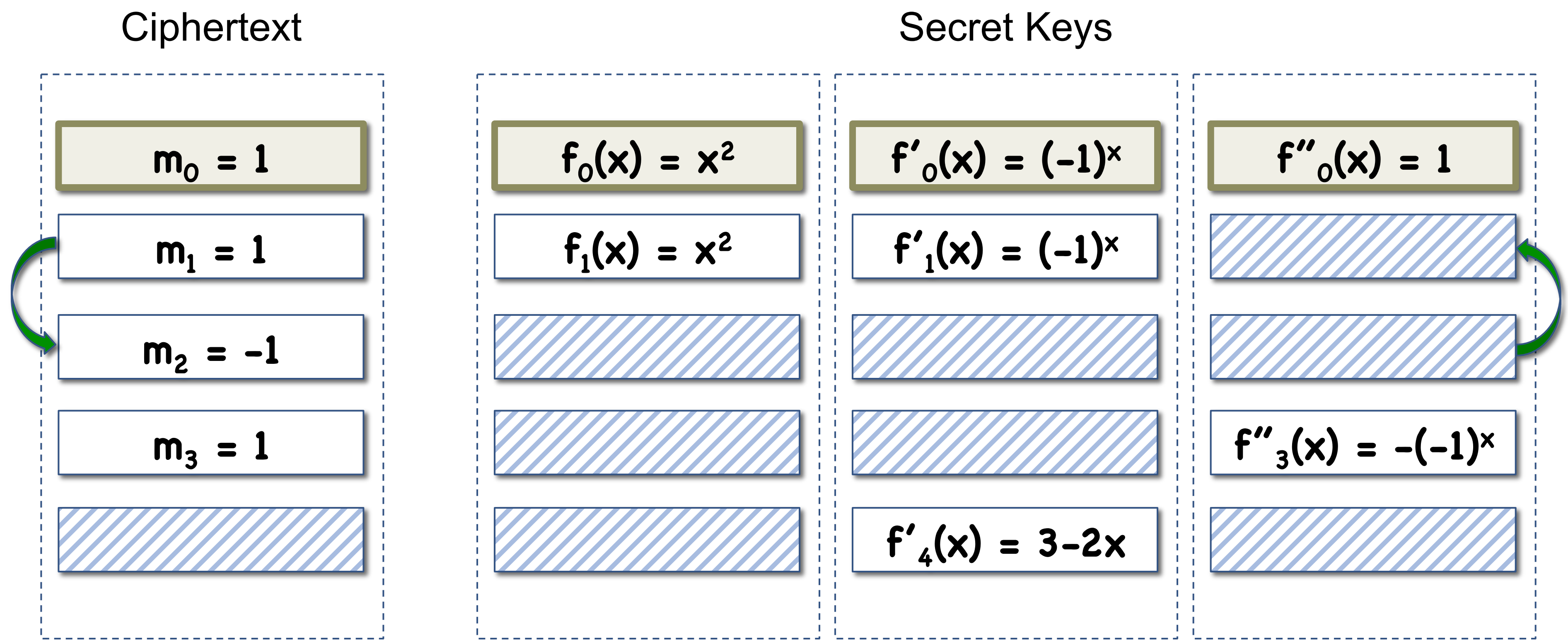
New Slot: In unused slot (except slot **0**), put any ciphertext val



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 1$	$f_1(x) = x^2$	$f'_1(x) = (-1)^x$	▨
$m_2 = -1$	▨	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

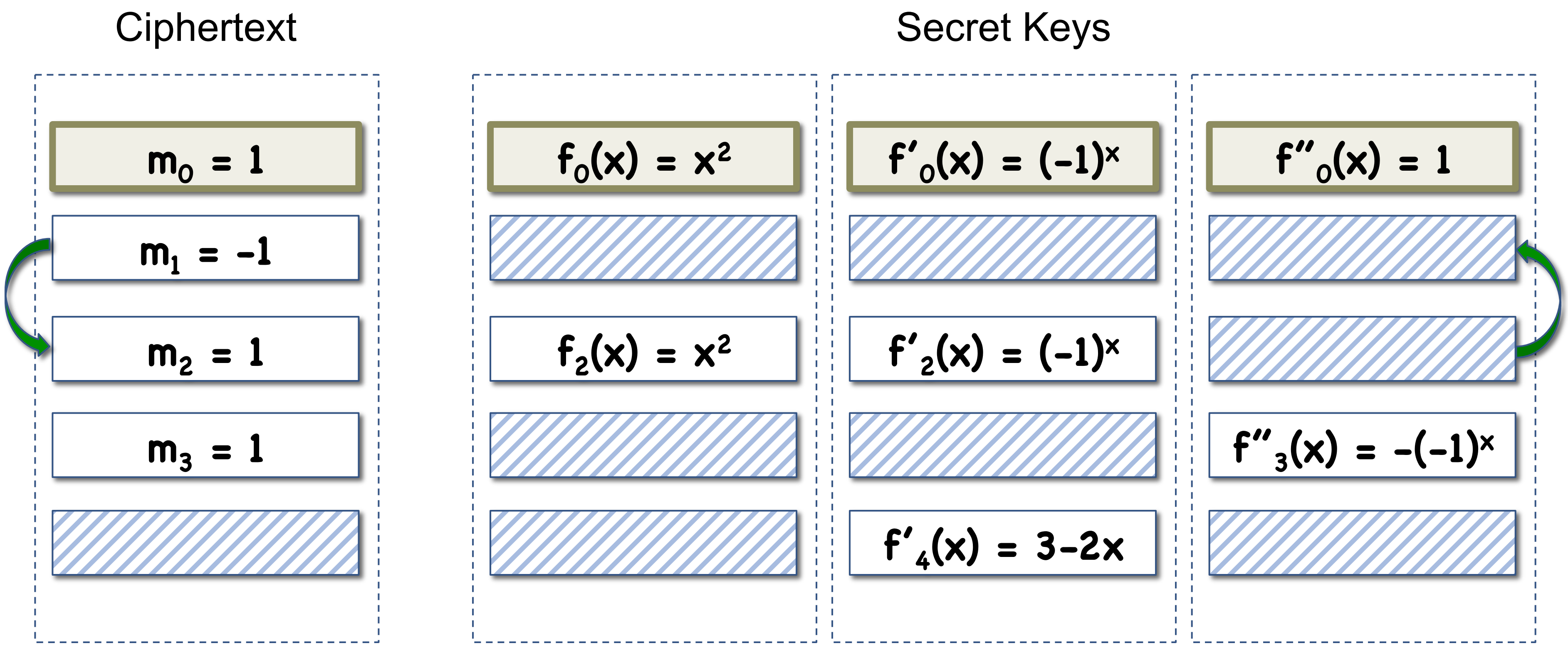
Slot Symmetry: Swap two slots (except slot **0**)



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 1$	$f_1(x) = x^2$	$f'_1(x) = (-1)^x$	▨
$m_2 = -1$	▨	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

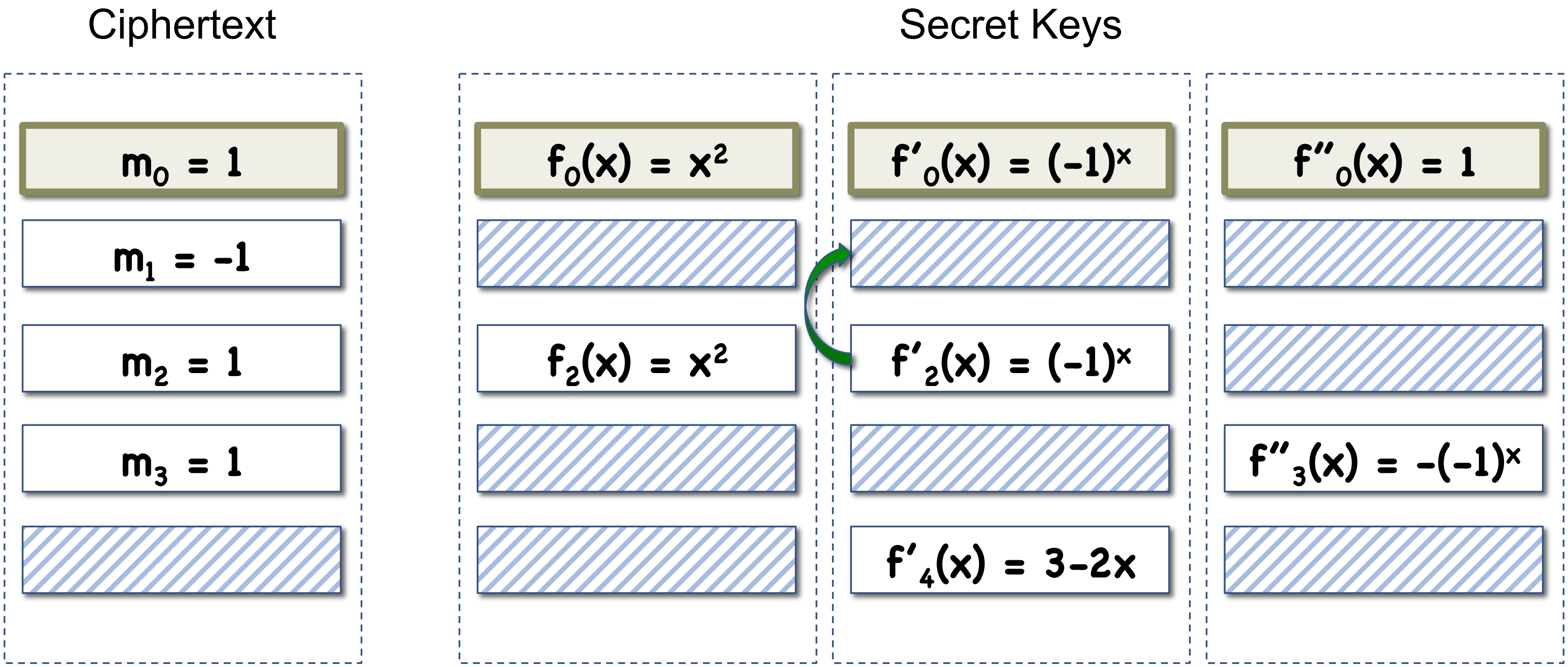
Slot Symmetry: Swap two slots (except slot **0**)



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	▨	▨
$m_2 = 1$	$f_2(x) = x^2$	$f'_2(x) = (-1)^x$	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

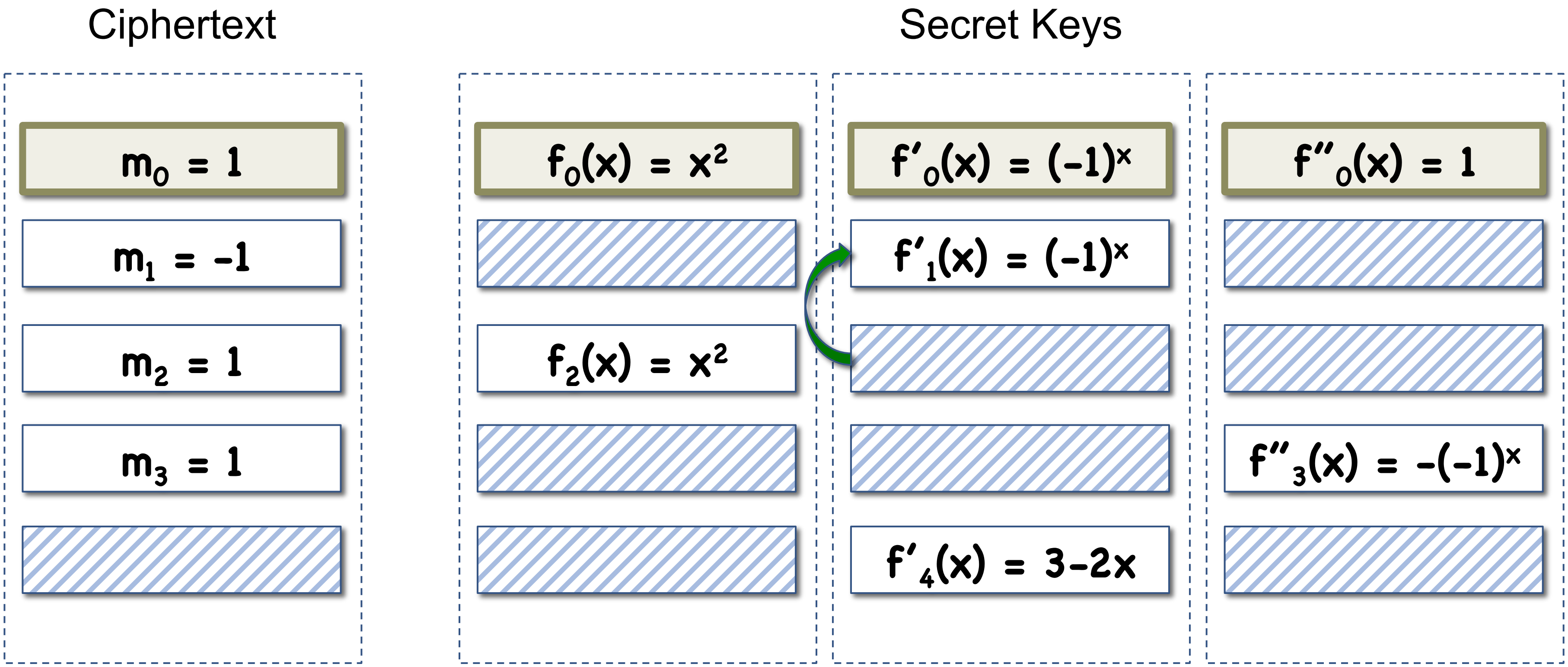
Strong Key Moving: Move any secret key slot into inactive slot (neither can be slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	▨	▨
$m_2 = 1$	$f_2(x) = x^2$	$f'_2(x) = (-1)^x$	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

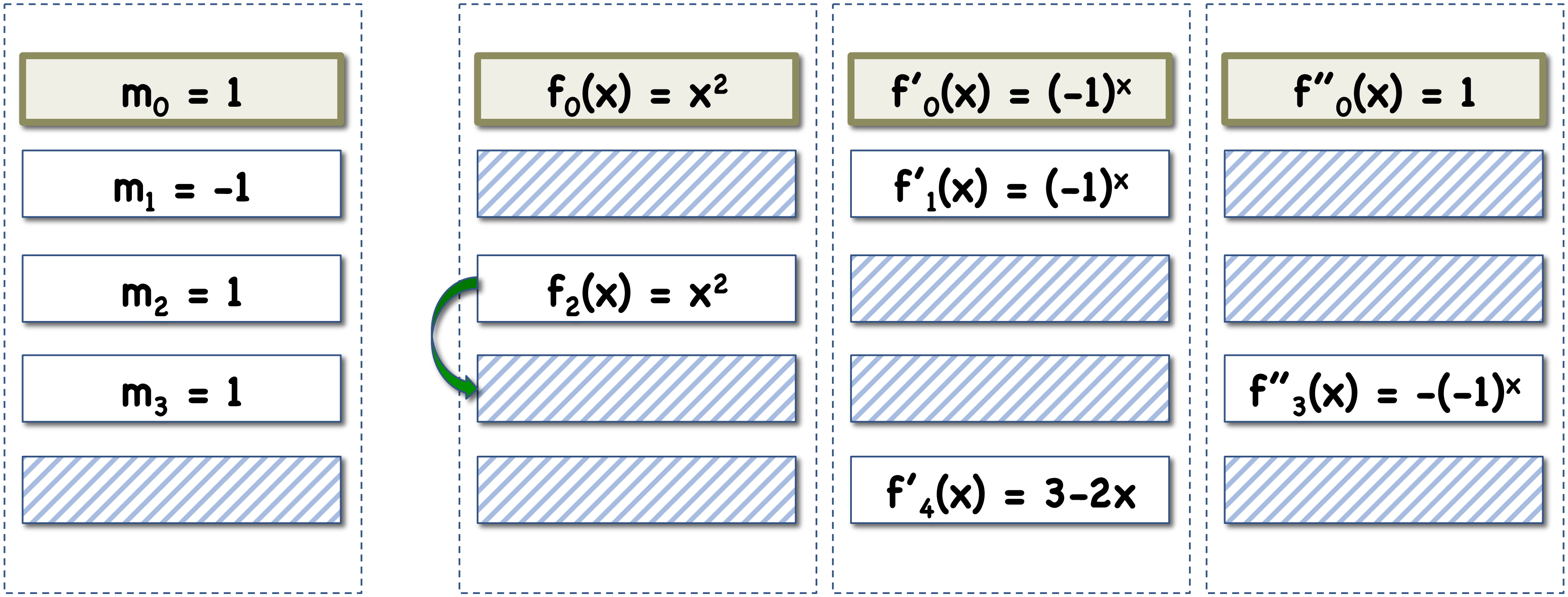
Strong Key Moving: Move any secret key slot into inactive slot (neither can be slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = (-1)^x$	▨
$m_2 = 1$	$f_2(x) = x^2$	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

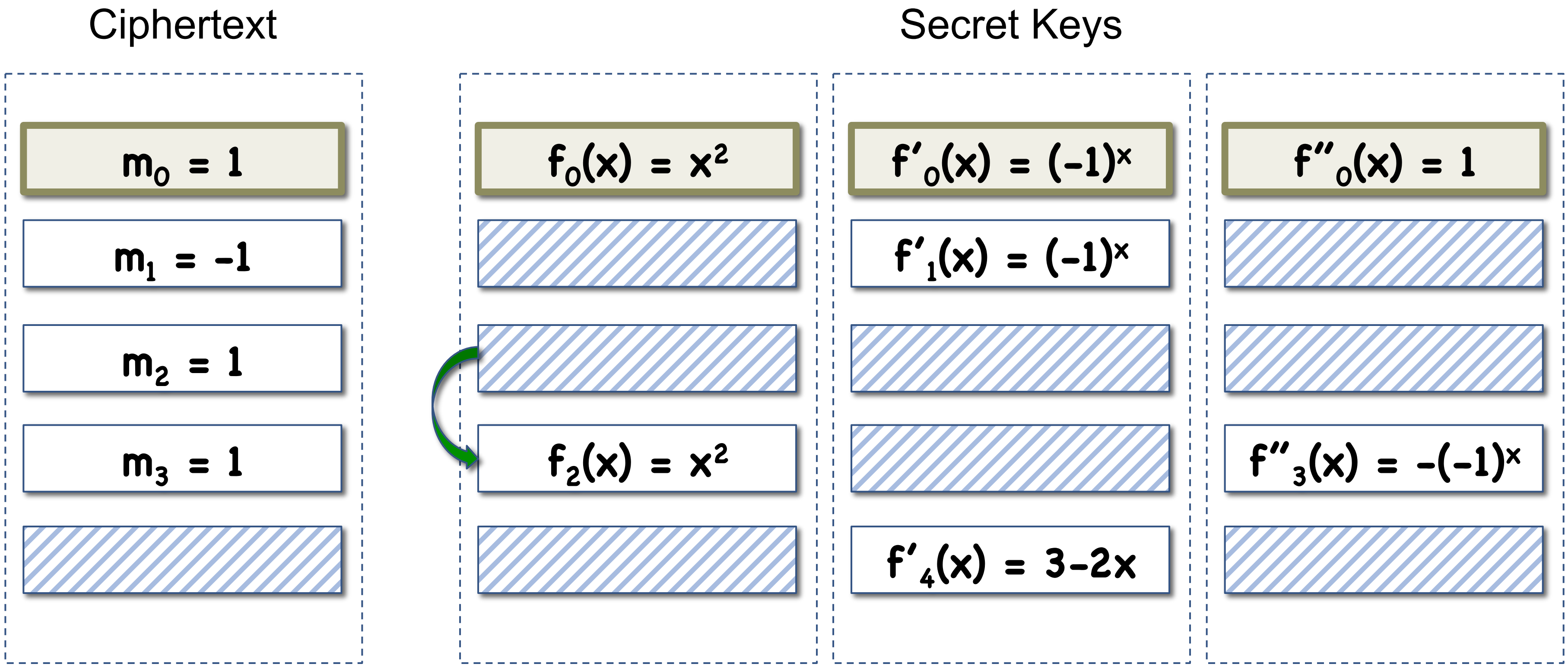
Weak Key Moving: Move any secret key slot into an empty slot (neither can be slot **0**) as long as **ciphertext identical**



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = (-1)^x$	▨
$m_2 = 1$	$f_2(x) = x^2$	▨	▨
$m_3 = 1$	▨	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

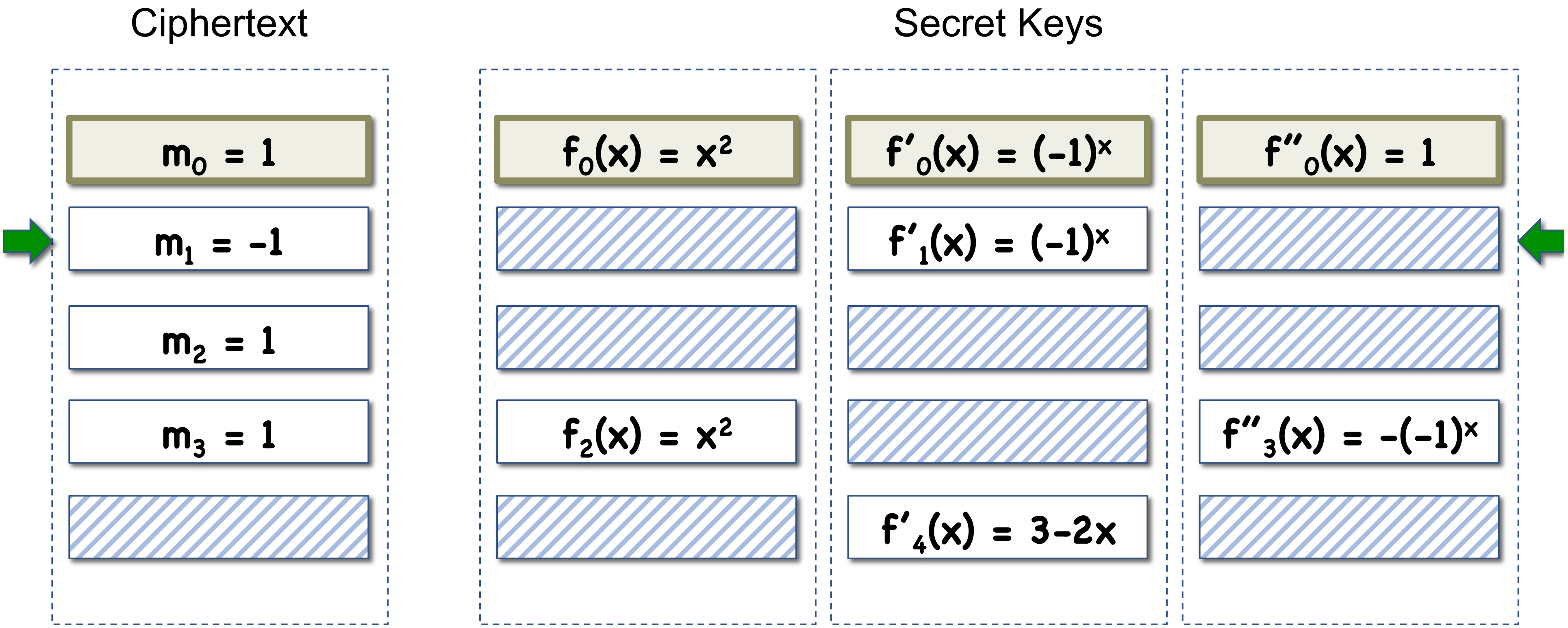
Weak Key Moving: Move any secret key slot into an empty slot (neither can be slot **0**) as long as **ciphertext identical**



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = (-1)^x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

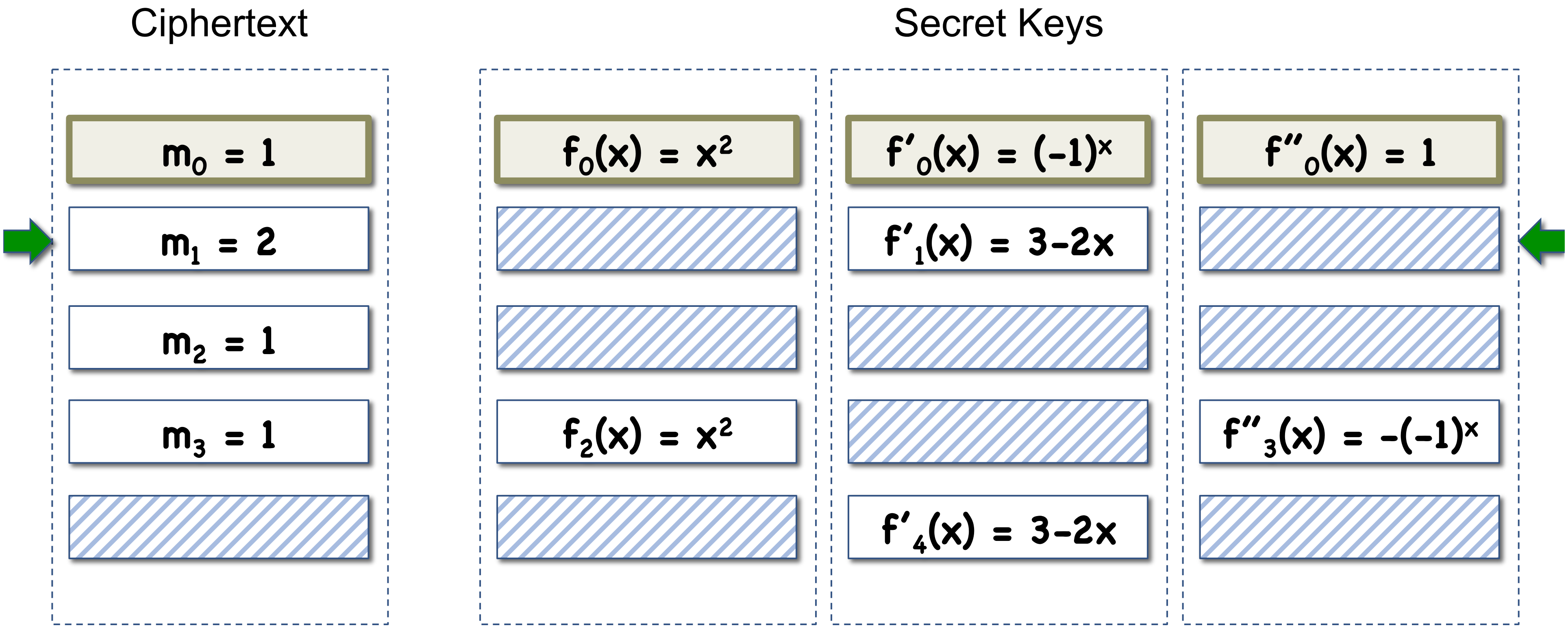
Single Use Hiding: Change ctxt and 1 sk in otherwise unused slot (except slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = (-1)^x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

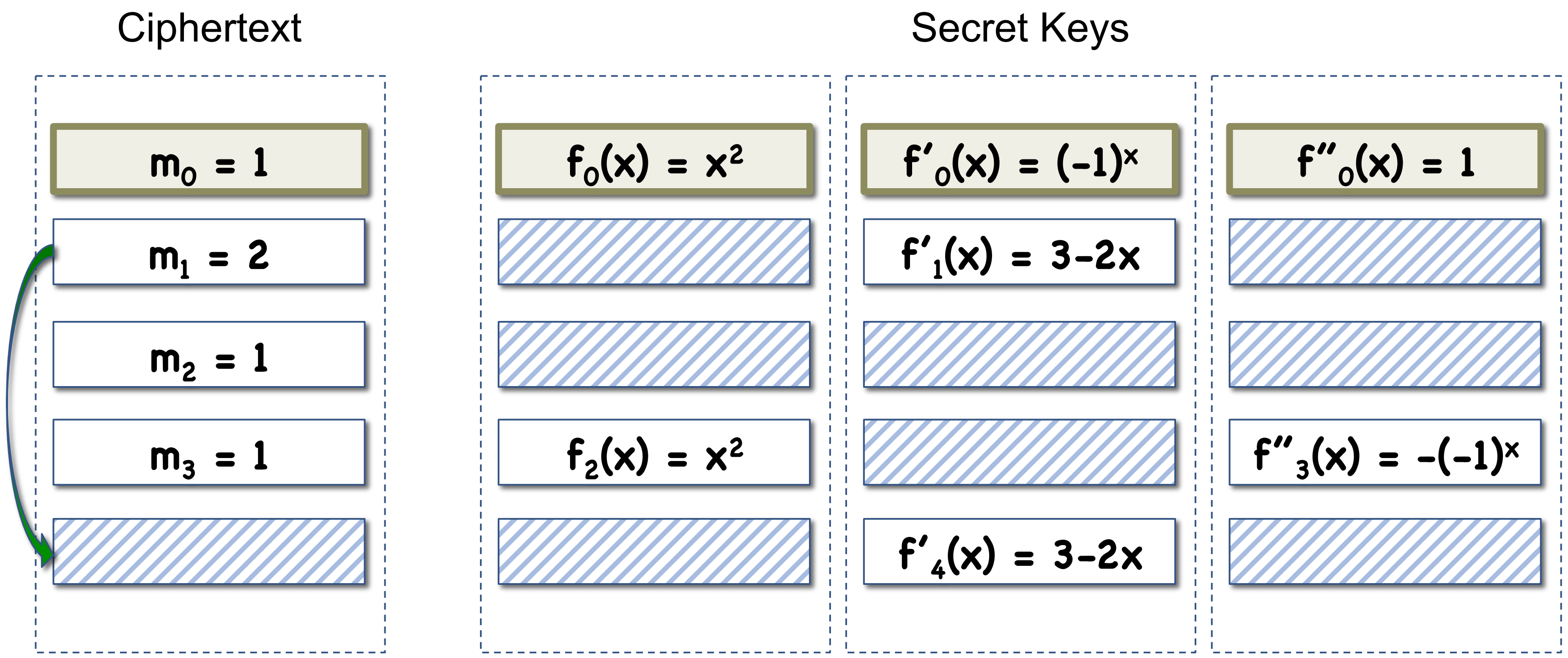
Single Use Hiding: Change ctxt and 1 sk in otherwise unused slot (except slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 2$	▨	$f'_1(x) = 3-2x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

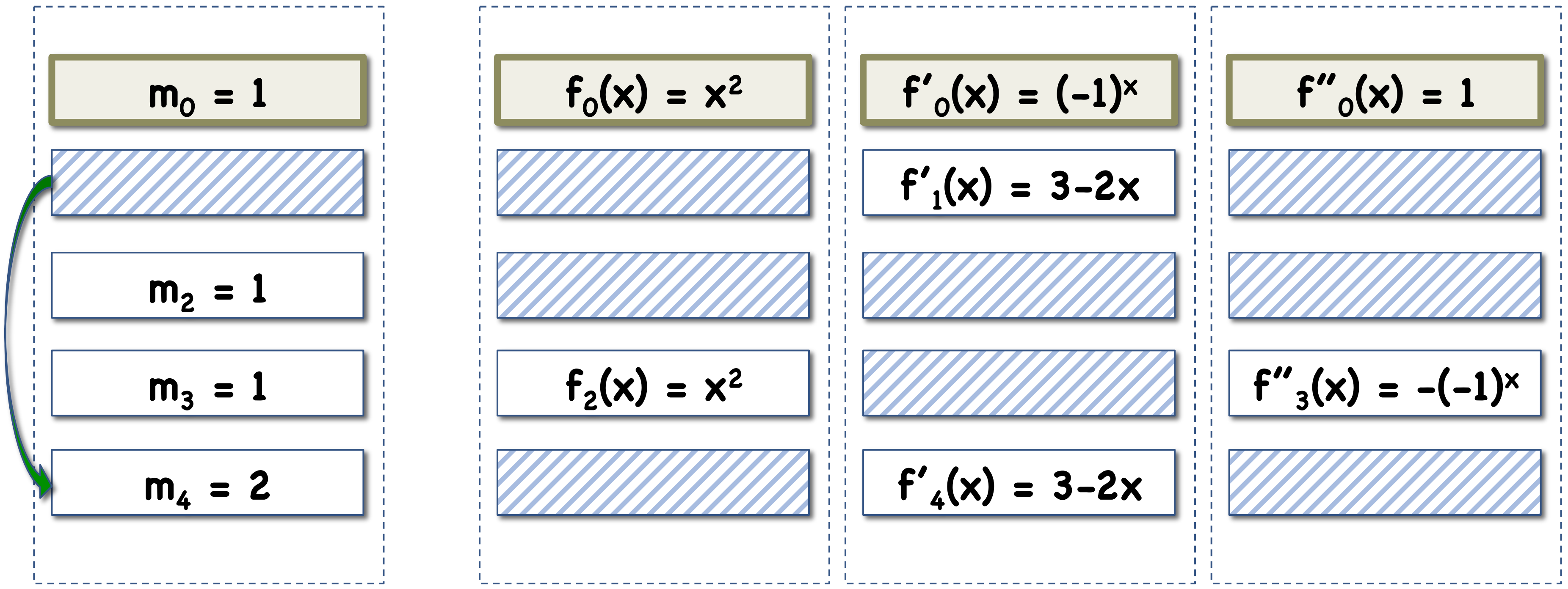
Ciphertext Moving: Move ciphertext into an empty slot (possibly slot **0**) as long as secret keys are all identical



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = 2$	▨	$f'_1(x) = 3-2x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
▨	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

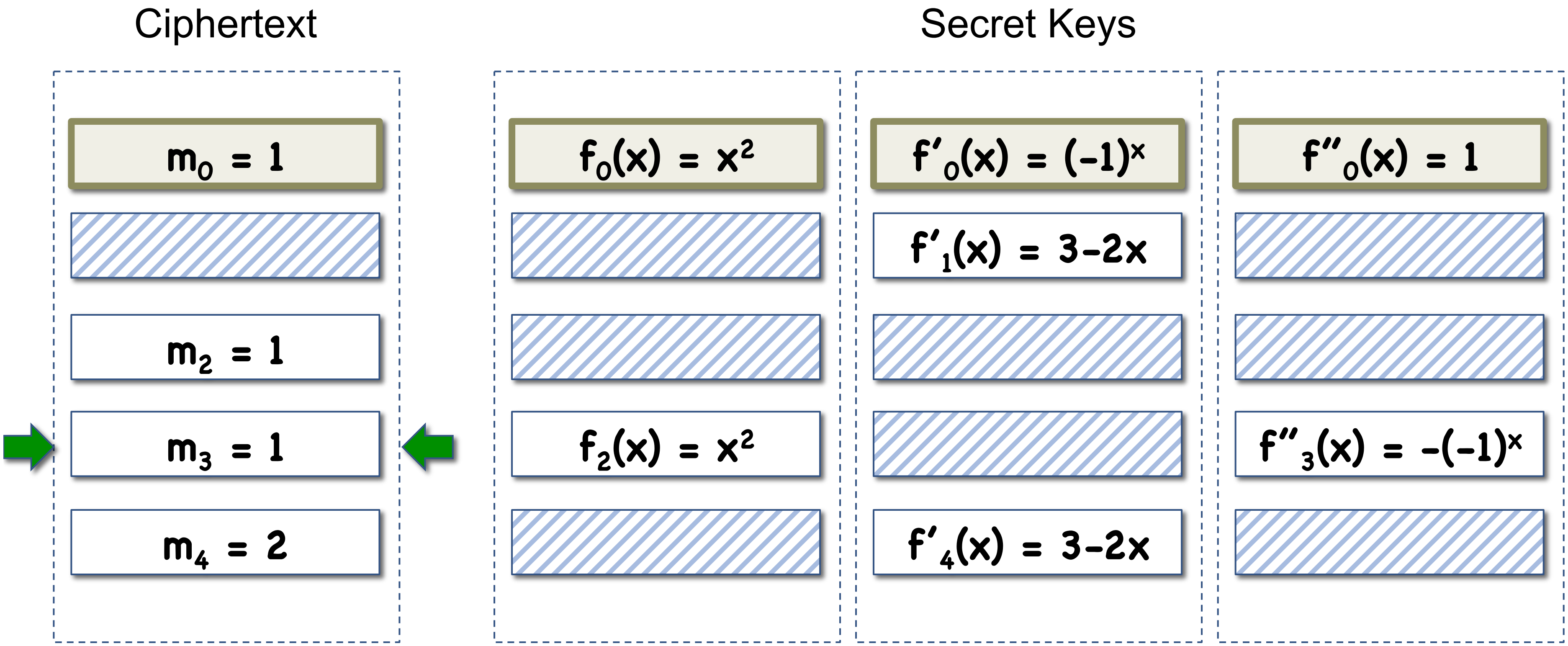
Ciphertext Moving: Move ciphertext into an empty slot (possibly slot **0**) as long as secret keys are all identical



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
▨	▨	$f'_1(x) = 3-2x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
$m_4 = 2$	▨	$f'_4(x) = 3-2x$	▨

Security of Slotted Functional Encryption

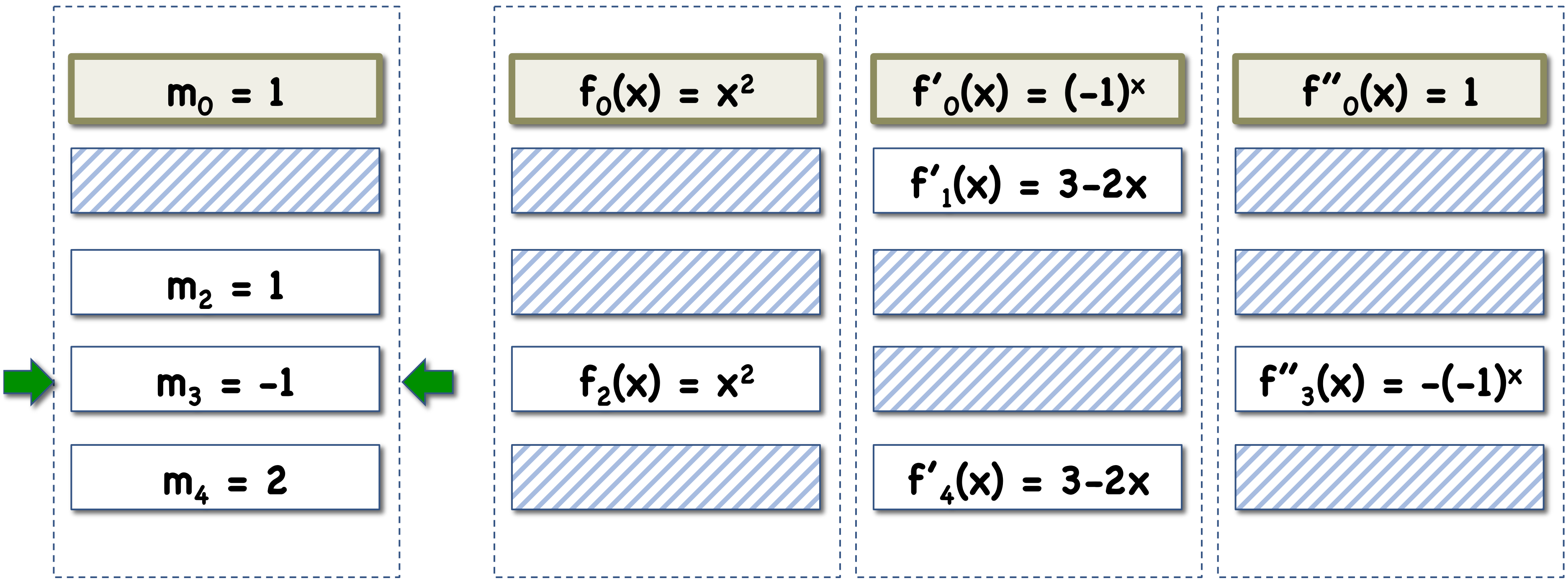
Weak Ciphertext Indistinguishability: change ciphertext slot (except slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
▨	▨	$f'_1(x) = 3-2x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = 1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
$m_4 = 2$	▨	$f'_4(x) = 3-2x$	▨

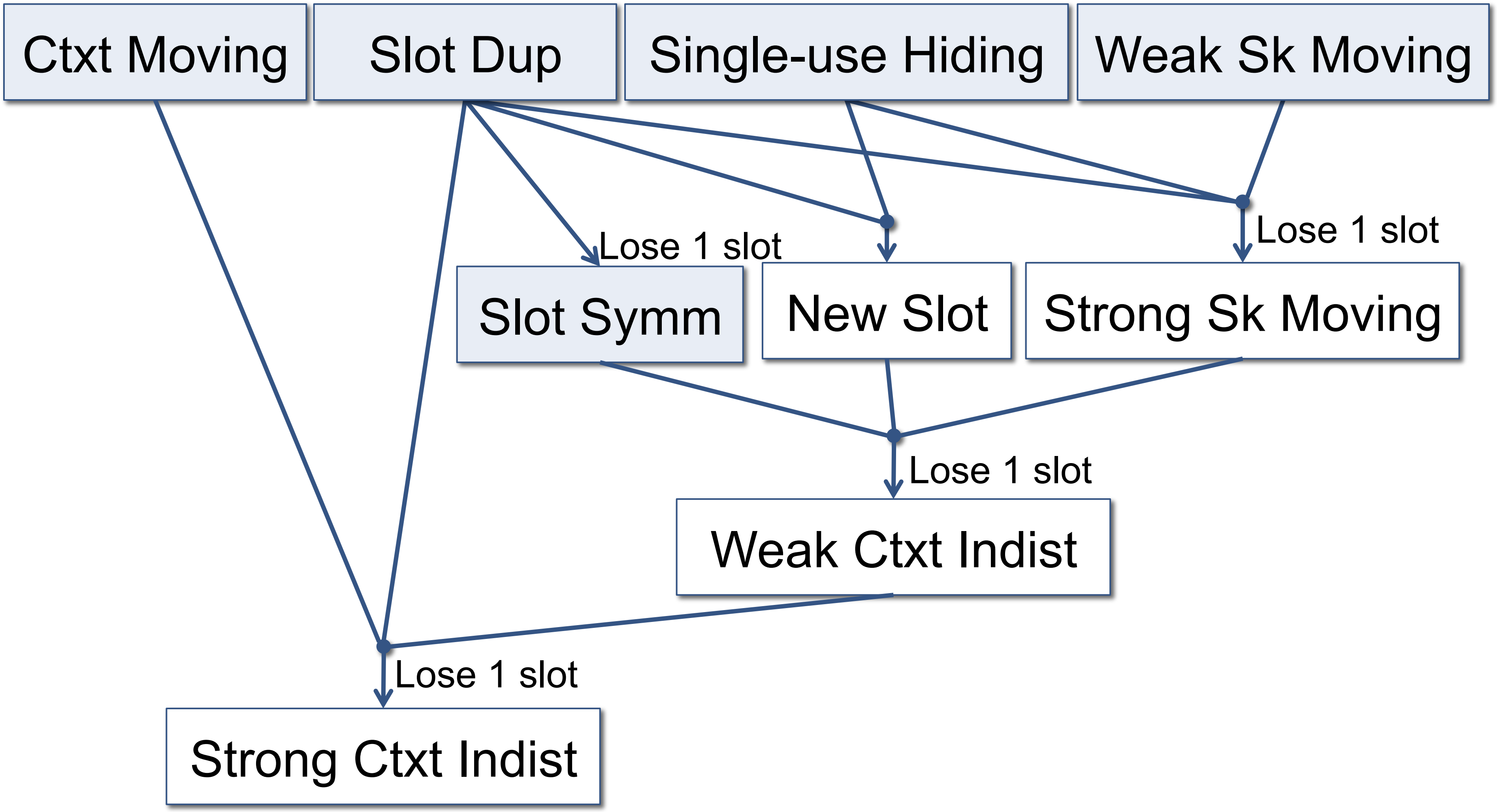
Security of Slotted Functional Encryption

Weak Ciphertext Indistinguishability: change ciphertext slot (except slot **0**) as long as decryption unaffected



Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
▨	▨	$f'_1(x) = 3-2x$	▨
$m_2 = 1$	▨	▨	▨
$m_3 = -1$	$f_2(x) = x^2$	▨	$f''_3(x) = -(-1)^x$
$m_4 = 2$	▨	$f'_4(x) = 3-2x$	▨

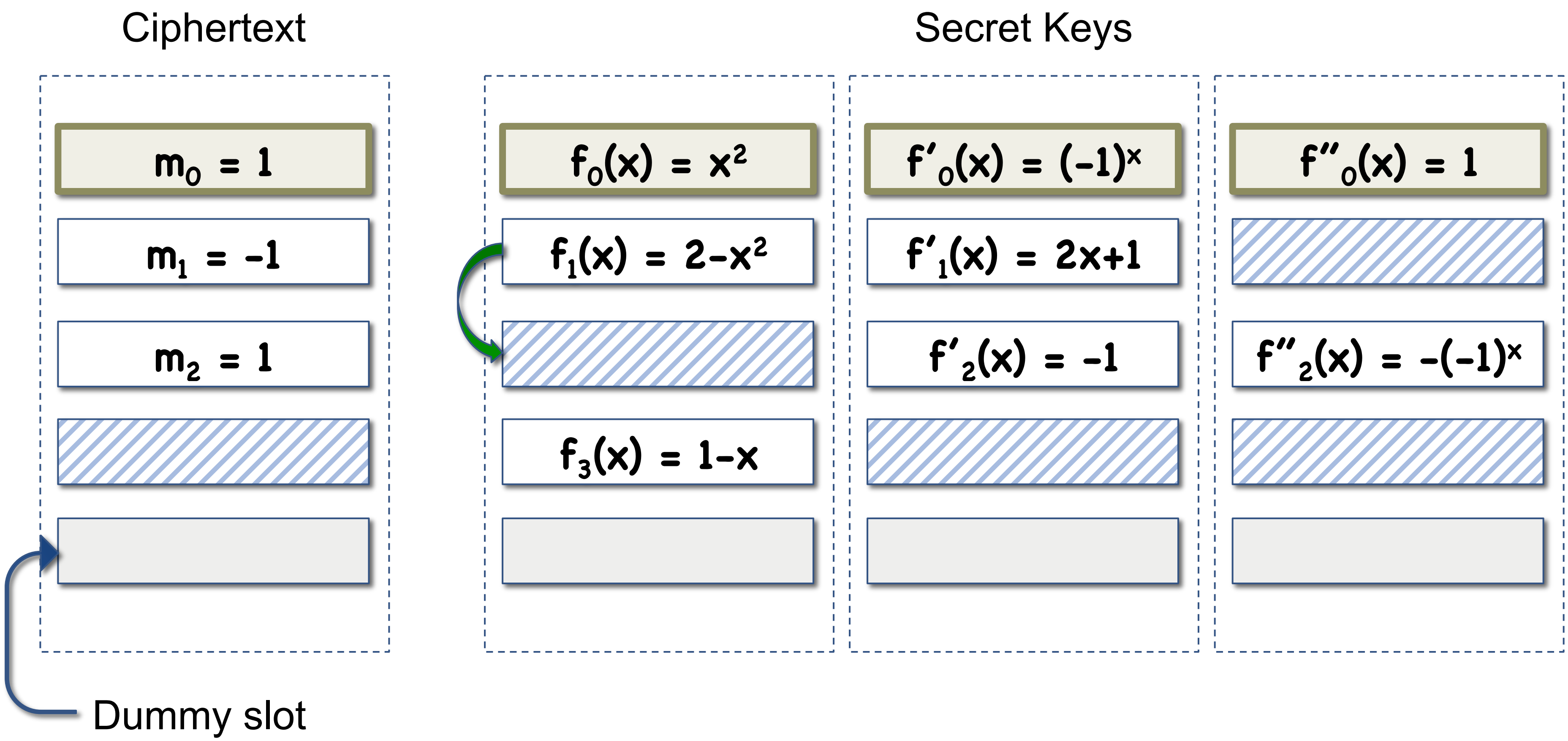
Reductions!



Sanity Check: Slot 0 in secret keys cannot change ⇒ no function hiding

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**



Ciphertext

Secret Keys

$m_0 = 1$

$m_1 = -1$

$m_2 = 1$

$f_0(x) = x^2$

$f_1(x) = 2-x^2$

$f_3(x) = 1-x$

$f'_0(x) = (-1)^x$

$f'_1(x) = 2x+1$

$f'_2(x) = -1$

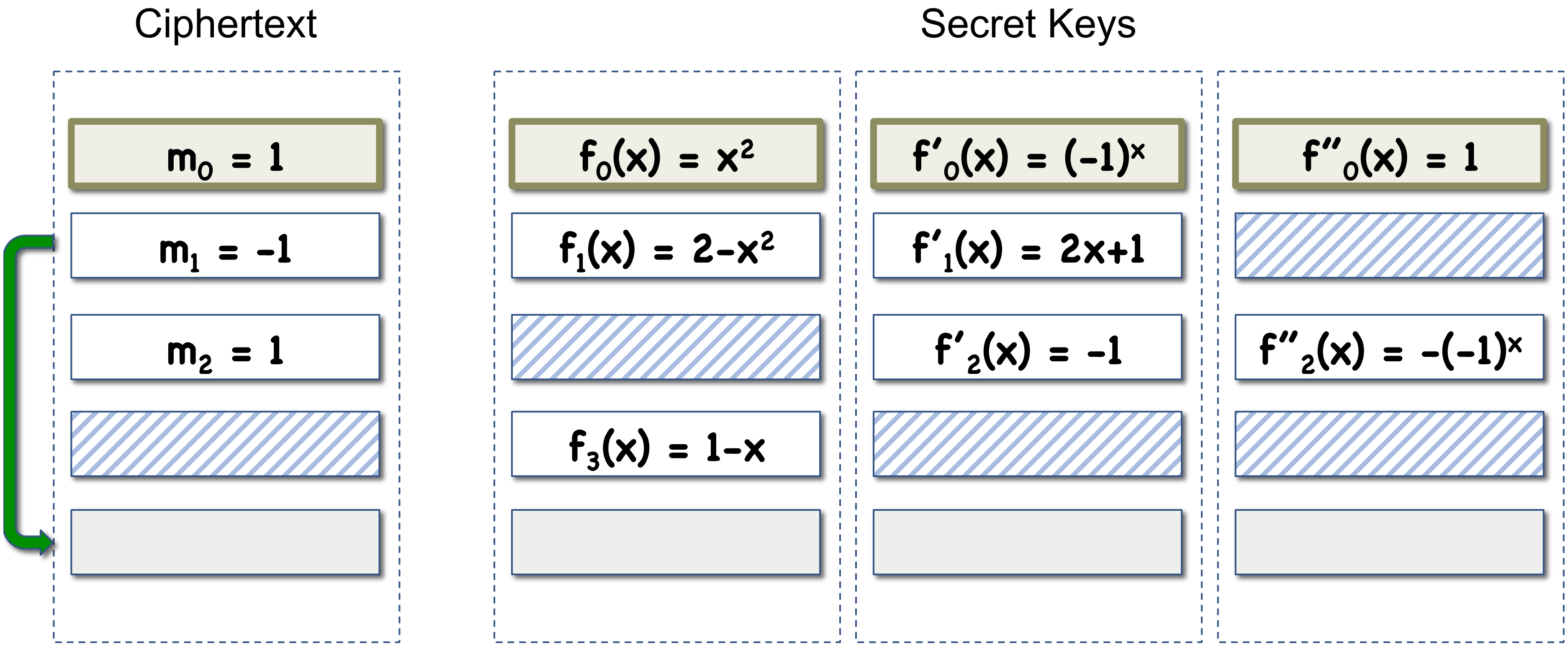
$f''_0(x) = 1$

$f''_2(x) = -(-1)^x$

Dummy slot

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

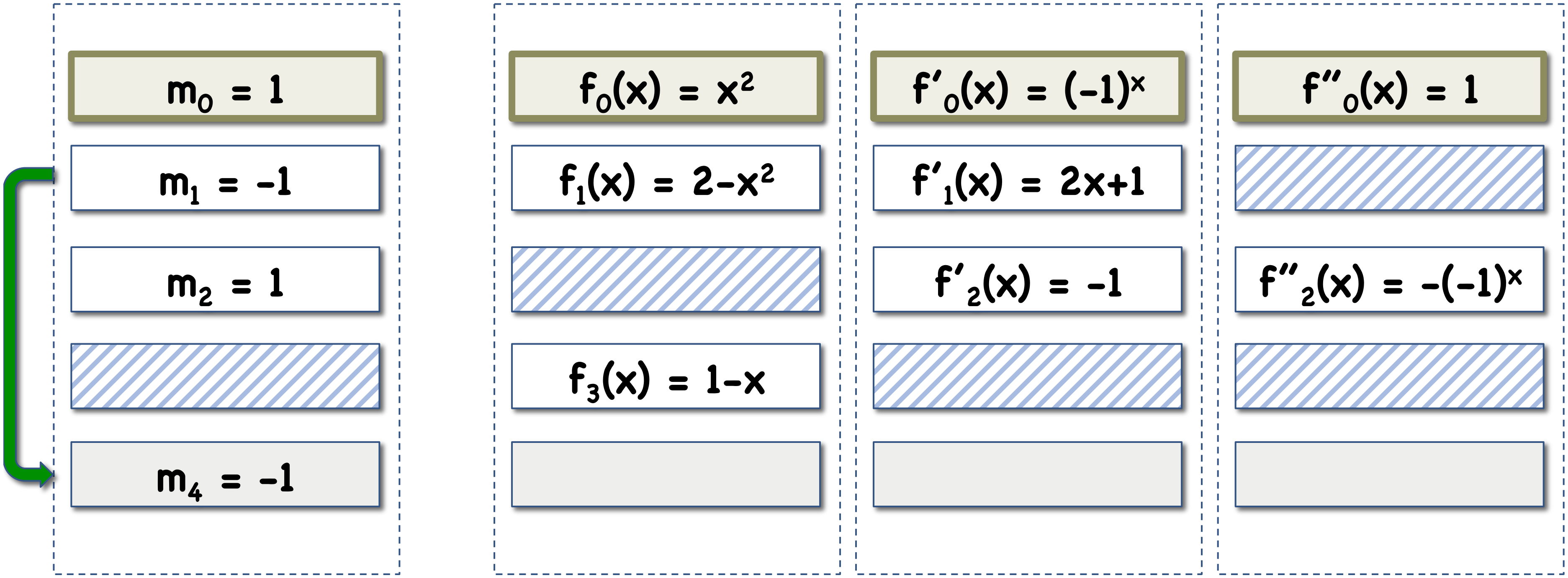


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

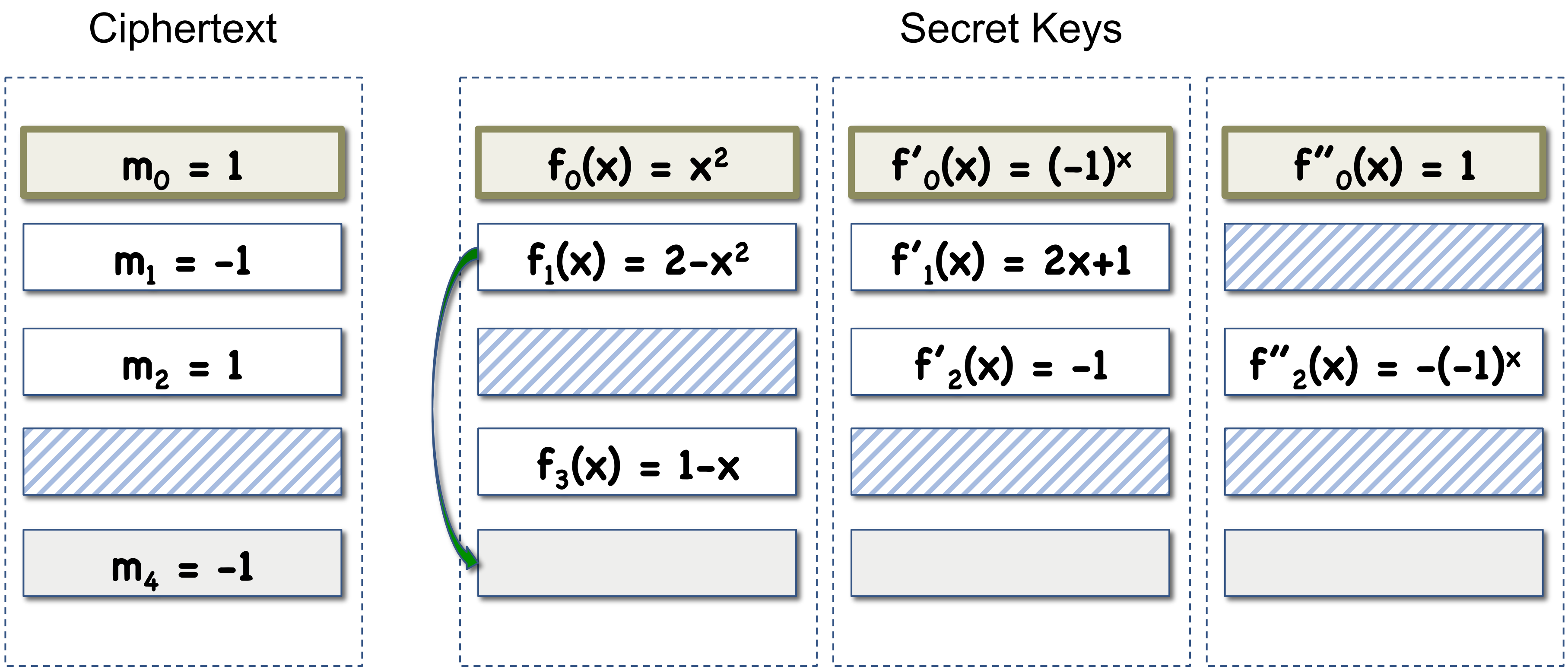


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$			

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

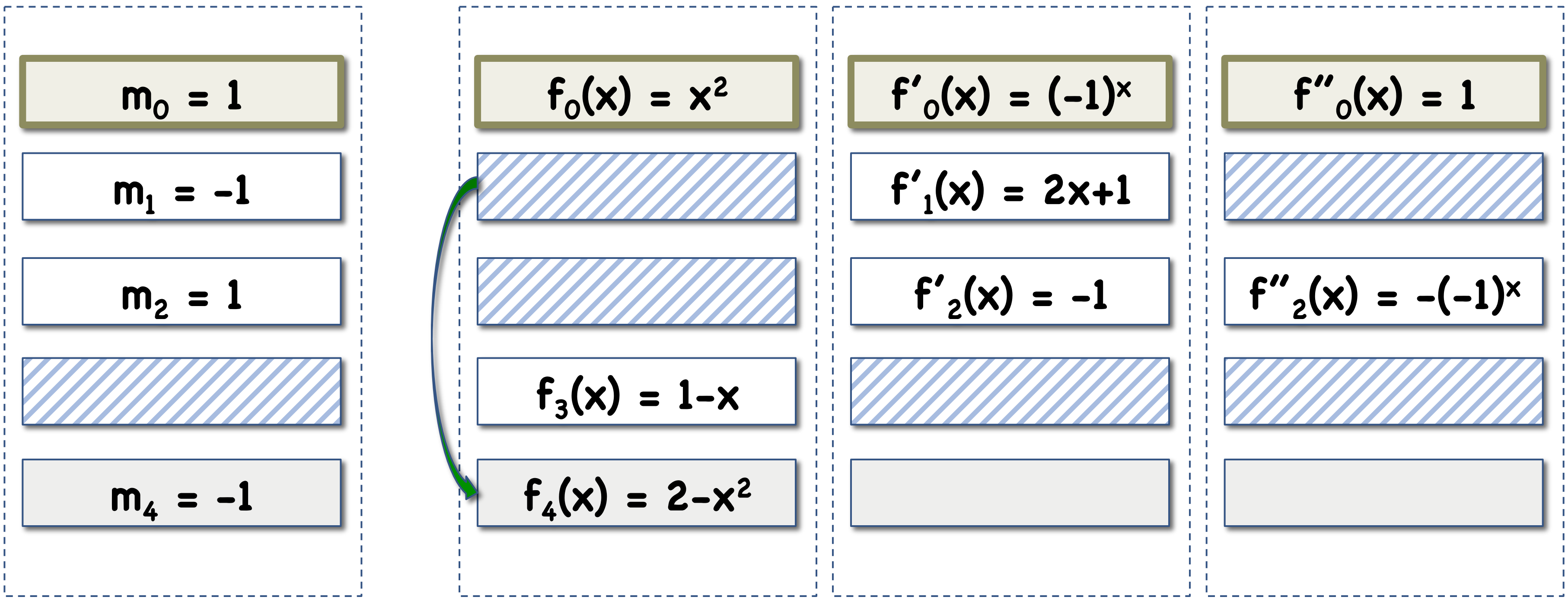


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	$f_1(x) = 2-x^2$	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$			

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

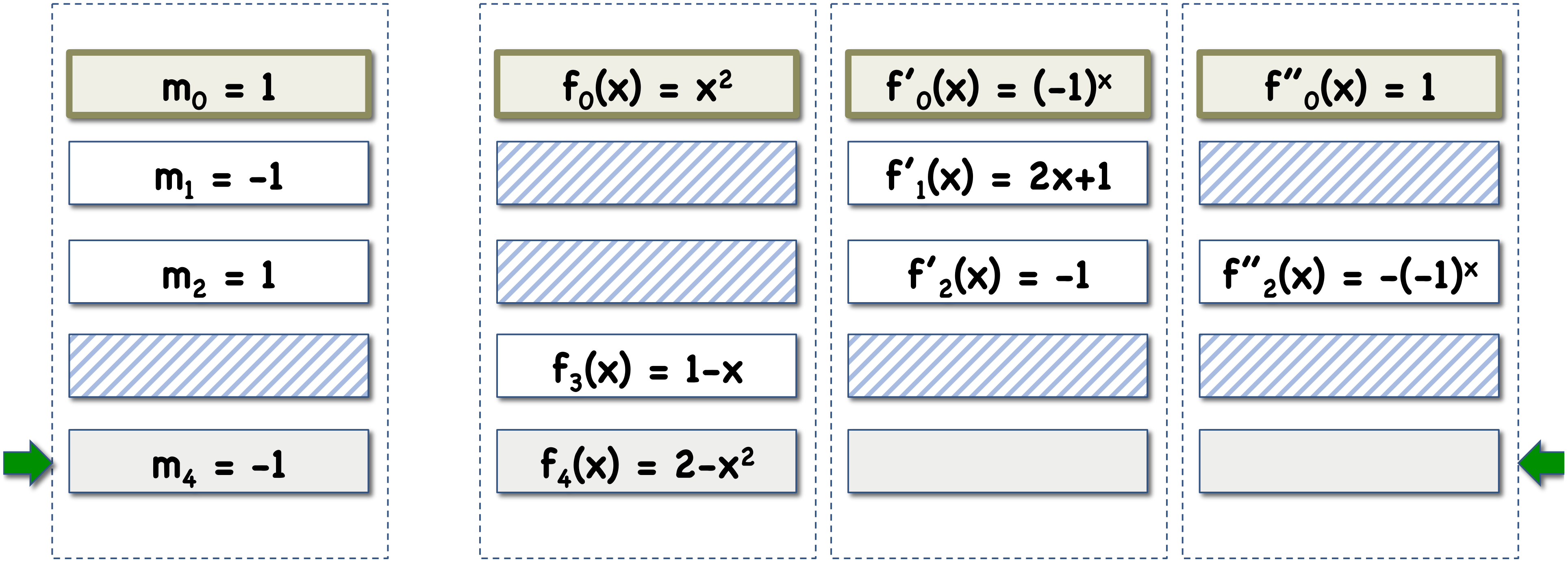


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

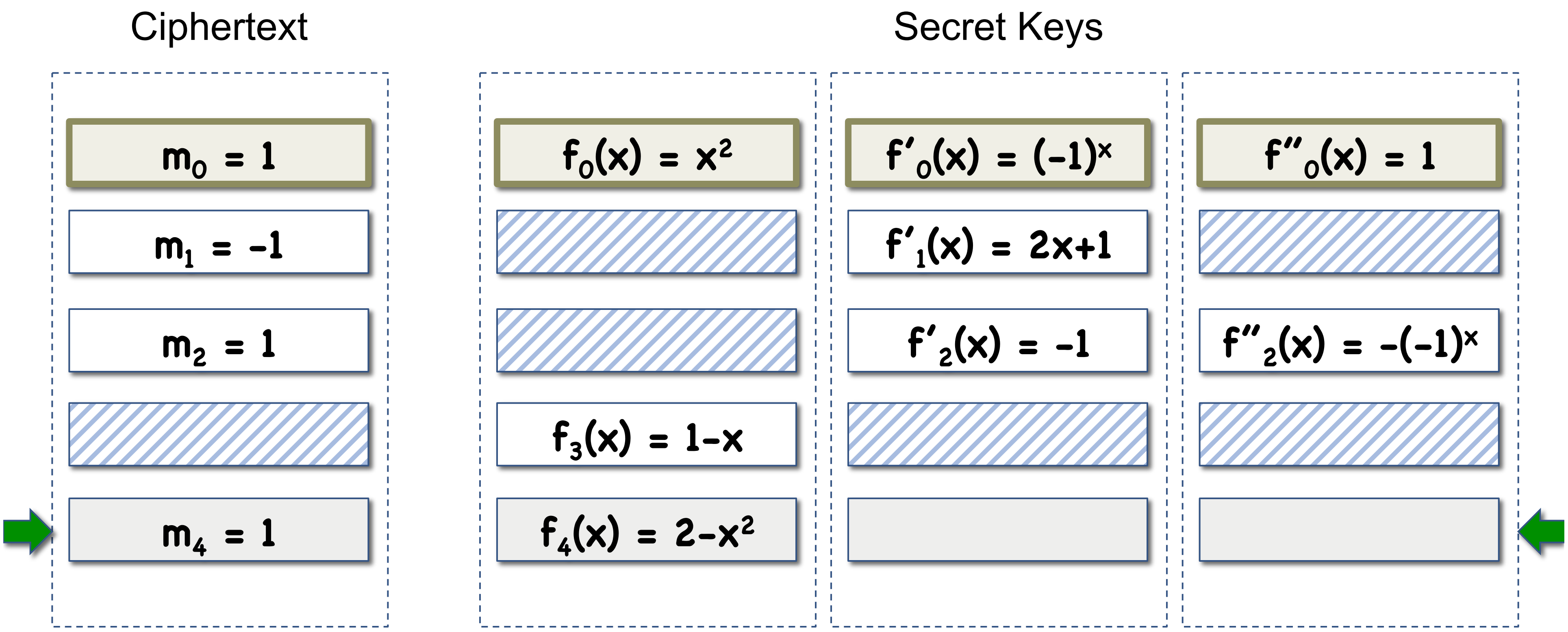


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Single Use Hiding

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

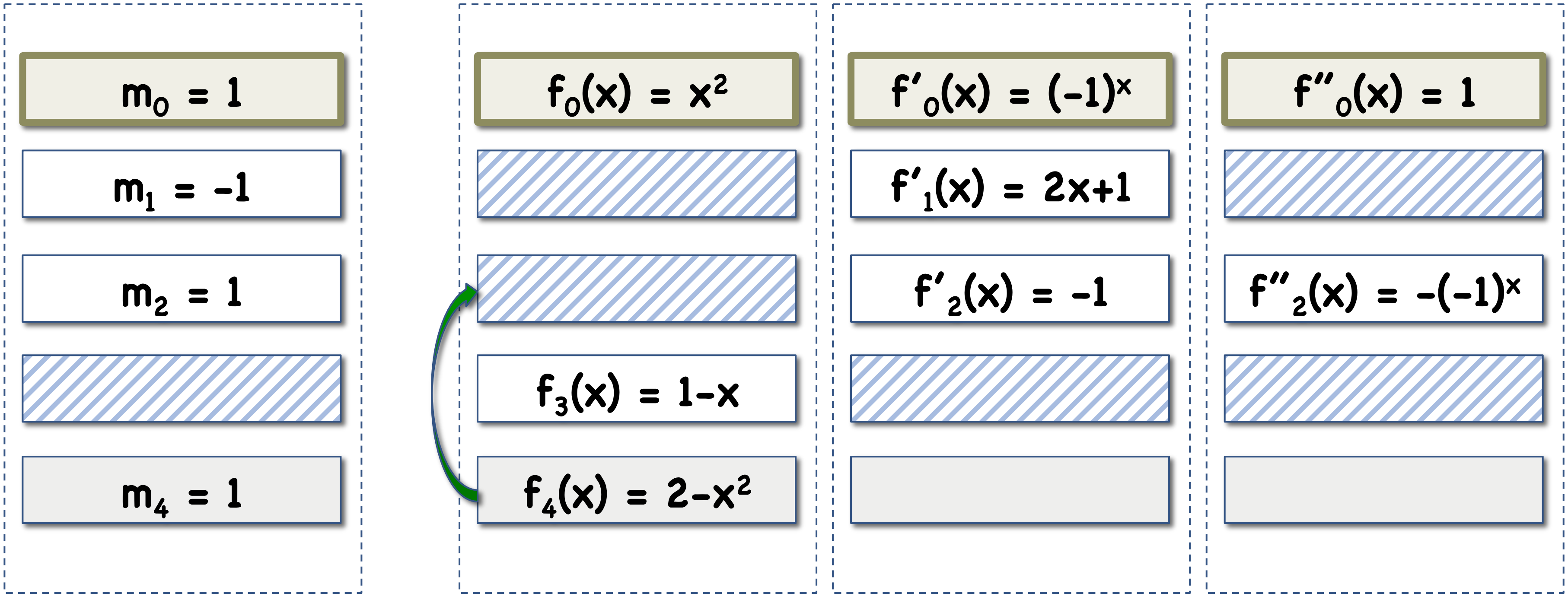


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$	$f_4(x) = 2-x^2$		

Single Use Hiding

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

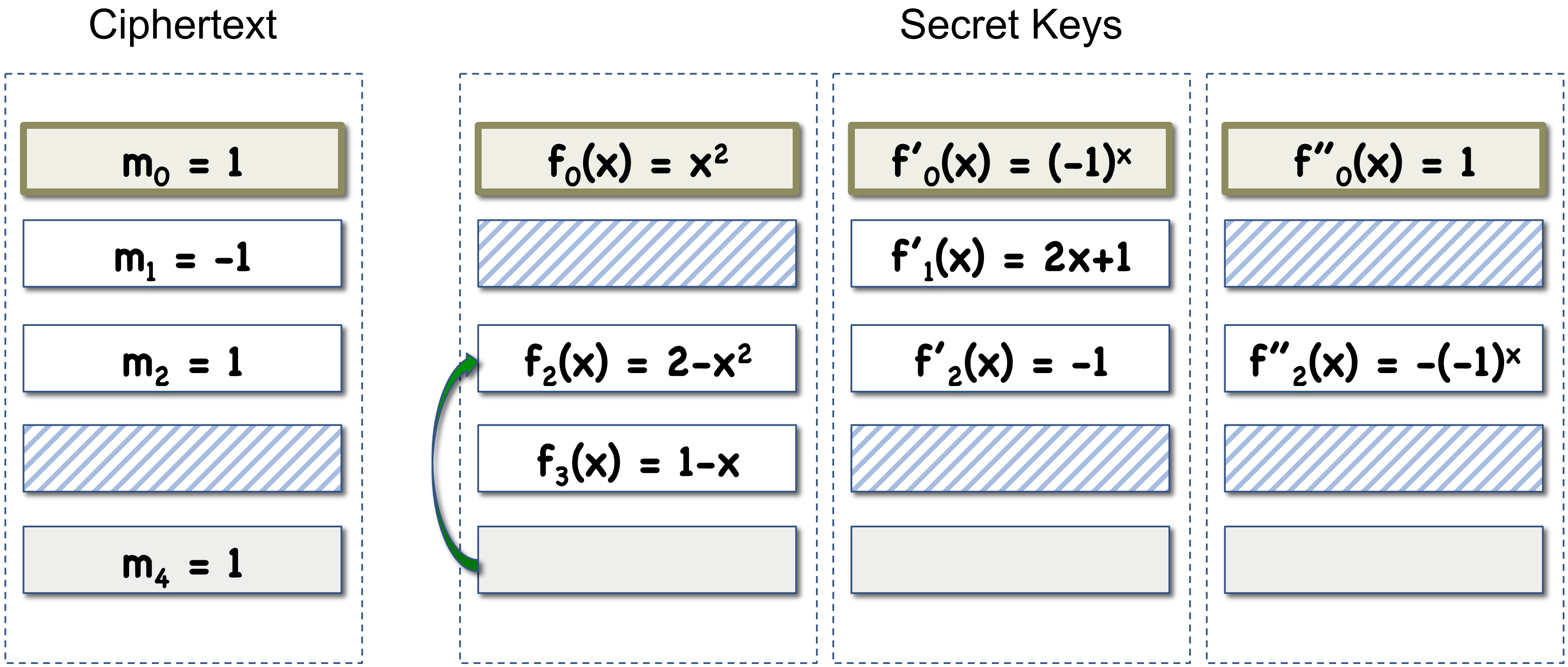


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$	$f_4(x) = 2-x^2$		

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

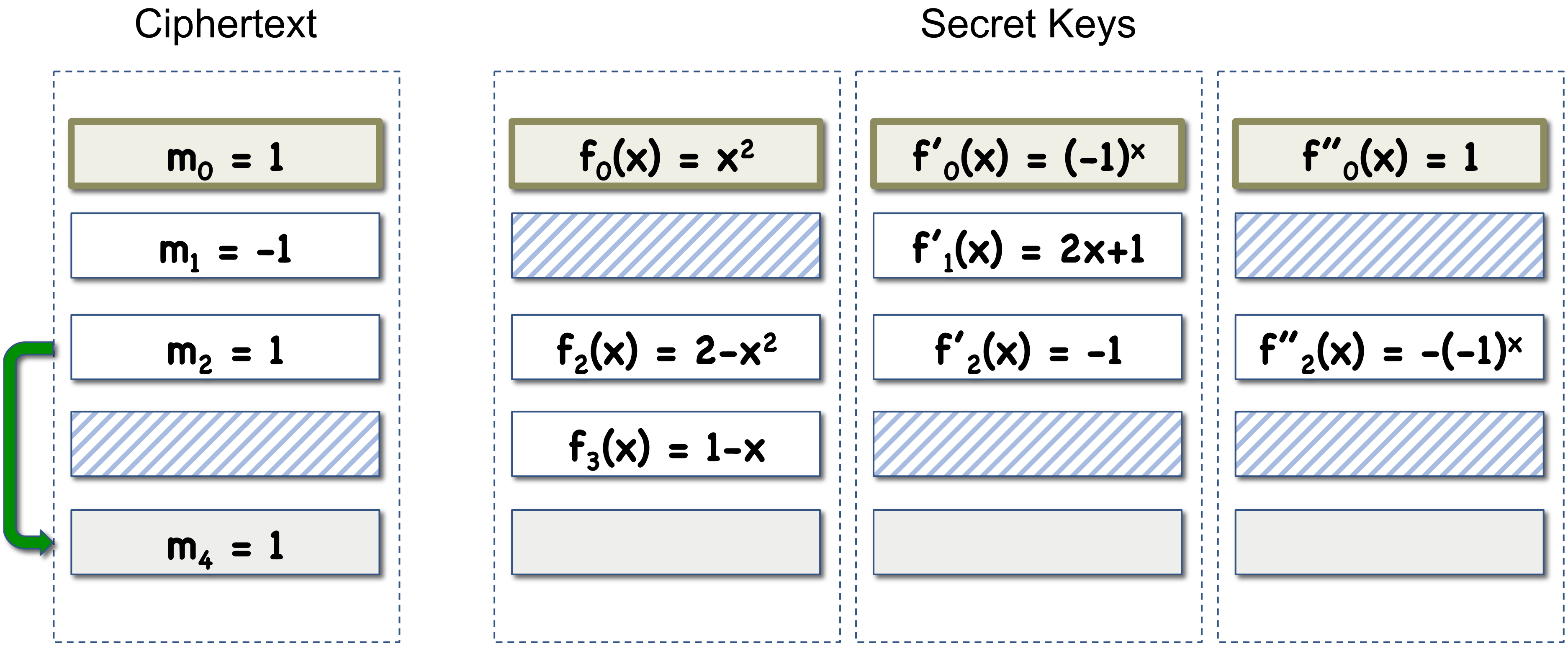


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$			

Weak Sk Moving

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

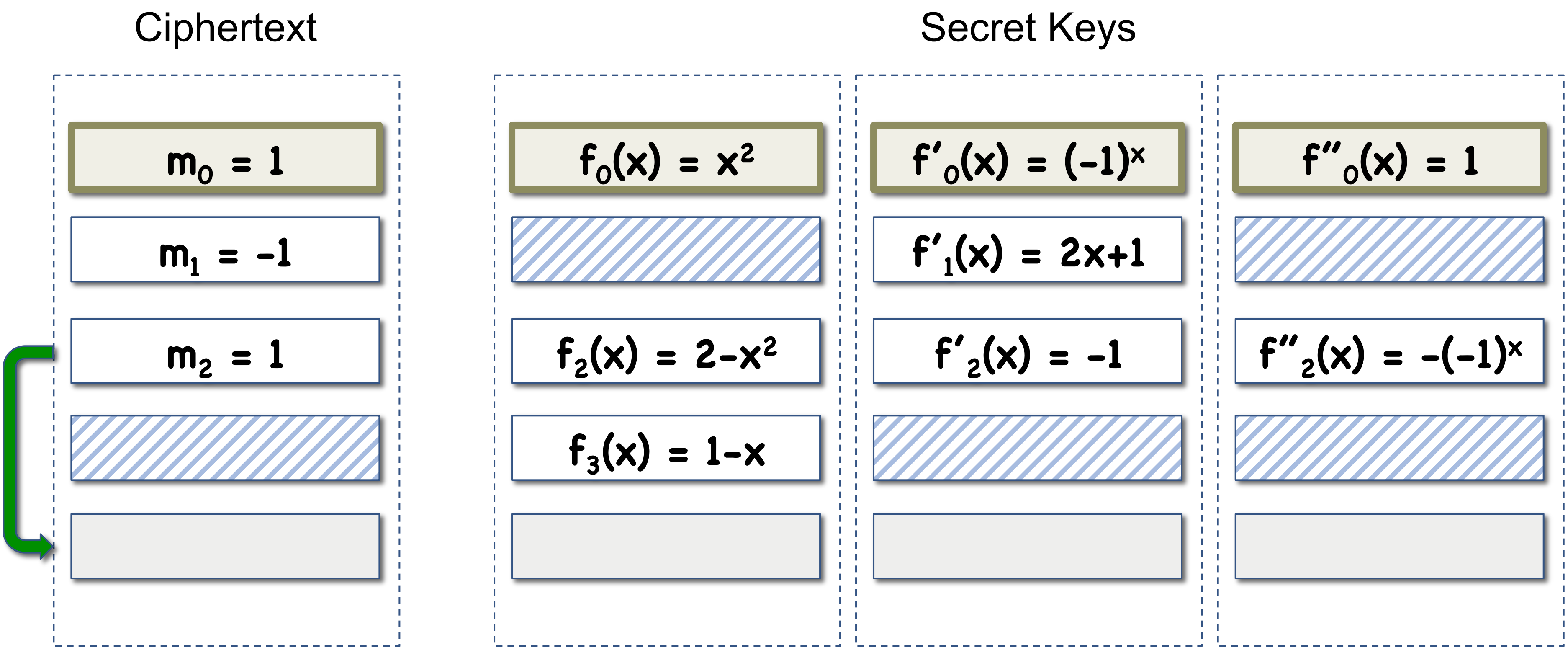


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = 1$			

Slot Duplication

Example Reduction: Strong Sk Moving

Goal: move $\mathbf{f_1}$ to slot **3**

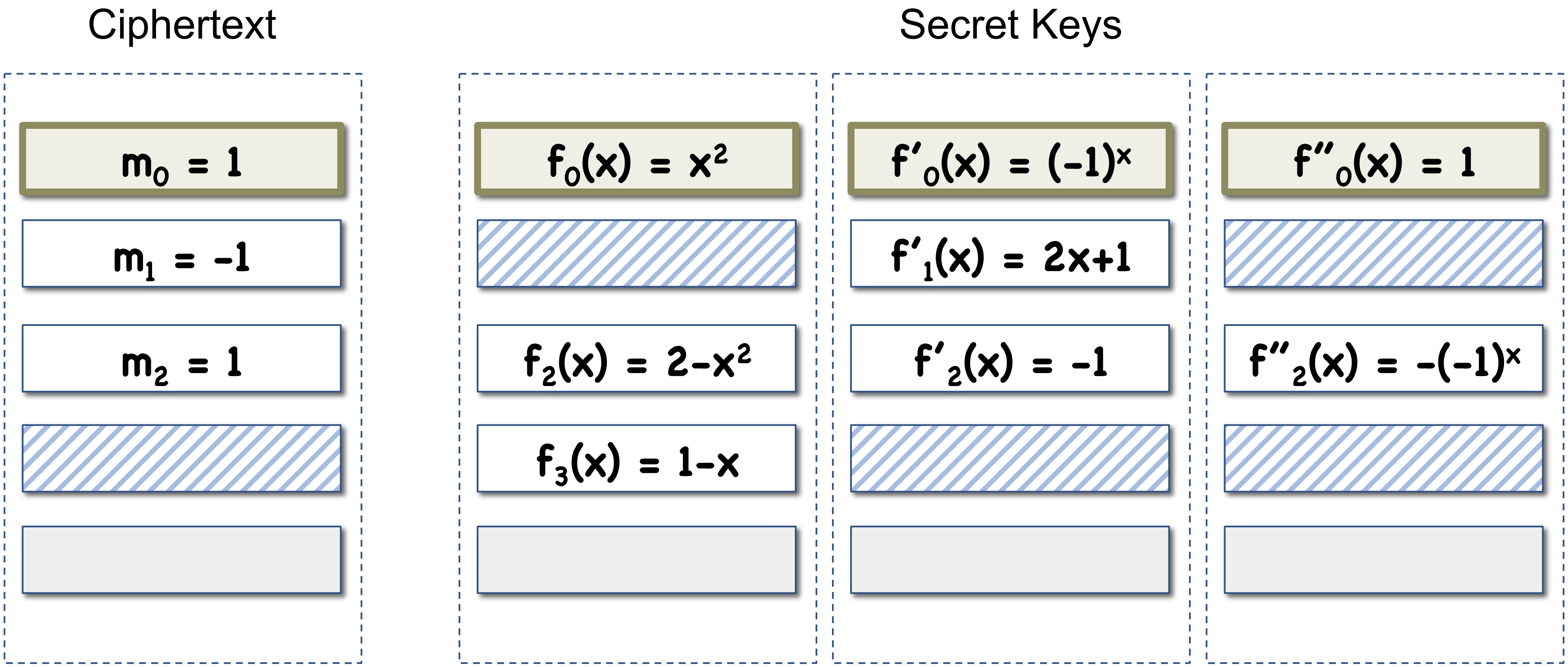


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Slot Duplication

Example Reduction: Strong Sk Moving

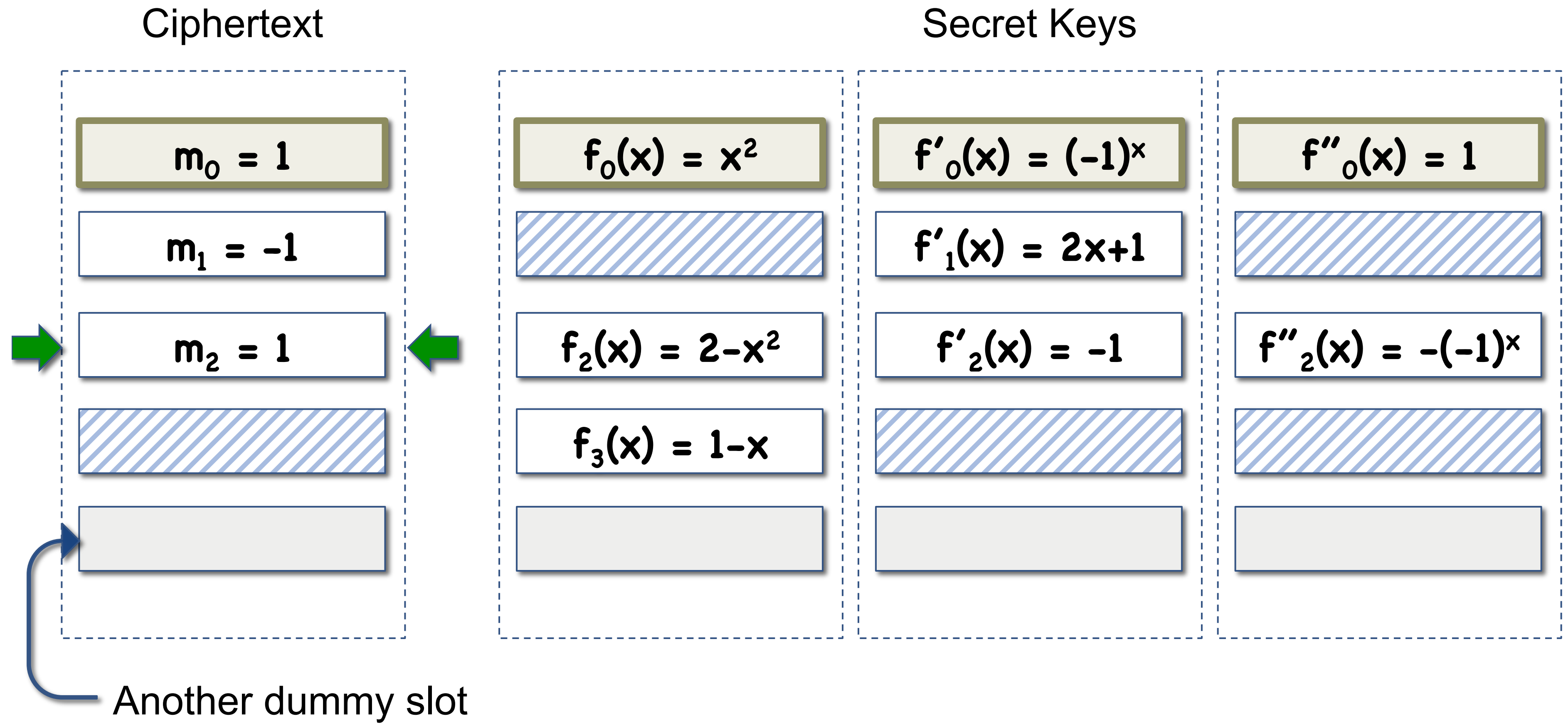
Goal: move $\mathbf{f_1}$ to slot **3**



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

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

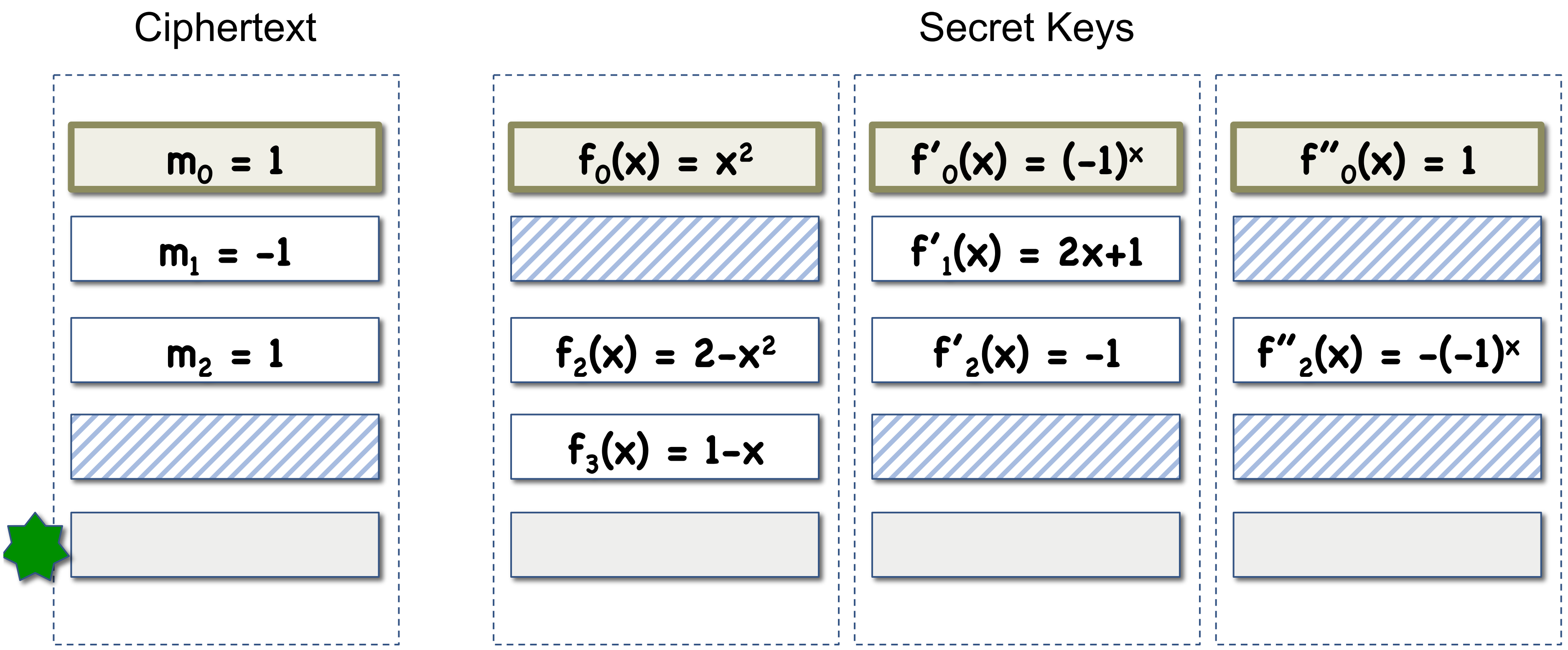


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Another dummy slot

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

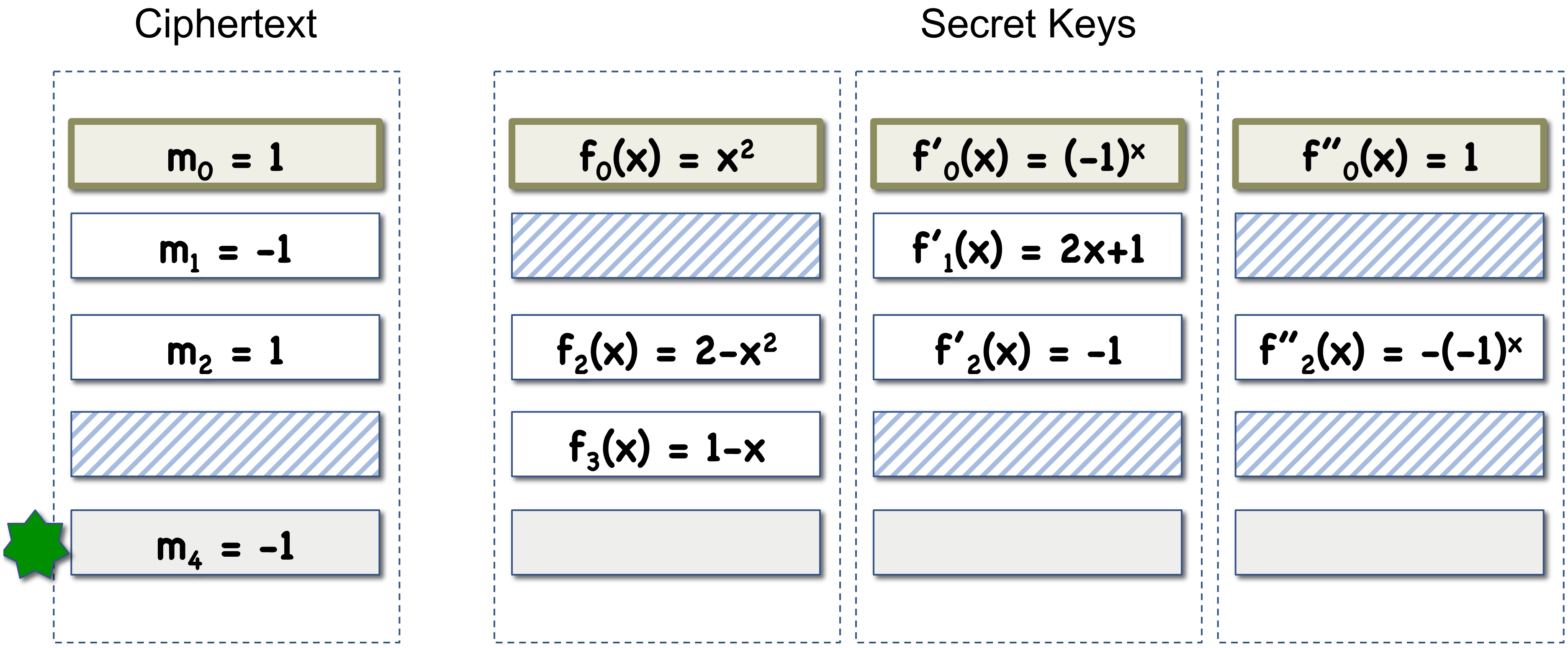


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

New Slot

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

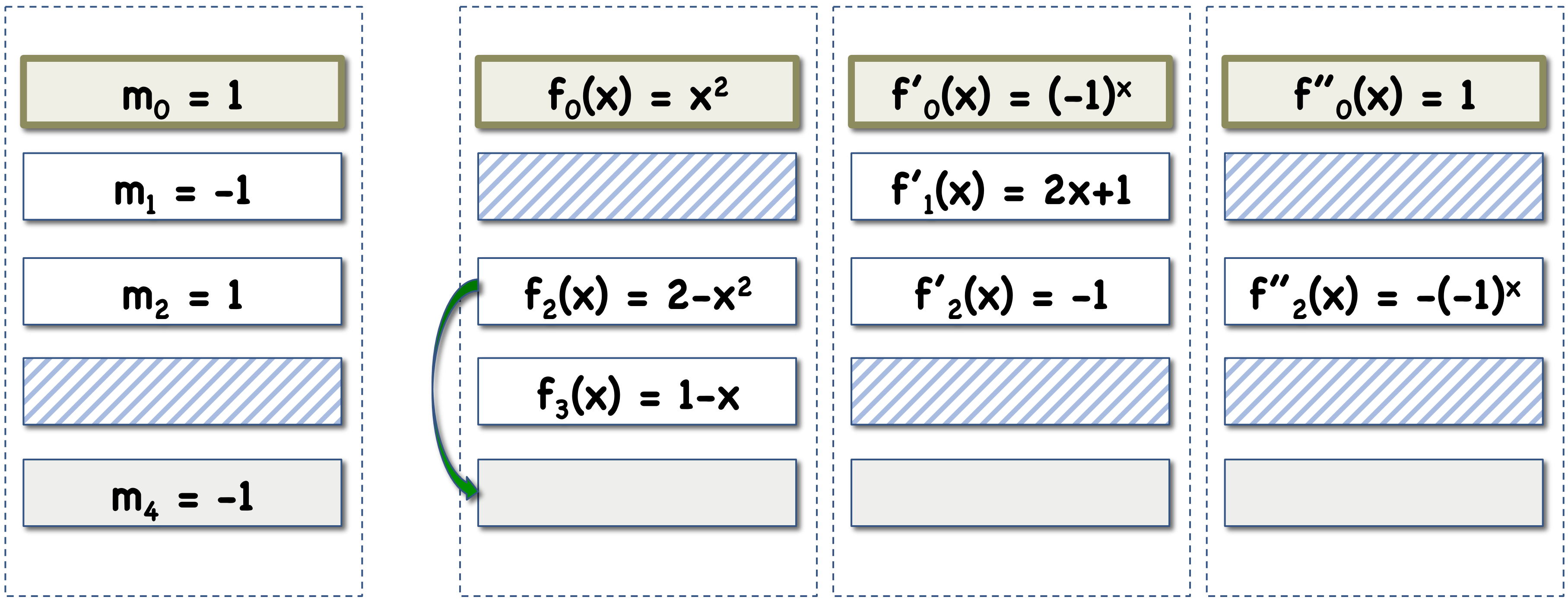


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
✶ $m_4 = -1$			

New Slot

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

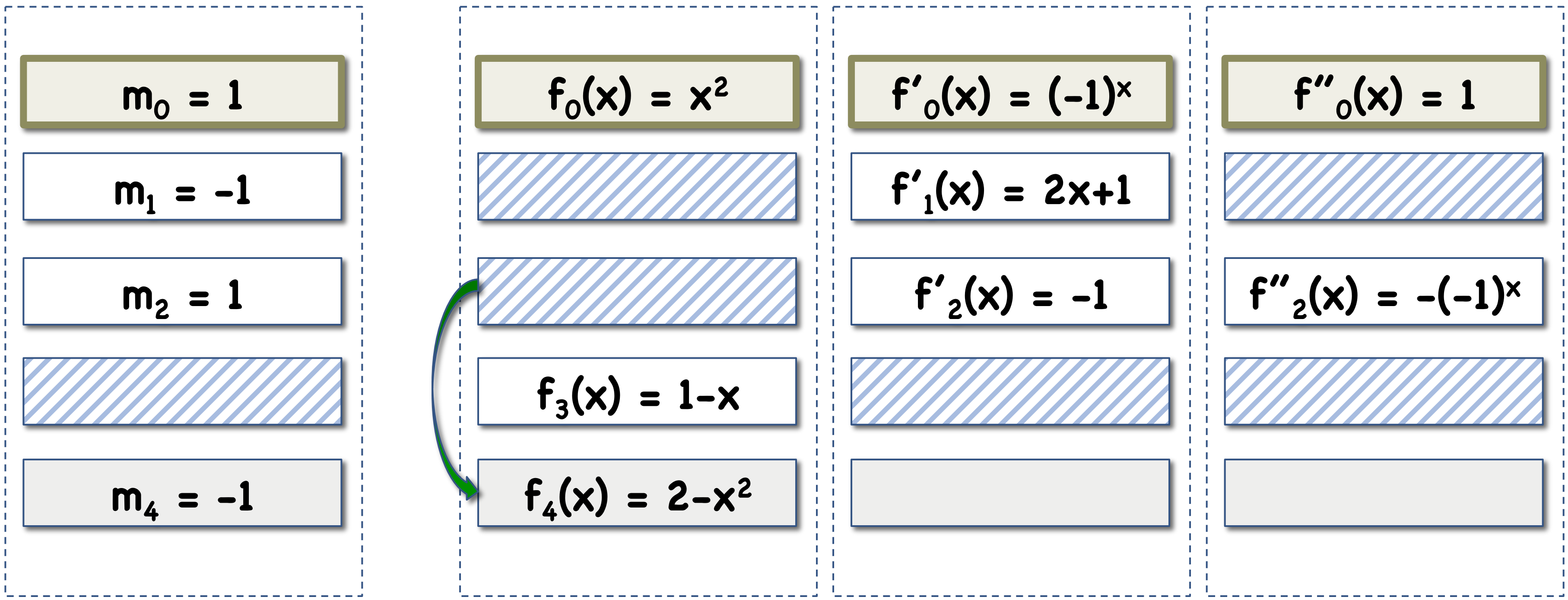


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$			

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to **-1**

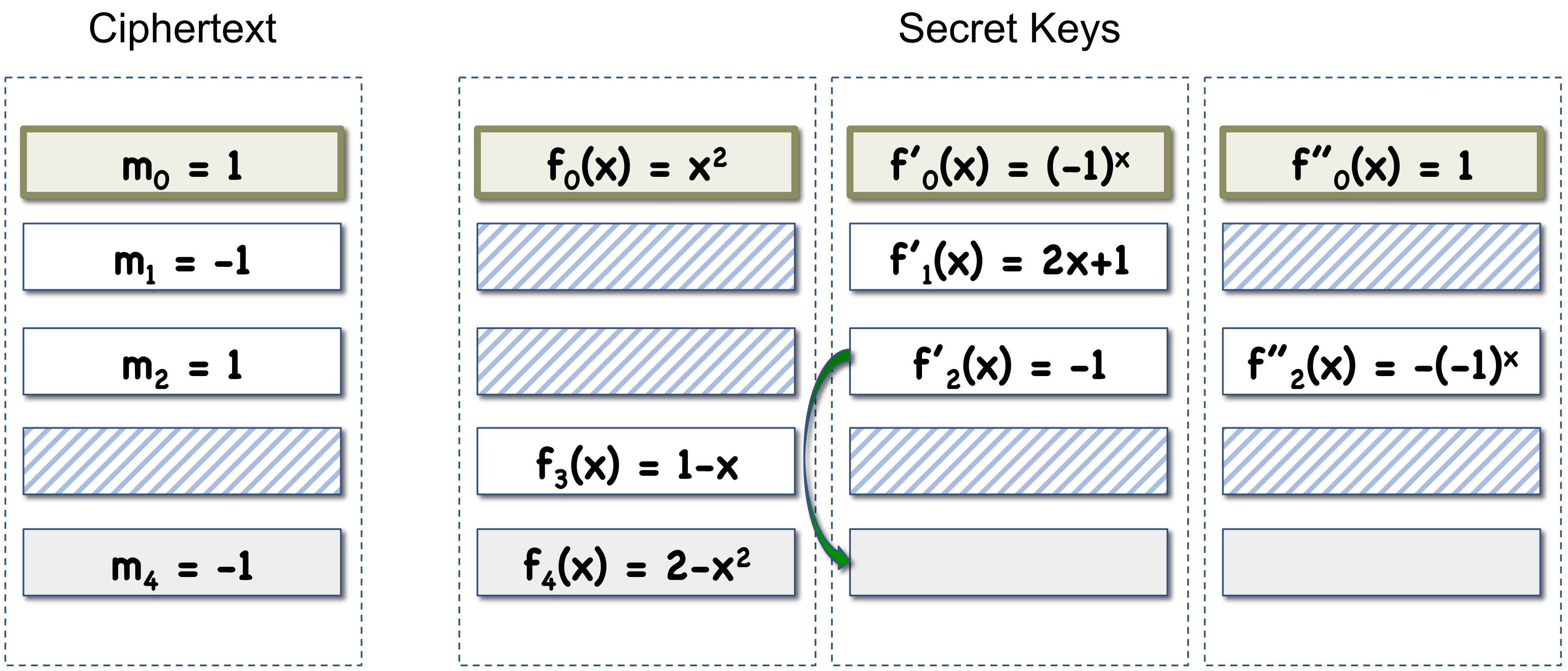


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

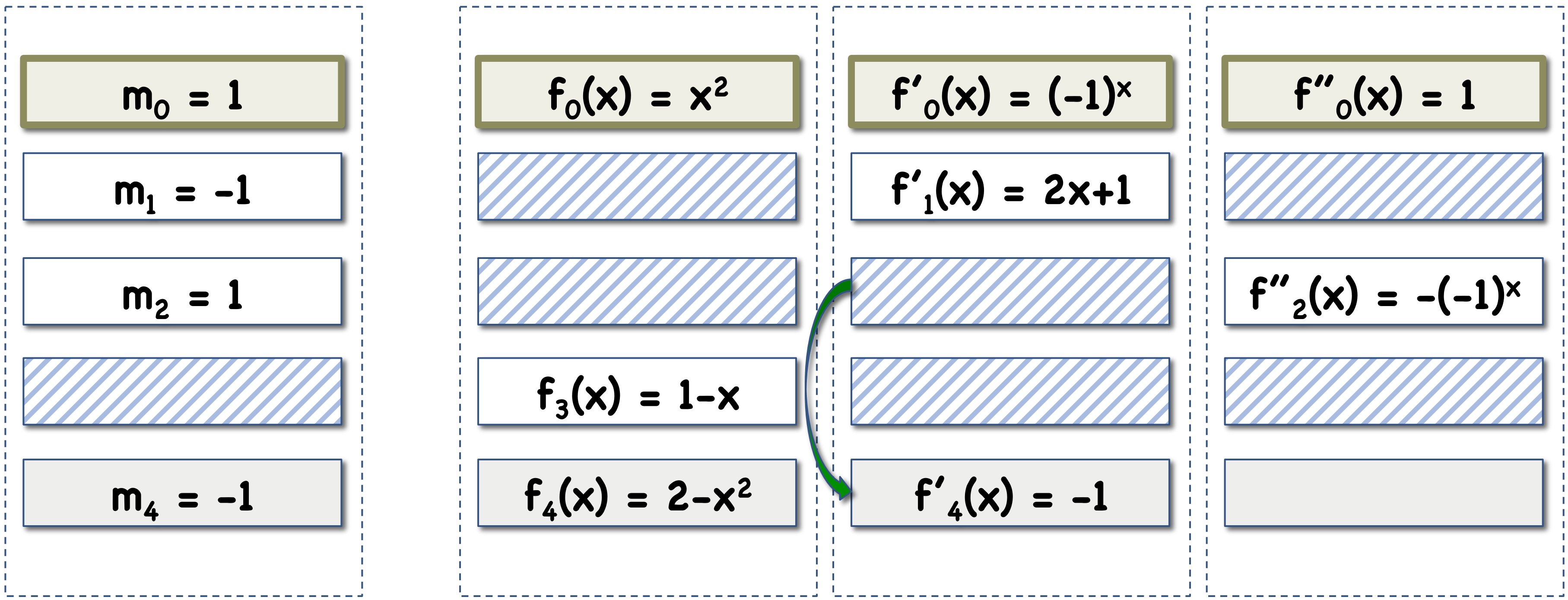


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$		

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

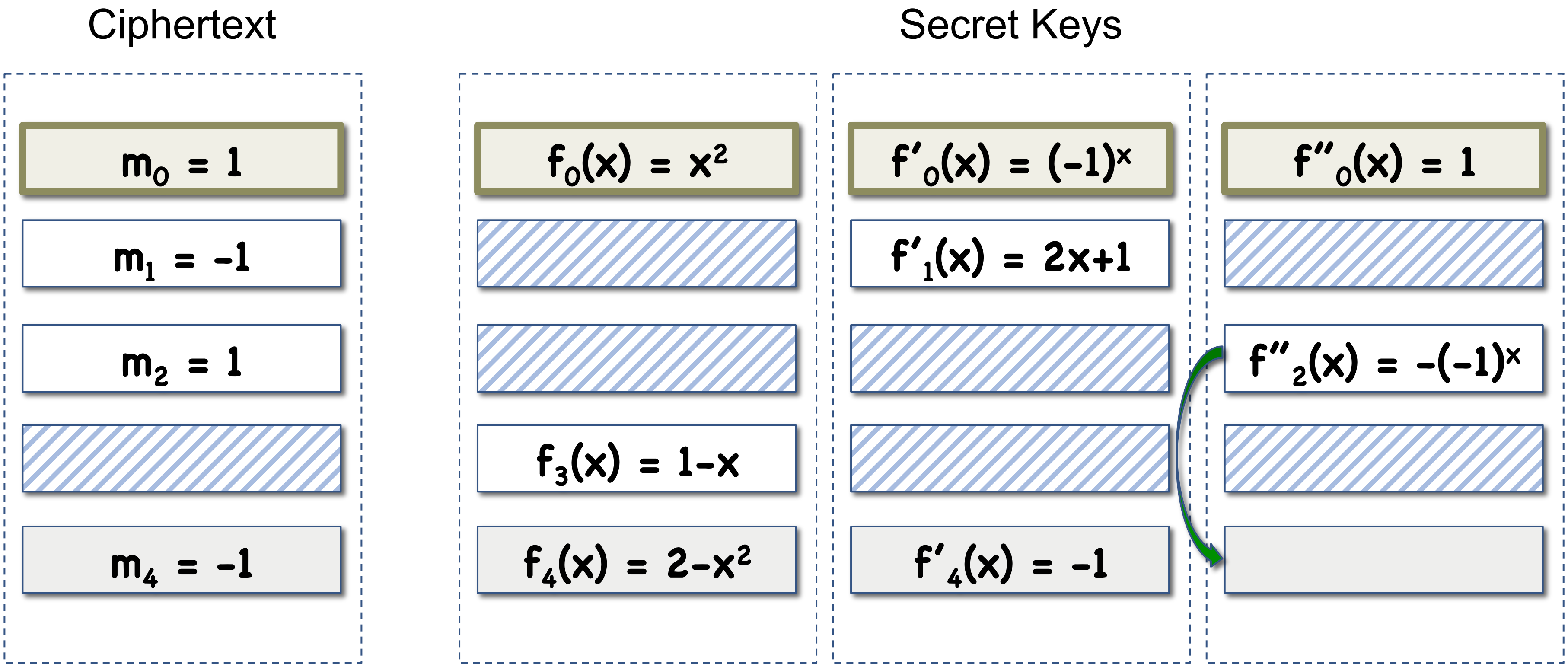


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	▨	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

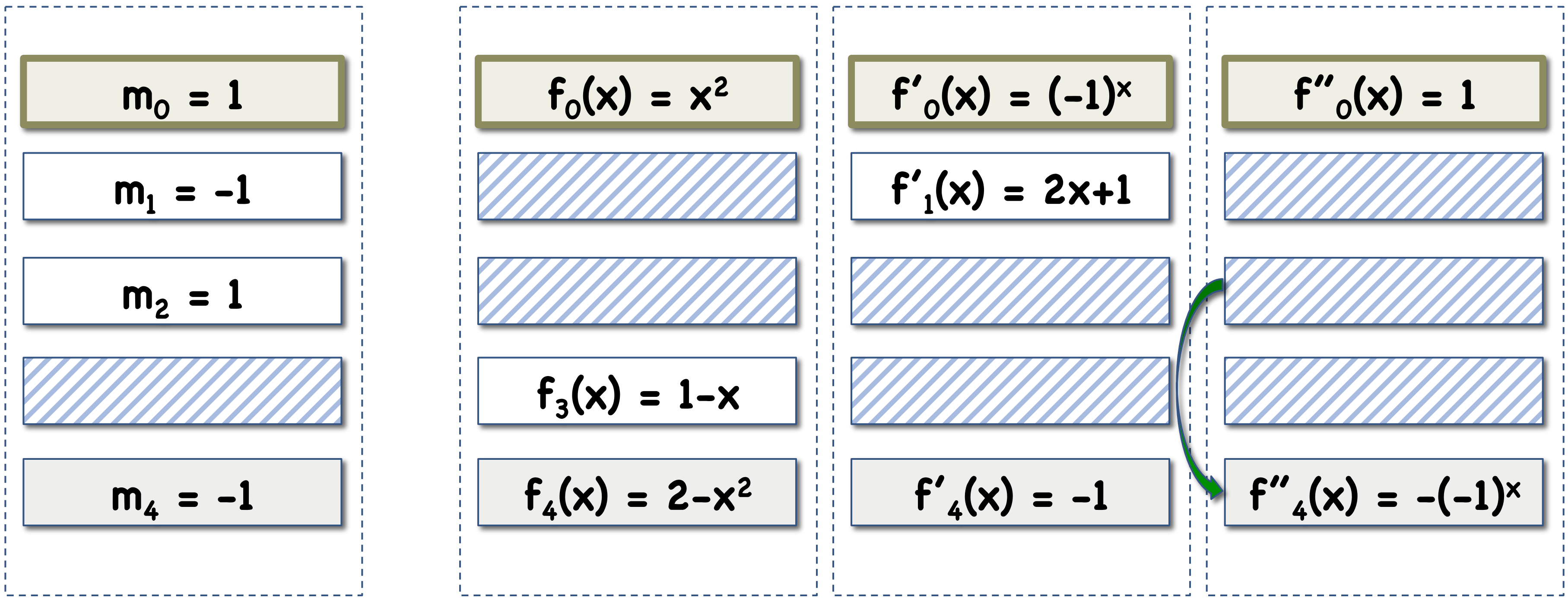


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	▨	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

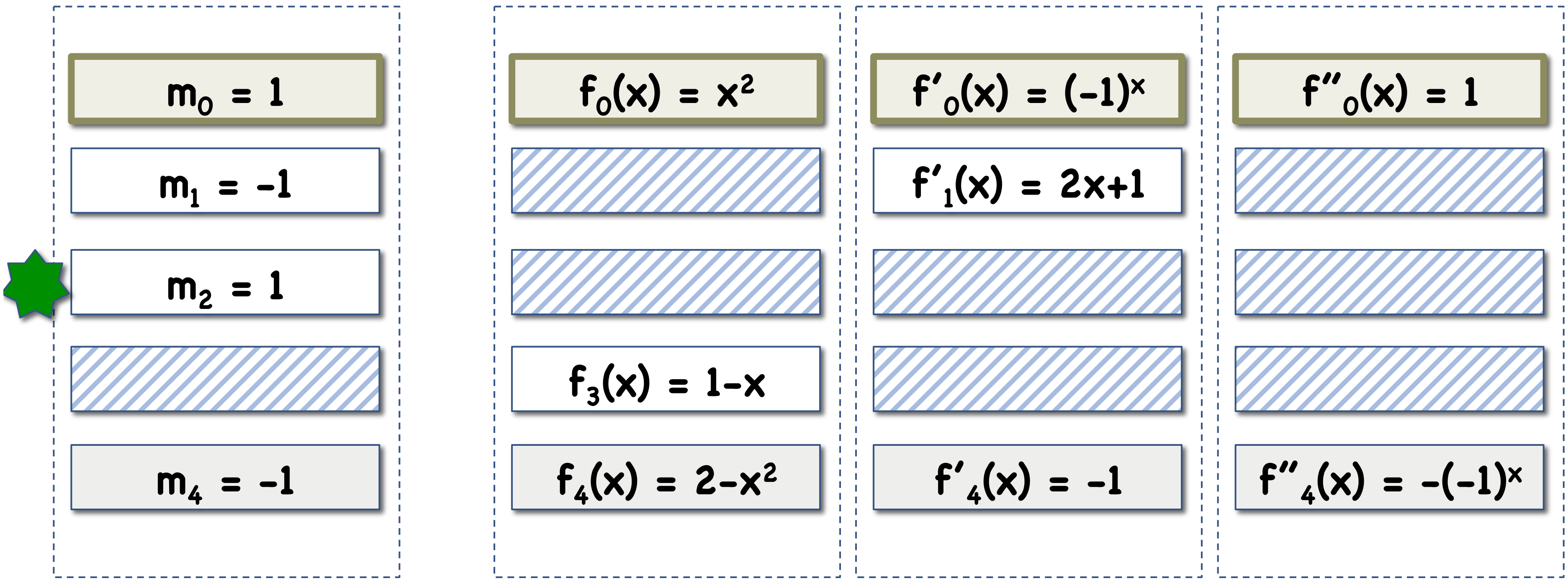


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	▨	▨
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	$f''_4(x) = -(-1)^x$

Strong Sk Moving

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

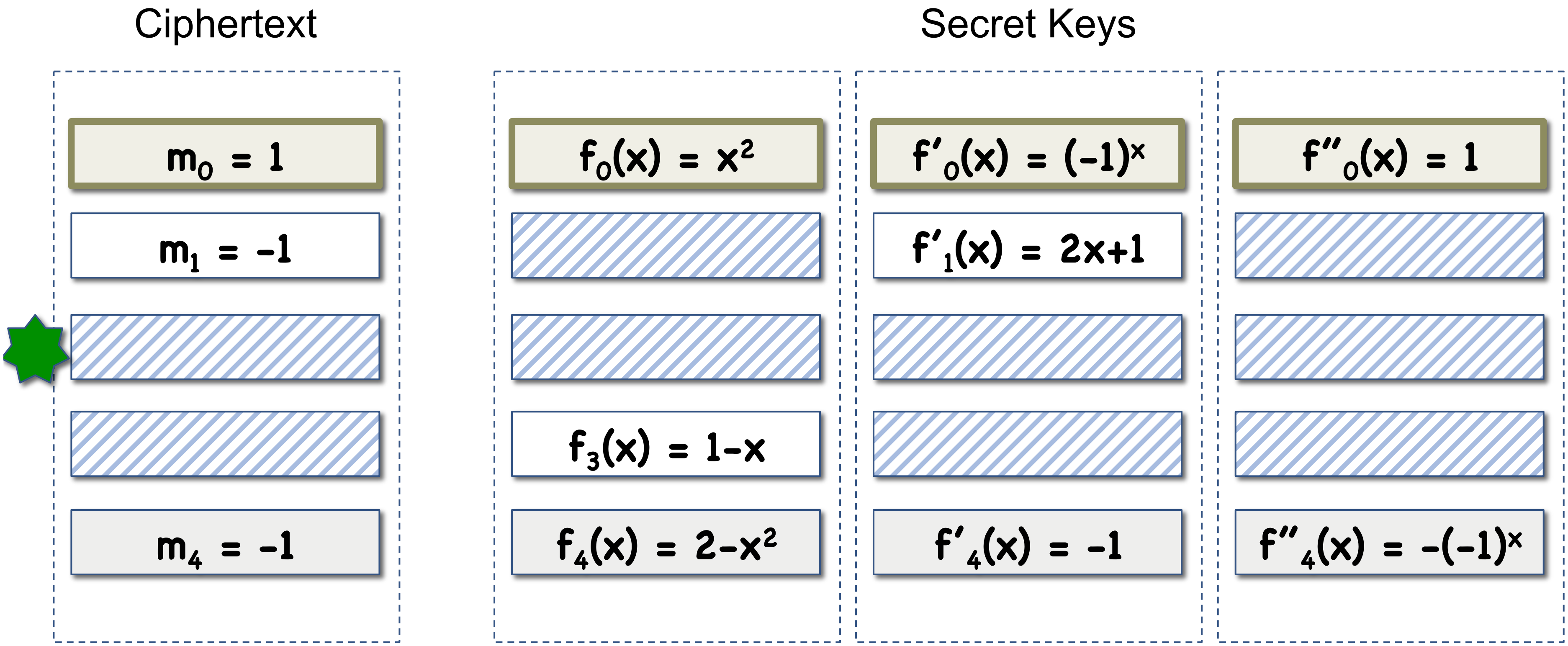


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = 1$	▨	▨	▨
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	$f''_4(x) = -(-1)^x$

New Slot

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

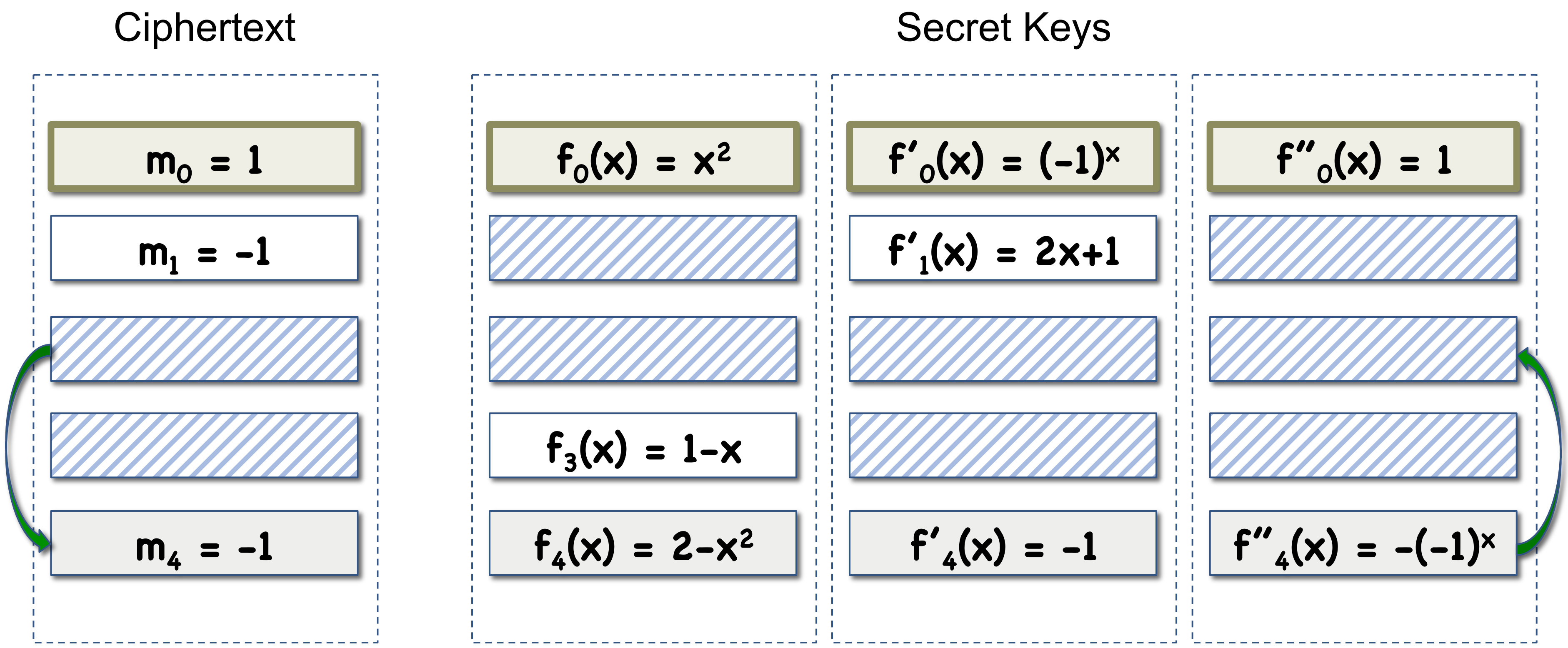


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
▨	▨	▨	▨
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	$f''_4(x) = -(-1)^x$

New Slot

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

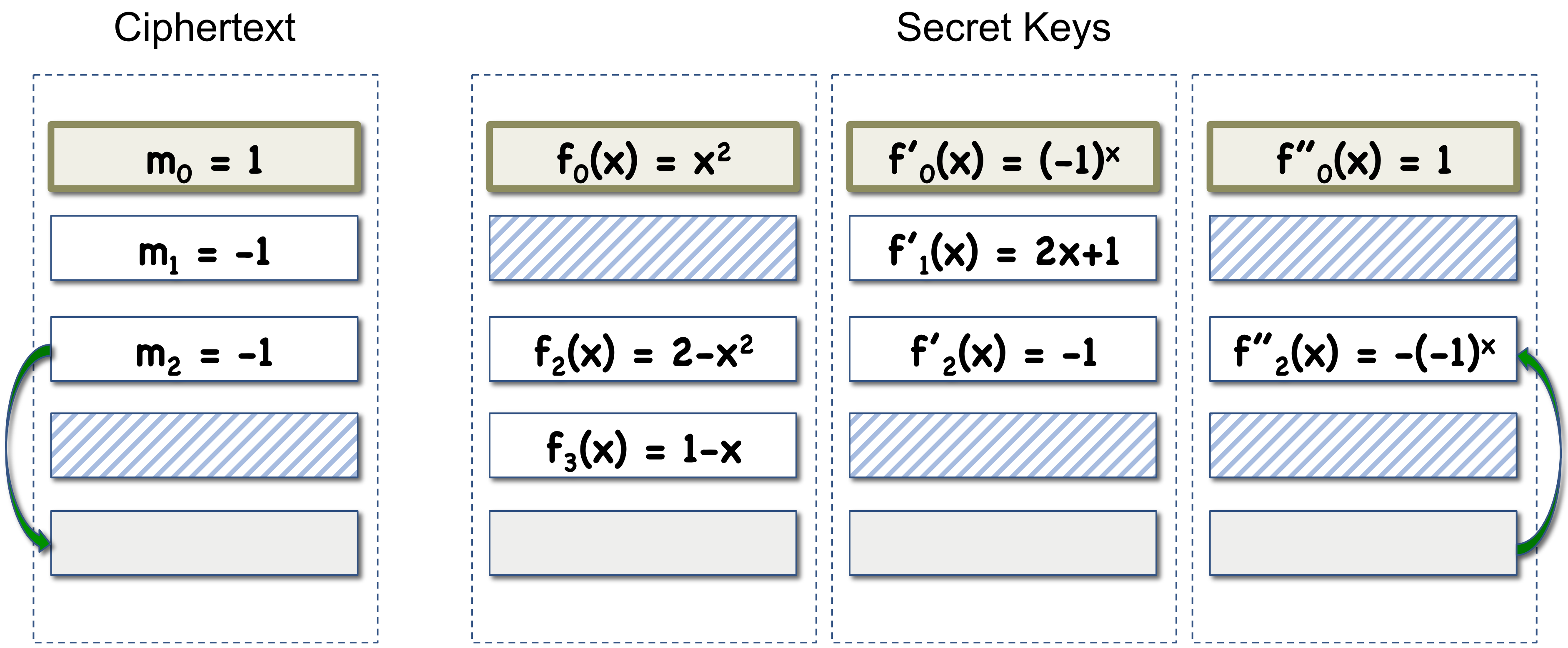


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
▨	▨	▨	▨
▨	$f_3(x) = 1-x$	▨	▨
$m_4 = -1$	$f_4(x) = 2-x^2$	$f'_4(x) = -1$	$f''_4(x) = -(-1)^x$

Slot Symmetry

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$

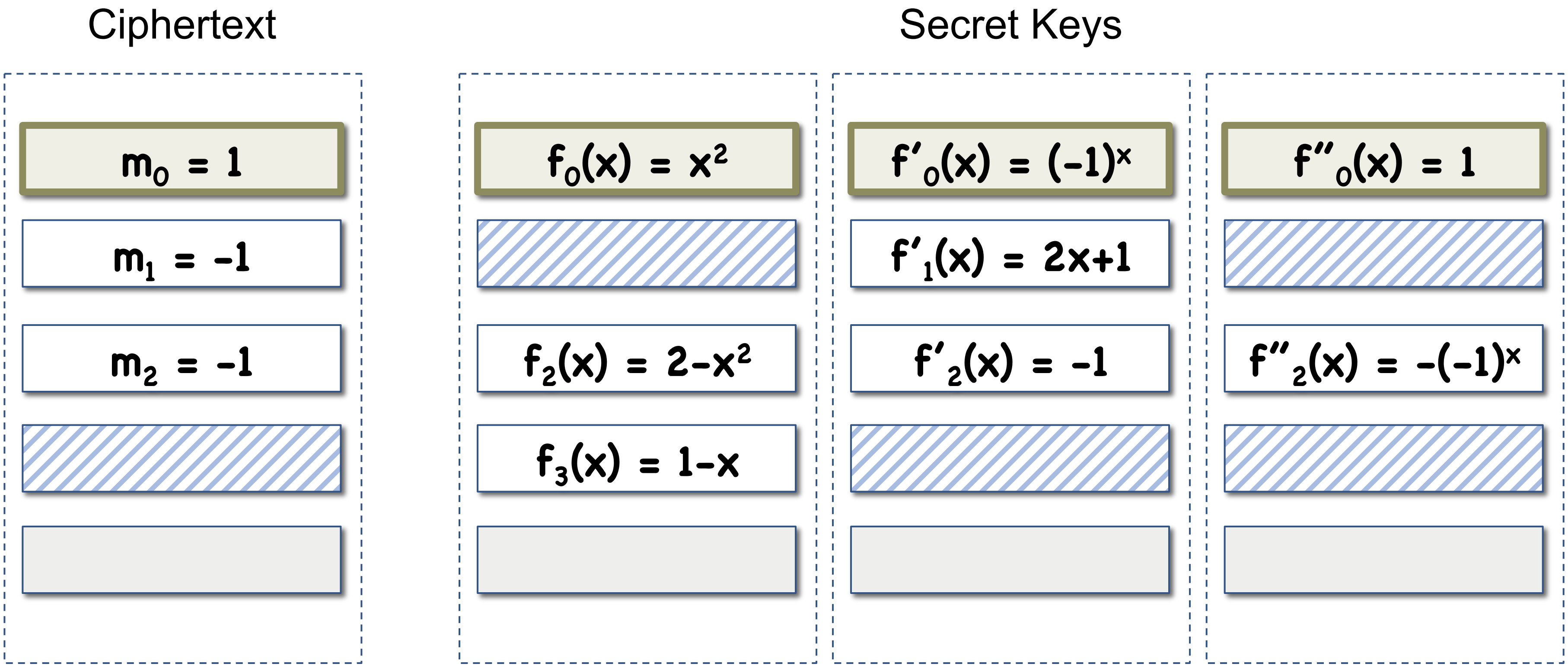


Ciphertext	Secret Keys		
$m_0 = 1$	$f_0(x) = x^2$	$f'_0(x) = (-1)^x$	$f''_0(x) = 1$
$m_1 = -1$	▨	$f'_1(x) = 2x+1$	▨
$m_2 = -1$	$f_2(x) = 2-x^2$	$f'_2(x) = -1$	$f''_2(x) = -(-1)^x$
▨	$f_3(x) = 1-x$	▨	▨

Slot Symmetry

Example Reduction: Weak Ctxt Indist

Goal: change $\mathbf{m_2}$ to $\mathbf{-1}$



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

Instantiating Slotted FE

We give construction for NC^1 circuits from composite-order graded encodings

- Slot Symmetry/Single-use Hiding: Information theoretic
- Slot Duplication/Ctxt Moving/Sk Moving: simple assumptions

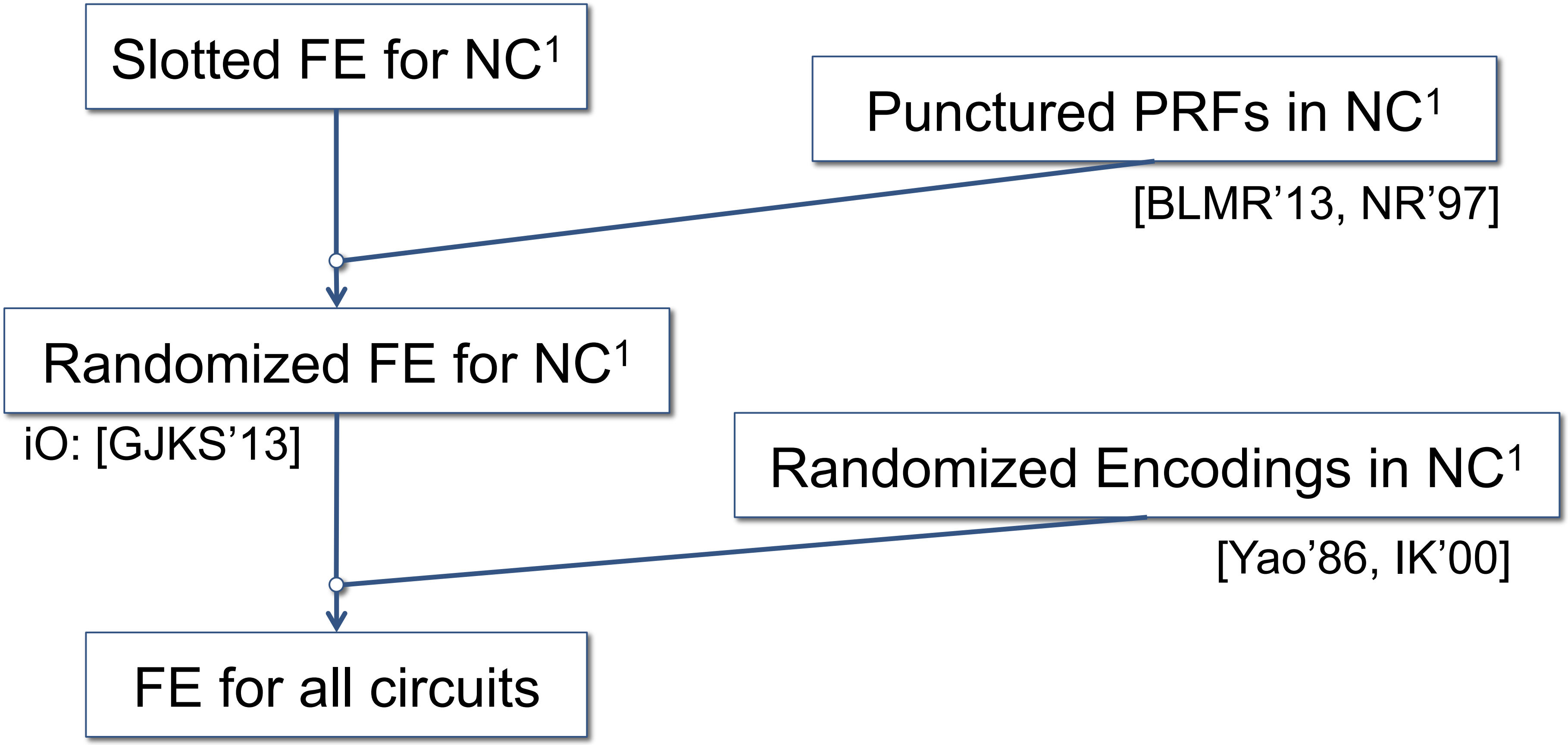
Construction requires new **extension** procedure on encodings

- bind ctxt (or sk) components together (no “mixing and matching”)
- Do not need to modify underlying encodings

Theorem: Relatively simple assumptions on mmaps
⇒ (adaptively) secure FE for NC^1

But I promised FE for all circuits…

Achieving FE for All Circuits



Slotted FE for NC^1

Punctured PRFs in NC^1

[BLMR’13, NR’97]

Randomized FE for NC^1

iO: [GJKS’13]

Randomized Encodings in NC^1

[Yao’86, IK’00]

FE for all circuits

Randomized FE for NC^1

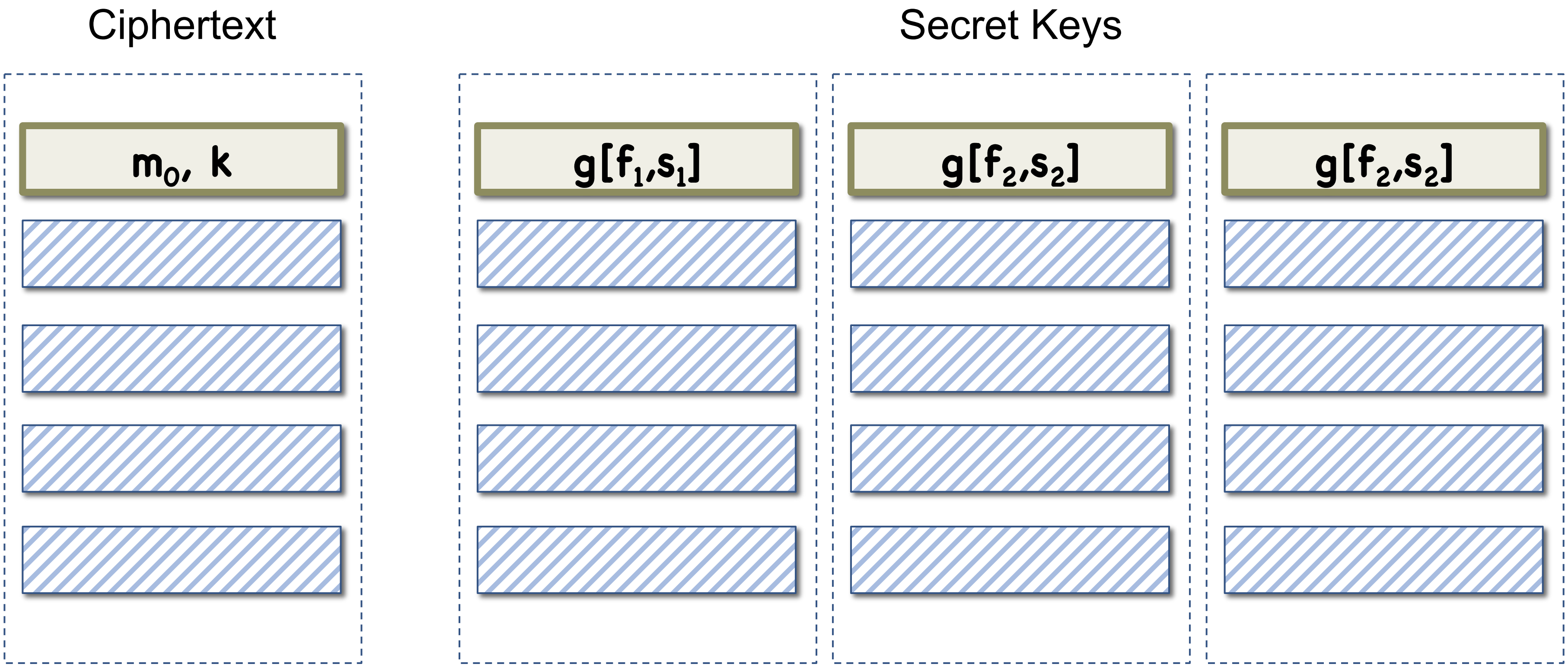
Basic idea: ctxt contains PRF key which generates randomness

```
Enc_R(mpk, m):      k ← {0,1}^λ
                    c ← Enc( mpk,  (m,k) )
                    Output c

Define:             g[f,s](m,k) := f( m ; PRF(k,s) )

KeyGen_R(msk, f):   s ← {0,1}^λ
                    sk_f ← KeyGen(msk, g[f,s])
                    Output sk_f
```

Actual scheme more complicated

Randomized FE for NC^1

Proof idea:



Ciphertext

Secret Keys

m_0, k

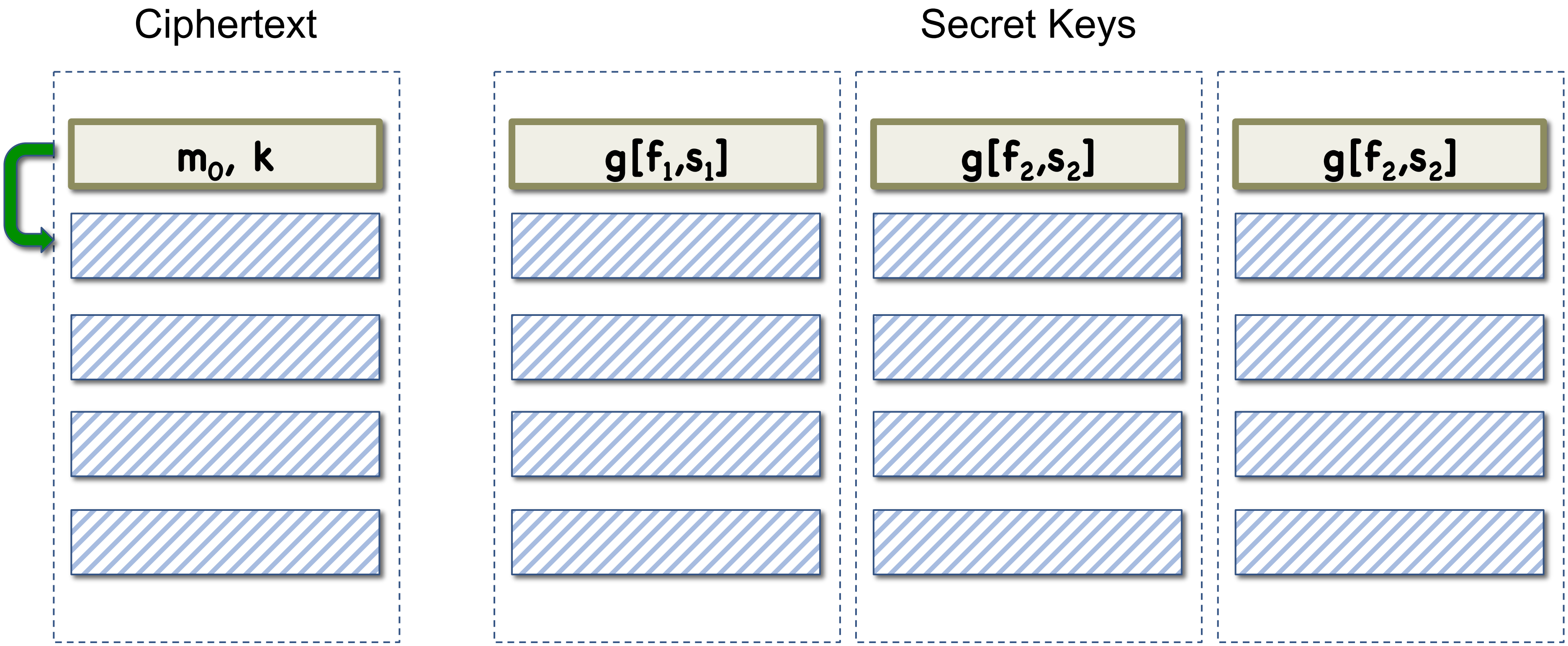
$g[f_1,s_1]$

$g[f_2,s_2]$

$g[f_2,s_2]$

Randomized FE for NC[1]

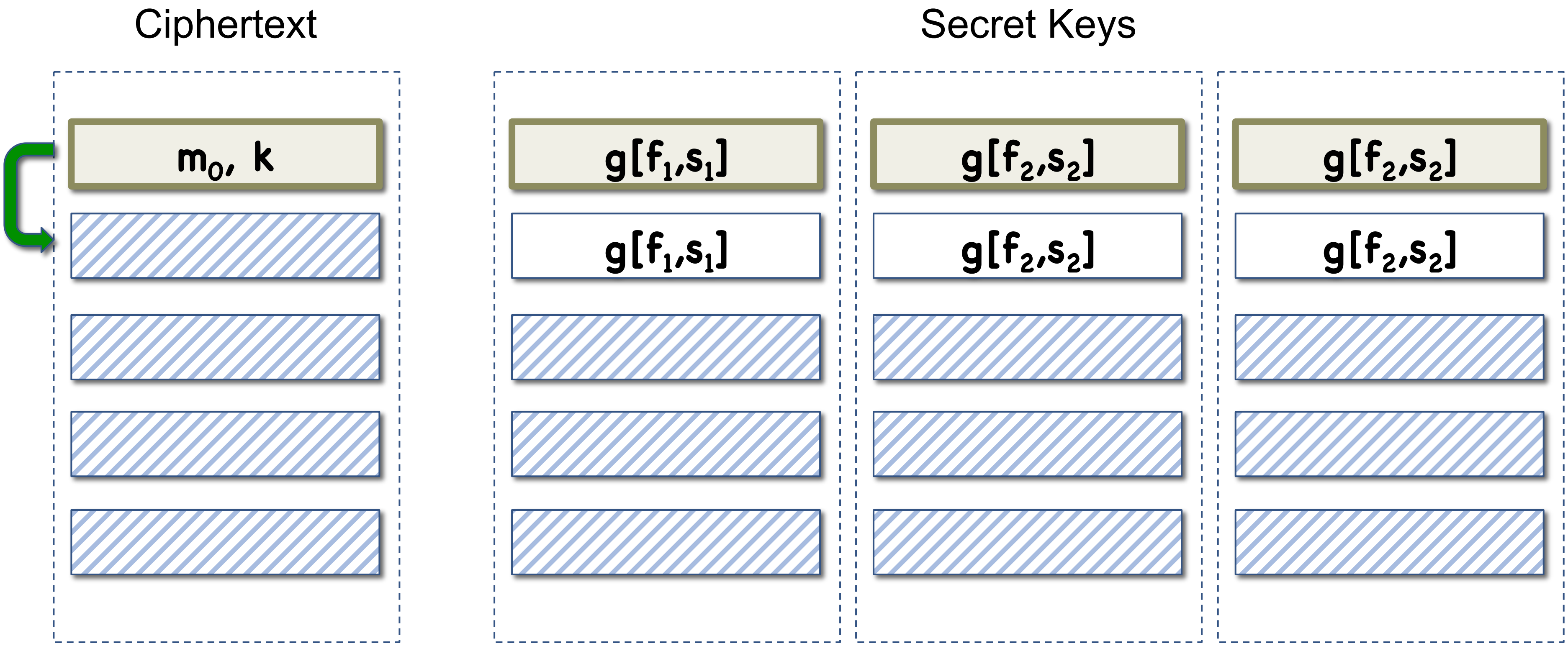
Proof idea:



Slot Duplication

Randomized FE for NC[1]

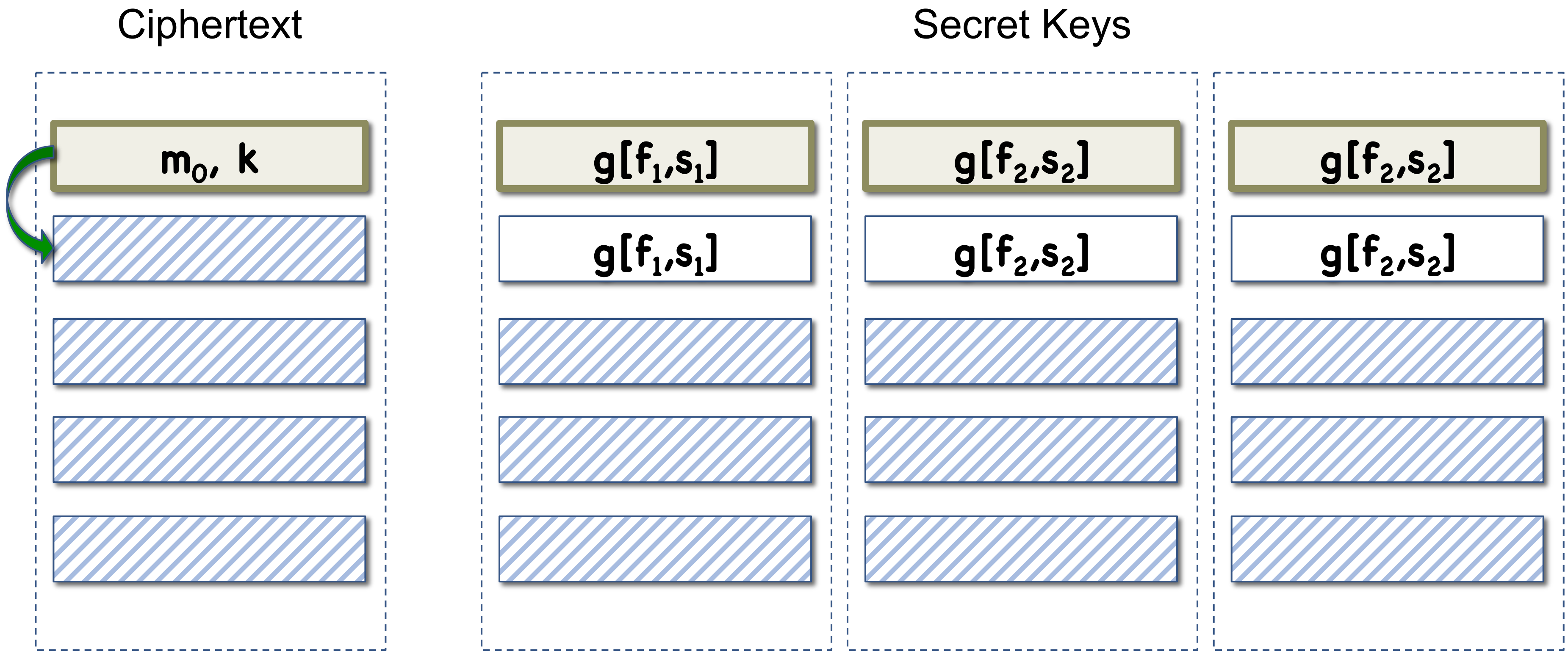
Proof idea:



Slot Duplication

Randomized FE for NC^1

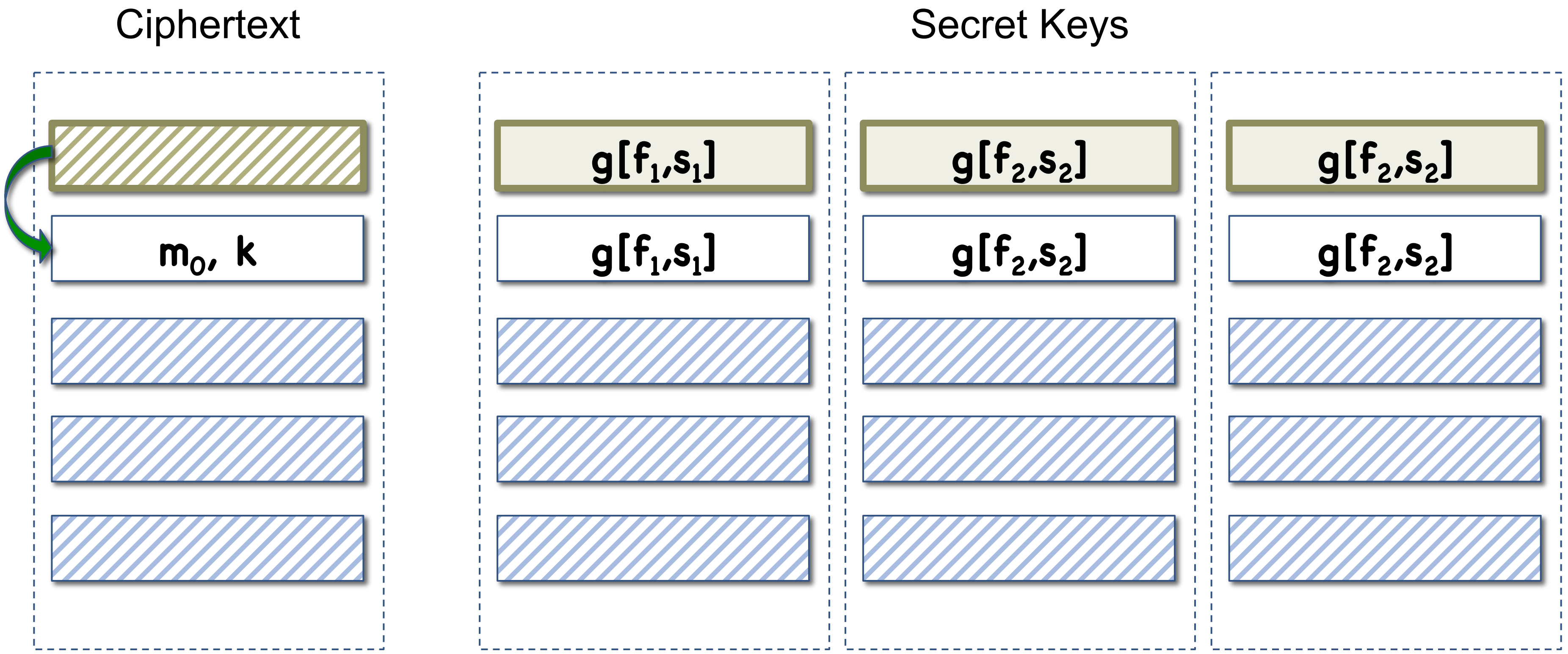
Proof idea:



Ciphertext Moving

Randomized FE for NC^1

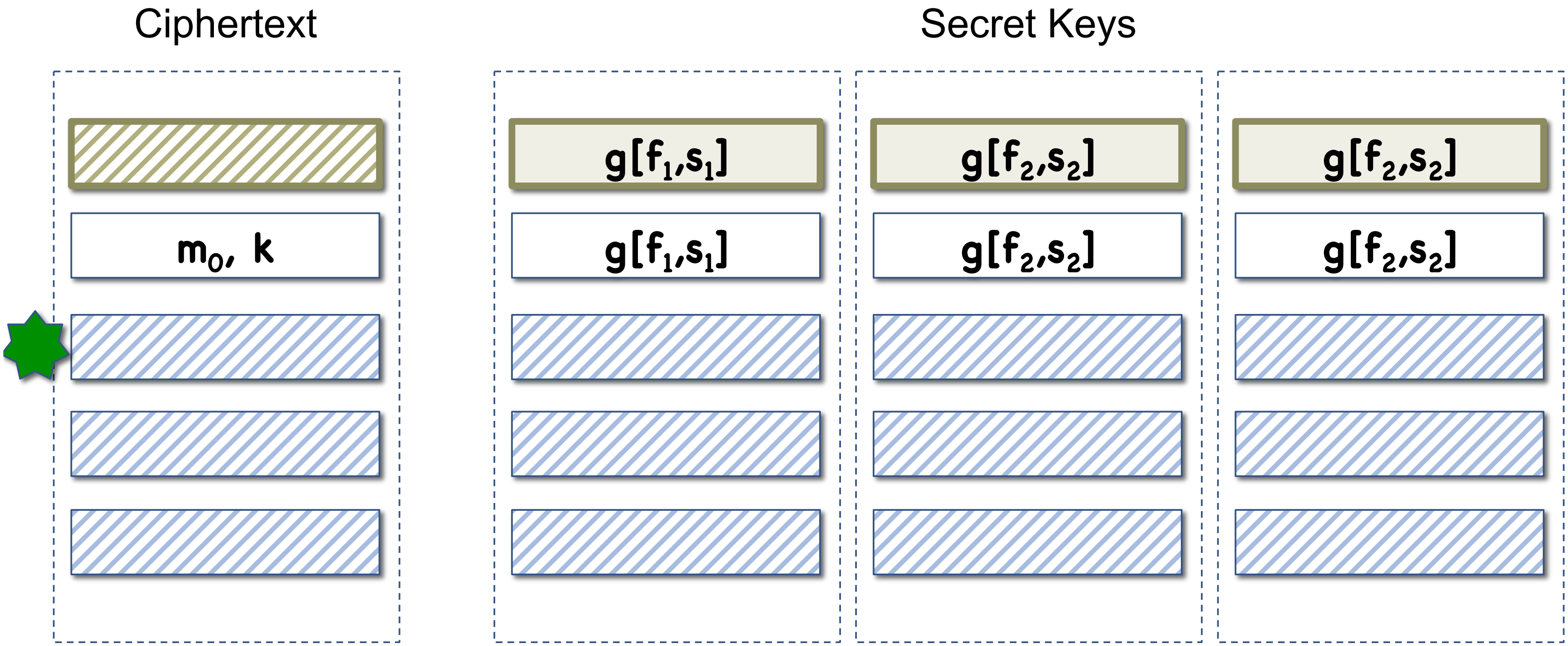
Proof idea:



Ciphertext Moving

Randomized FE for NC^1

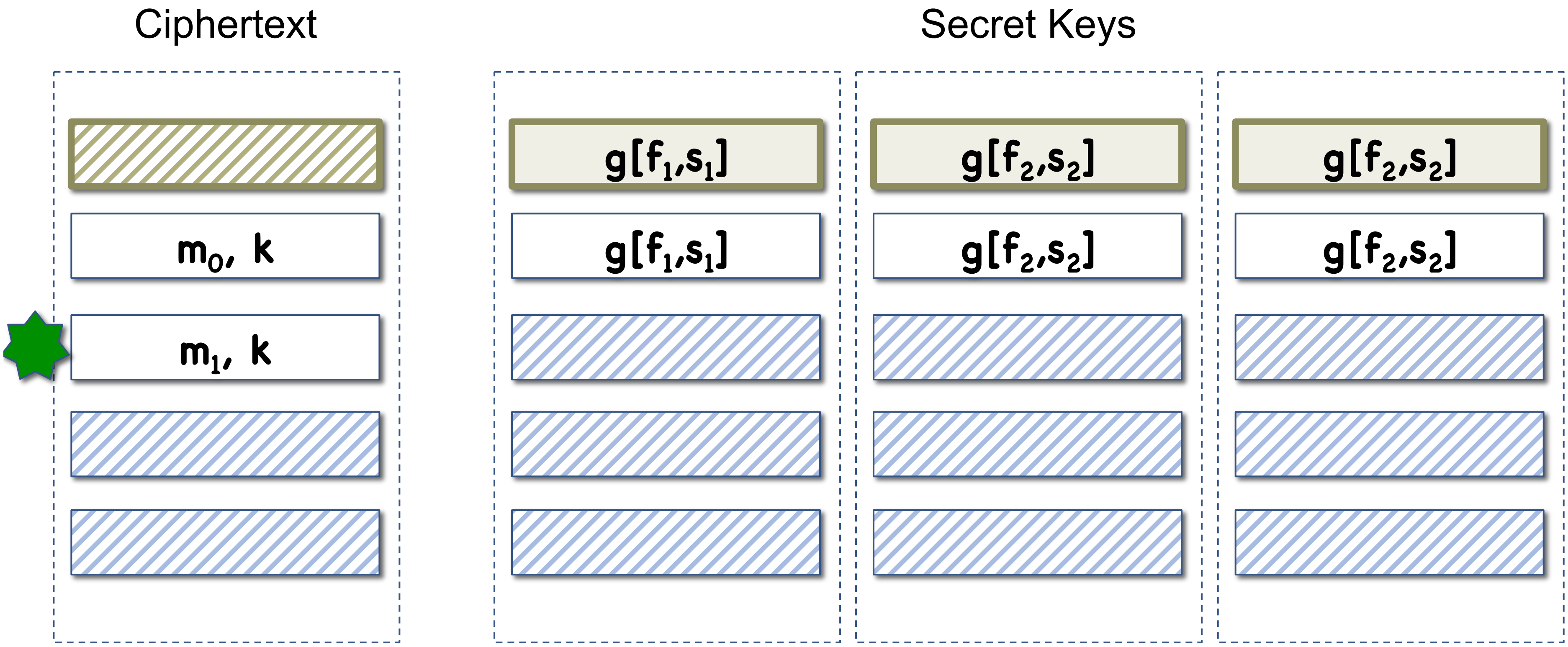
Proof idea:



New Slot

Randomized FE for NC^1

Proof idea:



Ciphertext

Secret Keys

m_0, k

m_1, k

g[f_1,s_1]

g[f_1,s_1]

g[f_2,s_2]

g[f_2,s_2]

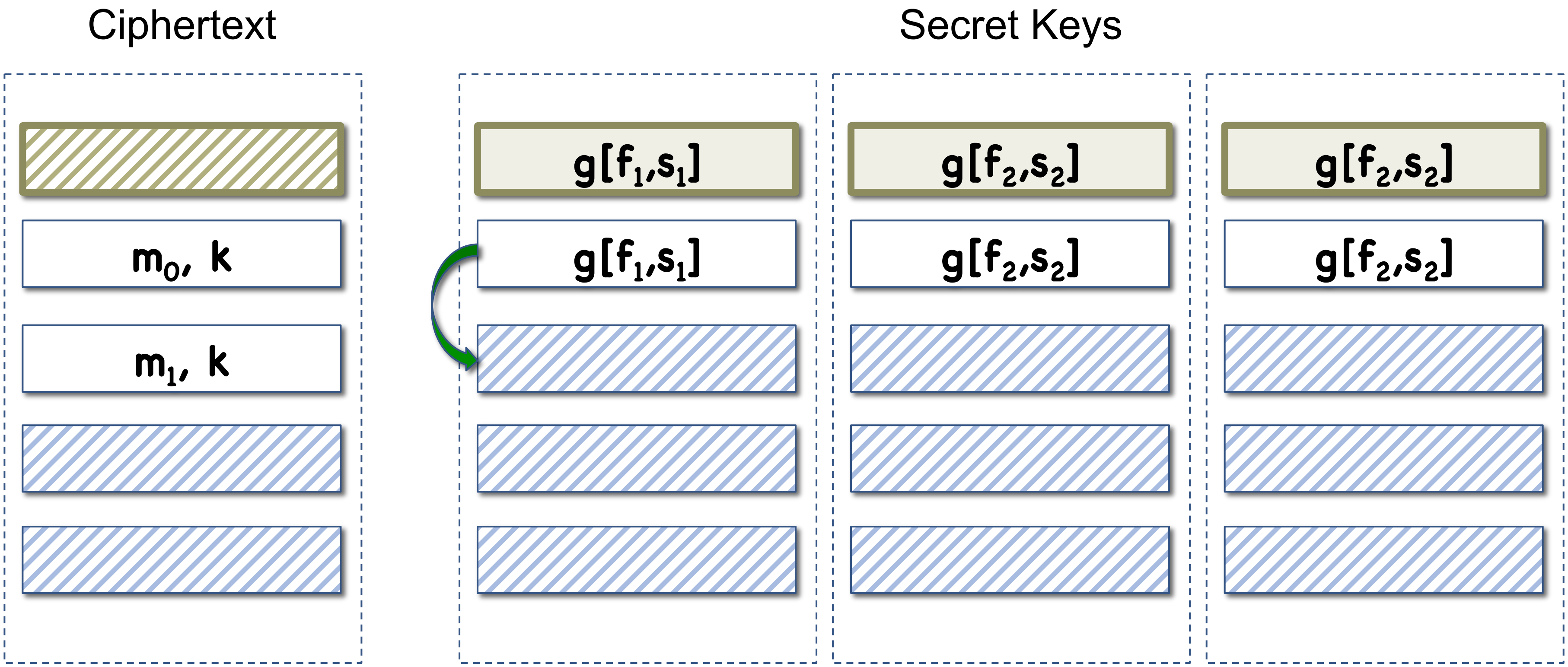
g[f_2,s_2]

g[f_2,s_2]

New Slot

Randomized FE for NC^1

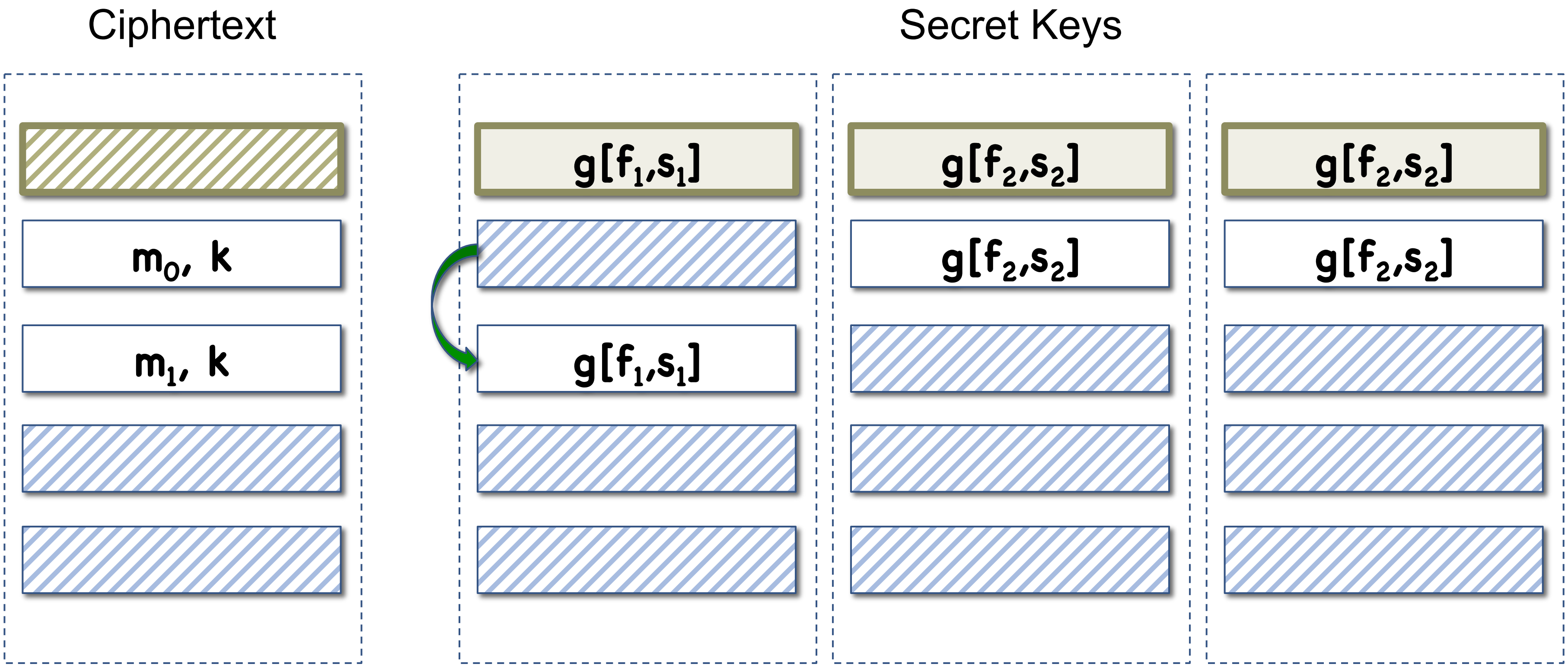
Proof idea:



“Super Strong Secret Key Moving”

Randomized FE for NC^1

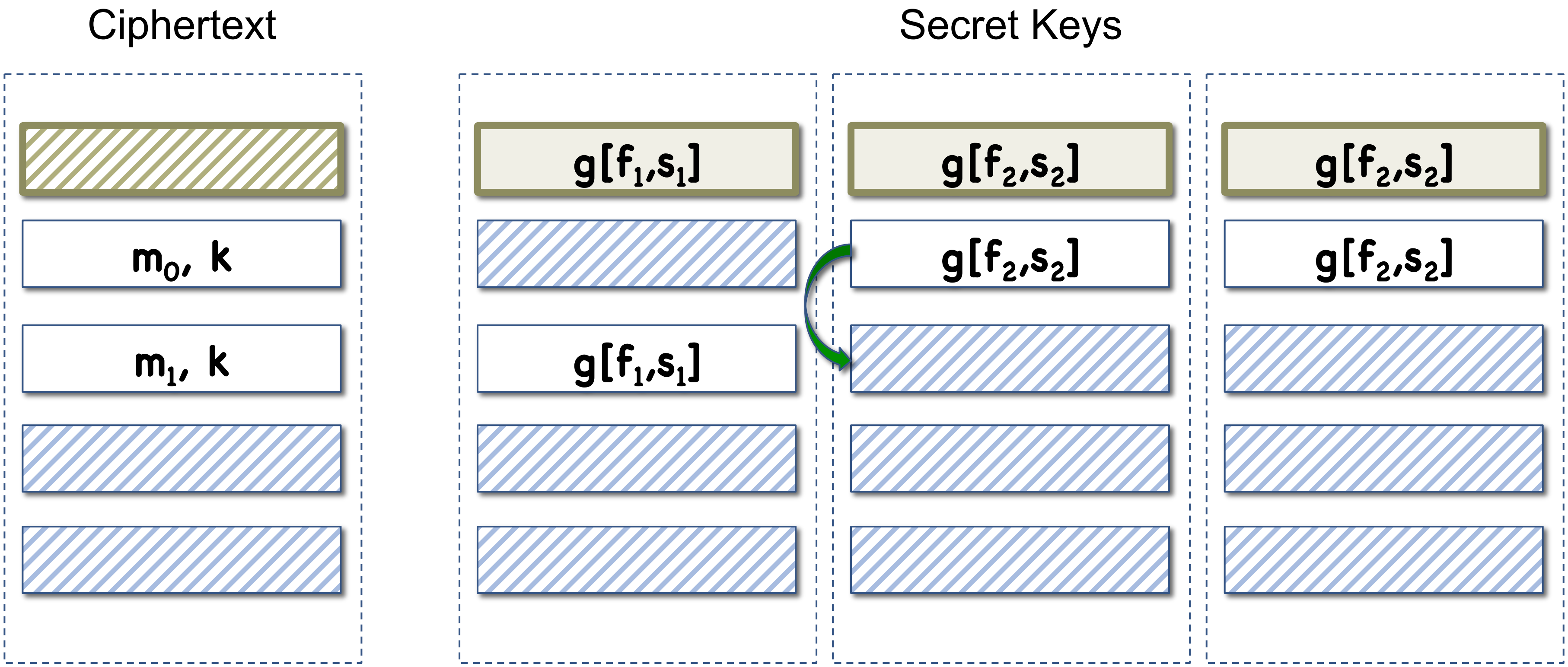
Proof idea:



“Super Strong Secret Key Moving”

Randomized FE for NC^1

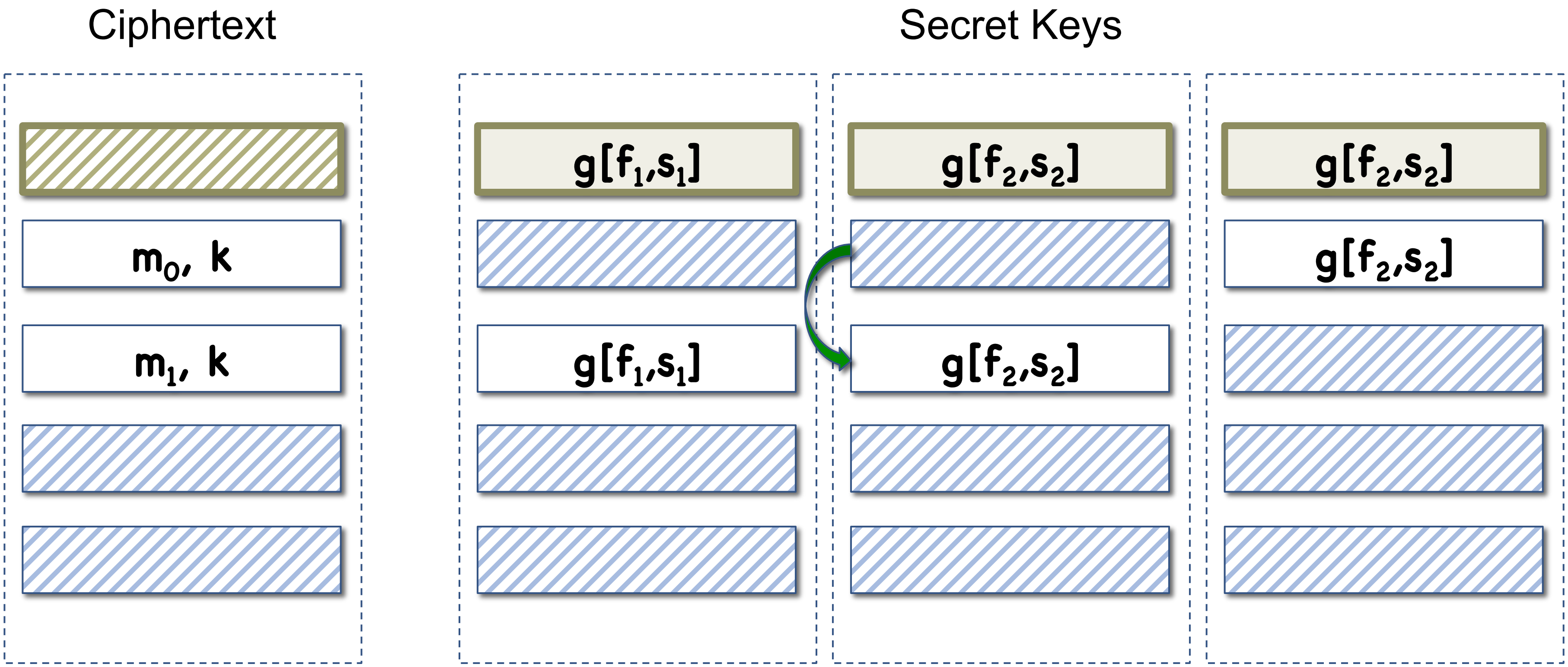
Proof idea:



“Super Strong Secret Key Moving”

Randomized FE for NC^1

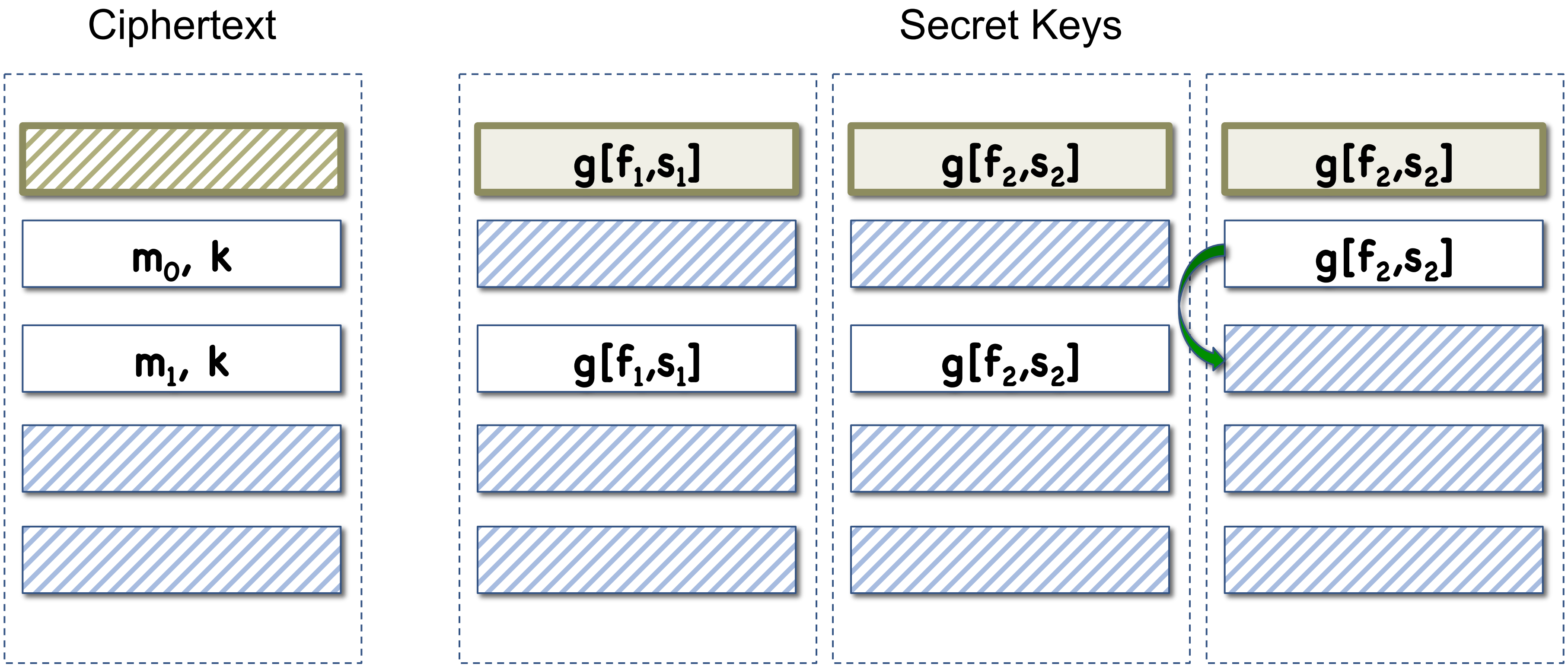
Proof idea:



"Super Strong Secret Key Moving"

Randomized FE for NC^1

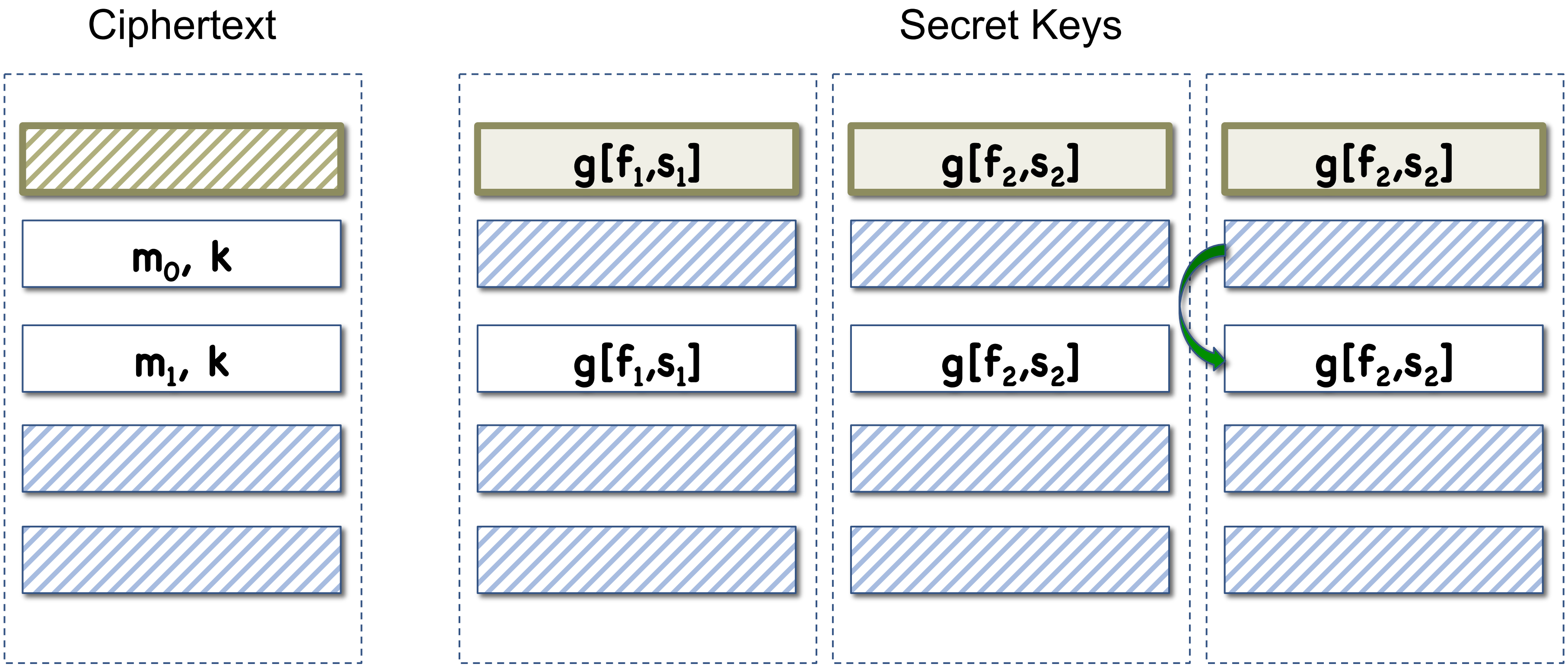
Proof idea:



"Super Strong Secret Key Moving"

Randomized FE for NC[1]

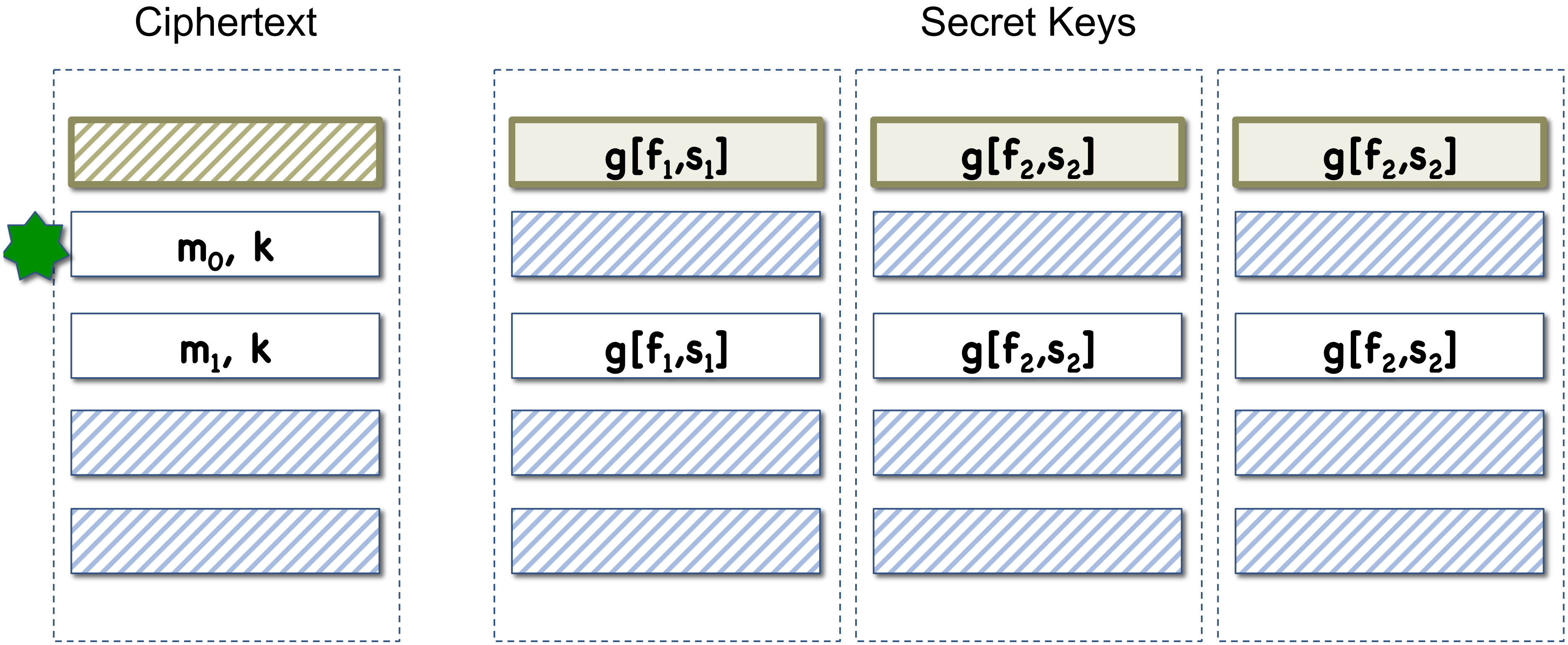
Proof idea:



“Super Strong Secret Key Moving”

Randomized FE for NC^1

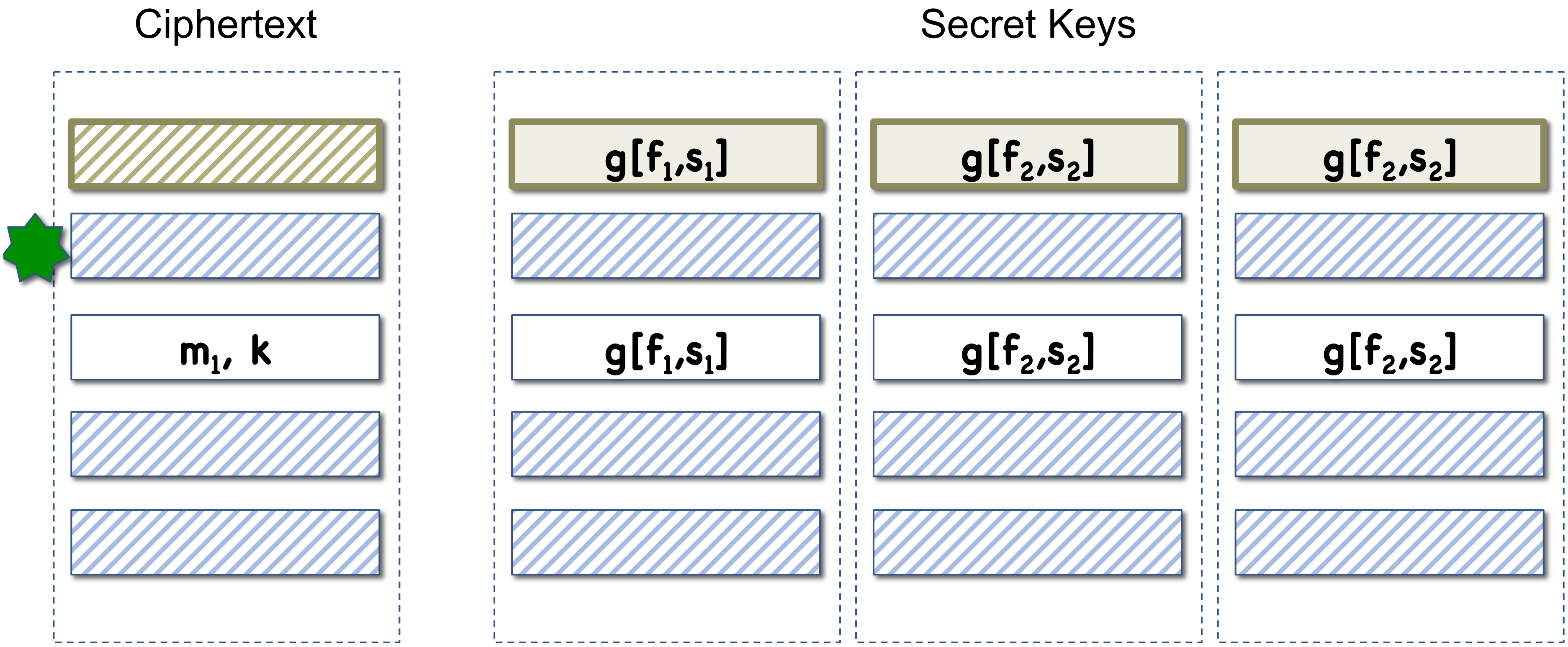
Proof idea:



New Slot

Randomized FE for NC^1

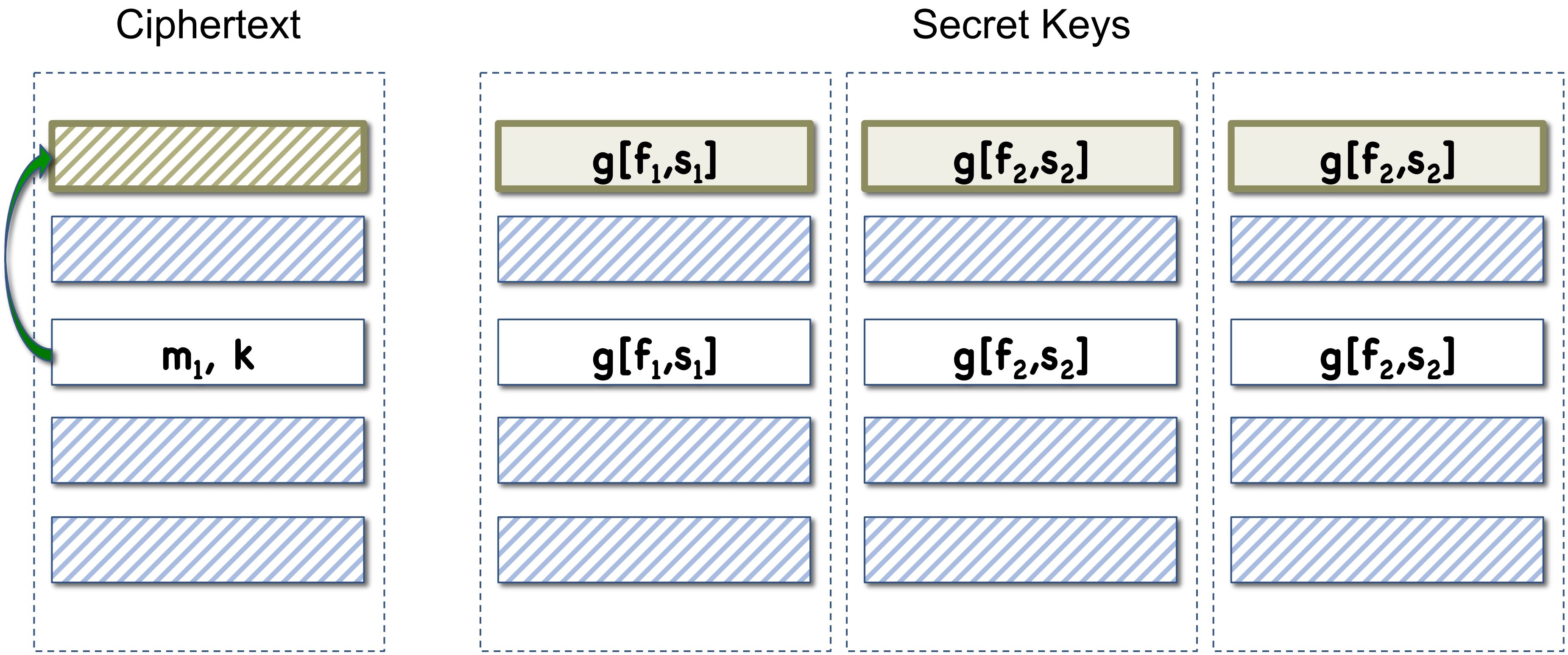
Proof idea:



New Slot

Randomized FE for NC^1

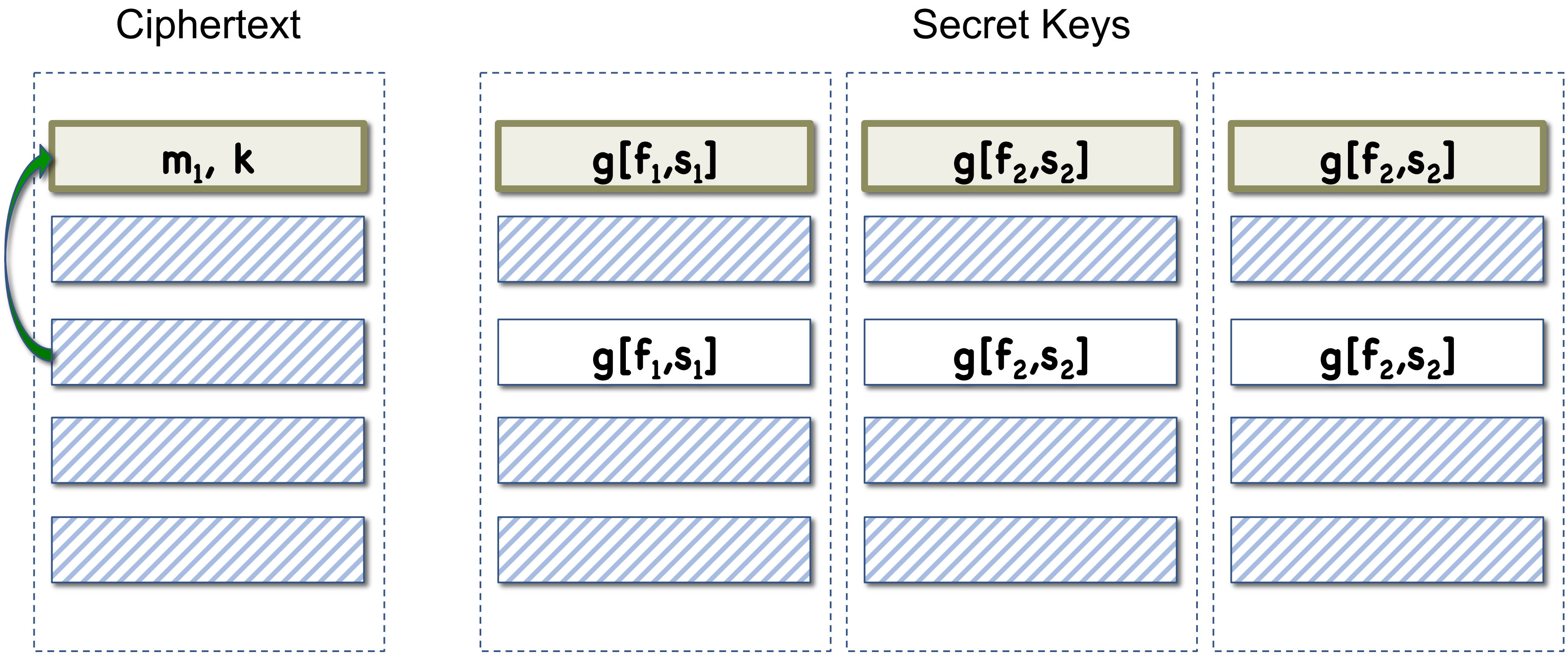
Proof idea:



Ciphertext Moving

Randomized FE for NC^1

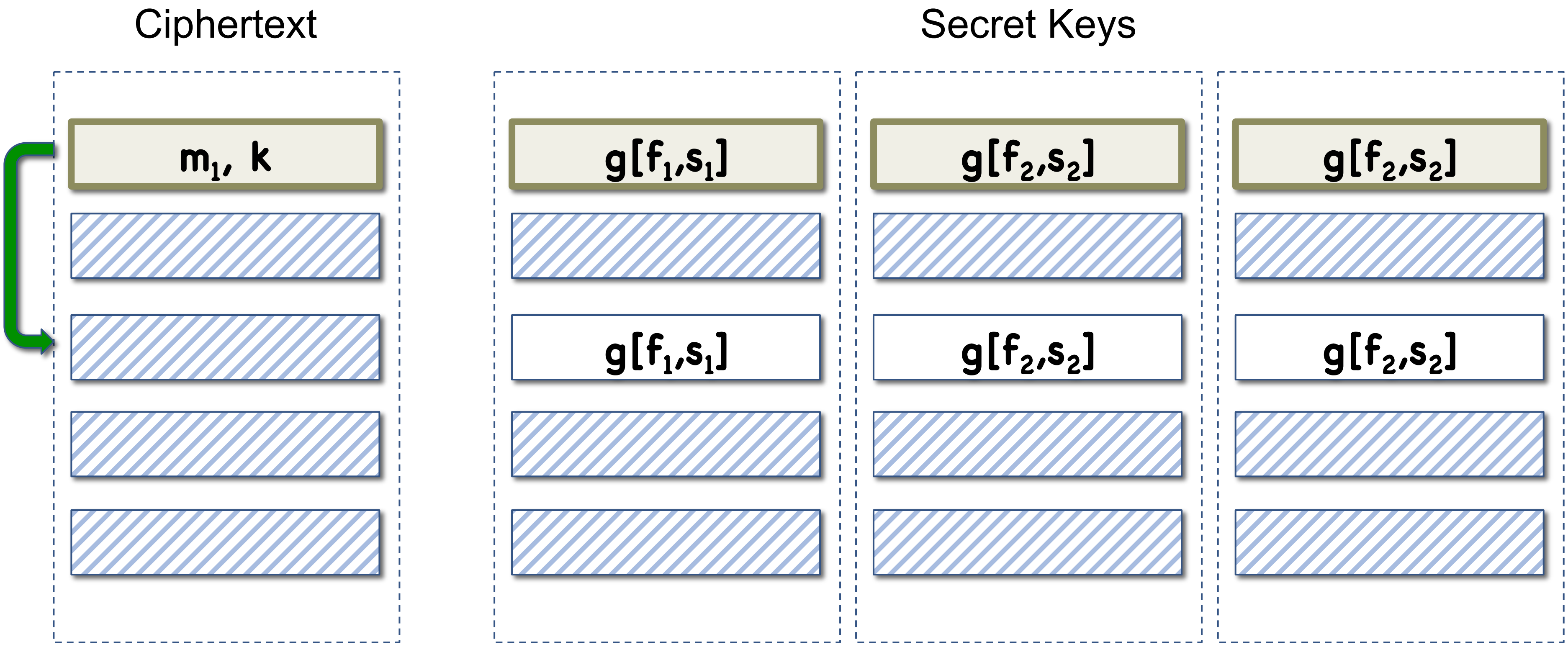
Proof idea:



Ciphertext Moving

Randomized FE for NC^1

Proof idea:



Ciphertext

Secret Keys

m_1, k

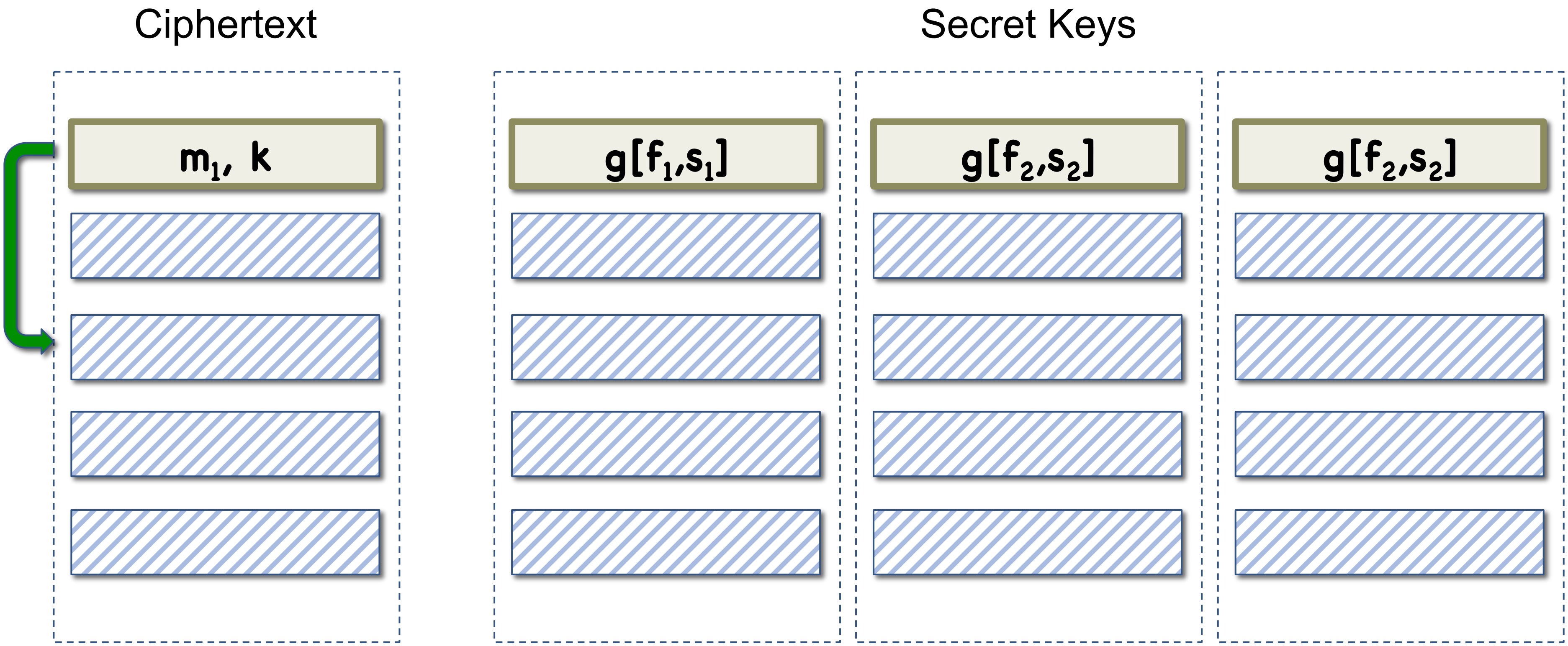
$g[f_1,s_1]$ $g[f_2,s_2]$ $g[f_2,s_2]$

$g[f_1,s_1]$ $g[f_2,s_2]$ $g[f_2,s_2]$

Slot Duplication

Randomized FE for NC^1

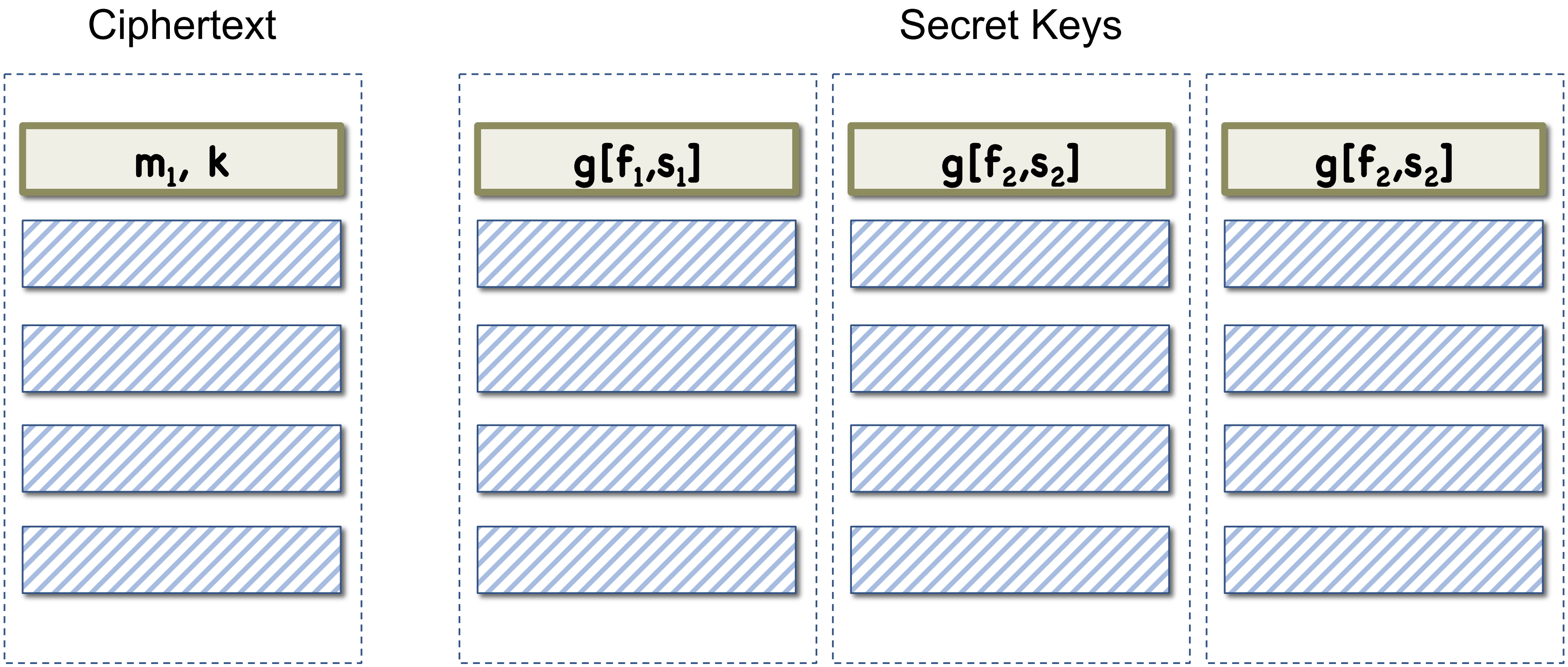
Proof idea:



Slot Duplication

Randomized FE for NC^1

Proof idea:



Ciphertext

Secret Keys

m_1, k

$g[f_1,s_1]$

$g[f_2,s_2]$

$g[f_2,s_2]$

Achieving "Super Strong Secret Key Moving"

Outputs different, even though indistinguishable

⇒ strong secret key moving not enough

More involved proof:

- Puncture **k** at **s**
- Hardcode **f(m_0, PRF(k, s))**
  - In ciphertext if secret key before ciphertext. Use ctxt indist.
  - In secret key if secret key after ciphertext. Use single-use hiding+
- Replace with **f(m_1, PRF(k, s))**
  - Using PRF security and sample indistinguishability
- Move secret key
- Un-puncture

FE for all Circuits

Basic idea: Output randomized encoding rather than actual val

$\mathbf{Enc_C(mpk, m)}$:

$c \leftarrow \mathrm{Enc}_R(\mathrm{mpk}, m)$
Output $\mathbf{c}$

$\mathbf{KeyGen_C(msk, f)}$:

$f'(m; r) := \mathrm{Encode}_f(m ; r)$
$sk_f \leftarrow \mathrm{KeyGen}_R(\mathrm{msk}, f')$
Output $\mathbf{sk_f}$

$\mathbf{Dec_C(sk_f, c)}$:

$e \leftarrow \mathrm{Dec}_R(sk_f, c)$
$o \leftarrow \mathrm{Decode}(e)$
Output $\mathbf{o}$

Conclusion and Open Problems

Simple assumptions → Slotted FE → Fully-secure unbounded FE

- iO/complexity leveraging/function hiding **not** inherent to FE

New tools on graded encodings

Open Problems:

- Other apps for slotted FE?
- Simplify: remove punctured PRFs / randomized encodings?
- Other ***iO*** apps → simple assumptions
  - Deniable encryption
  - Multiparty NIKE w/o trusted setup