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

Solution 0: Give cloud \( sk \)  \( \Rightarrow \) cloud learns entire message  \( \times \)
Solution 1: Use FHE  \( \Rightarrow \) cloud only learns \( \text{Enc}(f(m)) \)  \( \times \)
Solution 2: Functional encryption: cloud learns \( f(m) \), nothing else  \( \checkmark \)
Functional Encryption: Semantics [BSW’11]

\textbf{Gen():} \quad \text{Output keys } (\text{msk, pk})

\textbf{Enc(pk, m):} \quad \text{Output ciphertext } c

\textbf{KeyGen(msk, f):} \quad \text{Output decryption key } \text{sk}_f

\textbf{Dec(sk}_f, c): \quad \text{Output } f(m)
Functional Encryption: Security \([\text{BSW’10, O’N’10}]\)

Unbounded full adaptive game-based security:

\[ (\text{msk}, \text{pk}) \leftarrow \text{Gen()} \]

\[ \text{pk} \]

\[ f \]

\[ \text{sk}_f = \text{KeyGen}(\text{msk}, f) \]

\[ \text{sk}_f \]

\[ b \leftarrow \{0, 1\} \]

\[ m_0, m_1 : f(m_0) = f(m_1) \ \forall f \]

\[ c \leftarrow \text{Enc}(\text{mpk}, m_b) \]

\[ c \]

\[ f : f(m_0) = f(m_1) \]

\[ \text{sk}_f = \text{KeyGen}(\text{msk}, f) \]

\[ \text{sk}_f \]
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

- Fixed (simple) assumptions
- Uber assumptions
- Ideal Models

[GGHRSW'13, BR'13, BGKPS'13]

Selective Security
Adaptive Security

[GGHRSW'13, PST'13, GLSW'14, Wat'14, BCP'13]
Why Obfuscation Seems Inherent

\[ f(m) \]
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

\( f(m) \)

\( f \) is now hidden

Note: [BCP’13] does not have function hiding
**Function Hiding ⇒ IO**

\[ \text{iO}(C): \]
\[
(\text{msk}, \text{pk}) \leftarrow \text{Gen}() \\
\text{sk} \leftarrow \text{KeyGen}(\text{msk}, C) \\
\text{Output } (\text{pk}, \text{sk})
\]

\[ \text{Eval}( (\text{pk}, \text{sk}), x): \]
\[
e = \text{Enc}(\text{pk}, x) \\
y = \text{Dec}(\text{sk}, e)
\]

**Takeaway:** FE with function hiding implies iO.
Question 1:

Can we build FE without iO?
Why avoid Obfuscation?

\(iO = \text{exponentially many assumptions}\)

- One per pair of circuits

Assumption(\(C_0, C_1\)):

\[iO(C_0) \approx iO(C_1)\]

Seems inherent:

Reduction can only work for equiv \(C_0, C_1\)

\[\Rightarrow \text{must somehow decide equivalence (NP-hard)}\]
What about GLSW?

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

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

• Need to assume MSE really hard (complexity leveraging)

Note: Adaptive vs selective FE meaningless in this setting
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

<table>
<thead>
<tr>
<th>0</th>
<th>$m_0 = 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$m_1 = 1$</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$m_3 = 0$</td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

Active slots

Secret Key

<table>
<thead>
<tr>
<th>0</th>
<th>$f_0(x) = x^2-3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$f_3(x) = 1$</td>
</tr>
<tr>
<td>4</td>
<td>$f_4(x) = x+1$</td>
</tr>
</tbody>
</table>

Decryption

<table>
<thead>
<tr>
<th>0</th>
<th>$f_0(m_0) = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$f_3(m_3) = 1$</td>
</tr>
</tbody>
</table>

1
Slotted Functional Encryption

Private (slotted) encryption: encrypt in all slots

\[
\begin{bmatrix}
m_0 \\
m_1 \\
\bot \\
m_3 \\
\end{bmatrix} \rightarrow \text{msk} \rightarrow \begin{bmatrix}
m_0 \\
m_1 \\
m_3 \\
\end{bmatrix}
\]
Slotted Functional Encryption

Public (unslotted) encryption: encrypt in slot 0

\[ \text{Ciphertext} \]

\[ \text{m} \]

\[ \text{pk} \]
Slotted Functional Encryption

**Slotted keygen**: secret keys in all slots

\[
\begin{pmatrix}
  f_0 \\
  \bot \\
  \bot \\
  f_3 \\
  f_4
\end{pmatrix}
\]

\[\text{msk}\]

- \(f_0\)
- \(f_3\)
- \(f_4\)
Slotted Functional Encryption

**Unslotted keygen**: secret keys in slot 0
- Derived from slotted alg

\[ \text{Secret Key} \]

\[ f \rightarrow \text{msk} \rightarrow \]

\[ f \]

\[ \]
Slotted Functional Encryption

**Decryption:** decrypt all active slots, output result if agree

- $m_0$
- $f_0$
- $f_0(m_0) = 1$
- $f_0(m_0) = 1$

- $m_1$
- $f_3$
- $f_3(m_3) = 1$
- $f_3(m_3) = 0$

- $m_3$
- $f_4$

- $f_4$

- $f_0(m_0) = 1$

- $1$

- N/A
Slotted FE to (Unslotted) FE

Throw away slotted algorithms

\[
\text{Enc}(\text{msk}, (m_0, m_1, m_2, \ldots )) \\
\text{Enc}(\text{pk}, m) \\
\text{KeyGen}(\text{msk}, (f_0, f_1, f_2, \ldots )) \\
\text{KeyGen}(\text{msk}, f)
\]

\[
\text{Enc}(\text{pk}, m)
\]

\[
\text{KeyGen}(\text{msk}, f)
\]
Security of Slotted Functional Encryption

Ideal: can’t learn anything except through decryption

\[ m_0 = 1 \]
\[ f_0(x) = x^2 \]
\[ m_1 = 2 \]
\[ f_3(x) = 2x + 3 \]
\[ m_3 = -1 \]
\[ f_4(x) = 9 \]

\[ m_1 = 4 \]
\[ f_1(x) = (x/2) - 1 \]
\[ m_2 = 1 \]
\[ f_3(x) = 2x - 1 \]
\[ m_3 = 1 \]
\[ f_4(x) = -2x + 2 \]

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m_0 = -1 )</td>
<td>( f_0(x) = x^2 )</td>
</tr>
<tr>
<td>( m_3 = 1 )</td>
<td>( f''_0(x) = 1 )</td>
</tr>
</tbody>
</table>

\[ m_0 = -1 \rightarrow m_0 = 1 \text{ does not affect decryption} \]
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f''_0(x) = 1$</td>
</tr>
</tbody>
</table>

$m_0 = -1 \rightarrow m_0 = 1$ 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)

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>m₀ = 1</td>
<td>f₀(x) = x²</td>
</tr>
<tr>
<td>m₁ = 1</td>
<td>f’₀(x) = (-1)ˣ</td>
</tr>
<tr>
<td>m₃ = 1</td>
<td>f”₀(x) = 1</td>
</tr>
<tr>
<td>f₁(x) = x²</td>
<td>f’₁(x) = (-1)ˣ</td>
</tr>
<tr>
<td>f”₃(x) = -(-1)ˣ</td>
<td></td>
</tr>
<tr>
<td>f’₄(x) = 3–2x</td>
<td>f”₄(x) = 1</td>
</tr>
</tbody>
</table>
Security of Slotted Functional Encryption

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

### Ciphertext
- $m_0 = 1$
- $m_1 = 1$
- $m_3 = 1$

### Secret Keys
- $f_0(x) = x^2$
- $f_1(x) = x^2$
- $f_0'(x) = (-1)^x$
- $f_1'(x) = (-1)^x$
- $f_3'(x) = -(-1)^x$
- $f_4'(x) = 3-2x$
- $f_0''(x) = 1$
- $f_3''(x) = -(-1)^x$
Security of Slotted Functional Encryption

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

### Ciphertext
- $m_0 = 1$
- $m_1 = 1$
- $m_2 = -1$
- $m_3 = 1$

### Secret Keys
- $f_0(x) = x^2$
- $f_1(x) = x^2$
- $f'_0(x) = (-1)^x$
- $f'_1(x) = (-1)^x$
- $f''_0(x) = 1$
- $f''_3(x) = -(-1)^x$
- $f'_4(x) = 3-2x$
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Cipher Text</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>m₀ = 1</td>
<td>f₀(x) = x²</td>
</tr>
<tr>
<td>m₁ = 1</td>
<td>f'₀(x) = (-1)²</td>
</tr>
<tr>
<td>m₂ = -1</td>
<td>f''₀(x) = 1</td>
</tr>
<tr>
<td>m₃ = 1</td>
<td>f''₃(x) = -(-1)²</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cipher Text</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>f₀(x) = x²</td>
<td>f'₀(x) = (-1)²</td>
</tr>
<tr>
<td>f₁(x) = x²</td>
<td>f'₁(x) = (-1)²</td>
</tr>
<tr>
<td>f₄(x) = 3−2x</td>
<td>f''₄(x) = 3−2x</td>
</tr>
</tbody>
</table>
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m_0 = 1 )</td>
<td>( f_0(x) = x^2 )</td>
</tr>
<tr>
<td>( m_1 = -1 )</td>
<td>( f'_0(x) = (-1)^x )</td>
</tr>
<tr>
<td>( m_2 = 1 )</td>
<td>( f_2(x) = x^2 )</td>
</tr>
<tr>
<td>( m_3 = 1 )</td>
<td>( f'_2(x) = (-1)^x )</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m_0 = 1 )</td>
<td>( f_0(x) = x^2 )</td>
</tr>
<tr>
<td>( m_1 = -1 )</td>
<td>( f_2(x) = x^2 )</td>
</tr>
<tr>
<td>( m_2 = 1 )</td>
<td>( f'_0(x) = (-1)^x )</td>
</tr>
<tr>
<td>( m_3 = 1 )</td>
<td>( f'_4(x) = 3-2x )</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>m₀ = 1</td>
<td>f₀(x) = x²</td>
</tr>
<tr>
<td>m₁ = -1</td>
<td>f’₀(x) = (-1)ₓ</td>
</tr>
<tr>
<td>m₂ = 1</td>
<td>f’₁(x) = (-1)ₓ</td>
</tr>
<tr>
<td>m₃ = 1</td>
<td>f’’₀(x) = 1</td>
</tr>
</tbody>
</table>

f₀(x) = 1
f₀’(x) = x
f₀’’(x) = 1
f’’’₀(x) = -(-1)ₓ
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.

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = x^2$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f'_4(x) = 3-2x$</td>
</tr>
</tbody>
</table>

$f_0(x) = x^2$, $f'_0(x) = (-1)^x$, $f''_0(x) = 1$
### 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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m_0 = 1 )</td>
<td>( f_0(x) = x^2 )</td>
</tr>
<tr>
<td>( m_1 = -1 )</td>
<td>( f'(x) = (-1)^x )</td>
</tr>
<tr>
<td>( m_2 = 1 )</td>
<td>( f''_1(x) = 1 )</td>
</tr>
<tr>
<td>( m_3 = 1 )</td>
<td>( f'_{4}(x) = 3 - 2x )</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f'_1(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f'_2(x) = 3 - 2x$</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>m₀ = 1</td>
<td>f₀(x) = x²</td>
</tr>
<tr>
<td>m₁ = 2</td>
<td>f′₀(x) = (-1)ˣ</td>
</tr>
<tr>
<td>m₂ = 1</td>
<td>f″₀(x) = 1</td>
</tr>
<tr>
<td>m₃ = 1</td>
<td>f₂(x) = x²</td>
</tr>
<tr>
<td></td>
<td>f₁(x) = 3−2x</td>
</tr>
<tr>
<td></td>
<td>f″₃(x) = −(-1)ˣ</td>
</tr>
<tr>
<td></td>
<td>f₄(x) = 3−2x</td>
</tr>
</tbody>
</table>
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = 2$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f_2(x) = x^2$</td>
</tr>
<tr>
<td></td>
<td>$f'_1(x) = 3-2x$</td>
</tr>
<tr>
<td></td>
<td>$f''_3(x) = -(-1)^x$</td>
</tr>
<tr>
<td></td>
<td>$f'_4(x) = 3-2x$</td>
</tr>
</tbody>
</table>
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_4 = 2$</td>
<td>$f_2(x) = x^2$</td>
</tr>
<tr>
<td></td>
<td>$f'_1(x) = 3-2x$</td>
</tr>
<tr>
<td></td>
<td>$f'_3(x) = -(-1)^x$</td>
</tr>
<tr>
<td></td>
<td>$f'_4(x) = 3-2x$</td>
</tr>
</tbody>
</table>
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = x^2$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f_4(x) = 3-2x$</td>
</tr>
<tr>
<td>$m_4 = 2$</td>
<td>$f'_1(x) = 3-2x$</td>
</tr>
</tbody>
</table>

$0$ is the encryption slot.
Security of Slotted Functional Encryption

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

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
</table>
| $m_0 = 1$  | $f_0(x) = x^2$  
$m_2 = 1$  
$m_3 = -1$  
$m_4 = 2$  | $f'_0(x) = (-1)^x$  
$f'_1(x) = 3-2x$  
$f''_0(x) = 1$  
$f''_3(x) = -(-1)^x$  
$f'_4(x) = 3-2x$  |

$f_0(x) = x^2$  
$f_2(x) = x^2$  
$f'_0(x) = (-1)^x$  
$f'_1(x) = 3-2x$  
$f''_0(x) = 1$  
$f''_3(x) = -(-1)^x$  
$f'_4(x) = 3-2x$
Reductions!

Ctxt Moving  →  Slot Dup  →  Single-use Hiding  →  Weak Sk Moving

Weak Ctxt Indist  →  Strong Ctxt Indist

Lose 1 slot

Sanity Check: Slot 0 in secret keys cannot change ⇒ no function hiding
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$, $f'_0(x) = (-1)^x$, $f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2-x^2$, $f'_1(x) = 2x+1$, $f''_1(x) = -1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_3(x) = 1-x$, $f'_2(x) = -1$, $f''_2(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>

Dummy slot
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_1(x) = 2x+1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f''_2(x) = -(-1)^x$</td>
</tr>
<tr>
<td></td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td></td>
<td>$f_1(x) = 2-x^2$</td>
</tr>
<tr>
<td></td>
<td>$f'_2(x) = -1$</td>
</tr>
<tr>
<td></td>
<td>$f_2(x) = 1-x$</td>
</tr>
</tbody>
</table>

Slot Duplication
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

Ciphertext

- $m_0 = 1$
- $m_1 = -1$
- $m_2 = 1$
- $m_4 = -1$

Secret Keys

- $f_0(x) = x^2$
- $f_1(x) = 2-x^2$
- $f_2(x) = 1-x$

- $f'_0(x) = (-1)^x$
- $f'_1(x) = 2x+1$
- $f'_2(x) = -1$

- $f''_0(x) = 1$
- $f''_2(x) = -(-1)^x$

Slot Duplication
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2-x^2$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = 1-x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
</tbody>
</table>

Weak Sk Moving
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

Ciphertext

$\begin{align*}
m_0 &= 1 \\
m_1 &= -1 \\
m_2 &= 1 \\
m_3 &= -1
\end{align*}$

Secret Keys

$\begin{align*}
f_0(x) &= x^2 \\
f_1(x) &= -1 \\
f_2(x) &= 2-x \\
f_3(x) &= 1-x \\
f_4(x) &= 2-x^2
\end{align*}$

Weak Sk Moving
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2x+1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = 1-x$</td>
</tr>
<tr>
<td>$m_3 = 1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_4(x) = 2-x^2$</td>
</tr>
</tbody>
</table>

Single Use Hiding
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

Ciphertext

- $m_0 = 1$
- $m_1 = -1$
- $m_2 = 1$
- $m_4 = 1$

Secret Keys

- $f_0(x) = x^2$
- $f'_0(x) = (-1)^x$
- $f''_0(x) = 1$
- $f_1(x) = 2x + 1$
- $f'_1(x) = 2x + 1$
- $f''_1(x) = -(-1)^x$
- $f_2(x) = 1 - x$
- $f'_2(x) = -1$
- $f''_2(x) = -(-1)^x$
- $f_3(x) = 1 - x$
- $f'_3(x) = 2 - x^2$
- $f''_3(x) = 1$
- $f_4(x) = 2 - x^2$
- $f'_4(x) = -1$
- $f''_4(x) = -(-1)^x$

Single Use Hiding
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

**Ciphertext**

$m_0 = 1$
$m_1 = -1$
$m_2 = 1$
$m_4 = 1$

**Secret Keys**

$f_0(x) = x^2$
$f'_0(x) = (-1)^x$
$f''_0(x) = 1$

$f_3(x) = 1-x$
$f'_3(x) = 2x+1$
$f''_3(x) = -(-1)^x$

$f_4(x) = 2-x^2$
$f'_4(x) = -1$
$f''_4(x) = 1$

Weak Sk Moving
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = 2-x^2$</td>
</tr>
<tr>
<td>$m_4 = 1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
</tbody>
</table>

Weak Sk Moving
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = 2-x^2$</td>
</tr>
<tr>
<td>$m_4 = 1$</td>
<td>$f'_2(x) = -1$</td>
</tr>
</tbody>
</table>
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

Ciphertext

$m_0 = 1$
$m_1 = -1$
$m_2 = 1$

Secret Keys

$f_0(x) = x^2$
$f'_0(x) = (-1)x$
$f''_0(x) = 1$

$f_1(x) = 2x+1$
$f'_1(x) = (2x+1)$
$f''_1(x) = -(-1)x$

$f_2(x) = 2-x^2$
$f'_2(x) = -1$
$f''_2(x) = -(-1)x$

Slot Duplication
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to slot 3

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$, $f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2x+1$, $f''_1(x) = -(-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = -x^2$, $f''_2(x) = -(-1)^x$</td>
</tr>
<tr>
<td></td>
<td>$f_3(x) = 1-x$,</td>
</tr>
</tbody>
</table>

$f_0(x) = x^2$, $f'_0(x) = (-1)^x$, $f''_0(x) = 1$

$f_1(x) = 2x+1$, $f'_1(x) = 2x+1$, $f''_1(x) = -(-1)^x$

$f_2(x) = -x^2$, $f'_2(x) = -1$, $f''_2(x) = -(-1)^x$

$f_3(x) = 1-x$, $f'_3(x) = (-1)^x$, $f''_3(x) = 1$
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext

| $m_0$ = 1 |
| $m_1$ = $-1$ |
| $m_2$ = 1 |

Secret Keys

| $f_0(x) = x^2$ |
| $f'_0(x) = (-1)^x$ |
| $f''_0(x) = 1$ |
| $f_2(x) = 2-x^2$ |
| $f'_2(x) = -1$ |
| $f''_2(x) = -(-1)^x$ |
| $f_3(x) = 1-x$ |
| $f'_3(x)$ |
| $f''_3(x)$ |
### Example Reduction: Weak Ctxt Indist

**Goal:** change $m_2$ to **-1**

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$, $f'_0(x) = (-1)^x$, $f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2x + 1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f'_2(x) = -1$, $f''_2(x) = -(-1)^x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_3(x) = 1 - x$</td>
</tr>
</tbody>
</table>
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_1(x) = 2x + 1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f'_2(x) = -1$</td>
</tr>
<tr>
<td></td>
<td>$f''_2(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>

$f_0(x) = x^2$
$f_2(x) = 2 - x^2$
$f_3(x) = 1 - x$

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext
- $m_0 = 1$
- $m_1 = -1$
- $m_2 = 1$
- $m_4 = -1$

Secret Keys
- $f_0(x) = x^2$
- $f'_0(x) = (-1)^x$
- $f''_0(x) = 1$
- $f'_1(x) = 2x+1$
- $f'_2(x) = -1$
- $f''_2(x) = -(-1)^x$
- $f_3(x) = 1-x$
- $f_4(x) = 2-x^2$

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to -1

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$, $f'_0(x) = (-1)^x$, $f''_0(x) = 1$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_1(x) = 2x + 1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f'_2(x) = -1$, $f''_2(x) = -(-1)^x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_4(x) = 2 - x^2$</td>
</tr>
</tbody>
</table>

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_4(x) = 2-x^2$</td>
</tr>
</tbody>
</table>

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext

$m_0 = 1$
$m_1 = -1$
$m_2 = 1$
$m_4 = -1$

Secret Keys

$f_0(x) = x^2$
$f_1(x) = 2x+1$
$f_2(x) = -(-1)^x$

$f_3(x) = 1-x$

$f_4(x) = 2-x^2$
$f_4'(x) = -1$

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>$m_0 = 1$</th>
<th>$f_0(x) = x^2$</th>
<th>$f''_0(x) = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_1 = -1$</td>
<td>$f_1(x) = 2x+1$</td>
<td>$f'_1(x) = 2x+1$</td>
<td></td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_3(x) = 1-x$</td>
<td>$f'_3(x) = -1$</td>
<td></td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_4(x) = 2-x^2$</td>
<td>$f'_4(x) = -1$</td>
<td>$f''_4(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>

Strong Sk Moving
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext

- $m_0 = 1$
- $m_1 = -1$
- $m_2 = 1$
- $m_4 = -1$

Secret Keys

- $f_0(x) = x^2$
- $f_0'(x) = (-1)^x$
- $f_0''(x) = 1$
- $f_1(x) = 2x+1$
- $f_1'(x) = 2x+1$
- $f_1''(x) = -(-1)^x$
- $f_3(x) = 1-x$
- $f_3'(x) = -1$
- $f_3''(x) = 1$
- $f_4(x) = 2-x^2$
- $f_4'(x) = -1$
- $f_4''(x) = -(-1)^x$

New Slot
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext

- $m_0 = 1$
- $m_1 = -1$
- $m_4 = -1$

Secret Keys

- $f_0(x) = x^2$
- $f'_0(x) = (-1)^x$
- $f''_0(x) = 1$

- $f_3(x) = 1-x$
- $f'_3(x) = 2x+1$

- $f_4(x) = 2-x^2$
- $f'_4(x) = -1$
- $f''_4(x) = -(-1)^x$

New Slot
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

### Ciphertext
- $m_0 = 1$
- $m_1 = -1$
- $m_4 = -1$

### Secret Keys
- $f_0(x) = x^2$
- $f_1(x) = 2x + 1$
- $f_3(x) = 1 - x$
- $f_4(x) = 2 - x^2$

- $f'_0(x) = (-1)^x$
- $f'_1(x) = 2x + 1$
- $f'_4(x) = -1$

- $f''_0(x) = 1$
- $f''_1(x) = 2x + 1$
- $f''_4(x) = -(-1)^x$

Slot Symmetry
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

Ciphertext

- $m_0 = 1$
- $m_1 = -1$
- $m_2 = -1$

Secret Keys

- $f_0(x) = x^2$
- $f_1(x) = 2x+1$
- $f_2(x) = 2-x^2$
- $f_3(x) = 1-x$

- $f'_0(x) = (-1)^x$
- $f'_1(x) = 2x+1$
- $f'_2(x) = -1$
- $f''_2(x) = -(-1)^x$

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

Slot Symmetry
Example Reduction: Weak Ctxt Indist

Goal: change $m_2$ to $-1$

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0 = 1$</td>
<td>$f_0(x) = x^2$</td>
</tr>
<tr>
<td>$m_1 = -1$</td>
<td>$f'_0(x) = (-1)^x$</td>
</tr>
<tr>
<td>$m_2 = -1$</td>
<td>$f''_0(x) = 1$</td>
</tr>
<tr>
<td>$f_2(x) = 2-x^2$</td>
<td>$f'_2(x) = -1$</td>
</tr>
<tr>
<td>$f_3(x) = 1-x$</td>
<td>$f''_2(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>
Instantiating Slotted FE

We give construction for NC¹ 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 NC¹

But I promised FE for all circuits…
Achieving FE for All Circuits

- Slotted FE for NC^1
- Randomized FE for NC^1
- FE for all circuits
  - iO: [GJKS’13]

- Punctured PRFs in NC^1
  - [BLMR’13, NR’97]

- Randomized Encodings in NC^1
  - [Yao’86, IK’00]
Randomized FE for NC¹

Basic idea: ctxt contains PRF key which generates randomness

\[ \text{Enc}_R(\text{mpk}, m): \quad k \leftarrow \{0,1\}^\lambda \]
\[ c \leftarrow \text{Enc}( \text{mpk}, (m,k) ) \]
Output \(c\)

Define:
\[ g[f,s](m,k) := f( m ; \text{PRF}(k,s) ) \]

\[ \text{KeyGen}_R(\text{msk}, f): \quad s \leftarrow \{0,1\}^\lambda \]
\[ \text{sk}_f \leftarrow \text{KeyGen}(\text{msk}, g[f,s]) \]
Output \(\text{sk}_f\)

Actual scheme more complicated
Randomized FE for NC$^1$

Proof idea:

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Secret Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_0, k$</td>
<td>$g[f_1,s_1]$</td>
</tr>
<tr>
<td></td>
<td>$g[f_2,s_2]$</td>
</tr>
</tbody>
</table>
Randomized FE for NC¹

Proof idea:

Ciphertext

<table>
<thead>
<tr>
<th>m₀, k</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Secret Keys

<table>
<thead>
<tr>
<th>g[ƒ₁,s₁]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g[ƒ₂,s₂]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g[ƒ₂,s₂]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Slot Duplication
Randomized FE for NC$^1$

Proof idea:

Ciphertext

\[ m_0, k \]

\[ g[f_1,s_1] \]

\[ g[f_1,s_1] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

Slot Duplication

Secret Keys

\[ g[f_1,s_1] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]
Randomized FE for NC$^1$

Proof idea:

Ciphertext

$m_0, k$

$g[f_1, s_1]$

$g[f_2, s_2]$

$g[f_2, s_2]$

Secret Keys

$g[f_1, s_1]$

$g[f_2, s_2]$

$g[f_2, s_2]$

Ciphertext Moving
Randomized FE for NC$^1$

Proof idea:

Ciphertext

Secret Keys

Ciphertext Moving
Randomized FE for NC\(^1\)

Proof idea:
Randomized FE for NC¹

Proof idea:

Ciphertext

\[ m_0, k \]

\[ m_1, k \]

Secret Keys

\[ g[f_1,s_1] \]

\[ g[f_1,s_1] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

\[ g[f_2,s_2] \]

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 NC¹

Proof idea:

Ciphertext

\[ m_0, k \]

\[ m_1, k \]

\[ g[f_1, s_1] \]

\[ g[f_2, s_2] \]

Secret Keys

\[ g[f_1, s_1] \]

\[ g[f_2, s_2] \]

\[ g[f_2, s_2] \]

\[ g[f_2, s_2] \]

“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:

Ciphertext

\begin{align*}
\text{m}_0, k \\
\text{m}_1, k
\end{align*}

Secret Keys

\begin{align*}
g[f_1, s_1] \\
g[f_2, s_2] \\
g[f_1, s_1] \\
g[f_2, s_2] \\
g[f_2, s_2]
\end{align*}

New Slot
Randomized FE for NC$^1$

Proof idea:

- **Ciphertext**
  - $m_1, k$

- **Secret Keys**
  - $g[f_1, s_1]$
  - $g[f_2, s_2]$
  - $g[f_2, s_2]$

New Slot
Randomized FE for NC\textsuperscript{1}

Proof idea:

Ciphertext

\[ m_1, k \]

Secret Keys

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

Ciphertext Moving
Randomized FE for NC$^1$

Proof idea:

Ciphertext

\[ m_1, k \]

\[ g[f_1,s_1] \]
\[ g[f_1,s_1] \]
\[ g[f_1,s_1] \]

\[ g[f_2,s_2] \]
\[ g[f_2,s_2] \]
\[ g[f_2,s_2] \]

Secret Keys

\[ g[f_2,s_2] \]
\[ g[f_2,s_2] \]
\[ g[f_2,s_2] \]

Ciphertext Moving
Randomized FE for NC\(^1\)

Proof idea:

Ciphertext

\[ m_1, k \]

\[ g[f_1, s_1] \]

\[ g[f_1, s_1] \]

\[ g[f_2, s_2] \]

\[ g[f_2, s_2] \]

\[ g[f_2, s_2] \]

Secret Keys

Slot Duplication
Randomized FE for NC$^1$

Proof idea:

Ciphertext

<table>
<thead>
<tr>
<th>m$_1$, k</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Secret Keys

<table>
<thead>
<tr>
<th>g[f$_1$,s$_1$]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g[f$_2$,s$_2$]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g[f$_2$,s$_2$]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Slot Duplication
Randomized FE for $NC^1$

Proof idea:
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 $f( m_0 , \text{PRF}(k, s) )$
  • In ciphertext if secret key before ciphertext. Use $\text{ctxt}$ indist.
  • In secret key if secret key after ciphertext. Use single-use hiding+
• Replace with $f( m_1 , \text{PRF}(k, s) )$
  • Using PRF security and sample indistinguishability
• Move secret key
• Un-puncture
FE for all Circuits

Basic idea: Output randomized encoding rather than actual val

 Enc_C(mpk, m): \( c \leftarrow \text{Enc}_R(\text{mpk}, \text{m}) \)
Output \( c \)

 KeyGen_C(msk, f): 
\( f'(m; r) := \text{Encode}_f(m \ ; r) \)
\( \text{sk}_f \leftarrow \text{KeyGen}_R(\text{msk}, f') \)
Output \( \text{sk}_f \)

 Dec_C(sk_f, c): 
\( e \leftarrow \text{Dec}_R(\text{sk}_f, c) \)
\( o \leftarrow \text{Decode}(e) \)
Output \( o \)
Conclusion and Open Problems

Simple assumptions $\rightarrow$ Slotted FE $\rightarrow$ 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 $\rightarrow$ simple assumptions
  - Deniable encryption
  - Multiparty NIKE w/o trusted setup